S. HRG. 117–79

OPEN HEARING: HACK OF U.S. NETWORKS BY A FOREIGN ADVERSARY

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

TUESDAY, FEBRUARY 23, 2021

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
45–485 PDF WASHINGTON : 2022

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

MARK R. WARNER, Virginia, *Chairman*
MARCO RUBIO, Florida, *Vice Chairman*

DIANNE FEINSTEIN, California
RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS KING, Maine
MICHAEL F. BENNET, Colorado
BOB CASEY, Pennsylvania
KIRSTEN E. GILLIBRAND, New York

RICHARD BURR, North Carolina
JAMES E. RISCH, Idaho
SUSAN COLLINS, Maine
ROY BLUNT, Missouri
TOM COTTON, Arkansas
JOHN CORNYN, Texas
BEN SASSE, Nebraska

CHUCK SCHUMER, New York, *Ex Officio*
MITCH MCCONNELL, Kentucky, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*
JAMES INHOFE, Oklahoma, *Ex Officio*

MICHAEL CASEY, *Staff Director*
BRIAN WALSH, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

C O N T E N T S

FEBRUARY 23, 2021

OPENING STATEMENTS

	Page
Warner, Hon. Mark R., a U.S. Senator from Virginia	1
Rubio, Hon. Marco, a U.S. Senator from Florida	4

WITNESSES

Mandia, Kevin, CEO, FireEye, Inc.	6
Prepared statement	9
Ramakrishna, Sudhakar, CEO, SolarWinds Inc.	14
Prepared statement	16
Smith, Brad, President, Microsoft Corporation	23
Prepared statement	26
Kurtz, George, Co-Founder and CEO, CrowdStrike	41
Prepared statement	44

SUPPLEMENTAL MATERIAL

Responses of Kevin Mandia to Questions for the Record	86
Responses of Sudhakar Ramakrishna to Questions for the Record	90
Responses of Brad Smith to Questions for the Record	94
Responses of George Kurtz to Questions for the Record	107

OPEN HEARING: HACK OF U.S. NETWORKS BY A FOREIGN ADVERSARY

TUESDAY, FEBRUARY 23, 2021

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 2:32 p.m., in Room SD–106 in the Dirksen Senate Office Building, Hon. Mark R. Warner (Chairman of the Committee) presiding.

Present: Senators Warner, Rubio, Feinstein, Wyden, Heinrich, King, Bennet, Casey (via WebEx), Gillibrand, Burr, Risch, Collins, Blunt, Cotton, Cornyn, and Sasse.

OPENING STATEMENT OF HON. MARK R. WARNER, A U.S. SENATOR FROM VIRGINIA

Chairman WARNER. Good afternoon, everyone. I'd like to call this hearing to order and apologize to our witnesses and others with them. With COVID and a vote just been called, we're going to a little bit be playing this by ear. So I'm going to make my opening statement, ask the Vice Chairman to make his opening statement. We'll be monitoring the vote, which just opened a moment ago. We've got two, so we'll either tag team through this or take a five-minute recess to get us all a chance to go vote on both these items.

First, I'd like to take this opportunity to welcome our two new Members, one of which I think at least is on Zoom, Senator Casey, and also Senator Gillibrand, to the Committee. I look forward to working with both of you as Members of the Senate Intelligence Committee in the bipartisan tradition of this Committee.

The Intelligence Committee's record of working together in the interests of America's national security has been due, in no small part, to the tireless efforts of our former Chairman, Senator Burr, and our new Vice Chairman, Senator Rubio. So I want to take this opportunity during my first hearing as Chairman, to thank you both for your partnership and friendship. I'm confident that we'll be able to keep working together in a bipartisan way in the 117th Congress.

I'd also very much like to welcome our witnesses today: Kevin Mandia, CEO of FireEye; Sudhakar Ramakrishna, President and CEO of SolarWinds; Brad Smith, President of Microsoft Corporation; and, I believe remotely, George Kurtz, President and CEO of CrowdStrike. I would like for the record to note that we also asked a representative from Amazon Web Services to join us today but, unfortunately, they declined. But we will be expecting to get a full update—and we've had one update from our friends at Amazon—

but it would be most helpful if in the future they actually attended these hearings.

Today's hearing is on the widespread compromise of public and private computer networks in the United States by a foreign adversary, colloquially or commonly called "the SolarWinds hack." While most infections appear to have been caused by a trojanized update of SolarWinds's Orion software, further investigations have revealed additional victims who do not use SolarWinds's tools. It has become clear that there is much more to learn about this incident, its causes, its scope and scale, and where we go from here.

This is the second hearing this Committee has held on this topic. Our first was a closed hearing held on the now-infamous January 6th to hear from government officials responding to the SolarWinds incident. It's going to take the combined power of both the public and private sector to understand and respond to what happened. Preliminary indications suggest that the scope and scale of this incident are beyond any that we've confronted as a Nation and its implications are significant.

Even though what we've seen so far indicates that this was carried out as an espionage campaign targeting more than 100 or so companies and government agencies, the reality is the hackers responsible have gained access to thousands of companies and the ability to carry out far more destructive operations if they'd wanted to. And I want to repeat that. This intrusion had the possibility of being exponentially worse than what has come to pass so far.

The footholds these hackers gained into private networks, including some of the world's largest IT vendors, may provide opportunities for future intrusions for years to come. One of the reasons the SolarWinds hack has been especially concerning is that it was not detected by the multibillion-dollar U.S. Government cybersecurity enterprise or anyone else until the private security firm, FireEye—and I want to again complement our friend, Kevin Mandia, who's appeared before this Committee a number of times—on their own without a requirement to report, actually publicly announced that it had detected a breach of its own network by a nation-state intruder.

A very big question looming in my mind is: Had FireEye not detected this compromise in December and chosen on their own to come forward, would we still be in the dark today? As Deputy National Security Adviser, Anne Neuberger, who has been chosen by the President to lead the response in this, and to the SolarWinds hack, said last week, "The response to this incident from both the public and private sector is going to take a long time."

All of our witnesses today are involved in some aspect of the private sector response to this incident. I want to hear from them on the progress so far, the challenges we'll need to overcome in order to fully expel these hackers, and how we can prevent supply-chain attacks like this in the future. I'd also like to hear from them about their experiences working with the Federal Government, namely, the Unified Coordination Group, in mitigating this compromise.

The SolarWinds hack was a sophisticated and multifaceted operation: a software supply chain operation that took advantage of trusted relationships with software providers in order to break into literally thousands of entities. Combined with the use of this so-

phisticated authentication exploits, it also leveraged vulnerabilities and major authentication protocols, basically granting the intruder the keys to the kingdom, allowing them to deftly move across both on-premises and cloud-based services, all while avoiding detection.

While many aspects of this compromise are unique, the SolarWinds hack has also highlighted a number of lingering issues that we've ignored for too long. This presents us an opportunity for reflection and action. A lot of people are offering solutions, including mandatory reporting requirements, wider use of multi-factor authentication, requiring a software bill of goods, and significantly improving threat information sharing between the government and the private sector.

I've got a number of questions, but there are three that I'd like to pose in my opening.

One, why shouldn't we have mandatory reporting systems, even if those reporting systems require some liability protection, so we can better understand and better mitigate future attacks? As I pointed out, Senator Collins was way ahead of all of us on this issue, literally years and years ago, when she and Senator Lieberman first put forward legislation that required this critical, mandatory reporting on critical infrastructure.

There's an open question, though, on who should receive such report, even if you put that mandatory reporting in place. Do we need something like the National Transportation Safety Board, or other public-private entity that can immediately examine major breaches to see if we have a systemic problem, as we seem to see in this case? I think there's also some truth to the idea that if a tier-one adversary, a foreign nation-state, sends their A team against almost any ordinary company in the world, chances are they're going to get in. But that cannot be an excuse for doing nothing to build defenses and making it harder for them to be successful once inside an enterprise. I'm very interested in hearing from the witnesses what they think our policy response should be, and what solutions they will actually they think will actually improve cybersecurity and incident reporting in the United States.

Beyond the immediate aspects of the SolarWinds hack are larger issues that this Committee needs to consider. Do we need to finally come to some agreement on common norms in cyberspace, hopefully, again, on an international basis, that potentially are enforceable, and at least says to our adversaries: If you violate these warm norms, there will be known consequences? For example, we have these norms in other conflicts. We have military conflict that exists, but there's been for some time a norm that you don't knowingly bomb a hospital or bomb an ambulance that's got a Red Cross shield on it. Should we, therefore, consider efforts that subvert patching, which are all about fixing vulnerabilities to be similarly off limits?

Once again, I want to thank our witnesses for joining us today, both in person and remotely. I personally talked to nearly all of our witnesses, in some cases multiple times since this incident was first reported. I appreciate their transparency and willingness to be part of this conversation.

After our witnesses conclude their remarks, we'll move to a round of five-minute questions based upon order of arrival. As re-

minder to my colleagues, this incident is not over. So too are the criminal investigations by the FBI. So there might be some questions our witnesses cannot answer. However, I'm confident we'll get those answers at some point as we move forward. I now recognize the Vice Chairman for a statement.

OPENING STATEMENT OF HON. MARCO RUBIO, A U.S. SENATOR FROM FLORIDA

Vice Chairman RUBIO. Thank you, Mr. Chairman, and thanks for convening this hearing. And I'd like to welcome our witnesses from Microsoft, FireEye, SolarWinds, and CrowdStrike who are here to help the Committee's examination of what is the largest cyber-supply chain operation ever detected. So we really do appreciate you being with us.

As the Chairman mentioned, we had extended an invitation to Amazon to participate. The operation we'll be discussing today used their infrastructure, at least in part, to be successful. Apparently, they were too busy to discuss that here with us today and I hope they'll reconsider that in the future.

This operation involved, as has already been said, the modification of the SolarWinds Orion platform, which is a widely-used software product. It included a malicious backdoor that was downloaded, from my understanding, to up to 18,000 customers between March and June of last year. But the most insidious part of this operation was that it hijacked the very security advice promulgated by computer security professionals to verify and apply patches as they are issued.

So there are many concerning aspects to this first-of-its-kind operation, at least at this scale, that has raised significant questions. My understanding is that if FireEye had not investigated an anomalous event within their own network in November of last year, it's possible this would be a continuing and unfettered operation to this day.

I think everyone's asking, despite the investment that's been made in cybersecurity collectively between the government and the private sector, how no one detected this activity earlier, as it appears that they have been in the system for close to five to six months before it was detected—maybe even longer; closer to a year. But the bottom-line question is, how did we miss this? And what are we still missing? And what do we need to do to make sure that something like this, using these sorts of tools, never happens again?

Second, I think there's great interest in knowing exactly what these actors did. Based on what we know, to include what government has stated publicly, the actor seems to have undertaken follow-on operations against a very small subset of the 18,000 networks to which they potentially had access. So aside from the mechanical aspects of removing a hacker from a network, what do we know about why these actors chose the targets that they did? What actions did they undertake within those networks? And what do we know that we do not know? I always love that question. What do we know that we do not know? In essence, what are the open questions now and in the future about these sorts of tools and how they can be used? Or what do we still have open ended that we are not

able to answer at this time? And perhaps most importantly, who has the single comprehensive view of the totality of activity undertaken? That's another thing that everyone has struggled with is who can see the whole field here on this?

And third, what is it going to take to rebuild and have confidence in our networks? And speaking with several of you in the days leading up to this, one of the hallmarks of this operation was the great care that was taken by this adversary to use bespoke infrastructure and tradecraft for each victim. Unlike other malware or ransomware, cleanup operations, there is no template here that can be used for remediation. So what's it going to take to have confidence in both government and in the private sector networks again?

Fourth, what do we need to do to raise the bar for the cybersecurity of this Nation? Is cyber deterrence an achievable goal? How do we need to enhance cybersecurity information logging and sharing across the spectrum to protect against APTs in the future?

And finally, though this is a question for the government rather than the witnesses here today, I think it's important for this Committee to ask itself, and to inform the Members of the Senate, what does the United States Government need to do to respond to this operation?

Government officials initially stated this was an intelligence gathering operation. Just recently, however, the White House stated, quote: "When there is a compromise of this scope and scale, both across government and across the U.S. technology sector to lead to follow-on intrusions, it is more than a single incident of espionage. It is fundamentally of concern for the ability for this to become disruptive." End quote. While I share this concern that an operation of this scale, with a disruptive intent, could have caused mass chaos, those are not the facts that are in front of us. Everything we have seen thus far indicates that at some level, this was an intelligence operation and a rather successful one that was ultimately disrupted.

While there are a myriad of ways for sovereign states to respond, I caution against the use of certain terms at this time until the facts lead us to the use of terms such as attack and so forth. I've always advocated for standing up to our adversaries. I think that's important. I will continue to advocate for that. But I want to know today what the actor's intent seemed to be and to the extent of the damage before we categorize it. It may very well have reached that level.

This Committee and the rest of the Congress should consider what policies we need to pursue to better defend our Nation's critical networks, in order to get a fuller view of the problem. Perhaps we should consider mandating certain types of reporting, as the Chairman already mentioned. As it relates to cyber-attacks, we must improve the information-sharing, of this there is no doubt, between the Federal Government and the private sector. And I look forward to being an active and constructive participant in these debates on these new issues, as I know every Member on this Committee is.

And with that, I again, want to welcome you and thank you for the testimony and the insights that you will share with us and the

American people. It is important that the public understand the current persistent information conflict that the United States finds itself in against nation-state adversaries like Russia, but also like China and Iran and North Korea.

Thank you, Mr. Chairman.

Chairman WARNER. Thank you, Senator Rubio. I think we're going to go ahead and we'll just tradeoff. I believe the order of the speakers is going to be: FireEye, SolarWinds, Microsoft, and CrowdStrike.

So Kevin, if you want to start us off, that'd be great.

STATEMENT OF KEVIN MANDIA, CEO, FIREEYE, INC.

Mr. MANDIA. Thank you, Mr. Chairman, Vice Chairman Rubio, and the rest of the Members of the Senate Intelligence Committee. It is a privilege to be here with the opportunity to speak with you.

And as the first witness, I'm going to discuss what happened from a first-hand experience as a stage two victim to this intrusion. I have opinions on who did it. I have opinions on what to do about it. But in the next four minutes, I don't have enough time to get through all that. So I look forward to your questions.

I just want to give you a little background on FireEye. Responding to breaches is what we do for a living. We have a whole bunch of Quincy-type people that do forensics 2,000 hours a year. And people hire us to figure out what happened and what to do about it when they have a security breach. We responded to over 1,000 breaches in 2020. It was a tough year for chief information security officers. And as I sit here right now testifying to you, we're responding to over 150 computer security breaches.

In short, this is what we do for a living. And what we're going to tell you today, we tell you with high confidence and high fidelity on the intent of the attackers and what they did.

So now I want to present kind of the anatomy of this attack. You know, we're referring to it as the SolarWinds campaign. But it's a little bit broader than that. Whoever this threat actor is—and we all pretty much know who it is—this has been a multi-decade campaign for them. They just so happened to, in 2020, create a backdoor SolarWinds implant.

So the first part of this ongoing saga, stage one of this campaign, was you had to compromise SolarWinds. And the attackers did something there that was unique in that they didn't modify the source code there, they modified the build process, which to me means this is a more portable attack than just at SolarWinds. When you modify the build process, you're doing the last step of what happens before code becomes production for your buyers and customers, which just shows this is a very sophisticated attacker.

And once they did that stage one compromise of SolarWinds, we didn't find the implant till December 2020. And it had been out there, if you look at a timeframe perspective, from March 2020 and there was an update in June 2020, as well. But the attacker did something interesting when you get the timing. They did a dry run in October 2019, where they put innocuous code into the SolarWinds build just to make sure the result of their intrusion was making it into the SolarWinds platform production environment.

I want to explain how we found this implant because there's no magic wand to say where's the next implant? When we were compromised, we were set up to do that investigation. It's what we do. We put almost 100 people on this investigation. Almost all of them had 10,000 hours there, so to speak, 10,000 hours of doing investigations, and we unearthed every clue we could possibly find. And we still didn't know. So how did the attacker break in?

So we had to do extra work. And at some point in time, after exhausting every investigative lead, the only thing left was—the earliest evidence of compromised was a SolarWinds server. And we had to tear it apart. And what I mean by that is we had to decompile it. Specifically, there were 18,000 files in the update, 3,500 executable files. We had over a million lines of assembly code. For those of you that haven't looked at assembly, you don't want to. It's something that you have to have specialized expertise to review, understand, piece apart, and we found the proverbial needle in the haystack—an implant.

But how do we get there? Thousands of hours of humans investigating everything else. And that's one of the reasons I share that as you wonder why people missed it. This was not the first place you'd look; this was the last place you'd look for an intrusion. Over 17,000 companies were compromised by that implant.

So stage one was to compromise SolarWinds, get an implant in, and indiscriminately went to the 17,000 folks that downloaded it. That means the attackers had a menu of 17,000 different companies.

Stage two of this attack was the companies that these attackers intended to do additional action on and I want to talk about what they did during stage two victims. I want to say, stage one, the attacker hasn't done anything more than crack open the window into a company. But they haven't gone into the house to rob anything yet.

Stage two, they go into the house to rob it. When we look at the stage two threat actor, or stage two victims, this is where Microsoft's top-down viewpoint from their Cloud, where there's a lot of activity, comes up with approximately 60 victim organizations. And we read that the government is aware of about 100 organizations. For us being a stage two, we had first-hand account of what they do. The attackers came in through the SolarWinds implant. And the very first thing they did is went for your keys, your tokens. Basically, they stole your identity architecture so they could access your networks the same way your people did.

And that's why this attack was hard to find because these attackers, from day one, they had a backdoor. Imagine almost a secret door in your house and the first thing that happens when it comes to that secret door is all your keys are right there. They just grab them, and now they can get into any locks you have in your house the same way your people do. And I think, during a pandemic, where everybody's working from home, it's way harder to detect an attack like this, where the only indicator of compromise was just somebody logging in as one of your employees. And there's nothing else far-fetched about that.

Right after they got our valid credentials, our two-factor authentication mechanisms bypassed, they went to our O365 environment.

And whether it was O365, or something else, I've had enough experience over my 25 years of responding to breaches to know this group targets specific people, almost like they have collection requirements. So there they targeted emails and documents. So stage two was: get credentials so you could log in; get the keys to the safety deposit boxes; stage the next step. Step two of that was access email, access documents with said keys.

And then the third thing was dependent on who you were, and what you did, and what industry you are as a victim. But it's primarily what I put in the other category: steal source code, steal software. In the case of FireEye, take some of our red teaming tools that we use to assess people's security programs.

Bottom line: exceptionally hard to detect. And when I got my first briefing on this and reviewed the facts on day one, everything about this aligned to a threat actor, who, it is my opinion, was more concerned about operational security than mission accomplished. And that the minute you could detect these folks and stop them breaking through the door, they sort of evaporated like ghosts until their next operation.

So with that, on behalf of FireEye, I'd like to thank all of you for the opportunity to set the stage for the other witnesses. I'm very excited to work with all of you, and to my fellow witnesses and others in the private sector as well as the public sector to advance our Nation in defending ourselves in cyberspace. And I look forward to taking your questions.

[The prepared statement of Mr. Mandia follows:]

Prepared Statement of Kevin Mandia, CEO of FireEye, Inc. before the United States Senate Select Committee on Intelligence February 23, 2021

Introduction

Thank you Mr. Chairman, Ranking Member Rubio, and all the Members of the Committee, for this opportunity to share my observations and experience with you. As requested, I am going to discuss three things: 1) the cyber intrusion into FireEye; 2) how we discovered the SolarWinds implant we call SUNBURST; and 3) what the U.S. government can do to help protect the Nation, its government agencies, as well as private companies in cyberspace.

Background

Before I turn to these specific topics, let me share some background on myself and my company to establish some context for my narrative. I have been working in cybersecurity since 1993, when I was stationed at the Pentagon at the outset of my career as a Computer Security Officer. During my time investigating computer intrusions while I was in the Air Force, I came to recognize that the biggest cyber threats to our infrastructure were intrusions from other countries, most notably from Russia and China. I founded a company, called Mandiant, in 2004 to respond to cyberattacks so we could observe first-hand how threat actors circumvent cybersecurity safeguards, and to develop technologies and threat intelligence to better protect organizations from such attacks. Fast forward a few years, Mandiant was bought by FireEye, and I became FireEye's CEO in 2016.

As I testify today, FireEye employees are on the front lines of the cyberbattle, currently responding to over 150 active computer intrusions at some of the largest companies and organizations in the world. Over the last 17 years, we have responded to tens of thousands of security incidents. It is unfortunate, but we receive calls almost every single day from organizations that have suffered a cybersecurity breach. For each security incident we respond to, it is our objective to figure out what happened and to determine what organizations can do to avoid similar incidents in the future. We also maintain over 200 intelligence analysts, located in more than 20 countries, speaking over 30 languages, who pursue attribution and identification of the threat actors via research and sources.

The Cyber Intrusion into FireEye

When FireEye was compromised in late 2020, we approached our own situation as we would any other, by mobilizing a team of experienced investigators to understand the scope of the incident, and how to reclaim privacy and security on our networks. In fact, over the course of the weeks we spent investigating our security incident, we had over 100 of our employees working virtually around the clock to rapidly identify what happened and what we had to do about it. Incidents such as ours are complex and require special skills to scope, analyze, and remediate.

We first identified an intrusion in late November, upon investigating a peculiar alert indicating that one of our employee's accounts had registered a second phone in order to receive codes to

access our network via two-factor authentication. Although such activities are common during the release of popular new cell phones, we followed up on the alert and ascertained that the employee had *not* registered a new device. This signaled to us that an unknown third party had accessed our network without proper authorization.

As a company that develops software to enable complex security intrusion investigations, we were well-positioned to launch a full-scale investigation with pre-deployed technologies that gave us high-fidelity evidence into the activities of the intruder(s).

Early in our investigation, we uncovered some tell-tale signs that the attackers were likely working for and trained by a foreign intelligence service. We were able to discover and identify these signs in reliance upon our catalog of the trace evidence of thousands of computer intrusion investigations conducted over the last 17 years. We record the digital fingerprints of every investigation we have undertaken with great rigor and discipline, and we are often able to use this catalog of evidence in order to attribute the threat actors in many of the incidents we respond to.

Based on the knowledge gained through our years of experience responding to cyber incidents, we concluded that we were witnessing an attack by a nation with top-tier offensive capabilities. This attack was different from the multitude of incidents to which we have responded throughout the years. The attackers tailored their capabilities specifically to target and attack our company (and their other victims). They operated clandestinely, using methods that counter security tools and forensic examination. They also operated with both constraint and focus, targeting specific information and specific people, as if following collection requirements. They did not perform actions that were indiscriminate, and they did not appear to go on "fishing expeditions."

Such focused targeting, combined with the novel combination of techniques not witnessed by us or our partners in the past, contributed to our conclusion that this was a foreign intelligence actor. Therefore, on December 8, 2020, we publicly disclosed that we were attacked by a highly sophisticated threat actor -- one whose discipline, operational security, and techniques led us to believe it was a state-sponsored attack utilizing novel techniques.

During our investigation, we found that the attacker targeted and accessed certain Red Team assessment tools that we use to test the security of our customers' systems. These tools mimick the behavior of many cyber threat actors and enable FireEye to provide essential diagnostic security services to our customers. None of the stolen Red Team tools contained zero-day exploits.

While we were not certain that the attacker intended to use our Red Team tools or to publicly disclose them, we developed more than 500 countermeasures and proactively released these countermeasures for our customers, and the community at-large, to use in order to minimize the potential impact of the theft of the tools. We have seen no evidence to date that any attacker has used the stolen Red Team tools. We, as well as others in the security community, continue to monitor for any such activity. When we disclosed this incident in December, our top priority was ensuring that the entire security community was both aware, and protected against the attempted use, of these Red Team tools.

Following our initial disclosure to the public, we exhausted virtually every investigative lead in our effort to identify how the attackers initially accessed our network. Our investigation led us to perform forensic analysis of one of our SolarWinds servers. We decided to decompile and reverse engineer our entire SolarWinds platform to determine whether it contained an implant. This work requires very special skills, both in understanding malicious code, as well as how to read assembly language. During our analysis, we uncovered an implant of code in the SolarWinds Orion business software updates. This implant was designed to distribute malware we call SUNBURST.

After confirming our findings, we informed SolarWinds on December 12 that its Orion platform had been compromised. On December 13, in order to empower the community to detect this supply chain backdoor, we published indicators and detections to help organizations identify this global intrusion campaign. We have continued to update the public repository with host and network-based indicators as we develop new - or refine existing - indicators. Our goal in sharing this information not only with our customers, but more broadly, is to help all in the security community detect this malicious activity and hopefully put a stop to it.

As part of FireEye's continued analysis of SUNBURST, we identified a feature in the code that prevented SUNBURST from continuing to operate. Such features are sometimes referred to as "kill switches." FireEye collaborated with GoDaddy and Microsoft to enact this kill switch. Although this did not remove the intruders from victim networks that they had already infiltrated, it made it much more difficult, if not impossible, for the intruders to leverage SUNBURST.

While we are aware of a small number of victim organizations in Europe, Asia, and the Middle East, the majority of victims of the SUNBURST malware campaign were government, consulting, technology, and telecommunications entities in North America. We have notified those entities that we are aware have been affected.

Recommendations to Protect the Nation

Allow Confidential Information Sharing for More Rapid Defense

The SolarWinds implant led to dozens of organizations being breached, and thousands more becoming vulnerable. These victim companies had no idea they had been compromised until they were notified by either law enforcement or a business partner, such as FireEye and Microsoft.

Generally, victims of crime are the first to know when they have been violated. In constrast, only a few government agencies and a handful of security or other private companies are in the unique position to be the first to know that they themselves or others are the victim of a cyber attack. Rather than merely notifying victims long after their information has been stolen, a small group of "first responders" could prevent or mitigate the impact of cyber incidents through sharing contextual, actionable information quickly and *confidentially*.

Speed is critical to the effective disruption or mitigation of an attack by an advanced threat actor. However, challenges today prevent entities from sharing cyber threat intelligence. For example, organizations are concerned about public disclosure and the liabilities that stem from a breach. Fears over class action lawsuits, reduction to shareholder value, and public negative sentiment create an environment in which organizations are reluctant to voluntarily or rapidly share information.

A confidential information sharing solution should ensure a consistent flow of two-way information sharing between the public and private sectors to help maximize the ability to resolve and consider attribution. An interesting model to consider is the Federal Aviation Administration's Aviation Safety Reporting System, which is based on non-punitive, anonymous reporting and communication to communities about threats. Major tenets include:

- Continuous effort by government and industry to maintain and improve aviation safety;
- Collection, analyses, and response to voluntarily submitted aviation safety incident/situation reports from pilots, controllers, etc.;
- Dissemination of reports to private and public sector stakeholders;
- Identification of deficiencies and discrepancies in the National Aviation System (NAS) for remediation by appropriate authorities; and
- Policy formulation and planning support for, and improvements to, the NAS.

The U.S. government should consider a federal disclosure program for not only sharing threat indicators but for also providing notification of a breach or incident. Such a program should:

- Safeguard the protection and integrity of electronic and other types of data;
- Encourage entities to adopt recognized cybersecurity standards and practices with a minimum threshold;
- Focus less on punitive measures;
- Provide greater incentives for private sector entities, including liability protections and statutory privilege to not be disclosed in civil litigation (e.g., confidentiality obligations);
- Protect privacy and civil rights; and
- Provide technical assistance to small entities that do not have cybersecurity expertise or capabilities.

Increase Public and Private Sector Collaboration

The Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security has made great strides in recent years to encourage information sharing from the private sector and to develop capabilities that provide cyber threat hunting and incident response capabilities to government agencies and critical infrastructure partners. Unfortunately CISA's capacity is still limited compared to the relative demand, especially during periods of large-scale or widespread cyber attacks.

The only way CISA can be successful is to properly harness the power and respect of the private sector. Private companies have huge resources and talent, and already defend much of our Nation's infrastructure. We must be more creative about how CISA can leverage and work with private sector talent and resources. This also necessitates involving the National Security Agency and U.S. Cyber Command in certain instances of widespread cyber attacks.

In addition to encouraging private sector information sharing, focused attention should be given to building more effective collaboration between the government and private sector critical infrastructure organizations. Providing timely, contextual, and actional information and technical support prior to and during a cyber attack is key to building trust and providing mutual value and benefits to both parties.

Although we cannot eliminate or prevent every security incident, prompt and coordinated actions allow us to minimize the impact and consequences of an incident. Rapid detection of the intrusions, combined with more timely notification to victims, would provide organizations an opportunity to mitigate as opposed to just evaluating the impact of the compromise and the value lost to the adversary. Such speed could be achieved through efficient, consistent, and confidential information sharing between and among members of a small consortium of government agencies, law enforcement, security and other private companies.

Conclusion

On behalf of FireEye, I thank you for this opportunity to testify before the Committee. We stand ready to work with you and other interested parties in devising effective solutions to deter malicious behavior in cyberspace and to build better resiliency into our networks. I look forward to your questions.

Chairman WARNER. Thank you, Kevin.
Sudhakar?

STATEMENT OF SUDHAKAR RAMAKRISHNA, CEO, SOLARWINDS INC.

Mr. RAMAKRISHNA. Chairman Warner, Vice Chairman Rubio, and Members of the Committee, on behalf of SolarWinds' employees, partners, and customers in the U.S. and around the world, I would first like to say thank you for inviting us to this hearing.

By way of background, I'm Sudhakar Ramakrishna, and I joined SolarWinds on January 4th of this year. Prior to SolarWinds, I was with a company called PulseSecure for over five years, and previously held executive roles at other technology companies.

In my roles, I've been involved with cyber incidents and have seen firsthand the challenges they present, as well as the opportunities they create for learnings and improvements. While our products and customers were the subject of this unfortunate and reckless operation, we take our obligation very seriously, to work tirelessly to understand it better to help our customers, and to be transparent with our learnings with our industry colleagues and the government.

SolarWinds started in 1999 in Oklahoma as a provider of network tools and to this date, we have remained true to our mission of helping IT professionals solve their problems and manage their networks, now through more than 90 products. Today, we remain a U.S.-headquartered company, with over 3,000 employees working extremely hard to deliver customer success.

When we learned of these attacks, our very first priority, and that remains true today, was the safety and protection of our customers. Our teams worked incredibly hard and tirelessly to provide remediations within about 72 hours of knowing about these attacks. We also acted very quickly to disclose these events to the authorities, while providing remediations and starting our investigations of what do we learn about this, who may have done it, and what exactly happened in the process of insertion into our Orion platform?

We believe the Orion platform was specifically targeted in this nation-state operation to create a backdoor into the IT environments of select customers, as my colleague Kevin noted, as well. The threat actor did this by adding malicious code, which we call "Sunburst," to versions released between March and June 2020. In other words, a three-month window was when the code with the malicious Sunburst code was deployed.

I will note that this code has been removed and is no longer an ongoing threat to the Orion platform. Additionally, after extensive investigations, we have not found Sunburst in our more than 70 non-Orion products.

Perhaps the most significant finding to date in our investigation is what the threat actor used to inject Sunburst into other Orion platforms. This injected tool, which we call "Sunspot," was stealthily inserted into the automated build processes of Orion and was designed to work behind the scenes. Sunspot, which we discovered, poses a grave risk of automated supply chain attacks through

many software development companies, since the software processes that SolarWinds uses is common across the industry.

As part of our commitment to transparency, collaboration, and timely communications, we immediately informed our government partners and published our findings with the intention that other software companies in the industry could potentially use the tool to detect possible current and future supply chain attacks within their software build processes.

We understand the gravity of the situation and are applying our learnings of Sunspot and Sunburst and sharing this work more broadly. Internally, we call these initiatives "secure by design." And it's premised on zero-trust principles and developing a best-in-class secure software development model to ensure our customers can have the utmost confidence in our solutions.

We have published these details regarding our efforts in various blog posts. But in summary, they are focused on three primary areas:

The first is further securing our internal infrastructure.

The second is ensuring and expanding the security of our build environments.

And third, ensuring the security and integrity of the products we deliver.

Given our unique experience, we are committed to not only leading the way with respect to secure software development, but to share our learnings with the industry. While numerous experts have commented on the difficulties that these nation-state operations present to any company, we are embracing our responsibility to being an active participant in helping prevent these types of attacks. Everyone at SolarWinds is committed to doing so. And we value the trust and confidence our customers place in us.

Thank you again for your leadership in this very important matter. We appreciate the opportunity to share our experiences and our learnings. And I look forward to your questions.

[The prepared statement of Mr. Ramakrishna follows:]

Written Testimony of Sudhakar Ramakrishna

Chief Executive Office, SolarWinds Inc.

United States Senate Select Committee on Intelligence

February 23, 2021

Introduction

Chairman Warner, Vice Chairman Rubio, and Members of the Committee, thank you for inviting SolarWinds to assist in your efforts surrounding the unprecedented nation state attack on SolarWinds, its users and the technology industry more broadly. We appreciate the opportunity to share our findings, lessons learned and our recommendations to promote the public-private information sharing, collaboration and support that we believe are necessary to protect us all against these types of operations in the future.

My name is Sudhakar Ramakrishna, I am the new President & CEO of SolarWinds. I joined SolarWinds on January 4th. Prior to SolarWinds, I was the CEO of Pulse Secure for over 5 years. Pulse Secure is a provider of secure and zero trust access solutions, and previously, I held executive roles at Citrix, Polycom, and Motorola, amongst others.

SolarWinds is a provider of IT infrastructure management software. Our products give organizations worldwide, regardless of type, size or IT infrastructure complexity, the ability to monitor and manage the performance of their IT environments, whether on-premises, in the cloud, or in hybrid deployments. We are a Texas-based company with over 3,000 employees in 17 countries around the world.

SolarWinds' Commitment to Cooperation and Transparency

We sincerely appreciate your interest and assistance in helping us to address the many challenges that we and our users face because of this unprecedented nation state attack. While we understand that these challenges are much larger than SolarWinds, we recognize that we need to learn from this and share those lessons toward a greater solution. We are grateful for the opportunity to do so in font of this Committee and for the very valuable assistance we continue to receive from the FBI, CISA, and the Intelligence Community.

It is our goal to provide the Committee with information on our investigation, and critically, how we are applying what we've learned to incorporate systematic and systemic improvements to our environment and Software Development Life Cycle (SDLC) processes.

Our number one priority has been, and continues to be, to ensure that our users are safe and protected. To this end, our teams worked tirelessly to provide remediations to the affected product and accomplished that within 3 days of learning of the attack. We have also been very active in our user outreach and have dedicated significant resources to help users and partners across the public and private sectors.

We look forward to helping the Committee understand the attack and its implications, lessons we have learned as we have confronted it, and recommendations to help you and the Intelligence Community further protect U.S. cybersecurity.

Nation State Level Program

At this stage in our investigation, while we cannot definitively attribute the attack to any particular nation state, our external investigation partners CrowdStrike, KPMG and others confirm that the tactics, techniques and procedures displayed in this attack mirror that of a nation state.

There are three aspects of the attacker's activities that highlight the sophistication of the campaign: first, the malware, dubbed SUNBURST, they injected into the Orion Product for further deployment in our users' networks. Second, the malware they used in our build process to inject the SUNBURST code into Orion's final software package. And third, their stealthy use of U.S.-based cloud services to innocuously interact with victim networks.

Code Inserted into Our Users' Environment - SUNBURST

By way of background, SUNBURST is a malicious code that was injected by the threat actor(s) into specific versions of our Orion Software Platform which we released between March of 2020 and June of 2020. Based on our investigations, SUNBURST was not present in versions of our Orion Software Platform and related products which we released prior to March 2020, or after June 2020.

It is important to understand what the malicious SUNBURST code was designed to do and what was required for the malicious code to be utilized by the threat actor(s). The malicious code was designed in such a way that when the impacted versions of the Orion Software Platform were installed on a network, the malware tried to open a "back door" into the target network.

The back door only worked if the Orion Software Platform had access to the internet which is not required for the Orion Software Platform to operate. If a back door was indeed opened, the threat actor(s) had to take further steps to gain access to the victim's network, and then had to circumvent firewalls and other security defenses within a target's IT environment.

Code Inserted into our Environment - SUNSPOT

Further, working together with our partners, we have been able to locate the malicious code injection source by reverse engineering the code utilized in the nation state attack. The malicious tool that was deployed into the build environment to inject the SUNBURST backdoor into the Orion Software Platform has been code named SUNSPOT and was designed to be injected without arousing the suspicion of our software development and build teams.

Our investigations have also revealed that the threat actor(s) conducted an extensive intelligence reconnaissance and offensive operation inside of our networks. The reconnaissance element of the operation existed throughout our environment for months. The overall intent of this operation appears to have been to influence updates to our Orion Software Platform through the utilization of SUNSPOT to distribute SUNBURST deliberately and maliciously to Orion users.

The creation of SUNSPOT and its involvement in this operation is an alarming development for the software development community. Because of the extreme potential significance of this malicious tool to the wider IT community, I instructed our investigative team to immediately brief the U.S. law enforcement and Intelligence Community, including CISA and the UK NCSC, and publish information publicly on the details surrounding SUNSPOT and SUNBURST. My reasoning for doing so was to raise awareness swiftly and expeditiously to help the IT community identify similar attacks and to help prevent another company from having SUNSPOT or similar code embedded into their development environment.

Adversary Abuse of U.S. Cloud Infrastructure

Our analysis, confirmed in our conversations with U.S. Government partners, also suggests that by managing the campaign through multiple servers based in the United States and mimicking legitimate network traffic, the attackers were able to circumvent threat detection techniques.

Adversary Campaign Takeaways

We believe that the entire software industry should be concerned about the nation state attack as the methodologies and approaches that the threat actor(s) used can be replicated to impact software and hardware products from any company, and these are not SolarWinds specific vulnerabilities. To this end, we are sharing our findings with the broader community of vendors, partners, and users so that together, we ensure the safety of our environments.

The breadth of the nation state attack is large, and the level of potential impact is growing. We believe this increases the urgency for a coordinated response by the United States government and the technology industry. We are committed to contributing our lessons and experiences, and believe this response should build on recommendations from the Cyberspace Solarium Commission and the Fiscal Year 2021 National Defense Authorization Act (NDAA):

1. *Improving Industry Government Supply Chain Security Collaboration*
   Building on CISA's Information Communications Technology Supply Chain Risk Management Task Force and consistent with Solarium Enabling Recommendations 4.6.1 (Increase Support to Supply Chain Risk Management Efforts) and NDAA Section 1713 (Establishment of an Integrated Cybersecurity Center), advocate for a public-private initiative to secure enterprise software and services by increasing threat sharing and fostering greater joint collaboration between private firms and governments stakeholders including CISA, FBI, DoD and ODNI.

2. *Improving Federal Government Cybersecurity Standards*
   Building on DOD's Cybersecurity Maturity Model Certification (CMMC) effort for Department of Defense contractors and continued security enhancements to the Federal Information Security Modernization Act (FISMA), support the creation of industry-wide security standards based on continuous risk monitoring and measurement for current and potential government contractors.

3. *Improving Incident Notification to the Government*
   Consistent with Enabling Recommendation 4.7.1 (Pass a National Breach Notification Law), empower organizations with the appropriate incentives and liability protections to share more information on attempted or successful breaches with government cybersecurity authorities. Indicators of compromise associated with those events shared with software vendors in an anonymized way enriches the understanding of prevailing threat actor techniques and target sets, enabling software providers to improve defenses and better protect users.

In summary, certain initial important findings and conclusions based on our experience are as follows:

1. Various third-party experts have concluded that this attack shows that when a sophisticated nation state applies its full arsenal of resources, it is difficult for any enterprise to defend against it.

2. The use of SUNSPOT to compromise software build environments has exposed a significant threat to the global software supply chain at large. It has become increasingly clear that the risk of its use is not isolated to SolarWinds.[1] The threat affects the global software supply chain in general, as evidenced by the recent identification of additional companies that have been subjected to similar attacks.[2] Third-party experts now have confirmed SolarWinds was only one of the many supply chain vectors used by the nation state adversary, and perhaps not the largest one.

3. As testimony from cybersecurity expert Dmitri Alperovitch to the House Homeland Security Committee last week demonstrates, facts now reveal that the description of this issue as the "SolarWinds attack" is a misnomer. CISA's Acting Director Brandon Wales echoed this sentiment in an interview with the Wall Street Journal. Our nation faces a persistent, determined effort by adversarial nation states to attack, compromise, and exploit the software supply chain and labeling as the SolarWinds attack improperly narrows the scope of the threat.

4. We believe for any solution to be effective; prescriptions must apply a "zero trust" presumption, access provided on a least privileged basis, and must take account of the breadth of the problem across the entire U.S. supply chain.

5. Every enterprise can learn from these events and strive to improve their security posture and re-double their efforts towards public-private partnerships.

Protecting Our Users

Since becoming aware of the nation state attack, we have worked tirelessly to ensure that our products are free of malicious code, protecting our private and public sector users and enabling them to continue to use our products safely.

We promptly disclosed the attack and acted expeditiously to provide our users with information and remediation and mitigation measures, including upgrades to all impacted versions of the Orion Software Platform. We are also applying our lessons learned and implementing sustainable improvement initiatives.

We have formed a "Technology and Cybersecurity" committee of our board. Two current sitting members of our board, who are CIOs with significant cybersecurity experience, and I comprise the three-member committee. This committee has the responsibility to provide advice to management and oversight of our cybersecurity improvement initiatives.

---

[1] https://www.wsj.com/articles/suspected-russian-hack-extends-far-beyond-solarwinds-software-investigators-say-11611921601.

[2] https://www.wsj.com/articles/suspected-russian-hack-extends-far-beyond-solarwinds-software-investigators-say-11611921601.

Implementing Lessons Learned

We are applying our knowledge to evolve SolarWinds into a company that is "Secure by Design." These efforts are focused on three primary areas[3]:

- Further securing our internal environment;
- Enhancing our product development environment; and
- Ensuring the security and integrity of the products we deliver.

Key steps to further securing our internal environment which we are prioritizing as a central part of our operational fabric as we move forward include:

- Deploying additional, robust threat protection and threat hunting software on all our network endpoints, including a critical focus on our development environments;
- Resetting credentials for all users in the corporate and product development domains, including resetting the credentials for all privileged accounts, and for all accounts used in building the Orion Software Platform and related products; and
- Consolidating remote and cloud access avenues for accessing the SolarWinds network and applications by enforcing multi-factor authentication.

Key steps to enhancing our product development environment include:

- Performing ongoing forensic analysis of our product development environments identifying root causes of the breach and taking remediation steps; and
- Evolving to parallel build systems and environments with stricter access controls and deploying mechanisms to allow for reproducible builds from multiple independent pipelines. This will further improve the integrity of our software beyond code-signing practices which have proven to be inadequate.

Key steps to ensuring the security and integrity of the software that we deliver to users include:

- Adding additional automated and manual checks to ensure that our compiled releases match our source code after the completion of the compile process;
- Re-signing all Orion Software Platform and related products, as well as all other SolarWinds products, with new digital certificates;
- Performing extensive penetration testing of the Orion Software Platform and related products to identify any potential issues which we will resolve with urgency;
- Leveraging third-party tools to expand the security analysis of the source code for the Orion Software Platform and related products;
- Implementing least privilege access controls, network segmentation, and additional MFA and encryption for our development environments; and
- Engaging with and funding ethical hacking from white hat communities to quickly identify, report, and remediate security issues across the entire SolarWinds portfolio.

---

[3] We have published the elements of these dimension in a blog: https://orangematter.solarwinds.com/2021/01/07/our-plan-for-a-safer-solarwinds-and-customer-community/.

Our collective efforts are guiding our journey to becoming an even safer and more secure company for our users and other stakeholders.

We have also added additional levels of security and review in our software build process and in other areas of our environment– through tools, processes, automation, and, where necessary, manual checks to ensure the integrity and security of all our products.

Understanding the Impact of the Nation State Level Program

Federal and civilian users use a range of SolarWinds' approximately 100 products. When SolarWinds was notified about the cyber attack, we conservatively estimated the number of potentially impacted users.

Now, with the advantage of ongoing and in-depth investigations into the circumstances of the compromise, we are better positioned to provide more reliable estimates. Only three Orion Software Platform versions released between March and June 2020 were affected. The remediations provided by SolarWinds, together with the "kill switch" discovered and implemented by our colleagues, rendered the SUNBURST code inert in the three affected Orion Software Platform versions.

On December 30, the Cybersecurity and Infrastructure Security Agency (CISA) notified users that the National Security Agency had examined this version and verified that it "eliminates the previously identified malicious code." Beyond the affected versions of Orion, to date, investigators have not found SUNBURST or a similar cyber attack in SolarWinds' many non-Orion products and tools, or in the 16 non-affected Orion Software Platform versions.

Conclusion

Based on the challenges posed by SUNSPOT and SUNBURST and considering SolarWinds' extensive array of responses and initiatives, we believe that we can contribute meaningfully to a national solution. To that end, we hope the Committee will engage with SolarWinds on an ongoing basis and accept our assistance in any way that may be helpful.

Chairman Warner, Vice Chairman Rubio, and Members of the Committee, thank you for your leadership on the important topic of our nation's cybersecurity. We appreciate the opportunity to share our experience with you and some of the lessons we have learned. It is clear to me that we must work together to ensure the safety and stability of the digital ecosystem and I pledge to you SolarWinds' active participation and contributions. I look forward to your questions.

Vice Chairman RUBIO. Thank you. And for the Members who haven't yet voted, I guess everybody's voted because everybody's almost gone here.

So, Mr. Smith, thank you for being here. We appreciate it.

STATEMENT OF BRAD SMITH, PRESIDENT, MICROSOFT CORPORATION

Mr. SMITH. Well thank you, Vice Chairman Rubio, and a huge thank you to Chairman Warner for bringing us all together to discuss what is obviously such an important issue to the country, and indeed to the world. And I also just want to say thank you to Kevin and Sudhakar. It took the leadership, and I'll say even the courage, of companies like FireEye and SolarWinds to step forward and share information. And it is only through this kind of sharing of information that we will get stronger to address this.

I think Kevin and Sudhakar have done an excellent job of describing what happened. So I don't want to retrace the steps that they so ably took. Let me talk about two other things. First, what does this mean? And second, what should we do? Well, roughly 90 days or so since we first heard about this from Kevin's firm, from FireEye, I think we can step back and start to think about what it means.

First, we're dealing with a very sophisticated adversary. And Vice Chairman Rubio, I think your words of wisdom, of caution, about avoiding certain labels are well put. But I do think we can say this: at this stage, we've seen substantial evidence that points to the Russian Foreign Intelligence Agency and we have found no evidence that leads us anywhere else. So we'll wait for the rest of the formal steps to be taken by the government and others. But there's not a lot of suspense at this moment in terms of what we're talking about.

It's very, very clear that this agency is very, very sophisticated. And as Kevin noted, that has been true for a long time. That is not new. But I think two other things are new. The first is the scale of this attack, or hack, or penetration, or whatever we should call it. At Microsoft, as we worked with customers that had been impacted by this, we stepped back and just analyzed all of the engineering steps that we had seen. And we asked ourselves how many engineers did we believe had worked on this collective effort? And the answer we came to was at least 1,000. I should say at least 1,000 very skilled, capable engineers.

So we haven't seen this kind of sophistication matched with this kind of scale. But there's one other factor that I do believe puts this in a different category from what we have seen. And I think even with a thoughtful consideration, it is appropriate to conclude even now: this was an act of recklessness, in my opinion.

Why? Well, in part, I think Chairman Warner put it very well. The world relies on the patching and updating of software. We rely on it for everything. We rely on it not only for the safety and health of our computers, we rely on it for our physical infrastructure, for hospitals, and roads, and airports, because they all run on software. To disrupt, to damage, to tamper with that kind of software updating process is, in my opinion, to tamper with what is in effect the digital equivalent of our public health service. It puts the entire

world at greater risk. And it was done I think one must acknowledge in a very indiscriminate way: to seek to plant malware and distribute it to 18,000 organizations around the world is in truth an act without clear analogy or precedent.

We've seen this done in Ukraine, but we haven't seen it done quite like this. It's a little bit like a burglar who wants to break into a single apartment but manages to turn off the alarm system for every home and every building in the entire city. Everybody's safety is put at risk. And that is what we're grappling with here.

So what do we do?

I think we have to start by acknowledging and recognizing we need to do a lot. We all need to do a lot. We need to do a lot ourselves, and we need to do a lot together. Certainly, as Sudhakar was mentioning, we need to focus on the integrity, the protection of software build systems.

The International Data Corporation estimates that there will be half a billion—500 million software apps—created in the next three or four years. That's half a billion build systems. And it's not just software companies; it's banks, it's hospitals, it's governments. It's everyone that creates software. There are new steps that we will need to take to better secure and protect against the kind of attack that we saw here.

Second, I think we have a lot of work still to do, certainly across the United States, when it comes to the modernization of our IT infrastructure and to the application of IT best practices. At Microsoft, we can only see this attack among our customers when it got to their use of their cloud services and all of the attacks that took place, took place on premise. Meaning a server that was in a server room or a closet somewhere. And it points to the fact that until we modernize and move more people to the cloud, we're going to be operating with less visibility than we should.

Third, we do need to enhance the sharing of threat intelligence. That's the term in the cybersecurity community for information about attacks that people are seeing. And our basic challenge today is that that information too often exists in silos. It exists in silos in the government, exists in different companies. It doesn't come together.

Fourth, I think because of that need, it is time not only to talk about, but to also find a way to take action to impose in an appropriate manner some kind of notification obligation on entities in the private sector. And so of course you know, it's not a typical step when somebody comes and says, "place a new law on me, put it on ourselves, put it on our customers," but I think it's the only way we're going to protect the country. And I think it's the only way we're going to protect the world.

And finally, I do believe it is time—it's maybe even overdue time—for us to look at the rules of the road, the norms and laws, that if not every government is prepared to follow, at least the United States and our likeminded allies are prepared to step up and defend. And among other things, to say that this kind of tampering indiscriminately and disproportionately with a software supply chain needs to be off-limits. And there needs to be attribution and there needs to be accountability, as officials in the White House are now considering.

Finally, I'll close by addressing one question that Vice Chairman Rubio, I think you posed. Who knows the entirety of what happened here? One entity knows. It was the attacker. The attacker knows everything they did. And right now the attacker is the only one that knows everything they did. We have pieces. We have pieces at Microsoft, SolarWinds, FireEye, CrowdStrike others, we all have slices. People in the U.S. Government.

But we need to bring those slices together. And until we do, we'll be living and working and defending on an uneven playing field. That is not a recipe for success. But let's also acknowledge one other thing: we know more than we did 100 days ago. We are better informed, we are smarter, and we can turn that knowledge into a resolve and action. That's what we need to do. That's what I hope the Congress can do. That's what I think the country and our allies need to do. If we use what we have learned, we can better protect our future. Thank you.

[The prepared statement of Mr. Smith follows:]

Strengthening the Nation's Cybersecurity:
Lessons and Steps Forward Following the Attack on SolarWinds

Written Testimony of Brad Smith
President, Microsoft Corporation

Senate Select Committee on Intelligence
Open Hearing on the SolarWinds Hack

February 23, 2021

Chairman Warner, Vice Chairman Rubio, thank you for the opportunity to appear today to discuss the recent SolarWinds attack, contribute to an understanding of what happened, and address potential solutions for how we can work collectively to keep a cyber event of this magnitude from occurring again.

I will begin by sharing what Microsoft has learned about the SolarWinds attack. From what we know so far, this attack was sophisticated and complex. While we have completed our internal investigation of the attack's impact on Microsoft, there remains more to investigate and learn in terms of its impact on governments and other organizations around the world. No one should believe that this attack has yet been fully understood or is yet fully contained. At Microsoft we are committed to the continued sharing of what we learn. That is why I am here today.

If one thing is apparent, it's that we all have important work to do to strengthen the nation's cybersecurity. We must be prepared for even more sophisticated and well-resourced foreign attacks in the future. We will need new measures that are grounded in leadership by the public sector and even more collaboration with the private sector. We will all need to do more to help organizations large and small to secure their IT infrastructure. All this must start with more communication and sharing of information, both for more effective real-time responses during cyber incidents and to share new lessons afterwards.

Today, too many cyberattack victims keep information to themselves. We will not solve this problem through silence. It's imperative for the nation that we encourage and sometimes even *require* better information-sharing about cyberattacks.

This responsibility is especially important for the tech sector itself. For cybersecurity as for other areas, knowledge is power. Broader information-sharing is indispensable to strengthening the nation's cybersecurity protection.

After reviewing what we have learned in detail below, I will address several specific concrete areas where we believe action is essential:

- First, we need to **strengthen supply chain security** for the private and public sectors alike for both software and hardware.
- Second, we need **to broaden use of cybersecurity best practices**, including through improved cyber hygiene and a commitment to IT modernization.
- Third, we need a **national strategy to strengthen how we share threat intelligence** across the entire security community.
- Fourth, we need to **impose a clear, consistent disclosure obligation** on the private sector.
- Finally, we need to **strengthen the rules of the road for nation-state conduct** in cyberspace.

1. Background/Overview

We are here today because thousands of miles away, a capable and determined adversary of the United States executed a disciplined attack, penetrating large government agencies and key private sector companies. This sophisticated and successful attack shines a bright light on the need to significantly strengthen cybersecurity protection across all our vital enterprises, organizations, and government agencies. We must also take the necessary steps to prevent and respond more quickly to any future attacks, starting by advancing international consensus on establishing and enforcing a rules-based order online.

The US Government has attributed the attack to an "Advanced Persistent Threat Actor, likely Russian in origin."[1] While Microsoft is not able to make a definitive attribution based on the data we have seen, we do not disagree with the government's assessment. In short, and even after considerable review, we have seen no evidence that points in any other direction.

We know that what lies on the surface is only part of this attack's story, and we all should remain focused on what is not yet known. The victims that have been revealed to the public represent an important portion of the problem, but they are like the tip of the iceberg, and we do not know what lies beneath the surface. This is especially pertinent in this case because all of the attacks we've identified started "on premise," meaning on a server physically within an organization's presence. And yet we only have direct visibility to the attack when it then moved to the cloud. As a result, customers that haven't yet migrated to the cloud are more likely to be continued and undiscovered victims.

The fact that we are here today, discussing this attack, dissecting what went wrong, and identifying ways to mitigate future risk, is occurring only because my fellow witness, Kevin Mandia, and his colleagues at FireEye, chose to be open and transparent about what they found in their own systems, and to invite us at Microsoft to work with them to investigate the attack. Without this transparency, we would likely still be unaware of this campaign. In some respect, this is one of the most powerful lessons for all of us. Without this type of transparency, we will fall short in strengthening cybersecurity.

2. The Attack

At Microsoft we first became aware of the SolarWinds attack when FireEye contacted us in late November, just after Thanksgiving. They had uncovered a breach of their system and asked for our support in their internal investigation. In addition to reaching out to share threat intelligence, they took some critical steps swiftly and voluntarily, including alerting the federal government of what they found and disclosing the breach to the public.

After several days of intense research and collaboration, the story of what occurred started to come into focus. FireEye discovered that an attacker had successfully breached its on-premises network (its private data center housed in their own facility). FireEye had installed an update to software it used from SolarWinds, and when they did, they unknowingly also installed the attacker's malware, opening a back door into FireEye's private system.

While there is still more to investigate regarding how this occurred and the scale of the attack, we know SolarWinds itself had been breached through its own on-premises network, and the initial compromise happened in the fall of 2019. The Russian attackers placed malware into SolarWinds Orion software update, which was subsequently distributed to more than 17,000 customers. At Microsoft we call the initial backdoor malware installed with the Orion update Solorigate.

---

[1] Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) | CISA

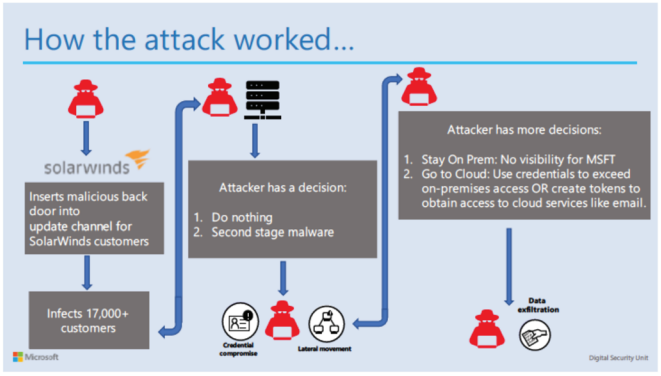
Attacks that compromise software updates have been observed since at least 2015.[2] We all recognized the potential power of this type of attack with NotPetya,[3] Russia's destructive attack on Ukraine in 2017. Much like the technique used by Russian attackers during NotPetya, the SolarWinds attack targets the civilian software supply chain. This is a particularly insidious vector as it undermines trust in the very systems technology companies use to update software, remediate vulnerabilities, and protect users from intrusions.

The SolarWinds attack can be thought of as a large-scale series of home invasions. The malware installed with the Orion update was, in effect, a key that unlocked and secretly opened the back door to over 17,000 houses, with each house representing an on-premises network, without the owner noticing the door was open. This attack worked against any network, no matter what company's technology was being used.

The Russian attacker then used information about each victim's network, transmitted to it by the malware in each house, to install a more powerful malware package in the houses that were most interesting to them. This second malware package opened a new way – let's call it a window – to communicate with the victim networks. With this new access point established, the attacker hid its presence by closing the back door so it would not be discovered.

Once inside the house, the attacker in effect turned off any security cameras – that is, it turned off event logging tools and in some cases antivirus software – and began sneaking around, looking for valuable things, like looking for keys that would give them access to the most precious possessions in the home. In network defense, we call this looking for tools and methods to elevate privileges, essentially finding a way to gain access to any guarded room or safe that houses valuable information.

In some houses the attacker found valuables, such as red-team tools or snippets of source code, which it then copied and took. Red-team tools are especially important here because they are the very tools used by cybersecurity organizations to evaluate the security posture of an enterprise system. In some cases, the Russian actors were looking for keys that would allow access to other environments, like a burglar looking for car keys inside a home. The keys they sought would give them access to the victim's cloud services, including resources like Office 365. And just like a stolen car, these cloud services can be accessed with the right set of keys.



[2] EvLog Security Note (eventid net)
[3] The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED

The SolarWinds Orion software update was the principal initial vector for many of these attacks, but it was not the only entry into these houses. In some instances we have seen, the Russian actor used aggressive password spray attacks to gain access. A password spray is when an attacker attempts to login using a variety of common or relatively simple passwords against many targets, knowing that someone in an organization is likely to have one of them as their password.[4] This is a technique that Russian actors have used many times in recent years. The attacker also appears to have leveraged other supply chain attacks[5] to create other entry points as well, and we are continuing to investigate as we do not believe all supply chain vectors have yet been discovered or made public. All told, we believe that the attacker may have used up to a dozen different means of getting into victim networks during the past year.

We have learned through our investigations that this attack was a multi-faceted campaign by this Russian attacker, but at its core it was an identity attack, a conclusion that White House Deputy National Security Advisor for Cyber and Emerging Technology, Anne Neuberger, confirmed during a press conference on February 17th. The Russians did not just want to get inside the houses of the victims. They wanted to find the most interesting valuables, which to them meant reading, examining, and in some cases taking data and information. Just as they used many ways to initially attack their victims and open a back door, they also used a variety of ways to compromise identity.

It is important to understand this aspect of the attack: unlike some attacks that take advantage of vulnerabilities in software, this attack was based on finding and stealing the privileges, certificates, tokens or other keys within on-premises networks (which together is referred to as "identity") that would provide access to information in the same way the owner would access it. This approach was made much easier in networks where basic cybersecurity hygiene was not being observed – that is, where the keys to the safe and the car were left out in the open.

3. The Victims

One of the first steps we took was to determine if we could help identify other victims of this attack. In doing this work Microsoft has discovered a great deal, but almost certainly we have not yet learned everything there is to know about this attack. There is much we and the rest of the security community still do not know.

Microsoft has notified 60 customers, most of which are in the United States, that they were compromised and likely had data accessed in this campaign. The primary targets (50%) are information and communication technology companies, with the rest of the victims being a combination of U.S. government agencies, government contractors, and NGOs including civil society organizations such as think tanks and academic institutions.

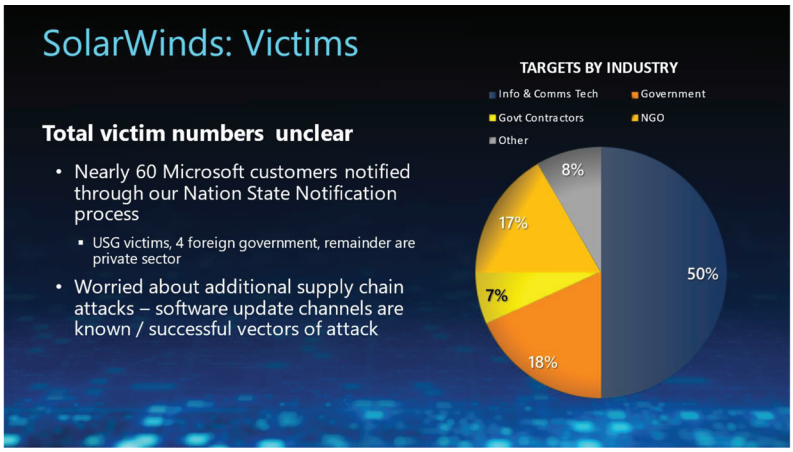
Without question, these are not the only victims who had data observed or taken. We do know that there are other companies whose customers have been compromised but who have not revealed victim information publicly. We also know from work we have done helping customers that there are victims where the Russian attacker stayed entirely within the on-premises network, and therefore are not among the 60 we discovered and notified. On February 17, Ms. Neuberger provided the government's first public estimate that the total number of victims was approximately 100 private sector companies and 9 U.S. government agencies. In addition to this estimate, we have identified additional government and private sector victims in other countries, and we believe it is highly likely that there remain other victims not yet identified, perhaps especially in regions where governments and other organizations where cloud migration is not as far advanced as it is in the United States.

In truth, no one yet knows for certain, except the Russian attacker.

---

[4] Protecting your organization against password spray attacks - Microsoft Security

[5] Mimecast says hackers abused one of its certificates to access Microsoft accounts | ZDNet



4. Microsoft's Response

To respond to this attack, Microsoft has taken an approach of detect, notify, remediate, and inform. Each of these steps is critical to incident response and in many cases the work needed to perform each step overlaps.

Detect

Armed with information learned from work with FireEye, Microsoft and other tech companies acted as a first responder. The first step, along with other anti-virus vendors, was to develop detections for the Solorigate malware so that our Microsoft Defender Antivirus technology could find and alert customers if the malware was present in their networks.[6] As we learned more about the Russian actor and the sophistication of the activity, we took more aggressive action and used Defender not just to detect, but to block the malware so it could not communicate with the attacker. Effectively, we slammed the back door shut.

We concluded that this was an essential first step, and as one commentator noted, we "released the Death Star"[7] on the Russian malware. We also worked with GoDaddy and FireEye to create a "kill switch" so that the Solorigate malware that opened the back door into victim networks would be disabled for everyone, not just our Defender customers. Despite these steps, however, we knew that the Orion update that contained the malware was installed before we could detect or disable it, sometime between March and June of 2020. By the time we blocked it, the attacker had a backdoor open into some victim networks for six to nine months, and during that time it could have opened "windows" into a large number of victim networks.

Our Microsoft Threat Intelligence Center, or MSTIC, which tracks the activity of nation-state actors, worked with the rest of Microsoft's security community to search for traces of activity by the Russian

[6] Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers - Microsoft Security
[7] Microsoft unleashes 'Death Star' on SolarWinds hackers in extraordinary response to breach - GeekWire

actors, including the use of credentials and other identity tools the actor stole from victims to obtain access to Office365 (O365). The 8 trillion signals coming daily into Microsoft from our ecosystem gave us a great deal of data to work with. However, the Russian actors hid their activity in legitimate network traffic and took other sophisticated steps to avoid detection.

Microsoft's only visibility into the Russian activity was communication between victim networks and O365, Microsoft's suite of productivity tools such as email and office applications. We could not look into on-premises networks to hunt for the Russian actor, and Microsoft has information only about networks on our cloud, not those hosted on other vendors' cloud services.

We have discovered that the Russians used several different approaches to obtaining the credentials O365 uses to identify legitimate users. In one approach they used elevated privileges in victim networks to generate what are called SAML tokens. These tokens are an industry-standard way for network resources and cloud services to recognize legitimate users. They are similar to an electronic key card that proves who you are so you can get access to a building or a particular doorway. As it turns out, however, the SAML token generation approach was only used by the Russian attackers 15% of the time among the victims we have identified. In the other 85% of cases, the Russians used a variety of other methods to obtain the credentials they needed to access O365 from an on-premises network.

Notify

As Microsoft teams identified victims, we quickly notified each of these 60 customers and offered information about the attack and the indicators of compromise (IOCs) that would help them start their own investigations.[8] This is a core commitment we make to our customers: we routinely notify customers when we see evidence that they have been threatened or compromised by a nation state actor. In the two years leading up to the Microsoft Digital Defense Report[9] in September of 2020, this amounted to more than 13,000 notifications globally.

Notification is important because it allows customers to take immediate steps to protect data and communications. It also enables customers to use their own logs to track and understand where in their environment an attacker is hiding, and where it might have opened other windows or stolen other information.

Remediate

Once victims were informed of the attack, there was much to do to respond. Victims had to identify how the Russian attackers got into their network – by SolarWinds, a different supply chain vendor, a password spray, or some other vector – as well as determine all the data and information the Russians were able to access.

Dozens of the 60 victims we notified, as well as other customers, asked us for additional support in investigating and remediating the attack. In many of those cases, our Detection and Response Team (DART) was engaged and helped customers assess their networks in search of the Russian actor and its activity. In many other cases we provided consulting and indirect incident response support to customers' own security teams.

We also continued investigating our own network to see if Microsoft was a target, and we confirmed that as a SolarWinds customer we had also been attacked. We began an intensive operation to find, isolate, contain, and expel the attacker, and to understand what the Russian actor was able to do while in our network.

---

[8] Ensuring customers are protected from Solorigate - Microsoft Security
[9] Microsoft Digital Defense Report 2020: Cyber Threat Sophistication on the Rise - Microsoft Security

Our investigation of the impact of this attack on our internal systems, which has just recently been completed,[10] confirms that the Russians were not able to access or use any of our services or systems to attack others. As we reported when the break was discovered,[11] we also have found no evidence that they accessed our production services or customer data or compromised our own O365 accounts.

We did detect unusual activity with a small number of internal accounts and discovered that the Russian attackers had viewed and, in a few cases, copied some subsets of source code from several source code repositories. Due to restrictions in our network, however, the Russian attackers were not able to modify any code or engineering systems, and our investigation further confirmed no changes were made. We have stopped this activity.[12]

While we of course were unhappy to learn of any network intrusion, we have concluded that the viewing and limited copying of some subsets of source code do not raise a significant security concern. This is because Microsoft manages source code through an inner source[13] approach, meaning we embrace open-source software development best practices and foster an open source-like culture by making our source code viewable by all Microsoft employees. This means we do not rely on the secrecy of source code for the security of our products, and our threat models assume that attackers have knowledge of our source code. In other words, the adversaries snuck into an additional room in our house, but it wasn't one that was guarded in a way that required especially elevated privileges or any special key to access. While the Russian actor saw and, in a few cases, copied some source code, in all cases it was just a small subset of the code for any particular product or service.

Inform

We are continuing to identify the risks and address the damage of this attack to ourselves and our customers. We have also publicly documented our efforts throughout the process,[14] publishing 31 blog posts and collecting them and other information in a centralized Resource Center open to the public. This details our findings and providing guidance for customers, hunters, and security teams that are doing their own investigations.

We applaud FireEye, SolarWinds and the handful of other companies that have been willing to speak publicly about this attack and raise awareness for hundreds more who were affected. But only a select few of the companies, organizations, or government agencies that were attacked, whose technologies or services were implicated in the attack, or that have information about this attack have been willing to come forward or to share information publicly. It is important that the private sector speak out and share relevant information so that we can all respond to an incident rapidly and efficiently and learn from each incident how to be more resilient in the future. If the industry continues to hide what we know, we cannot effectively defend ourselves.

As we testify today, industry does not know the total number of confirmed victims beyond what Microsoft and a few others have shared publicly and the recent disclosure of over 100 total American victims. Unfortunately, not all who are in a position to do so are searching hard enough to find those victims that may be still lost in the rubble. Government inquiry needs to learn what it can from those who have stepped forward but must also seek truth from those who have not. There are still too many missing pieces of the puzzle.

We need a full examination of what other cloud services and networks the Russians have accessed. Before we as a nation can secure our digital ecosystem, we need to know that the Russian attackers are no

[10] Turning the page on Solorigate and opening the next chapter for the security community - Microsoft Security
[11] Microsoft Internal Solorigate Investigation Update – Microsoft Security Response Center
[12] https://msrc-blog.microsoft.com/2021/02/18/microsoft-internal-solorigate-investigation-final-update/
[13] Inner source - Wikipedia
[14] Solorigate Resource Center – updated February 5, 2021 – Microsoft Security Response Center

longer present in the dozens or hundreds of networks in which they have accessed data or information through this attack.

In addition, it is of critical importance that all organizations scan their networks with one of the leading antivirus services, like Microsoft 365 Defender. Anyone who has – or ever had – the malware on their system is at risk of this Russian actor looking at or stealing information from their network or cloud services. It's important for all of us to recognize that this Russian actor is extremely skilled at hiding and covering their tracks and we know for certain they are interested in information beyond Office 365 email.

It is also important that governments and the security community have the ability to focus on victims beyond those that Microsoft has identified. Focusing primarily on the victims that have been identified would present a selection bias that is likely to distort any analysis of the attack. It's a virtual certainty that there are victims in which the attacker has remained entirely on premises or accessed other company's cloud services.

The security community collectively also needs to take steps to defend against future such attacks. To do that, the first and most important step is for every company, organization, or agency to take even more seriously the security of identity in their networks. This can best be done by applying "zero trust"[15] principles to ensure that attackers cannot gain access to information or resources meant only for authorized users. Microsoft has published extensive guidance on how to look for this type of attack, remediate identity risks, and adopt zero trust and we recommend you review it closely.[16]

5. Government and Private Sector Collaboration

As Ms. Neuberger reported, a number of victims were U.S. government agencies. As with all our identified customers, Microsoft reached out to notify impacted government agencies, share relevant information on how to initiate a response, and identify the IOCs they could use to hunt for the Russian actor in their networks. In every case where we notified a victim, we were the first to recognize that they had been compromised. In the process of notification and subsequent communication, we observed two important opportunities for improvement.

Baseline cyber hygiene

What we found in several cases was troubling. Basic cyber hygiene and security best practices were not in place with the regularity and discipline we would expect of federal customers with the agencies' security profiles. In most cases, multi-factor authentication, least privileged access, and the other requirements to establish a "zero trust" environment were not in place. Our experience and data strongly suggest that had these steps been in place, the attacker would have had only limited success in compromising valuable data even after gaining access to agency environments.

This incident serves as a reminder that we must all remain vigilant in driving implementation of basic cyber security practices – multi-factor authentication, patching and updating, deployment of strong detection tools and logging, use of least privileged access, creation of an incident response playbook that is up to date and routinely exercised for readiness, and other vigilant work to improve our defense and resilience to attacks.

The role of the cloud in mitigating these types of attacks also cannot be understated. The success of this attack depended primarily on the Russian actor's ability to compromise on-premises identity systems. We

[15] Zero Trust Deployment Center | Microsoft Docs
[16] Solorigate AzureAd IOCs (microsoft.com); Azure AD workbook to help you assess Solorigate risk - Microsoft Tech Community; Using Zero Trust principles to protect against sophisticated attacks like Solorigate - Microsoft Security

continue to strongly recommend that identity should be moved to the cloud, where it can be defended with the latest technologies.

Despite this observation, we have been heartened by our many conversations since this attack with leaders in the relevant agencies. The Administration has quickly put skilled and knowledgeable leaders in place and has committed to improving the security of government agencies and the ecosystem generally. We are confident that Anne Neuberger, in her new role as Deputy National Security Advisor for Cyber and Emerging Technology, and other leaders in critical cybersecurity roles will apply the lessons learned and take the necessary steps to improve the government's defensive readiness.

Improved information sharing

As the SolarWinds hack unfolded, government agencies were also key stakeholders in investigating and responding to the attack. We applaud the speed with which the Cyber Unified Coordination Group put out a joint statement attributing the attack to a likely Russian actor.[17] This was one of the fastest public attributions of a nation-state attack by the United States. It takes time to get attribution right, and while we strongly support public attribution of nation state attacks, we also support taking the steps required to ensure that those statements of attribution are well-founded.

Avenues of communication between the private and public sectors, however, continue to offer room for improvement. As we look to the future, especially given our understanding of this sophisticated attack, crucial incident response details can be shared more quickly, information sharing can become more specific and detailed, and action can be taken in ways that are clearer and better coordinated.

Nonetheless, it's important to recognize the recent rapid, transparent, and effective public information sharing, especially by the NSA. In addition, CISA used the playbook it developed in successfully defending the integrity of the 2020 U.S. elections to reduce the burden of communication during a time of intense incident response effort.

There nonetheless remain important opportunities to apply recent lessons learned and strengthen the nation's cybersecurity protection. One such area would involve better implementation of the foundational principles and plans the government has crafted in collaboration with private sector partners. For example, the 2016 Presidential Policy Directive 41 (PPD 41)[18] and National Cyber Incident Response Plan (NCIRP)[19] highlight the importance of "unity of governmental effort" – and states explicitly that "the first federal agency to become aware of a cyber incident will rapidly notify other relevant federal agencies to facilitate a unified federal response and ensure that the right combination of agencies responds to a particular incident." This was not our experience in observing the immediate aftermath of the SolarWinds attack. We recommend that the government reconsider the multiple leadership roles required in a cyber incident and work to establish a more unified incident response approach, with clear goals to assess, respond, and recover from large incidents going forward.

If there is a declaration of a "significant cyber incident" as contemplated in the NCIRP and PPD 41, the expectations and needs from the U.S. government to the private sector should be communicated clearly and response should be run collaboratively. A lead agency should be identified to consolidate information useful to the private sector and to ensure rapid and thorough disclosure. In our view, this is best done by a part of the government outside of law enforcement, given the latter's critical but different obligation to investigate crimes and often to keep information secret to help advance an investigation.

---

[17] Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) | CISA

[18] Presidential Policy Directive -- United States Cyber Incident Coordination | whitehouse.gov (archives.gov)

[19] National Cyber Incident Response Plan - December 2016 (cisa.gov)

The SolarWinds attack also saw imperfect incident response information sharing across the private sector and with government. There are valid limitations to what the private sector will share in order to protect business models that fund security resources and innovation. But the private sector also faces obstructive concerns of legal liability, fears of reputational damage, and outdated silos that prevent the communication and transparency that are necessary to best protect our digital ecosystem collaboratively. In this instance, while some private sector participants have been transparent, others have chosen to be less forthcoming, a failure that needs to be addressed.

For both governments and the private sector, there may be risks to exposing methods by which information is obtained. Governments rightly want to protect sources and methods of acquiring information, much of which is justifiably classified. Private sector organizations likewise do not want to reveal to adversaries how they track and discover malicious activities, because this would enable attackers to better disguise their activities in ongoing and future campaigns. In some cases, sharing is also justifiably limited due to customer privacy concerns, given that entities affected by or investigating an attack (both government and private sector) are appropriately responsible for protecting the privacy of individuals and sensitive information they control or manage on behalf of customers. As technology use continues to become even more ubiquitous throughout society , it will become even more critical to have an incident response plan that enables the public and private sectors to partner more fully, thereby ensuring the continuity of essential services and restoration of impacted functions.

6. Next Steps and Policy Recommendations

Given this recent experience and lessons learned, we believe there are several key steps the federal government and private sector can take to improve our readiness to protect against future attacks.

First, we need to strengthen supply chain security for the private sector and the U.S. Government for both software and hardware.

Across federal agencies and the broader ecosystem, organizations currently struggle to manage supplier inventories, understand dependencies, and set cybersecurity requirements for critical suppliers. Just three months ago, the Government Accountability Office highlighted that no civilian agencies manage agency-wide supply chain risk assessments or fully implement requirements for suppliers.[20] There clearly is both a need and opportunity for improvement.

There are existing best practices to draw upon, especially for software supply chain security. Any software developed or procured by federal agencies, including software that powers cloud services to which agencies subscribe, should reflect secure development practices[21] and clear commitments to maintain software, including through vulnerability management,[22] during the defined life of a product.[23] Federal agencies should also require use of integrity controls throughout the software development, testing, and delivery processes, mitigating the risk of an attacker inserting malicious code before a new software product or update is delivered to users.[24]

There are also gaps to address with urgency – and the recognition that widely deploying high-quality approaches takes time. One such gap is related to software itself. Today, most software projects are built

[20] https://www.gao.gov/assets/720/711266.pdf
[21] Microsoft Security Development Lifecycle; Resource: Secure Development Practices Archives - SAFECode; ISO - ISO/IEC 27034-1:2011 - Information technology — Security techniques — Application security — Part 1: Overview and concepts
[22] https://www microsoft.com/en-us/msrc/cvd; ISO - ISO/IEC 29147:2018 - Information technology — Security techniques — Vulnerability disclosure; ISO - ISO/IEC 30111:2019 - Information technology — Security techniques — Vulnerability handling processes
[23] Microsoft Lifecycle Policy | Microsoft Docs
[24] http://safecode.org/wp-content/uploads/2018/01/SAFECode_Software_Integrity_Controls0610.pdf

by leveraging third-party components – both commercial and open source. When selecting third-party components to use, it's important to consider the impact that a vulnerability could have on the security of the larger system into which the components are integrated. Microsoft's Security Development Lifecycle requires our software engineers to maintain an accurate inventory of third-party components, a plan to respond when new vulnerabilities are discovered, and additional validations as determined by context. We're also working alongside partners to develop industry standards for enhancing transparency and improving integrity checks for third-party components, providing a consistent way for software buyers to pursue greater visibility.[25]

Another gap is related to software developers. We need to drive implementation of best practices across the vast and diverse community of developers, whether they're working at major technology companies or chasing the next big idea in someone's garage – including through better automation and security tools. At Microsoft we are working continuously to improve access to and simplify use of security tools and automation on our developer platforms, and we've extended recent security enhancements we've made to internal tools to the broader developer community through GitHub.[26] In August, Microsoft also announced that we joined industry partners in creating the Open Source Security Foundation (OpenSSF),[27] which is focused on providing the best security tools for open source developers and securing critical open source projects.[28]

As these efforts continue to mature, standards and learnings should be integrated into requirements for federal software providers. Implementation of this year's National Defense Authorization Act provides an opportunity to develop new software acquisition[29] security requirements that may be appropriate for re-use across federal agencies.

We also need to address hardware supply chain security with requirements for critical hardware components, and we need to enhance resiliency by ensuring access to trusted suppliers of critical ICT products and services. The U.S. needs a whole-of-government approach, closely coordinated with industry partners and global allies that share our commitments to responsible use of technology, human rights, and other fundamental values.

Second, we need to broaden use of cybersecurity best practices, including through improved cyber hygiene and a commitment to IT modernization.

When Microsoft's cloud services are attacked, we can detect anomalies and indicators of compromise in ways that are not possible in an on-premises environment.[30] This capability is critical to discovering, remediating, and recovering from an attack – but doesn't prevent the risk of on-premises security lapses that result in escalations of privilege that ultimately enable attackers to access cloud services.

Cloud migration is critical to improving security maturity across many organizations. At the same time, it's not a panacea; even as technology users modernize legacy systems, they need to have strong basic security practices in place. This includes fundamentals for establishing a Zero Trust environment, assessing the security of cloud providers, and re-orienting risk management activities to complement third party services and security automation.

---

[25] Software Bill of Materials | CISQ - Consortium for Information & Software Quality (it-cisq.org); in-toto | A framework to secure the integrity of software supply chains (in-toto.io)
[26] GitHub Security · GitHub; Features · Security · GitHub; DevSecOps with Azure | Microsoft Azure
[27] Home - Open Source Security Foundation (openssf.org)
[28] Microsoft Joins Open Source Security Foundation - Microsoft Security
[29] CRPT-116hrpt617.pdf (congress.gov)
[30] We've also issued guidance to support customers detecting Solarigate attack activity in on-premises networks, Using Microsoft 365 Defender to protect against Solorigate - Microsoft Security

At a national level, Microsoft recommends that the U.S. government, and particularly CISA, drive a national effort to improve cyber hygiene, with a particular focus on identity and access management. The SolarWinds incident makes plain why all organizations, including governments, must heighten their focus on implementing basic security best practices, even as we harden technology development processes and explore other steps. It bears repeating that this attack was simultaneously sophisticated and ordinary; a sophisticated Russian adversary created and quickly shut backdoors, quietly cracked open windows, and hid its tracks as it sought ways to gain elevated privileges; but it also used known techniques like password spray and identity compromise that could have been prevented or better resisted with basic cybersecurity hygiene.

IT modernization can also help with the implementation of cyber hygiene best practices, including supply chain risk management.[31] There is no question that using cloud services for identity management can also be safer and more secure than on-premises identity systems. Cloud-based identity can be easier to maintain – with fewer moving parts for attackers to exploit and organizations to defend. It can also benefit from the use of global telemetry, rich analytics, and automation to signal when something is amiss.[32] Our ability to guard against password spray attacks, which account for more than one third of account compromises, is a good example. This tactic attacks many users with a small number of common passwords, rather than many common passwords against one user, which triggers password lockout. When a customer moves to the cloud, we can detect password spray patterns by looking at failed login attempts as "password hashes" (i.e., passwords scrambled by encryption) across millions of tenants around the world.[33] Recent Government Accountability Office reports[34] clearly demonstrate that, more broadly than supply chain or identity management, the use of cloud services can result in better security, more productivity, and lower costs. But cloud users can only fully capture these benefits if they also effectively manage their ongoing security responsibilities,[35] including by managing visibility across cloud platforms and assessing whether cloud services fit their security needs.[36] Federal agencies have not yet consistently used cloud services that have demonstrably met federal security requirements, citing resource constraints and other challenges.[37] Clear, consistent requirements and streamlined compliance programs can help agencies choose cloud services that help them prevent and respond to attacks and ultimately empower human resources to focus on complementary security operations and tasks.

Third, we need a national strategy to strengthen how we share threat intelligence across the entire security community.

While we believe that migrating to cloud services and focusing on cyber hygiene will help to prevent and limit the impact of future attacks, we also must recognize that some of the nation's adversaries are sophisticated, well-resourced, and persistent. We need to ensure that we identify and remediate the next sophisticated attack swiftly, limiting the time during which intruders can lurk in networks and quietly steal data and information.

One of the ways we can accelerate our detection of intrusions and strengthen remediation efforts is to improve threat intelligence sharing. In response to this attack, our ability to develop indicators of

---

[31] While supply chain risk management programs require alignment of people, processes, and policies as well as technology, cloud services can also help monitor remote access, protect data exchanged between suppliers and customers, and detect and diagnose issues across applications and dependencies. Supply Chain Risk Management for Zero Trust with Microsoft Azure (6 of 6) | Azure Government

[32] Using Zero Trust principles to protect against sophisticated attacks like Solorigate - Microsoft Security

[33] Advancing Password Spray Attack Detection - Microsoft Tech Community

[34] GAO-19-471, INFORMATION TECHNOLOGY: Agencies Need to Develop Modernization Plans for Critical Legacy Systems; https://www.gao.gov/assets/700/698236.pdf

[35] Shared responsibility in the cloud - Microsoft Azure | Microsoft Docs

[36] Modernizing the security operations center to better secure a remote workforce - Microsoft Security

[37] https://www.gao.gov/assets/710/703193.pdf

compromise and detect intrusions was enhanced by our early coordination with FireEye. Greater shared visibility among all responders about anomalies and consistent indicators across environments may have further accelerated or informed our activities – and those of others conducting investigations.

The current state of threat intelligence sharing across both the private and public sectors is far from where it needs to be. Our own internal experience has demonstrated that it is critical for our MSTIC team to rapidly aggregate and analyze data from across all our data centers and services, and the federal government should do the same. In addition, while parts of the federal government have been quick to seek input, information sharing with private sector first responders in a position to act has been more limited than it should be. Rapid declassification of information is essential to successful information exchange.

The time has come for a more formal and cohesive national strategy for the exchange of cybersecurity threat intelligence between the public and private sectors. This strategy should have provisions for threat intelligence sharing during incident response – when collaboration should be at its best and when competitors and others should set aside differences to focus on the security of the nation and the interconnected global technology ecosystem. But to make this strategy work in any context, foundational issues must be addressed, strengthening cross-government visibility, declassification, and trust in private sector actors to not misuse information that can facilitate threat hunting and remediations.

Fourth, we need to impose a clear, consistent disclosure obligation on the private sector.

Transparency in incident response is extremely challenging. In addition to challenges posed by threat intelligence exchange, organizations impacted by an incident fear reputational damage and liability for compromises.

But transparency also enables more effective incident response. FireEye was transparent and collaborative in response to this attack, enabling our two companies to work together more rapidly and effectively to investigate, identify victims, and support remediation. But few other companies have been willing to come forward to acknowledge what they've found and strengthen our collective response. That's not unique to this attack. Few victims are willing to share information about ransomware attacks. State and local governments, hospitals, and countless other entities are constantly under attack – and yet silence reigns. This is a recipe for making a formidable problem even worse, and it requires all of us to change.

We need to replace this silence with a clear, consistent obligation for private sector organizations to disclose when they're impacted by confirmed significant incidents. In the U.S., there is currently a patchwork of obligations in place. This includes state data breach notification requirements, which cover instances in which customer data is accessed, and federal procurement requirements, including a Department of Defense regulation that requires contactors to report cyber incidents and conduct investigations.[38] By comparison, other parts of the world have requirements that are applied more consistently across organizations operating in their jurisdictions. In the European Union, for example, all digital service providers are required to notify their competent authority of any incident having a substantial impact on the provision of a service.[39]

There are difficult tactical and organizational questions that need to be addressed in determining how to structure such an obligation. Should any obligation be balanced with incentives, such as limited liability protections? What should the threshold be for defining when incidents have a significant or substantial impact and thus need to be reported? And by what timeline should private sector actors be required to provide reports? As incident reporting requirements proliferate around the world, we have real concerns about the mismatch in expectations for quick reports with usable data and the time-intensive process of

[38] 252.204-7000 Disclosure of Information. (osd.mil)
[39] EUR-Lex - 32016L1148 - EN - EUR-Lex (europa.eu)

investigating an incident and reaching meaningful conclusions about scope of impact. Also, on the government side, who should receive private sector incident reports? How will disclosed information be protected from adversaries?

Disclosure should not be limited just to the private sector. In exchange for imposing such an obligation, government should also commit to faster and more comprehensive sharing of relevant information with the relevant security community.

These are important questions, but we should not get lost in them before answering an even more fundamental question: how can we use these disclosures to strengthen incident responses and better protect the nation? A private sector disclosure obligation will foster greater visibility, which can in turn strengthen a national coordination strategy with the private sector which can increase responsiveness and agility. The government is in a unique position to facilitate a more comprehensive view and appropriate exchange of indicators of comprise and material facts about an incident.

Finally, we need to strengthen the rules of the road for nation state conduct in cyberspace.

Nation state attacks represent some of the most advanced and persistent threat activity that Microsoft tracks; nation state activity groups are focused, have the means to develop and deploy novel techniques and tactics, and are constantly working to improve their capabilities.[40] These threats impact the global technology ecosystem, which all of us rely on for everyday life and essential services.

Globally, governments and private sector and civil society partners must cooperate to establish and reinforce clear expectations for responsible behavior in cyberspace. In recent years, they've made meaningful progress. The United Nations has endorsed[41] a foundational 2015 report[42] on appropriate government behavior, and more than 1,100 organizations have signed the Paris Call for Trust and Security in Cyberspace,[43] which calls for stronger protection of democratic and electoral processes. As hospitals and COVID-19 vaccine research have been impacted by significant cyberattacks over the last year, a group of more than 100 experts has confirmed that international law prohibits nation state cyber operations that have significant harmful consequences on health care infrastructure.[44]

However, as it stands, existing rules are sometimes considered ill-defined and rarely enforced. Despite recommendations by a global group of experts,[45] the United States and like-minded allies need to speak more boldly to make clear that indiscriminate and disproportionate supply chain attacks that put technology users at risk and undermine trust in the very processes designed to protect them are out of bounds for state actors. As Anne Neuberger acknowledged last week, even if the Russian actor primarily leveraged its extraordinary potential access to exfiltrate data, the scope and scale of the attack on SolarWinds customers denote much more than an isolated case of espionage. Attacks that leverage supply chains and widely disrupt confidence in data, systems, and update processes impact many users beyond those targeted. If enough users doubt the integrity of their systems or data, the stability of cyberspace and our readiness to rely on it could be impaired.

As we strengthen rules, we also need clearer commitments and coordinated public attributions and imposition of consequences to hold nation-states accountable for cyberattacks that run afoul of

---

[40] Download Microsoft Digital Defense Report, September 2020 from Official Microsoft Download Center
[41] https://undocs.org/A/RES/74/28
[42] https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
[43] https://pariscall.international/en/call
[44] The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector | Oxford Institute for Ethics, Law and Armed Conflict; The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research | Oxford Institute for Ethics, Law and Armed Conflict
[45] https://cyberstability.org/norms/#toggle-id-3

international law and norms. Today, the costs of widely disruptive nation-state activity are unclear, leaving citizens and the infrastructure they rely on at risk and undermining confidence in the stability of cyberspace.

The U.S. government has a critical leadership role in advancing international consensus on establishing and enforcing a rules-based order, and we urge policymakers to lead in ongoing international processes such as at the United Nations and to join the Paris Call for Trust and Security in Cyberspace.

We are encouraged by the recent steps taken by Congress and the new Administration, including the strong nominations and appointments and initial policy positions the Administration has taken. There remains a great deal to do, and we and others in the private sector stand ready to partner with you, your colleagues, and U.S. government agencies to improve the nation's digital safety and security.

Vice Chairman RUBIO. Thank you. And finally Mr. Kurtz, I believe, is on virtual?

Mr. KURTZ. Yes.

Vice Chairman RUBIO: All right. Excellent.

STATEMENT OF GEORGE KURTZ, CO-FOUNDER AND CEO, CROWDSTRIKE

Mr. KURTZ. Thank you. Good afternoon, Chairman Warner, Ranking Member Rubio, and Members of the Committee, thank you for the opportunity to testify today.

During my three-decade career in cybersecurity, I have seen first-hand the evolution of adversary techniques and have been at the forefront of developing the solutions to thwart them. By the time I co-authored the original edition of "Hacking Exposed" in 1999, which later became the No. 1 selling book in security, it was clear that organizations consistently failed to adequately defend themselves.

When I co-founded CrowdStrike in 2011, it was based on a conviction that the then-dominant approaches to security were no match for adaptive and well-resourced adversaries. We set out to elevate the industry's focus from stopping malware to preventing breaches regardless of their source.

My testimony today is based on my prior and current experiences protecting thousands of organizations across the globe. I will begin by discussing our high-level findings in the supply chain compromise and what lessons we might take away from it.

In mid-December, SolarWinds engaged our professional services team to perform incident response. Although we had not worked with SolarWinds prior to this engagement, nor had they used our software in the past, our teams collaborated effectively to investigate the breach, enhance their security posture, and share actionable intelligence with the entire security community. With their encouragement, we continue to coordinate and share findings with customers, industry partners, and Federal agencies as appropriate.

Today, I would like to highlight a few significant capabilities this particular threat actor exhibited. Notably, the threat actor took advantage of systemic weaknesses in the Windows authentication architecture, allowing it to move laterally within the network as well as between the network and the Cloud by creating false credentials, impersonating legitimate users, and bypassing multi-factor authentication.

The threat actor modified code within the development pipeline immediately prior to the software build, the final stage before source code becomes software. The threat actor leveraged unique IP addresses for commanding and controlling infrastructure for each of its victims, complicating investigations into the scope of the campaign, but used common encryption methods and scrubbing techniques to avoid leaving behind unique indicators.

The threat actor was selective in activating the backdoors it implanted, purposefully selecting its victims from the wider universe of those who were vulnerable. With respect to attribution, CrowdStrike refers to this activity cluster behind these events using the name "StellarParticle." We are aware that the U.S. Government has stated this threat actor is likely of Russian origin.

While we currently are unable to corroborate that finding, we have no information to suggest it is incorrect.

Regardless of attribution, there are a number of takeaways from these events. This campaign, in particular, emphasized the need to improve two important security disciplines: those involving supply chains and those involving security development.

StellarParticle is just the latest demonstration of supply chain attacks as a threat factor. This follows a number of previous high-impact campaigns where the origins of attack are at the vendor level. With respect to software development, in addition to ensuring secure coding practices and adequate code review, organizations must protect the development platforms and code repositories at least as well as their enterprise environment.

Next, I would like to extend our considerations beyond this particular campaign, and address six essential cybersecurity concepts and emerging technologies.

The first is threat hunting. We know that the adversaries periodically breach even very well-defended enterprises. Properly trained and resourced defenders can find these bad guys and thwart their goals.

The second concept is speed. Every second counts to stop threat actors from achieving their objectives.

Third is the power of machine learning prevention. The core state-of-the-art cybersecurity solution is the ability to defeat novel threats. Machine learning and artificial intelligence are essential.

Fourth is the need to enhance identity protection and authentication. As organizations further embrace Cloud services and work-from-anywhere models, enterprise boundaries have continued to erode. This trend increases the risk of relying upon traditional authentication methods and further weakens legacy security technologies.

One of the most sophisticated aspects of the StellarParticle campaign was how skillful the threat actor took advantage of architectural limitations in Microsoft's Active Directory Federation service. The Golden SAML attack allowed them to jump from customer on-premise environments and into Cloud and cloud applications, effectively bypassing multi-factor authentication. This specific attack factor was documented in 2017 and operates at Cloud-scale version of similar identity-based attacks I originally wrote about in 1999.

Moving to the fifth concept, let's touch upon principles of zero trust. Instead of authenticating to a network or device once and having ready access to everything that's connected, users must re-authenticate or otherwise establish permission for each new device, or resource they wish to access. This reduces or prevents lateral movement and privilege escalation.

Finally, I will touch upon something known as XDR, which stands for "extended detection and response." Security teams demand contextual awareness and visibility from across their entire environments, including within Cloud and ephemeral workloads. As this Committee will appreciate, XDR generates intelligence from what otherwise may be no more than information overload. Each of these concepts applied equally to all organizations and regardless of size is a must.

The last point is critical. Often, adversaries specifically target smaller organizations as a means to a greater end. This is part of the supply chain problem. We are proud that a number of security companies, including CrowdStrike, are committed to offering comprehensive, easy-to-use solutions and managed security services to organizations of all sizes with varied budgets. We also appreciate the need for improvements to government cybersecurity.

Some of the most talented people in the field have worked, or currently work, in government organizations. Unfortunately, in many instances, our government colleagues are hobbled by legacy technologies, programs, complex procurement processes, or compliance obligations that detract from their core security work.

I realized that I've described a set of enormous challenges today. But I would like to close in a positive note. With CrowdStrike's visibility into trillions of security events across thousands of customers globally, I'm encouraged by the silent victories the security community experiences every second of every day. Defenders face an endless, evolving threat. But I remain optimistic that working together, we can prevail.

I hope my testimony today has offered some guidance on how we can accomplish that shared goal. CrowdStrike has its sleeves rolled up and is ready to continue to work with this Committee and the greater security community to achieve success. I would like to thank the Committee for inviting me to testify today and for its leadership. I look forward to answering your questions.

Thank you.

[The prepared statement of Mr. Kurtz follows:]

SENATE SELECT COMMITTEE ON INTELLIGENCE

George Kurtz
Co-Founder and CEO
CrowdStrike

Testimony on Cybersecurity and Supply Chain Threats

February 23, 2021

Chairman Warner, Ranking Member Rubio, and Members of the Committee, thank you for the opportunity to testify on timely cybersecurity events.

The recent campaign targeting critical software supply chains, leading to the breach of numerous organizations across industry and government, is notable due to its scope and sophistication. Nevertheless, the campaign represents an amalgamation of concepts, as well as tactics, techniques, and procedures (TTPs) we've observed adversaries using for years.

During my three decade career in cybersecurity, I have seen firsthand the evolution of adversary techniques and have been at the forefront of developing the solutions to thwart them. By the time I co-authored the original edition of Hacking Exposed in 1999, which later became the number one selling book in security, it had already been clear for some time that organizations were consistently failing to adequately defend themselves. But the problems were systemic and, despite the book's wide adoption in private sector and government security education programs and as a go-to resource in practice, they would not be solved by a book alone. Around that time I founded a cybersecurity company that focused on identification and remediation of vulnerabilities, called Foundstone. That company was later purchased by a large anti-virus vendor, for which I then became the worldwide CTO. I gained a lot of insight into how the traditional cybersecurity market was working, and I determined that, in fact, it was not working. At least, not very well.

When I co-founded CrowdStrike in 2011, it was based on a conviction that the then-dominant approaches to security were no match for adaptive and well-resourced adversaries. We set out to elevate the industry's focus from stopping malware to preventing breaches regardless of their source. To this end, from the very start we focused on unified, scalable, and multifaceted approaches to security that empower defenders against a wide range of breach vectors.

My testimony today is based on my prior and current experiences, protecting thousands of small, medium, and large organizations across the globe. While I cannot disclose certain details about any ongoing investigation, CrowdStrike's experience with sophisticated threat campaigns inform my recommendations for how we — the government and the private sector, working together — are best suited to approach this problem.

Recent Developments

I will begin by discussing our high-level findings in the supply chain compromise and what lessons we might take from it.

In mid-December, following public disclosures by multiple victims, SolarWinds engaged our professional services team to perform incident response. Although we had not worked with SolarWinds prior to this engagement, nor had they used our software in the past, our teams collaborated effectively to investigate the breach; enhance their security posture; and share actionable intelligence with the security community. With their encouragement, we continue to coordinate and share findings with customers, industry partners, and federal agencies, as appropriate.

Today, I would like to highlight a few significant capabilities this particular threat actor exhibited that were quite sophisticated, and later in my testimony I will address ways to combat these threats. Notably:

- The threat actor took advantage of systemic weaknesses in the Windows authentication architecture, allowing it to move laterally within the network, as well as between the network and the cloud, by creating false credentials, impersonating legitimate users, and bypassing multi-factor authentication.
- The threat actor modified code within the development pipeline immediately prior to the software build, the final stage before source code becomes software.
- The threat actor leveraged unique Internet Protocol (IP) addresses for command and control infrastructure for each of its victims, complicating investigations into the scope of the campaign.
- The threat actor leveraged a common encryption key to encode its malicious code and, in doing so, left fewer clues for attribution than had it used a unique method.
- The threat actor "scrubbed" the backdoor itself using a process of compiling and then decompiling the malicious code. This step, which we call *code washing*, had the effect of removing "tool marks" (clues) from which investigators could determine attribution.
- The threat actor was selective in activating the backdoors it implanted. This means that the actor actively and purposefully selected its victims from the wider universe of those who were vulnerable.

As far as scope is concerned, on Wednesday of last week, the White House noted that 18,000 organizations downloaded the malicious update, leading to known compromises of 9 federal agencies and about 100 private sector organizations.[1] Although we cannot confirm those

[1] Press Briefing, The White House, Press Secretary Jen Psaki and Deputy Nat'l Security Advisor for Cyber and Emerging Tech. Anne Neuberger (Feb. 17, 2021), https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-[…]er-and-emerging-technology-anne-neuberger-february-17-2021/.

numbers, we have no indication that would contradict this assessment, and it is consistent with what CrowdStrike has observed.

Relatedly, CrowdStrike itself may have been indirectly targeted, albeit without success, in what appears to be the same campaign. We became aware that threat actors directly targeted a third party IT reseller that managed Microsoft licenses for a number of companies, including CrowdStrike. The incident involved abnormal activity in the Microsoft Azure account the reseller uses to validate Microsoft customer licenses via API with Microsoft. However, this activity did not result in any harm to CrowdStrike, its infrastructure, or its data. Nonetheless, it is a healthy reminder that most every company and government agency employs a wide range of third party vendors, resellers, and business partners that make up its individual supply chain.

With respect to attribution, CrowdStrike refers to the *activity cluster* behind these events using the name *StellarParticle*. Members of the Committee are likely aware that we utilize a cryptonym naming convention for threat actors once we achieve a reasonably robust confidence level in our attribution.[2] For example, hacking groups associated with the People's Republic of China government are labeled as PANDAS, those associated with the Russian government as BEARS, and so on. In this case, we have yet to make such a designation based on the information available to us. We note, however, that other organizations, particularly those with access to classified intelligence, have different inputs and vantage points. In that regard, we are aware that the US Government has stated this threat actor is likely of Russian origin. While we currently are unable to corroborate that finding, we have no information to suggest it is incorrect.

Lessons for Industry & Government

Cybersecurity is an iterative process. I'd like to spend the balance of my time sharing my sense of how these events should affect cybersecurity policy and practice. Over the past few years, many within industry have begun to effectively address enterprise security. But performance is uneven, and there is much more work to be done. Areas like product security, operational technology (OT) security, and Internet of Things (IoT) security still lag behind. This campaign in particular emphasizes the need to improve two important security disciplines:

1. **Supply chain security**. An initial intrusion or data breach is not always an adversary's end goal. StellarParticle is just the latest demonstration of supply chain attacks as a threat vector. This follows a number of previous, high-impact campaigns--most notably, NotPetya in 2017 -- where the origins of attack are at the vendor-level. Fundamentally, securing the supply chain is a complex third-party partner and vendor risk management problem that spans across numerous disciplines. It demonstrates that cybersecurity is an ecosystem issue, where organizations impact one another, either for better or worse. In

[2] These names generally take the form of a community- or researcher-derived codeword with some significance, followed by an animal type determined by the actor's geography or motivation. This name scheme is designed to be somewhat more descriptive than others, and can simplify communication and information sharing with government and industry counterparts, as well as assist clients' threat modeling process. For more detail, see: Adam Meyers, "Meet The Threat Actors: List of APTs and Adversary Groups," CrowdStrike Blog (Feb. 24, 2019), https://www.crowdstrike.com/blog/meet-the-adversaries/.

the private sector context, risk decisions should be reviewed and accepted up to the Board-level.

2. **Secure software development**. In addition to ensuring secure coding practices and adequate code review, organizations must protect their development platforms and code repositories at least as well as their enterprise environment. In practice, this means that beyond the other security concepts I am discussing today, organizations must incorporate secure implementation of both hardware and software, conduct architecture reviews, deploy code signing via tamper resistant hardware, engage in ongoing monitoring, and regular testing. Fortunately, the security community has been focusing on these issues, and we commend the National Institute of Standards and Technology (NIST) for their significant and ongoing contributions to this area.

Some essential cybersecurity concepts and emerging technologies differentiate elite defenders from the pack. We encourage our customers to focus on *workload security*. Adversaries do not draw much of a distinction between targeting data on an endpoint versus a cloud environment--and defenders do so at their own peril. Legacy approaches to this problem and legacy technologies have proven ineffective time and again, with increasingly adverse impacts. Concretely, some of the keys to a strong cybersecurity posture today include:

- **Threat hunting**. We know that adversaries periodically breach even very-well defended enterprises. Properly trained and resourced defenders can find them and thwart their goals. In our experience, whether organizations accept this premise -- that cybersecurity involves not just a passive alarm, but a sentry actively looking for trouble -- is the leading indicator of the strength of their cybersecurity program. Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. And the better-instrumented the environment, the more chances defenders give themselves to intervene as a breach attempt progresses through phases, commonly referred to as the kill chain. Multiple opportunities for detection help avert "silent failures" -- where a failure of security technology results in security events going completely unnoticed.

- **Speed**. We advise customers that when responding to a security incident or event, every second counts. The more we can do to detect and stop adversaries at the outset of an attack, the better chance we have to prevent them from achieving their objectives. The reason for this is that adversaries move fast, especially when engaging in lateral movement through an enterprise. This means that measuring response time and severity, essentially a DEFCON for security, is critical to ultimately stopping a malicious chain of events and improving performance.

- **Machine Learning-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats. Machine learning and artificial intelligence are essential to this end. For example, during a retrospective review, a CrowdStrike machine learning model that shipped to customers in September 2019 detected with

high confidence the SUNSPOT malware, which was likely created in February 2020.[3] Leveraging these technologies is the best way to gain the initiative against adversaries.

- **Identity Protection and Authentication:** As organizations embark on a digital transformation to work from anywhere models, Bring-Your-Own-Device policies become commonplace, and cloud services multiply, enterprise boundaries continue to erode. This trend increases the risk of relying upon traditional authentication methods and further weakens obsolescent legacy security technologies. Identity-centric approaches to security use a combination of real-time authentication traffic analysis and machine learning analytics to quickly determine and respond to identity-based attacks.[4]

  Significantly, one of the most sophisticated aspects of the StellarParticle campaign was how skillfully the threat actor took advantage of architectural limitations in Microsoft's Active Directory Federation Service credentialing and authentication process. The *Golden SAML*[5] attack leveraged by StellarParticle actors allowed them to jump from customers' on-premise environments and into their cloud and cloud-applications, effectively bypassing multi-factor authentication. Although this specific *Golden SAML* attack has been documented since 2017, in a sense it operates as a cloud-scale version of the *Golden Ticket* attack and similar identity-based attacks I originally wrote about back in 1999.

  Unfortunately, based on flaws in the authentication architecture itself, this campaign is only the latest and surely not the last of a long string of major breaches in which hackers can impersonate most anybody on a network, gain the permissions needed to perform any actions on the network, bypass multi-factor authentication entirely and, every bit as devastating as it sounds, have the ability to sign in as a compromised user no matter how many times that user resets their password. The only silver lining to the *Golden Ticket/Golden SAML* problem is that, should Microsoft address the authentication architecture limitations around Active Directory and Azure Active Directory, or shift to a different methodology entirely, a considerable threat vector would be completely eliminated from one of the world's most widely used authentication platforms. It is our every hope and, I imagine, the hope of the entire cybersecurity community either that they are able to do so or that we can move to a more community-driven approach to authentication.

---

[3] Sven Krasser, "Stellar Performances: How CrowdStrike Machine Learning Handles the SUNSPOT Malware," CrowdStrike Blog (Jan. 21, 2021) https://www.crowdstrike.com/blog/stellar-performances-how-crowdstrike-machine-learning-handles-the-sunspot-malware/.

[4] For more detail on how this concept relates to recent supply chain attacks, see Michael Sentonas, "The Imperative to Secure Identities: Key Takeaways from Recent High-Profile Breaches," CrowdStrike Blog (Dec. 15, 2020) https://www.crowdstrike.com/blog/identity-security-lesson-from-recent-high-profile-breaches/.

[5] SAML stands for Security Assertion Markup Language. For more information about how the hackers compromised SAML security tokens, see CISA Alert (AA20-352A), "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations" (revised Feb. 8, 2021).

- **Zero Trust**. Due in part to many of the fundamental problems I've described about today's antiquated authentication architecture, organizations must incorporate new security protections focused on authentication. Zero Trust is a design concept that brings a holistic view of authorized identity to the enterprise. Instead of authenticating to a network or device once and having ready access to everything that's connected, users must reauthenticate or otherwise establish permission for each new device or resource they wish to access. This radically reduces or prevents lateral movement and privilege escalation during a compromise.

- **Extended Detection & Response (XDR)**. Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. No box on a network or a single-purpose software agent will address the full scope of the problem. Security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments. The XDR concept seeks to apply order to a sometimes chaotic array of security tools by deriving actionable insights wherever they exist within the enterprise. As this Committee will appreciate, XDR generates intelligence from what otherwise may be no more than an information overload.

Taken together, these concepts apply equally in commercial industry, critical infrastructure, healthcare, and government, as well as within small entities. Much more could be said about each domain, but I'll quickly address two.

First, we think the cybersecurity industry has lagged over the years in making enterprise-grade security solutions accessible to small- and medium-sized businesses. Often, adversaries specifically target smaller organizations as a means to a greater end. We are proud that a number of security companies, including CrowdStrike, are committed to offering comprehensive, easy-to-use solutions for organizations of all sizes and with varied budgets. Increasingly, even the smallest of organizations look to substitute or augment their security programs not only with state-of-the-art technologies, but also with comprehensive managed security services. Mature cybersecurity programs constantly evolve, and operate on the cutting edge of human skill and technical ability. Managed security service providers, including CrowdStrike, bring this level of capability and capacity to organizations that otherwise could not create comparable programs internally.

Second, from our perspective, there is room for improvement in Federal cybersecurity. Some of the most talented people in the field have worked or currently work in government organizations. Like us in industry, they confront adversaries daily. But in some instances, our government colleagues are hobbled by legacy technologies and programs, complex procurement processes, or compliance obligations that detract from core security work. For the Cybersecurity and Infrastructure Security Agency (CISA), new authorities to hunt across the ".gov" domain recommended by the Cyberspace Solarium Commission and granted by the FY21 National Defense Authorization Act (NDAA) could be a game-changer. Programs like the National

Cybersecurity Protection System (NCPS/"EINSTEIN") and Continuing Diagnostics and Mitigation (CDM) should be enhanced to realize this vision. And across the broader Federal government, more progress and investment can be made on IT modernization, with security as a central consideration. Finally, we support ongoing, bipartisan efforts in this Chamber to review and reform the Federal Information Security Modernization Act (FISMA).

Although I've mentioned some important, specific issues and solutions today, I'll close by encouraging the Committee to view cybersecurity holistically. Employing qualified personnel, conducting specialized training, implementing valid methodologies, strategically leveraging third-party capabilities and expertise, and having informed and involved leadership are all critical factors in a successful overarching cybersecurity risk management program. To close on a positive note, with our visibility into more than 5 trillion security events a week across thousands of customers globally, I will say that I am encouraged by the silent victories the security community experiences every second of every day. Defenders face an endless, evolving threat, but I remain optimistic that, working together, we can prevail.

I would like to thank the Committee for inviting me to testify today and for its leadership. I look forward to answering your questions.

###

Vice Chairman RUBIO. Thank you. Let me just begin, Mr. Kurtz, by saying you've shown tremendous operational security behavior there. That backdrop you have in that video, you could be anywhere in the world.

[Laughter]

There's no way we could tell where you are just looking at that. I'm going to get that backdrop. That's awesome.

So let me ask you and Mr. Mandia the same question. So let me just say, you know, everyone is familiar—I think the general public is familiar—with cyber-attacks and hacks. And the general guidance everyone is given is, you know, don't put some simple password like "1234." They're easy to guess. Because we've seen, you know, they can guess it. There's all kinds of things out there that are also to be able to be cracked by them.

Then there's the infamous—or the well-known—phishing email. You get an email, you click on it, and they're in your system. These are all hardware-type, sort of brute-force intrusions.

For folks at home, who may watch this later or trying to understand what the big deal about all this, this involves the other thing we're told that we need to do all the time, which is constantly upgrade your software. Every time you get a software update, put it in because it's got new security features. So these guys get into that software update and you're basically in. It's almost like bringing them into your system under the guise of protecting you.

And that's what we're dealing with here today. And this has been a known vulnerability; something that people knew was a theoretical possibility. My understanding is this is the first time we've ever seen it at this scale or scope. And you'll correct me in your answer if I'm wrong.

The question I would have for all of you, but really for Mr. Mandia and Mr. Kurtz, is this a sophisticated technique? This is not something that someone could do out of the basement of their home. Or is this something that could eventually we could see it become widespread? What level of sophistication do you need to embed yourself in the software upgrade that ultimately winds up in someone's system?

Mr. MANDIA. You know, I'll jump on that first. And this was a planned attack. This is not something done in somebody's basement. There is somebody that thought about this. My gut is this attack started somewhere where somebody said, "If we wanted to compromise these entities, where's the supply chain?" They probably had a list of five to ten companies. SolarWinds was one of them. And they figured out who can we get into? How do we do the implant?

When they got into SolarWinds, they didn't just rush right to the implant. They wanted to make sure they could inject code first in the build process. That was in October '19. Then four to five months later, they have an implant. In that four to five months, they designed an implant that masqueraded to look like SolarWinds traffic. It was hard to pick up on the network. It had things in it in the malware, and you know malware—a lot of times you hear that word, you just shut down. And what's he going to say next?

Well, this is what this malware did. It slept for the first 11 days after it was installed. So that if somebody did detect its beacon going out, they wouldn't be able to associate a beacon from the SolarWinds machine to the update they did randomly 11 days sooner. Another thing it did is it looked for nearly 50 different products and shut them down when it ran.

So people are like, why didn't anybody detect this implant? It's because when it executed, it looked to see if CrowdStrike's agent was on the endpoint, if FireEyes agent was on the endpoint, if Windows Defender was on the endpoint, and it shut it off. You don't make a backdoor as a bad guy as a regular user. You make one as the root user, a system-level backdoor.

Senator Rubio, there's no doubt in my mind this was planned. It was an operation. There was a lot of people involved. And the question really is: where's the next one? And when are we going to find it?

Vice Chairman RUBIO. Mr. Kurtz, I'm guessing you probably agree with that assessment. So this is all without little doubt a nation-state actor. It would take that level of sophistication, is that right? Do both of you agree with that?

Mr. MANDIA. I do.

Mr. KURTZ. Yes.

Vice Chairman RUBIO. Who? Who is that nation-state actor? Have you seen indications in it that tell you this is who we believe it is?

Mr. MANDIA. George, you want to go first on that one?

Mr. KURTZ. Well, when we look at the adversaries across various nation-state actors, obviously, there's a level of sophistication and tradecraft. And as I pointed out in my testimony, the tradecraft and operational security was superb. One of the things that we typically look for are things like markings within tool chains. And what we saw, in particular with the back door and the build process, was something we call "code washing." And that was actually removing these tool chains to these fingerprints that Kevin indicated that our company and his company keep on file, right? So we know who the bad guys are and how they operate.

In this particular case, these tool chains and the infrastructure is very unique. What that means is they took particular care to actually conceal their identity. And at the highest level, we've attributed, as I said in my written and verbal testimony, to a particular a cluster of activity. I know the government has talked about Russia as being one of the threat actors. You know, from our perspective, we have nothing further to add to either confirm or deny that; but what I can tell you, it is absolutely a sophisticated nation-state actor.

And as Kevin said, this took a lot of work. A lot of planning went into this. And we think about how difficult software is to build. Each one of my esteemed panelists are in the software business. We know how hard it is to build software, to get software working. And the idea to actually inject something and have it all work without errors, and without anyone actually seeing it is, again, superb tradecraft and something you have to look at and say it's very novel in its approach.

So I'll turn it back to Kevin and Brad, they probably have some further thoughts on the attribution piece. But as I mentioned, a sophisticated actor that we continue to track.

Mr. MANDIA. And one thing unique to this case is when you do the evidence on 1,000 cases a year and something doesn't fall into a grouping, that's odd. That's peculiar. And then when you go back 17 years of cases and digital fingerprints, and it still doesn't fall into it. You start doing process of elimination. You talk. You know, when we found the IP addresses used to attack FireEye, we did go to partners like Microsoft, we went to the U.S. Government—what I call "ring zero." You go to the intel agencies. Nobody had seen them in use before.

I'll just sum up my comments this way. We went through all the forensics. It is not very consistent with cyber espionage from China, North Korea, or Iran. And it is most consistent with cyber espionage and behaviors we've seen out of Russia.

Chairman WARNER. Appreciate those answers. I do think we've had the previous Administration acknowledge likely Russian. We've had testimony of the people in front of us. We've had the current Administration acknowledge this source as well. I think the sooner we make even more fulsome attribution, the better because we need to call out our adversary—know we know who did it—and plan an appropriate response.

And I agree with Senator Rubio: we don't even have our language down entirely. Sometimes we know we know what espionage is; we know what a denial of service attack would be at the other end of the spectrum. Where this fits is, I think, one ongoing question.

But I think we've oftentimes talked about this as "the SolarWinds hack." But there are other vectors. In my understanding, the Wall Street Journal has reported that as many as 30 percent of the victims were not accessed through SolarWinds but by other means—and maybe this is best for FireEye and CrowdStrike. And obviously, Microsoft would have a view as well.

Why aren't we getting more details about the other vectors that the adversary has entered? The other platforms that may have been utilized? Again, I think this is reflective of the point that since we are totally waiting on willing participants, we could still be uninformed because other major enterprises could be victims as well but had not chosen to come forward. So how can we get a better handle on the non-SolarWinds component of this attack?

Mr. MANDIA. I can tell you this is—we're doing Stage Two investigations right now for our customers. And the number one other way we're seeing these attackers break in is what's called "password spraying." They're just popping passphrases that they got from some breach over here and they're recognized. If you think about it, all of us probably have Amazon accounts; we have Microsoft accounts; we have Google—whatever we're using. We have an email account and a passphrase that we may use to access a whole bunch of applications. Some of those third-party breaches make our user ID and passphrase aware to the threat actor and then they try it on your corporate networks.

So these aren't when I say password spraying, I almost feel like, sir, they know some of these passphrases by the time they show

up and knock on your door. So you know, we have 3,300 employees at FireEye, I have to believe that some of them use their FireEye.com email to access dozens, if not more, of the apps on the internet. If any of those vendors get compromised and their passphrase is compromised and they use the same passphrase for Amazon.com as FireEye.com, we may have a problem. So that's another attack that they use.

And here's the reality: this group has zero-day capability, most likely. They're going to—how they get initial foothold to them network will continue to change. But the way you know it's them is when they come back in, they target the same things, the same people, the same emails, similar documents, like they have collection requirements.

Chairman WARNER. To my question, Brad and George, if you want to add to this. Again, we've talked about this as a SolarWinds hack, but there are other vectors that they entered. And, but for the fact that you came forward, both SolarWinds and Microsoft came forward, there may be other very large enterprises that have not been as forward leaning that may mean this vulnerability still exists.

Mr. SMITH. Yes. I would say, Mr. Chairman, a couple of things. First, absolutely. There are more attack vectors and we may never know exactly what the right number is.

I think the first question you're in effect asking is well, why? And I would analogize to this: you know, this is like finding someone in the building and now you have to figure out how they got in. And you know, in our case at Microsoft, we identified 60 customers where we figured out that they had obtained, once they got in, typically, the password to somebody, an IT administrator who could get them into, say, something like Office 365. But in each instance, they got in on premise, so it wasn't in our server or our service. And so we need to work with somebody else to get to the bottom.

Chairman WARNER. But doesn't that mean, though, that this is not demonstrating a unique vulnerability that's in Microsoft enterprise?

Mr. SMITH. Oh absolutely.

Chairman WARNER.—or Microsoft Cloud? But there may be other brand-name players that may have been penetrated that have not been as forthcoming who are leaving policymakers and potentially customers in the dark. Is that true or not true?

Mr. SMITH. It is absolutely true. I think it means two things. One is yes, there's a variety of services. And there are a lot of ways in. I also would just pick up on one of the things that Kevin said, because he used a phrase that is familiar to all of us in the cybersecurity community but probably not to, say, somebody who is watching this hearing from home—this notion of a "password spray."

Yes, I think in recent years, we've all sort of learned that people may try to figure out our own individual password. A password spray is when you use a single password, and you apply it to a lot of accounts. For example, if I were to go back to where I grew up near Green Bay, Wisconsin and have 1,000 email addresses from people in Green Bay, and I just applied the password "gopackgo," I'll bet dollars to doughnuts, there's a Green Bay Packers fan who's

using that password. In fact, I'll bet there's more than one. And if I find ten of those, 1,000, then I'm in and I can go from there.

So it just points to a variety of tactics. From the most sophisticated really, when you're talking about disrupting a supply chain, to the very broad that point to just a lot of factors. We all need to keep learning about how to secure our own email and other accounts.

Chairman WARNER. Well, I'm going to move to Senator Cornyn. But it does beg the question that Senator Rubio and I both asked about when a large enterprise like Amazon is invited they ought to be participating. There are other brand name known IT and software and cloud services that may have been vulnerable to this kind of incident as well, and their public and active participation, we're going to make sure that takes place.

Senator CORNYN.

Senator CORNYN. Thank you, Mr. Chairman. And thanks to each of you for testifying here today. I share the concern that has been expressed that Amazon Web Services declined to participate. I think that's a big mistake. It denies us a more complete picture that we might otherwise have. And I hope they will reconsider and cooperate with the Committee going forward.

Mr. Ramakrishna, thank you for talking with me yesterday. And since you're headquartered in Austin, Texas, I took particular note of that fact and appreciate that conversation.

I think one of the things we discussed is something that Chairman Warner brought up and that is, even though SolarWinds is the focus of what we're discussing here today, this is not unique to SolarWinds. Correct?

Mr. RAMAKRISHNA. Senator Cornyn, thank you for that question. You're absolutely right. I'll elaborate on the question that Senator Warner asked and tie the two comments together here.

Supply-chain attacks are happening as we speak today, independent of solo events. There was a report just two days ago about a French company being hacked and it was dubbed as a supply-chain attack.

As we discovered what we call Sunspot—the code, the injected tool—and as we evaluated it, it is blindingly obvious that that can be applied to any software development process, which is the reason why we believe that dubbing it simply as a solo-events hack is doing injustice to the broader software community and giving us a false sense of security, possibly, which is the reason why that—even though we are taking corrective steps and learning from this experience—we consider it our obligation to be a very active participant in this endeavor to make us all more safe and secure by promptly outlining our findings and communicating them with both our government authorities as well as the industry.

Senator CORNYN. Our time is limited today and I hope at some point we can talk about the attribution and the putting the Russian intelligence services or whoever is responsible here at risk because right now it seems to me that we are doing a very bad job, generally speaking, of punishing the people who are perpetrating these attacks.

But let me just ask you, at different times, I know there's been legislation offered. Senator Collins and I discussed some that she

had introduced previously with Joe Lieberman, our friend the former senator. It seems to me that there should be an obligation of some sort, on the part of a victim of a cyber-attack like this, to share what they know, what they've learned, with the appropriate authorities. And I can only imagine the chills that run up and down some people's backs when I say that. I think about liability concerns, other reputational risks, and the like.

But if we're going to get our arms around this at all, it seems to me we need to know a lot more than we know under the current practices in terms of the obligation of the victims to step forward. Before I asked you about that and what that would look like with perhaps with some sort of liability protection associated with it. I will tell you that I'm a Member of the Judiciary Committee, as Senator Feinstein is. And we actually have designated seats on the Intelligence Committee from certain authorizing committees like the Judiciary Committee.

And Mr. Smith, from your experience testifying there, usually when we're talking about data breaches, people want to talk about the company that allowed the data breach, how could we sue them? And which is an entirely different perspective than I think we need to have—a more complete approach to this and one that does not treat the victim as the offender, but one that works more cooperatively.

So what about some sort of mandatory disclosure obligation that maybe would be coupled with some sort of liability protection? I know in the intelligence field in the past, phone companies that have cooperated with certain collection have gotten liability protection as part of part of that.

Mr. Smith, do you have a view on that?

Mr. SMITH. Yes, I do. I think the time has come to go in that direction. I think Senator Collins was either ahead of her time or the rest of us were behind our time. But either way, I think we can find a way to move forward this year.

I could perhaps use the word notification rather than disclosure. We should notify someone. We should notify. I think a part of the U.S. Government that would be responsible for aggregating threat intelligence and making sure that it is put to good use to protect the country, and for that matter people outside the country. I think we need to decide upon whom it should be that that duty should fall on. It should certainly fall on those of us in the tech sector who are in the business of providing enterprise and other services.

I think it's not a bad idea to consider some kind of liability protection. It will make people more comfortable with doing this. This is about moving information fast to the right place so it can be put to good use.

Senator CORNYN. Mr. Chairman, can I ask the other witnesses if they have a different view or additional views on that topic?

Mr. MANDIA. No, I agree with it. And coming down to another level of specificity to me, notification needs to be confidential or you don't give organizations the capability to prepare for those liabilities. And so we like the idea of you can notify with threat intelligence that's actionable, you get speed from that if it's confidential because you can have threat data today and your arms around the incident three months from now. And it's just too big of a gap to

have a disclosure law, and we're getting the intel three months to five months too late.

So I like the idea of confidential threat intelligence sharing to whatever agency has the means to push that out to places, then disclosures that were a legal requirement to inform those who are impacted. And you don't know that day one. In FireEye's case, we were sharing intel really fast. And we did not know what we had lost in our breach yet, but we knew there was something different about it. So I just think that's an extra detail. Get the intel out there quickly if it's confidential.

Senator CORNYN. Mr. Chairman, my time is expired so I'll yield back.

Chairman WARNER. I think this is a subject that we're going to come back around to and there are models out there. I don't think our traditional reporting mechanisms necessarily work. So the National Transportation Safety Board or others. Senator Wyden's up next.

Senator WYDEN. Thank you, Mr. Chairman.

The impression that the American people might get from this hearing is that the hackers are such formidable adversaries that there was nothing that the American government or our biggest tech companies could have done to protect themselves. My view is that message leads to privacy-violating laws and billions of more taxpayer funds for cybersecurity.

Now, it might be embarrassing, but the first order of business has to be identifying where well-known cybersecurity measures could have mitigated the damage caused by the breach. For example, there are concrete ways for the government to improve its ability to identify hackers without resorting to warrantless monitoring of the domestic internet.

So my first question is about properly configured firewalls. Now the initial malware in SolarWinds' Orion software was basically harmless. It was only after that malware called home that the hackers took control and this is consistent with what the Internal Revenue Service told me, which is while the IRS installed Orion, their server was not connected to the internet. And so the malware couldn't communicate with the hackers. So this raises the question of why other agencies didn't take steps to stop the malware from calling home.

So my question will be for Mr. Ramakrishna, and I indicated to your folks I was going to ask this. You stated that the backdoor only worked if Orion had access to the Internet, which was not required for Orion to operate. In your view, shouldn't government agencies using Orion have installed it on servers that were either completely disconnected from the internet or were behind firewalls that blocked access to the outside world?

Mr. RAMAKRISHNA. Thanks for the question, Senator Wyden. It is true that the Orion platform software does not need connectivity to the internet for it to perform its regular duties, which could be network monitoring, system monitoring, application monitoring on-premises of our customers.

Senator WYDEN. It just seems to me—what I'm asking about is network security 101 and any responsible organization wouldn't allow software with this level of access to internal systems to con-

nect to the outside world, then you basically said almost the same thing.

My question then, for all of you: is the idea that organizations should use firewalls to control what parts of their networks are connected to the outside world is not exactly brand new. NSA recommends that organizations only allow traffic that is required for operational tasks, all other traffic ought to be denied. And NIST, the standards and technology group, recommends that firewall policy should be based on blocking all inbound and outbound traffic, with exceptions made for desired traffic. So I would like to go down the row and ask each one of you for a yes or no answer. Whether you agree that the firewall advice would really offer a measure of protection, from the NSA and NIST? Just yes or no. And if I don't have my glasses on, maybe I can't see all the name tags, but let's just go down the row.

Mr. MANDIA. And I'm going to give you the "it depends." The bottom line is this. We do over 600 red teams a year; a firewall has never stopped one of them. You know, a firewall is like having a gate guard outside of New York City apartment building and they can recognize if you live there or not and some attackers are perfectly disguised as someone who lives in the building and walks right by the gate guard. In theory, it's a sound thing. But it's academic in practice. It is operationally cumbersome.

Senator WYDEN. I don't want to use up all my time.

Mr. MANDIA. Nope.

Senator WYDEN. We'll say that your response to NSA and the National Institute of Standards, "it depends." Let's just go down the row.

Mr. RAMAKRISHNA. So my answer, Senator, is yes to standards such as NIST 800–53 and others that define specific guidelines and rules.

Senator WYDEN. Very good.

Mr. SMITH. I'm squarely in the "it depends" camp.

Senator WYDEN. Okay.

Mr. SMITH. For the same reasons that Kevin is.

Senator WYDEN. Okay, I think we have one other person, don't we?

Mr. KURTZ. Yes. And I would say firewalls help but are insufficient. And, as Kevin said, and I would agree with him, there isn't a breach that we've investigated that the company didn't have a firewall or even legacy antivirus. So when you look at the capabilities of a firewall, they're needed. But certainly they're not the be-all and end-all. And generally, they're a speed bump on the information superhighway for the bad guys.

Senator WYDEN. I'm going to close and my colleagues are all waiting. The bottom line for me is that multiple agencies were still breached under your watch by hackers exploiting techniques that experts had warned about for years. So in the days ahead, it's going to be critical that you give this Committee assurances that spending billions of dollars more after there weren't steps to prevent a disaster attack, disastrous attacks, that experts had been warning about was a good investment. So that discussion is something we'll have to continue.

Thank you, Mr. Chairman.

Chairman WARNER. Is Senator Cotton on the web?

Senator COTTON. Yes, I am here. So thank you, Mr. Chairman. Gentlemen, thank you for your appearance today.

I want to start, Mr. Smith, with you. Microsoft has said some of its source code was stolen. Does that present future security risks? And if so, what are you doing to mitigate it at Microsoft?

Mr. SMITH. Well, the short story is, our security system does not depend on the secrecy of our source code. I mean, we live in a world where probably there's more source code by tech companies published in open-source form than there is that's not published. And at Microsoft, our source code is accessible to every Microsoft employee. It's not considered to be a particular secret, and our entire threat and security model is based on the premise that there will be times when people will have access to source code.

Do we like the fact that this actor saw it? Absolutely not. But we do not believe that it undermines or threatens our ability to keep our customers or ourselves secure. We will, by the way, as we always do, to answer the rest of your question, Senator, we'll ask ourselves, what do we change? It's not apparent to me that I need to have access to our source code. It's not apparent to me that our Senate lobbyists need to have access to our source code. So we may have fewer people that have access to source code in the future, but it's really not at all the heart or center of what we're focused on here.

Senator COTTON. Okay. Mr. Ramakrishna, approximately 30 percent of the victims of the attack were not using SolarWinds software. What do you think that tells us about the nature of the attack and what victims were targeted and how they were targeted?

Mr. RAMAKRISHNA. Senator Cotton, thanks for the question. This is referring to the Wall Street Journal report, I believe. Thirty percent is an approximation. As best as we know, there are many different types of attacks and different types of threat vectors. We are not a security company per se. So we wouldn't have detailed information about those types of threat vectors. But what I can share is the discoveries that we have made with Sunspot can apply to any supply chain out there, and it's quite possible that there are active supply chain attacks ongoing right now, some of which we may know about, some of which are yet to be discovered.

Senator COTTON. Mr. Mandia or Mr. Kurtz, would you like to respond as well?

Mr. MANDIA. George, go ahead.

Mr. KURTZ. Well you know, again, when you look at the supply chain of attacks here, it is very difficult obviously to identify these things. And when we look at the adversary's capabilities, and we look at what was actually done, as we talked about earlier, it's not an easy problem to solve. And you know, from my perspective, it's one that we have to come together, we have to continue to share intelligence and information. And we have to realize that there are many other techniques and actors that are out there. And when you look at the overall landscape you know, 30 percent weren't from SolarWinds. This isn't a surprise.

Over the last year, we stopped 75,000 breaches that are in process, and probably a quarter of them were nation-states. So this happens every day from every nation-state actor, every e-crime

actor, and their variety of tools and different techniques and tasking orders that are out there. So it's an ongoing effort and I wish there was a silver bullet. There isn't. But I think a big part of this is exposing the techniques and just how prevalent these attacks are to the American people. So that we can do something about it. And we can come together as a group, both in the technology field as well as in government.

Mr. MANDIA. And Senator Cotton, this is Kevin Mandia speaking. To me, the attacker did the SolarWinds implant. They've already moved on to whatever's next. We've got to go find it. This attacker, you know, maybe their pencil's down for a few months. But the reality is, they're going to come back. They're going to be an ever-present offense that we have to play defense against, and how they break in will always evolve. And all we can do is close the window and close the security gap better next time.

Senator COTTON. Okay, then one final question. I think I'll direct this toward Mr. Mandia and Mr. Kurtz again.

To what extent do we think this was designed toward what we might call "collection" in the intelligence world; simply trying to collect information to learn more about America's intentions, plans, capabilities, or what you might call a "covert action" in the intelligence world, say, sabotage of public utilities or military applications or so far, so forth? Or could it be both?

Mr. MANDIA. Yes, George, I'll jump first. Just because we got to see what they did first-hand when they broke in us. The reality is this. They were very focused. They had specific individuals that they targeted, they had keyword searches that they did when they broke in. So this was not a group that operated like a tank through a cornfield. They had a plan, they had collection requirements, and to some extent, I would say they were disciplined and focused on those collection requirements. Not efficient with tradition to just grab whatever they could grab.

Mr. KURTZ. And just to add what Kevin says, I think it's important to realize that as technology companies, we all leverage big data. The adversary does as well. And while they're collecting this information, they're also storing it, they're indexing it, and they have the ability to go back to it. So if a new order comes in—a new, specific order to target a company, target a government organization—they can look for that access, they can look at what's already been collected, they could leverage that.

The second piece of this is in the early days it was network exploration. Then it turned into data exfiltration. And then it turned into data destruction and an impact, right? So certainly, when you have this level of access, you can collect data. If you start impacting systems, it's a pretty good way to get caught.

So could it be turned into that? Absolutely. But in general, what we've seen is collection, and that simply goes into the big machine, the big apparatus to be used again for further missions.

Chairman WARNER. Senator Bennet.

Senator BENNET. Thank you. Thank you all for being here today. Thank you, Mr. Chairman, for holding this hearing.

I wanted to get some clarification along the same lines as Senator Cotton, actually. Mr. Mandia, maybe I'll start with you just for

people at home who don't understand how, you know, what they've read is this is a SolarWinds——

Mr. MANDIA. Right.

Senator BENNET [continuing]. investigation. That's what they imagine what we're dealing with here. That's clearly not the case, based on what we saw in the Wall Street Journal report with only 30 percent of the folks who somehow got pulled into this who had no SolarWinds——

Mr. MANDIA. Right.

Senator BENNET [continuing]. connection. Help us understand what that means in terms of the ongoing nature of this. You know, when you say they put their pencils down, have they really put their pencils down? Or are they out there working their pencils and we just can't see it because we don't know?

You started out at the beginning saying maybe they went through a list of, like, five to ten vendors and said these are the likely ways in and we'll pick this one. But clearly they picked other ways in as well. So I'm just trying to get a sense of the full scope of how.

Mr. MANDIA. Yes. And you know when I said pencils down, I mean they were so successful on this breach they probably got a few days off because they collected so much information.

Senator BENNET. Right. So they're waving the flag.

Mr. MANDIA. Basically, right now, there's such vigilance in the security community they're not going to spoiler their latest technique right now. We're all looking for it. So they're pencils down for the next great implant.

Senator BENNET. Right

Mr. MANDIA. I would be if I were them. Every intrusion starts with initial access. How an attacker gets that varies. When we say the "SolarWinds implant," that was the initial access for a campaign this group did from March of last year until about December of last year when we started detecting it.

But this group's been around for a decade or more. Different people go in and out of that group probably. We're probably responding to the kids of the people I responded to in the 90's when this group was active. So the bottom line, how they gain a foothold in a victim network, SolarWinds was a way. They will always have other ways.

This is a group that hacks for a living. And then when they break in, what they do after they break in really doesn't change that much. They target specific people, primarily folks, at least in our case, that did work with the government. They target government projects. They target things that are responsive to key words. We respond to a lot of threat groups that when they break in, you can tell they broke in to make money or they broke in and there's a manual review where somebody's literally going through every file alphabetically on a desktop.

These folks have economy of movement. If they broke into your machine, Sir, they string search it, they find responsive documents, they get out of Dodge. They have an economy that shows they're professional. And that doesn't change. So if they broke in yesterday via SolarWinds and we patched that and fixed it like we have, tomorrow they're going to have something else. And they're going to try to come back through whatever doorway they can find.

Senator BENNET. And tomorrow they might be looking for something else, too.

Mr. MANDIA. The good news is usually they aren't. But you're exactly right. The collection requirements could change. We've identified this group because they'd break into a company. And then we'd get them out. And if they got back in, they're after the same sort of things and that's one of the indicators; it's still them. So their tools and tactics can change but a lot of what they target does not.

Senator BENNET. And I'm happy for anybody to jump in if you'd like to. But with the rest of my time—there was some discussion earlier—sorry, we were in and out going to votes and things—about reasons they might not want to actually destroy data or destroy systems because they might get detected if they do that. Whereas if they stay in there and they don't mess around with stuff—. But if they wanted to really do mayhem in our systems, what would that look like? What does our worst nightmare look like?

Mr. Smith?

Mr. SMITH. Well I'd offer a few quick thoughts. First building on your answering your prior question and then answering this one. I would just add that in addition to targets in the United States we have identified targets in Mexico, Canada, the U.K., Belgium, Spain, Israel, and the UAE. So it was broader and international in scope.

Second, 82 percent of the 60 target victims that we identified were outside government. So I think there's an aspect to your question well: who else were they targeting and why? And I would say that there are at least two other reasons that we would surmise, two motives if you will. Sometimes if you're going after a government agency that has very good security practices in place, you might look for a third party that might have an individual who was given password and network access to, say, the government's network.

And you might hope that that third party organization—maybe it was a computer service provider, maybe it was an accounting or consulting firm, maybe it was a think tank that was working on a contract—you would hope that maybe they had lesser security in place and that's why you would start there. It's a vehicle to get somewhere else.

And then I do think at times they target tech companies in part to understand how technology works. But frankly it's perhaps in the category of counter-intelligence. Every day we are looking—you heard the reference to threat hunting—we are looking for evidence of this organization engaged in attacks. I think they want to know what we know about them and what their methods are.

But then I do think your other question is so important, because at the end of the day, what do you do once you're inside? Do you just collect information? Or do you wreak havoc? Well, this agency typically collects information. But we know exactly what havoc looks like. All you have to do is look at a day in June in 2017 when another part of the Russian government used exactly the same technique. A supply-chain disruption with a Ukrainian accounting software program. That, too, was an update. It turned off, damaged, 10 percent of that country's computers. ATMs stopped working. Grocery stores stopped the capacity to take credit cards. Tele-

vision news stations went off the air. That is what havoc looks like and that is what we need to be prepared to defend against as well.

Chairman WARNER. We're going to move to Senator Heinrich. What Mr. Smith just referenced was what we refer to as NotPetya——

Mr. SMITH. NotPetya.

Chairman WARNER [continuing]. but was that the potential existed at—even this attack.

Senator Heinrich.

Senator HEINRICH. Thank you, Chairman.

So if I have this right, a nation-state actor that is in all likelihood the Russians, used U.S. software and then command and control servers in U.S. data centers to conduct this attack. And I think the fact that this attack was launched from within the U.S. is potentially a really important part of this story. Advanced persistent threat actors know that the NSA is prohibited from surveilling domestic computer networks. So it makes sense for them to circumvent U.S. surveillance whenever possible.

For any of you: do you believe that the adversary launched the attack from U.S. servers in a deliberate effort to avoid surveillance?

Mr. SMITH. I think it was sort of an I.Q. test. We can't know exactly what they thought but it looks like they passed the I.Q. test. They figured out that it would be more effective and less likely to be detected if it was launched from a U.S. data center.

Senator HEINRICH. Anyone else want to add to that or in agreement?

Mr. RAMAKRISHNA. No, I think I would agree.

Mr. MANDIA. I agree with those statements.

Mr. KURTZ. Yeah.

Senator HEINRICH. For Mr. Smith, while the focus continues to be on how the private sector shares information with the government, we also want to ensure that the government is doing enough to share information with the private sector. Mr. Smith, you expressed concerns in a blog following the SolarWinds attack about the Federal Government's insistence on restricting through its contracts our ability to let even one part of the Federal Government know that the other part has been attacked.

Can you elaborate a little bit about this comment? And in what ways could the Cybersecurity Information Sharing Act of 2015 be improved to ensure that that is possible?

Mr. SMITH. Yeah, it was, I have to admit, one of the things I found surprising and a bit frustrating for us. Because the first thing we do when we identify a customer who's been attacked is we let them know. We notify each and every customer. It was immediately apparent to us that it was important not just to let an individual department or agency of the U.S. Government know but to make sure that there was some central part of the government that would have this information about the government as a whole.

And what we found was that our contracts prohibited us from telling any other part of the U.S. Government. So we would basically go to each agency and say can you please tell so and so in this other place? And the good news is, people did. They acted quickly. But it does not strike me as the type of practice that

makes a lot of sense for the future. So there is an opportunity for reform.

Senator HEINRICH. Probably not the most efficient way to make sure information travels quickly.

Mr. SMITH. It doesn't seem like it's consistent with the year 2021 and technology.

Senator HEINRICH. Mr. Mandia. In your statement for the record you said that victims of crime are the first to know when they've been violated. But in a case like this, only a few government agencies and a handful of security or other private companies are in a position to be the first to know. I agree that doesn't seem right. You suggested that a small group of cyber first responders could prevent or mitigate the impact of cyber incidents through sharing information quickly and confidentially. That's a very intriguing idea.

Can you describe how you think that would work?

Mr. MANDIA. You bet. There's got to be a way for folks who are responding to breaches to share data quickly to protect the Nation, protect industries. And that would require (A) defining what is a first responder. And I think it's pretty simple. If you're trying to figure out what happened to unauthorized or unlawful access to a network, you're a first responder.

And if you do that for other companies beside yourself, you're a first responder. And first responders should have an obligation to share threat intelligence to some government agencies so that, without worrying about liabilities and disclosures, we're getting intel into people's hands to figure out what to do about it. Right now the unfortunate reality is, a lot of times when you share threat intel, it's just a public disclosure.

And it makes people weary to do so and we slow down the process. So that's what I mean by that. I could articulate more. But first responders know who they are. And I think it's easy to define. We have many laws that define certain categories like Internet provider. We need to know. If you're a first responder, you're obligated to get threat intel into the bucket so we can protect the Nation.

Senator HEINRICH. No, I think that's very helpful. When you detected this activity were you obligated to tell the U.S. Government? Why or why not? And was that obligation legal or moral?

Mr. MANDIA. We notified the government customers we had before we went public with the breach. And we found out later based on contractual reviews who we had to notify or not. But the reality is the minute we had a breach, I was talking to what I call ring zero. The intelligence community, law enforcement—you don't want to get email when you don't know if your email's secure. So the reality is, I would say on the record, I think we told every government customer we had that we had a problem, period, before we even went public.

Senator HEINRICH. Thank you.

Chairman WARNER. Senator Heinrich, both the points that this was launched from domestic servers and the lack of information sharing were really important points. And now one of our new Members joining us remotely, Senator Casey. Your first intelligence questions.

Senator CASEY. Mr. Chairman, thanks very much. And thanks for the welcome to the Committee. And I appreciate the testimony of our witnesses.

I wanted to start with the role of the Federal Government here. And maybe we'll just go down the panel starting with Mr. Mandia to give us an assessment of the Federal Government's response to date. And then I'll move to a second question regarding what we do going forward.

So Mr. Mandia, why don't we start with you?

Mr. MANDIA. Without a doubt, the number one thing the Federal Government can do that the private sector cannot do is impose risk and repercussions to the adversaries. Period. So we've got to have some kind of public doctrine to Mr. Smith's idea of rules of the road. We've got to communicate where there's a red line. I know we think it's a tough thing to define, and we admire the problem, but we've got to come up with what's tolerable, not tolerable, communicate it so we don't see a gradual escalation. But to impose risk and repercussions is the purview of the government.

And the second biggest thing is the attribution. The government's in the best place to get attribution the most right. So those two things without—, and by the way, there is no risk of repercussions if you don't know who did it. So those are the two things that I'd firmly place into—the government is best suited to do that. And I'll leave it to some of the other witnesses on the government's role and how to safeguard the private sector and work with the private sector, because I know we have a lot of great ideas.

Mr. RAMAKRISHNA. Senator, I'll keep it quick. And the suggestion I would make is to leverage some of the recommendations in the Solarium Commission report and have a single entity in the government, that public sector entity where all private sector entities can go and communicate with and communicate to and have the responsibility of that agency to then disseminate it to every relevant party.

To date, we feel like we have to communicate with multiple agencies and sometimes that doesn't help us from a speed and agility perspective.

Mr. SMITH. Let me if I could point to two successes that I think are worth building on. First, I think it's really notable that the NSA in December published a circular that described in technical detail the nature of the attack, how people could identify whether they were victimized by it, and how they could protect themselves from it.

And I think that it was extremely well done from a technical and cyber-security perspective and it was published to the world. And I think that the NSA and the U.S. Government did the world a great service. And that's the kind of thing that we should aspire to have our government do in the future.

Second, last week I thought Anne Neuberger at the White House in a press conference took a similarly critical step. She shared to all of us information that frankly none of us had; namely, that the government had identified roughly 100 private companies and nine Federal agencies that had been impacted by this incident. And that tells me that there is now at work real efforts to consolidate this

information across the different parts of the government. So that's encouraging.

She's also indicated that her work is far from done. They're focused on next steps that need to be taken in a variety of ways. But I do think this is a very important moment. The government can speak authoritatively about the nature of attacks and how to protect ourselves, and the government can speak authoritatively about the scope that has happened.

Mr. KURTZ. I would also just like to jump on this. I would also say that CISA's done a lot of work here—a lot of great work. Has put out some, I think, interesting information, indicators, some scripts that helped the public. And while we're talking about the government and we're talking about corporations, there's a whole host of smaller entities that are out there that have no real way to protect themselves. So I think, to Kevin's point, as a first responder—which we are, which he is and others—it's important that we have a single source that we can go to.

We're doing incident response not only for big companies and governments but for many small companies. We need to be able to share this information as quickly as we can without impacting the customer themselves.

Senator CASEY. Mr. Kurtz, I'll end with you, just with one follow-up. When you go through what I think were six proposals or recommendations, what do you think is the most urgent, at least as it relates to the Federal Government?

Mr. KURTZ. Well I think there's probably a couple things. But certainly threat hunting is one of the biggest areas. And as we've talked about before, it's a sophisticated actor. With enough time and effort, they're going to go get into somewhere. And we always make the distinction between an incident and a breach.

There isn't a major company or a government on this planet that hasn't had an incident, and they will continue to have incidents. But you want to be able to identify those very quickly so they don't turn into breaches. And these are like sentries that are looking for the bad guys. They're looking for these indicators, they're looking for these back doors. And it's a tall task. I pointed out things like machine learning and artificial intelligence.

All of my fellow witnesses are working on these sort of techniques as well as us. And that's a big part of a go-forward strategy. Figure out what's there, use the technology to our advantage.

Senator CASEY. Thanks, Mr. Chairman.

Chairman WARNER. Thank you, Bob.

Senator Burr.

Senator BURR. Thanks very much.

Let me thank all of our panelists today for your willingness to be here and, more importantly, for your knowledge in this.

I've got to reflect for just a minute and I'm going to do it even though Senator Wyden left, because I strongly disagree with what he implied. He implied that because NSA and this—said that proper hygiene is a firewall that should be something that should be mandated and everybody should use it and that would solve our problem.

And the three of you that deal specifically in searching out intrusions said no, no, no. No. It's helpful, but it doesn't solve it. And

to suggest that in the day of COVID that you've got a choice between washing your hands, hand sanitizer, and masks, but if you choose just to wash your hand and not do the other two, you're never going to get COVID. It's ludicrous. And I want the record to show that what the response from those who track these was listen, this is sophisticated. They're way past this.

So yeah, that's a good thing for companies to adhere to. But don't think that that's going to solve it with the adversaries we're up against right now. I want to turn to George just real quick, and I want to go on Senator Heinrich's question. In the SolarWinds attack, Amazon Web Services hosted most of the secondary command and control nodes. And all of AWS's infrastructure was inside the United States.

Now I feel like having a cyber-attack deja vu here, whether it's Russian hack of DNC in 2016, the North Korea and Sony hack, or current supply chain hacks, we constantly see foreign actors exploiting domestic infrastructure for the command and control to hide the nefarious traffic in legitimate traffic. Here's the problem. Given the legal restrictions on the intelligence community, we don't have the ability to surveil the domestic infrastructure. So what should the U.S. Government role be in identifying these types of attacks?

Mr. KURTZ. Well I think it's working with providers like AWS, working with folks like Microsoft, working with others, CrowdStrike and FireEye and others. Because when you look at this particular attack, why did they use U.S. infrastructure? Because they just wanted to blend in. Right? And I can tell you there's a ton of attacks that we look at that use foreign infrastructure, that use bulletproof hosting, which is you know the ability to anonymize and pay for hosting and infrastructure. And we know who they are and we tend to look for those bad actors. Right?

So if you can use infrastructure that looks legitimate no matter whose infrastructure it is, you're going to blend in and make it harder. And this particular attack was insidious just the way it communicated and the protocols it used. It looked like legitimate traffic going to infrastructure that you know is normal. But that's why it's important, when you think about these attacks, to have visibility. I talked about threat hunting, to have visibility on the end points, because that's at the tip of the spear.

And these network access devices are just speed bumps, as I talked about earlier. What's actually happening is on the end point. What's actually happening is beaconing out. And you have to have visibility. And you have to collaboratively work with the private sector and the public sector together. And I think that's the only way we're going to solve it.

Senator BURR. Kevin, I want to turn to you and I want to ask for a little more specific statement. You alluded to the fact that this is not going to stop without a government dictate that says: here's what we're going to do. Let me just ask it this way. Will it stop if they pay no price for what they do?

Mr. MANDIA. No. I think if you don't impose risks or repercussions we're all—you know I've used this analogy for so long, you'll get how long I've used it. We're all playing goalie and we're taking slap shots from Wayne Gretzky. I mean, the puck's going to get in

the net sooner or later. And that's what's happening in cyber space right now. Folks are taking slap shots and literally there is no risk or repercussion to the folks doing it.

So we're all fighting a losing battle over time.

Senator BURR. So Sudhakar, as it relates to SolarWinds, can you build software today without the risk of what happened?

Mr. RAMAKRISHNA. Thanks for the question, Senator. We've done extensive analysis with our partners at CrowdStrike and KPMG of our entire build environment and entire infrastructure. And we've seen no evidence of the threat actor in our environment or in our build systems and our products.

We've also learned from this experience and applied them to what I've been describing as "secure by design." One of the key tenants of that is to evolve software development life cycles to secure development life cycles. And related to that, we've come up with a methodology where source code doesn't get built in traditional ways and we use parallel build systems with different people accessing them, with different access types.

And we correlate the output of them across those three to significantly reduce the potential for a threat actor to consistently compromise every one of our build systems at the same time. That is the level of effort our teams are going through to build safe and secure solutions. Which I hope will be a model for others.

Senator BURR. Are these practices that you're sharing with others in the industry?

Mr. RAMAKRISHNA. We are completely committed to doing it, and we are doing it as we do it.

Senator BURR. Thank you, Mr. Chairman.

Chairman WARNER. I would simply want a quick comment that I agree with my friend, Senator Burr's comment that a firewall alone cannot keep out a sophisticated actor. But it doesn't mean the corollary—and I had conversations with the CEO of SolarWinds on this—that just because it's a sophisticated actor then that means that you shouldn't do good cyber hygiene.

Mr. RAMAKRISHNA. Absolutely.

Chairman WARNER. It is not an either/or.

Senator BURR. No, I agree with you totally. I think what we're hearing—and maybe we're just not saying it right—is that even with the best cyber hygiene, even with the best protocols in place because of how good and persistent and how much money a nation-state has like Russia, we're susceptible

Mr. RAMAKRISHNA. Yes.

Senator BURR. You know the puck is going to get in the goal, as Kevin said, and if we've missed anything and you've got something that assures us the puck won't get in the goal, then here or privately share what it is so that we can begin to pursue and flesh out that type of policy.

Chairman WARNER. But the problem is we may not know the puck was even in the goal. But if you've got good cyber-hygiene, chances are you will discover the puck at some point. We'll continue that hockey analogy. Now as we move to our next new Committee Member, Senator Gillibrand. Welcome to the Committee and your first Intelligence Committee questions.

Senator GILLIBRAND. Thank you, Mr. Chairman.

I want to follow-up on knowing whether you've had the puck go into the goal. One of you said that the hack that shut down CrowdStrike and other defense software—and it affected them before they could start working. So why do these programs—why was there no alarm, and how were they shut down?

And related, why were there no alarms in the SolarWinds and anti-virus software logs which should have shown the unusual behavior, access, or other traces of unauthorized access?

Mr. KURTZ. Yeah, so this is George. Maybe I can take that. There were probably multiple, dozen software technologies that were targeted to actually be shut down. In our particular case, you can think about the camera. You know if someone came up to a camera and smashed the camera you'd actually see what they did. And our particular software has a level of monitoring where if someone tries to tamper with it we would actually be able to see that.

And in fact, you'd actually have to reboot the system. As Kevin mentioned, pretty persistent where it waited and kind of did things you know over a number of days.

Senator GILLIBRAND. But there was nothing? There was no alarm? Even the after the 11 days?

Mr. KURTZ. Well once you have admin access on a particular system, if you're shutting it down you know you can pretty much do anything you want on it. And that's just a function of how the operating system works. And what we focus on, and I talked about this in my written testimony, is no silent failure. And we've designed our system that even if there is a failure somewhere along which we call the kill chain, this attack sequence, we're still going to detect something down the road.

And I think this is really important when I talked about threat hunting. You may not catch the initial stage of the attack, but you're looking to catch it along the way, and you're looking to do that with speed. If someone's going to rob a bank there's only so many ways to rob a bank. You've got to get there; you got to get the money; you have to get out. Right? What car they drive, what weapon they use, how they do it doesn't really matter.

So as long as you can identify the chain of activity, which is really important, you can stop these breaches. And that's why we stopped over 75,000 breaches just last year. So it's obviously a challenging problem but that's why when we look at this, it's really about risk mitigation; using multiple technologies and having visibility across your network.

Senator GILLIBRAND. Alright. Mr. Smith, I think you said on "60 Minutes" that there were more than 1,000 developers working on writing this malicious code. Why do you know that or how do you know that? And with a group that big, if it is based in Russia, how come we didn't detect it or see it before?

Mr. SMITH. Well there was a lot more than a single piece of malicious code that was written. And so one of the things we analyze: what was done from an engineering perspective on each of these second stage attacks that Kevin was talking about before. And in essence what we saw was a very elaborate and patient and persistent set of work. They entered. Then, as they were in through that back door, they in effect opened a window. They then swept up behind themselves. They closed the back door. They used that

window. They identified accounts. They were able for the most part to really rely on stealing passwords and accessing credentials, especially where credentials were not well secured, meaning they weren't stored on a hardware dongle or they weren't stored in the cloud. But they were able to get people's passwords. They were then very persistent in using that at what we call elevated network privilege to work across a network.

And we just were able to look at our estimate of how much work went into each of these individual attacks, how many attacks there appear to be in total, and we asked our engineering teams: these threat hunters that you were hearing about before—what do you think is on the other side of this? And that was their estimate. And we have asked around with others: does this estimate seem off base? And no one has suggested it is.

Senator GILLIBRAND. Let me ask Mr. Ramakrishna a final question. So the Wall Street Journal reported that there was as many as a third of the victims were accessed by means other than SolarWinds. However, those access vectors, including TTPs and infrastructure, have not been made public. Why is that and do you expect to release the full details of the other access vectors? And what other ways did the cyber actors use to gain access to victims?

Mr. RAMAKRISHNA. Senator that's a very good question. We, as a manufacturer or producer of IT management tools, do not have the security capabilities to be able to investigate other threat vectors. And that's where the colleagues at this witness table with me will be able to help us and the broader industry identify those threat vectors. On our part, what we have committed to doing and continue to do is sharing everything that we are finding.

And the significant discovery that I mentioned about Sunspot is one key element of eliminating threat vectors. As we learn some new vectors ourselves at SolarWinds, we are committed to sharing those. But I think the broader security industry will take the mantle on that.

Senator GILLIBRAND. Thank you, Mr. Chairman.

Chairman WARNER. Thank you.

Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Chairman, let me echo the concerns that Senator Cornyn and you have raised about Amazon not being present. I think they have an obligation to cooperate with this inquiry and I hope they will voluntarily do so. If they don't, I think we should look at next steps.

I also want to thank both of you for mentioning legislation that Senator Joe Lieberman and I authored and brought to the Senate floor back in 2012, which was defeated largely due to the lobbying efforts of a large business group. And the irony is that this grit business group, at the time that they were lobbying against mandatory reporting, was itself being hacked, which I found out about from the FBI later. I take no pleasure in that. I think that shows how widespread this problem is.

I want to follow-up on two issues. One is the issue of reporting. Mr. Mandia, we know from the White House report and from our own briefings that the hackers did gain access to at least nine Federal agency networks. Yet the U.S. Government learned of this

cyber-attack through FireEye. So, in your judgment is it reasonable for us to assume that our government probably would still be in the dark about the Russians or whoever the hackers were—likely the Russians—being on our systems if it were not for your voluntary disclosure?

Mr. MANDIA. I think over time I believe we would have uncovered this. I think there's a lot of activity that out of context nobody could put their finger on the larger problem. The minute we found the implant and the minute we disclosed what had happened, it connected a lot of dots for a lot of folks. All I can tell you is when I spoke to the government about this basically as it was unfolding for us nobody was surprised as to what I was telling them.

So I think we could sense there was behavior on certain networks that wasn't right. But we couldn't find the cause until we put it all together.

Senator COLLINS. But none of those agencies had taken actions until you contacted them. Is that accurate?

Mr. MANDIA. I don't know what actions they may or may not have taken.

Senator COLLINS. The second issue that I want to talk about is our critical infrastructure: 85 percent of the critical infrastructure in this country is owned by the private sector, and that's one reason that I think mandatory reporting is so critical. We have only to look at what happened in Texas from natural causes to imagine the damage that could be done by a cyberattack.

Now it's my understanding that our government has assessed that this operation was focused on stealing information rather than taking down networks. But how difficult—and I would like to ask the entire panel this—how difficult would it have been for the hackers to disrupt these networks if they wanted to?

Why don't we start with you, Mr. Mandia, and just go down the panel.

Mr. MANDIA. Two comments, Ma'am, very quickly on that. Disruption would have been easier than what they did. They had focused, disciplined data theft. It's easier to just delete everything in a blunt force trauma and see what happens, which other actors have done. But what I've observed this group do—and I think this is an important detail—a lot of times when you break into a network you get what's called the domain admin account. And just use that to grab everything.

It's the keys to everything. It's the master key in the hotel. What this group actually did is they wanted to break into room 404. They got a room key that only worked for room 404. Then they got the room key for 407. They actually did more work than what it would have taken to go destructive. But obviously, they had the access required and the capability required should they have wanted to be destructive to have done so.

Senator COLLINS. Thank you.

Mr. RAMAKRISHNA. Senator Collins, I would agree with that based on my studies and research of other similar breaches in other countries, such as in Ukraine.

Senator COLLINS. Thank you. Mr. Smith.

Mr. SMITH. I would agree as well. And I'd just highlight a couple of aspects that I think are important. First, especially when we're

talking about publicly owned critical infrastructure in this country, a lot of it is too old. It needs to be modernized. And I'll just point to one example was some of our work with a state agency responsible for public health.

When our consultants went in to work with them they found that the manual for the software was more than 20 years old, meaning the software itself was more than 20 years old. So and that's why you see these ransomware attacks which need to connect with this. They so often target municipalities, we've seen Baltimore, we've seen New Orleans. They target hospitals.

So that that is in critical need of improvement. I do think the other thing that is really worth thinking about more broadly for the whole Committee is I don't think we can secure the country without investing in more cybersecurity people for the country. There's really a critical shortage nationwide of cyber security professionals and I think we can put our community and technical colleges to work in part to get more people into public agencies, into small businesses and others.

We are doing a lot to try to publish information. At Microsoft we have published 31 blogs since we learned about SolarWinds you know from FireEye. But there's just not enough people in many places to read them and act on them.

Senator COLLINS. Thank you. I know my time has expired. Maybe Mr. Kurtz could respond for the record.

Chairman WARNER. Okay. And I don't.

Mr. KURTZ. Sure, thank you.

Chairman WARNER. I'd just simply mention as well, Senator Collins, you appropriately pointed out the failure to report on the private sector side. There's no obligation on the public sector side.

Senator COLLINS. Right. Well part of the problem is that there should be this exchange.

Chairman WARNER. Yep.

Senator COLLINS. Of information that's not occurring now on either side.

Chairman WARNER. Absolutely. Senator Blunt.

Senator BLUNT. Thank you, Chairman. Mr. Mandia, did you feel when you found this problem in your system did you think there was a legal obligation to report it to anybody?

Mr. MANDIA. Yeah, we had third party counsel involved. We did not have a legal requirement at least based on the legal advice that I got to disclose at the time that we did. So we did so based on we're a security company, we work to a higher order. Yeah, it's all built on trust. And you got to report.

Senator BLUNT. And Mr. Ramakrishna, what did you think there was a legal obligation to report this when you found out about it to the government or anybody else?

Mr. RAMAKRISHNA. Senator, I was not with the company when this particular incident happened.

Senator BLUNT. Got it.

Mr. RAMAKRISHNA. So I will take it on record and come back to you with exactly what happened at that point in time.

Senator BLUNT. And Mr. Smith, from your testimony I think it was point four in the things we should do though there was some element of it in point three. It's your view that there should be a

requirement now that these kinds of things be reported. Is that right?

Mr. SMITH. Yes. And I think we should build on the conversation we had here. But you know, we too concluded we had no legal obligation to report. But I think we had a duty nonetheless first of all to each customer, second of all to the U.S. Government and third of all to the public which is why we published those 31 blogs.

Senator BLUNT. So do you think we should create a legal obligation for you to report if you're aware of a problem like this?

Mr. SMITH. I do. I think we need to be thoughtful, tailor it, make it confidential. But we will not secure this country without that kind of sharing of information.

Senator BLUNT. So on that topic and we'll just stay with you and then work our way back down. On that topic, you know these companies. All four of the people represented here have great expertise and great resources which I'm sure you've used a lot of to figure out how they got there, if you figured that out, how long they've been there. How would we expect a normal person that does business with your companies to be able to do that on their own? And maybe, Mr. Smith, that goes to your view we need more cyber expertise.

But how would we expect a regular company, unlike these companies at the table today, to have any sense whether anybody was in their system or not?

Mr. SMITH. Well the first thing I would say is I think it's a decision for you to make as to whom you want this obligation to apply. You know certainly it should apply to tech companies. Should it apply to every customer of a tech company? I think that is a separate question. Second, of course people cannot report something they're not aware of. Our customers who use our cloud services know when we are able to detect that they are being breached in the cloud or they're being attacked because we tell them. And so we let them know.

Now ironically one of the episodes we've learned from this time was in some instances we called people on the phone and we said we're from Microsoft and we want you to know you're being attacked and they're like yeah, right and they hung up. They didn't believe that this big company was calling this small business. But that is our job, our responsibility I think—to help our customers. And we can provide information to the government, or in certain instances others could as well.

Are you going to ask every small business to do that? It's probably not necessary for this purpose.

Senator BLUNT. Yeah. I think if we move forward on that discussion some helpful thoughts from all of you about when that obligation to report. If you've called a customer and said you've been hacked, is there an obligation you should have then to report? We could work on that.

Mr. Mandia, how long do you think this had been in your system whenever you found it? And I know it was the two telephone verification seeing that extra verifier in there that was the tip off.

Mr. MANDIA. Right.

Senator BLUNT. How long do you think it had been there?

Mr. MANDIA. Well a couple ways to answer that. Bottom line it was a couple months from initial access but the attacker wasn't alive every single day. I think, in other words, they were on our system for maybe three hours in one day, a week would go by, couple hours on another day. We weren't a full-time job for the intruders that broke into us. Because they had broken into 60 plus other organizations if not 100. So we did get their attention and there's several days of activities before we detected them.

But over time it was several months.

Senator BLUNT. And of course you'd contend that very few companies would be better prepared than yours to find out.

Mr. MANDIA. Right.

Senator BLUNT. If somebody's in your system because that's what you do.

Mr. MANDIA. Right.

Senator BLUNT. Mr. Kurtz, you mentioned on the bank robbery example I think it was something like you get there, you get in, you get the money, you get out. It seems to me that in this intrusion they weren't all that interested in getting out. What do you think that means? That they would get there and just hang around, as Mr. Mandia said, and do something and a week later might look and do something else?

What kind of hacker is that? What are they positioning themselves to do? Clearly not to shut down your system at that moment. But why do you think they were persistent in this, what I think, is a relatively different way than we might have anticipated?

Mr. KURTZ. Well this is indicative of a nation-state actor and it's in their interest to maintain persistence. If they were collecting data, they want to continue to collect information over a period of time. If the campaign as was pointed out this is the way it works, right? You've got different mission objectives and campaigns. If the campaign is over, they certainly would want to remove their tool so they weren't found by companies like CrowdStrike and FireEye and Microsoft and others.

So it's in their best interest to maintain the persistence because you never know what they're going to need. And one of the things that I really want to point out and how this works in practice is that when you get into a system when an adversary gets in they don't necessarily know what they're going to find. And then they find some interesting tools, they find some emails that may lead them to another company they can compromise.

And it's a massive spider web of interrelated entities and information that they have to collect. And when you draw that out, if you can imagine a crime scene where you kind of put everything on the bulletin board and you start connecting the dots between the actors, that's what it's like for the victims. And from one company to the next company to the next company to a government agency, they can all be connected together with some of these campaigns.

And there's no reason for them to get out unless that campaign is over. And certainly unless they want to remove that malware and their tools which typical which we've seen in this particular case cause they didn't want anyone else to find them.

Chairman WARNER. Senator King.

Senator BLUNT. Thank you. Thank you, Mr. Chairman.

Senator KING. Thank you, Mr. Chairman. Excellent, excellent hearing. A lot of important points. A couple just I want to emphasize. Mr. Mandia, I'll give you another analogy to use as well as Wayne Gretzky, and that is if all we ever did was lock our windows and robbers never had to worry about going to jail, there'd be a lot more robbers. I think deterrence is one of the most important parts of a national strategy and frankly it's one that really hasn't been very well developed in this country. And as you pointed out I think it has to be declared.

It has to be public. The adversary has to know what the capabilities are and that costs will be imposed. That leads me to a second point that I think Brad Smith mentioned but we didn't really develop. And that is the importance of internationalizing this problem and that is working with our allies because we're not the only ones. I think you mentioned there was an attack on a French company by this same group.

And to the extent that we have the international community and the establishment of some kind of international norms, red lines, guardrails, whatever you want to call them then things like sanctions are much more effective. I want the hackers to not be able to go to Monte Carlo as well as Miami. So deterrence is key. And the international piece of it is also important.

And then the final thing that I think has come out today very clearly is the importance of some kind of joint collaborative environment where there can be an easy and quick and efficient flow of information. Liability protection may be necessary. Anonymizing the data may be necessary. But some kind of mandatory breach notification is also part of this package.

All of these bills, all of these ideas by the way are part of the work that we're going to be doing on the solarium this year and I look forward to working with the Members of this Committee on things like the collaborative environment, breach notification, the international aspect of it.

Let me ask a specific question. Mr. Mandia, do we need a central Federal attribution office? It strikes me that attribution the FBI has a piece of it, the NSA has a piece of it, maybe the CIA, and whomever somewhere else. Attribution is key. You can't do deterrence, you can't respond unless you have attribution.

Should there be a central attribution department, if you will, that could act quickly and do attribution more efficiently than is the case today?

Mr. MANDIA. Well I can say this, sir. I don't know if it needs to be a single committee or single agency. But attribution is critical and all that you know any time I get to advise a head of state it's very simple. If you don't know who did it, you can't do anything about it. So I would argue it's one of the most critical issues we have to solve as a Nation is we got to know who did every breach.

I think that those data points will automatically come from multiple agencies with multiple missions and areas of responsibility. And then bring it to domestic challenges like the SolarWinds breach and all the liabilities hitting companies. It is helpful and maybe it's CISA, maybe it's the FBI, but it is helpful that most or-

ganizations recognize that we are expected to defend ourselves from the drive by shootings on the information highway.

But we shouldn't have to defend ourselves from the SVR. I mean that doesn't seem like a benchmark that this Nation should set for every small to medium sized company out there that you need to defend yourself from a foreign intelligence service trying to hack you. So I would say this. Categorical attribution for these companies that do disclose is very helpful for those companies. So in other words, if there was public attribution that said SolarWinds was compromised by a nation-state, good enough.

Because it takes the wind out of the sails of all the plaintiff lawsuits that we all get when we get compromised and we tell the world about it. Thank you.

Senator KING. Thank you. And it seems to me that moving on, we clearly ought to do attribution better. The other piece that's come out today is, and Senator Burr mentioned this, is gaps in our authority. The NSA and the CIA cannot spy on Americans. They cannot watch what's going on in American networks. That sort of leaves the FBI which is really a law enforcement agency as the intelligence agency for domestic cyberattacks.

It seems to me that we need to think of how these authorities fit together and what the gaps are to be sure that we have the tools to protect ourselves. Not that we want to spy on Americans, but we also want to be able to protect Americans. Mr. Mandia, your thoughts on that?

Mr. MANDIA. I do believe there's got to be a way for the U.S. Government when we need to mobilize to understand how we can do it domestically. And the example I've always used, sir, is very simple. If the intelligence community recognizes there's going to be an attack on Wilkes Barre hospital this Friday by the best hacking group on the planet, we'd just start moving the patients out of the hospital. And that seems like we can do better than that as a Nation.

We ought to be able to impose the risk profiles that we need to and project our capability domestically when we need to. And right now, I don't see the ability to do that.

Chairman WARNER. Senator Feinstein.

Senator KING. Appreciate it.

Chairman WARNER. Dianne.

Senator FEINSTEIN. Oh, excuse me. Thank you very much, Mr. Chairman. I'm looking at this worldwide threat assessment of the United States intelligence community. It was done by Dan Coates, a former colleague of ours when he was Director of National Intelligence. And it's deeply concerning to me because it points out really the seriousness of this thing and the impact of it, the length of time eight months that it went on.

Nine Federal departments, over 100 companies, and we don't know what, at least I don't, what the Russians took. And it seems to me to have this kind of situation out there and I've been on this Committee for a long time. And just have a hearing and not do anything about it. And know that we know now that there is this kind of vulnerability available.

So let me begin with you, Mr. Mandia. You're a Californian. What do you advise this Senate to do about this?

Mr. MANDIA. Yeah there's several recommendations. I still believe it is critical we find a way to have a centralized agency that we can report threat intelligence to confidentially and that if you're designated as a first responder in cyber space, whether private or public sector, you report to that agency. That means we get the intelligence into the hands of people that can take actionable steps way faster than disclosure of incidents which just takes too long.

To Brad Smith's point and you have those six bullet points. I think it's actually five bullet points. And they're all right. It's what we should do. I'm specifically talking about the threat intelligence sharing. Let's up it a notch. Let's say you have to if you're a first responder.

Senator FEINSTEIN. How would you do that? When you say up it a notch, what specifically would you do?

Mr. MANDIA.—Have legislation that defines who a first responder is. That if you respond to unlawful, unacceptable, or unauthorized access to networks as a business and you see certain things that threat intelligence and we know what it is in the community that needs to be shared with a specific agency. Confidentially shared so that you don't have to know who the victims are because the victims have liabilities that make them delay.

They'll do months of investigation before they would disclose everything. But we want to get the intel faster and into the hands of the right people more quickly. I do believe it needs to be a central agency inside the government. You can't go to three or four, you've got to pick one. And that if we're responding, we got to let you know here's what's going on.

Senator FEINSTEIN. And this would be private sector as well as government sector?

Mr. MANDIA. Yes.

Senator FEINSTEIN. So it would be a comprehensive bill that essentially would set a kind of operational protocol that has to be followed.

Mr. MANDIA. It it's similar to operating agreements for all the folks who accept credit card use. The Visa operating agreements. You literally have 24 hours to start sharing information regardless once you know. And it's not based on all the things that you may have lost. You've got to get the intel into the hands of the folks that can start safeguarding the Nation far faster than what we're doing today.

Senator FEINSTEIN. Could I ask the other two witnesses to reflect on what Mr. Mandia has said?

Mr. RAMAKRISHNA. Senator, I agree with that single agency to report to and the public private partnership. Clearly that is one of our recommendations as well and that will be consistent with the goal of having speed and agility in responding to these types of events.

As you noted, some of these have gone for too long and we've lost time in detecting the perpetrators and taking corrective steps.

Senator FEINSTEIN. Mr.

Mr. RAMAKRISHNA. Additionally, I would recommend in the context of public and private partnerships standards, such as NIST, and procedures, such as CMMC, can be improved with better collaboration, better transparency between private and public to

evolve those from what are today compliance based methodologies to focusing on excellence.

That is where I think Brad's idea of having a larger pool of STEM based focused education as well as specific cyber security education will come in handy.

Senator FEINSTEIN. Thank you.

Mr. RAMAKRISHNA. And then the last thing I would say in the context of coming out and identifying breaches and encouraging people even to come out and identifying the breaches there was a concept of liability protection that was discussed. There is significant brand reputation that people are worried about as well. And in the context of this broader work, I'd recommend that we address those as well which are not strictly liability but broader than that.

Senator FEINSTEIN. Thank you. Mr. Smith.

Mr. SMITH. Yeah, I would endorse everything that you just heard. I would add in the areas of rules of the road I think there are three areas that are just clearly ripe for this Committee and others to say are off limits. The patching and updating of software should be off limits, certainly when an and a this disproportionate.

Senator FEINSTEIN. Well wait, the patching and off date—

Mr. SMITH. And updating.

Senator FEINSTEIN. Updating of software.

Mr. SMITH. Yeah. Yeah that was.

Senator FEINSTEIN. Should be off limits to whom?

Mr. SMITH. For these types of nation-state attacks. That would be the first thing. The second would be cyberattacks on hospitals and healthcare providers. Vaccine distributors. I mean there's been a ground swell of both concern about what we've seen in the last year and attacks on that sector. And the third is attacks on our electoral infrastructure. On voting, on the tabulation of votes, on voter registration rolls.

And I think there's a ready vehicle that's ripe because 75 governments, but not our own, have already signed the Paris Call for Trust and Security in Cyberspace. More than 1,000 private organizations, including my own, has signed that. And I hope this White House and this State Department will act on that. The consensus is there if U.S. leadership can help push it across the finish line.

Senator FEINSTEIN. Mr. Mandia, would you just reflect for a moment?

Chairman WARNER. Can we.

Senator FEINSTEIN. Oh, just one question.

Chairman WARNER. Yeah. We've gone through the five minutes so we're.

Senator FEINSTEIN. Okay. Thank you.

Chairman WARNER. Senator Sasse.

Senator SASSE. Thank you, Chairman. And thank you to all four of you for being here. This has been a very constructive hearing. I would just associate myself with the many comments of folks expressing frustration that Amazon isn't here. I think they should be and I think we should pursue whatever is necessary. Hopefully they'll do that voluntarily.

I'd also like to underscore a few things that were said along the way by Angus King about some of the deterrence objectives of the Cyber Solarium Commission. He and Mike Gallagher, House Mem-

ber from Wisconsin, have invested tons of time. I was a commissioner but those two guys co-chaired it. There's a whole bunch of work to be done about breach notification that they've been thinking on in addition to some of the work that Susan Collins has done.

Mr. Mandia, I know you answered it multiple times through the course of the last three hours but your summary five minutes ago about the need for a central single repository at the Federal Government for these breach notifications I think was very succinct and compelling, so thank you for that.

Mr. Smith, when I came back from voting a little while ago I think I heard you say, I was just walking into the room, that you thought there were a thousand highly trained engineers involved in planning this attack. Did I hear you right?

Mr. SMITH. That that is our best estimate, yes.

Senator SASSE. And could you kind of give us a level set of other attacks or espionage efforts in the past? Like, say the CCP's OPM hack. Do we have any theory of how many people would have been involved in that, trained folks?

Mr. SMITH. Well, I don't. But you certainly didn't need an engineering group of similar magnitude to steal data. You really need to then think about how to use that data which is probably some combination of engineering and artificial intelligence. And you know, I do think as we scan the horizon around the world, we are seeing variation in tactics. You know we are seeing in one part of the world more of this I'll call it engineering intensive effort to you know penetrate individual organizations with great patience and persistence.

And then extract data on an ongoing basis as you would if you are a foreign intelligence agency. You know in another part of the world you're probably seeing you know more collection of very large data sets. And in all probability the way one would make use of those data sets is to aggregate them and use artificial intelligence machine learning you know to start to knit them together and then say use them for disinformation.

And so you know as we look at the world, we have espionage threats. We have disinformation threats. And then ultimately we always have the threat we were talking about before of actually damaging a society or a country as we saw in Ukraine.

Senator SASSE. Right. Very helpful. Is there any equivalent breaches that you can think of that would have had this scale of human capital involved in planning them?

Mr. SMITH. I can't think of a similar operation that we have seen that would have similar human scale, no.

Senator SASSE. So this is arguably the largest planned cyberattack ever?

Mr. SMITH. I haven't seen anything larger. I think we were having a good conversation before about what label precisely to attach to this. But it was a very it's the largest and most sophisticated operation of this sort of that we've seen.

Senator SASSE. So going back to some of Martin Heinrich's questioning and then Chairman Senator Burr's follow-up on the same thought. It'd be useful for those of us who are not technologists to hear the three of you kind of talk about the difference between the design flaws, not that anybody is particularly responsible inside

the U.S. Government for having failed to detect this, because it's a new kind of attack. But design versus execution flaws given Martin's points about the NSA being prohibited from surveilling domestic systems.

Who should in our current structure have found this earlier? Again I'm not looking for you to blame cast, I'm looking at us as the Congress to recognize that we have an IC that is not structurally prepared to respond to something like this. When your greatest capabilities are at the NSA and they're prohibited from surveilling the systems where they would detect it, the FBI is chiefly responsible for law enforcement investigations after the fact. Structurally, we're not prepared to defend against this, are we?

Mr. MANDIA. I guess I'll jump in on that one. There's no question you have to have private and public partnership in it. Period. When you look at critical infrastructure and who's running it. I want to be clear though, why people didn't detect this, the Achilles heel, is because the front door was locked. So the attackers had to break in to SolarWinds, implant something, we still don't know how they broke in to SolarWinds that I'm aware of. And this is probably the last avenue in cyber security.

Now we know you've got to worry about supply chain risk and you're going to see the elevation in security there. So the reason everybody didn't detect this right away is over the last 30 years in cyber security you used to be able to drive through the front door. And we kind of closed that and then it became spear fishing and tailored attacks against individuals. And we got really good at that. And now they went to the supply chain.

And it was inevitable. We knew they'd get there. Apparently it takes something like this for us to really decide to up the game.

Senator SASSE. But if we think about how many questions you've had to answer today about reporting requirements, you also had a sense, Mr. Smith, you said something about the reporting prohibition on you going from one government agency to the next. How long was that delay in our structure? If you had been able to notify everybody once you knew once your four companies knew what you knew how much faster would it have been than it was in the situation where you actually had prohibitions on information sharing intra-USG?

Mr. SMITH. Well I think in this instance when we spoke to officials in one agency typically within a day I think they spoke to officials in another. So they understood and they were fast moving. I do think that one of the challenges in this space is the nature of all threat intelligence, whether it's cyber-based or physically based, is that it's always about connecting dots. So the more dots you have, the more likely you are to see a pattern and reach a conclusion.

And so I think one of the challenges here is that the dots are so spread out, they're in a variety of different private companies and they always will be. And then they're spread out across different parts of the public sector as well. So this notion of aggregating them is key. The one thing that we haven't talked about though that I would add to this is there should be some level of information sharing in an appropriate way back to those of us in the private sector that really are first responders.

You know I look at the Microsoft threat intelligence center and we are able to aggregate all of this data across our services. And you heard from CrowdStrike or FireEye and they do similar things. But we too are operating with imperfect information when we don't have access to this knowledge. So that's another key question I think that really merits consideration.

Senator SASSE. I'm over time but thank you to all four of you and I'll follow-up with some of you for more as well. Thanks Chairman.

Chairman WARNER. Well I'm I want to thank all the witnesses but I also want to make sure people have hung in if Senator Blunt, Senator Burr, Senator Rubio I've got one more question but I want to see if Senator Blunt do you have anything else?

Senator BLUNT. No, sir.

Chairman WARNER. And do you have Richard? Marco?

Vice Chairman RUBIO. I mean I think one of the things about this is you know corporations and government we do we trust a number of software vendors now to run programs remotely in the cloud. They even allow them access to our networks to provide updates to help perform better, for safety and so forth. So this is really is not just a national security thing, it really goes at the heart of how we conduct business across multiple sectors.

By the way, I would venture to guess that most companies, midsized companies and above, have no idea how many different pieces of software they don't know what their own inventory is of what they're running. And so it would be now's probably a good time to have someone in charge of knowing that in case something like this comes up.

I have three quick questions. On SolarWinds, I'm not sure I've heard yet, do we do we know what the initial entry point into the network was?

Mr. RAMAKRISHNA. Senator, our investigation on how which is initial entry point is still active at this point. We have had a number of hypotheses over the last couple of months working with our investigation partners. We've been able to narrow them down now to about three, which I hope will help us conclude to one. But just the nature of the investigation is we are still sifting through terabytes of data to figure out if we can pinpoint that particular one.

Vice Chairman RUBIO. So is TeamCity produced by JetBrains any indication they could be one potentially?

Mr. RAMAKRISHNA. Senator, TeamCity is a tool used in the build processes by us and many other companies out there. We, to date, have no evidence that it was the backdoor used to get into SolarWinds. Although we haven't eliminated that possibility, we haven't proven it.

Vice Chairman RUBIO. And for on Microsoft, as far back as 2017 that the forged identity credentialing you were aware of that vulnerability as far back as when were you aware of that and what was done from the point you knew moving forward on the to address that?

Mr. SMITH. Well the forged identity refers to an industry standard, SAML, a markup language. It's an industry standard that is supported by a wide variety of products including our own. Actually as we investigated this incident, we found that it was relevant in

only 15 percent of the cases and in those 15 percent, in every instance you know this tool was used to in effect add access capability only after the actor was in the network, had obtained access with what we call elevated privileges, and was able to move around and then use this.

But to answer your question this particular standard, the SAML standard, was created in 2007. So long before 2017 we and many other companies in the industry have been working to move people towards a more modern authentication standard. And there has been one that has been around since 2012. More broadly, independent of what security standard you use for this kind of authentication the thing that we have been advising our customers and the practice that we have been following ourselves is really to do the following.

One, move your authentication service into the cloud. Number two, secure all of your devices. We have a service called Intune that does that. Number three, you know, make sure you're using multi-factor authentication. Number four, have what's called least privileged access meaning don't give individuals access to the entire network or to be able to do things that they don't need to do. And number five, use a contemporary or a modern anti-virus or anti-malware service like Windows Defender.

And the reality is any organization that did all five of those things, if it was breached it in all likelihood suffered almost no damage.

Vice Chairman RUBIO. Because it would have been contained or whatever in the individual compartment they entered. Okay.

Mr. SMITH. Absolutely. Yeah. And these are five practices that the world knows about and this goes back I think to this point that we do need more cyber security professionals to work with more organizations. And obviously it's incumbent on us. We every day we're working to make it easier for our customers to deploy all of this stuff.

Vice Chairman RUBIO. Yeah, and I think that just touches on the notion that even if you can't prevent the attack or the intrusion you can mitigate its impact if you can do some of these things that you've discussed. Mr. Mandia, this is my last question. We talked about notification. Not disclosure but notification. And this seems to me that and you may have some thoughts on this what is the threshold for that?

Is it a major breach? Is it breach? Is it breaches that have indications of nation-state involvement?

Mr. MANDIA. It's hard.

Vice Chairman RUBIO. Because I think every day someone's getting pinged by somebody. So what's

Mr. MANDIA. I agree and you don't want to spread fear, uncertainty, and doubt by folks who can't do a proper investigation or lack the expertise or quite frankly they don't know what really happened but they disclose so fast that they do create an unnecessary fear. That is the hardest part because every disclosures going to have some discretion built into it. And that's why when I'm talking about notification I'm trying to there's public disclosure and legal disclosure.

I'm trying to separate that, and Brad Smith did in his testimony very well, to threat intelligence sharing. And I'm more talking about threat intel, get it out there fast, get it out there confidentially so you have the time to figure out the threshold for disclosure. But that's a lot of work because I think it depends on the industry you're in whether you should disclose. I think it there's contract law that'll apply. You should disclose to your customers at least that are impacted.

But I still feel disclosure is always going to be based on the impact of a breach which requires investigation.

Chairman WARNER. Well let me thank all of the panel and George who's online. We actually had well Senator Risch didn't want to ask a question. We had full participation from the Committee and that is a sometimes rare occurrence. I take away four issues that I'd like for the record since it's been a long afternoon.

The fact that Smith said this was potentially one of the most serious breaches he's seen. We know that it got into Mr. Ramakrishna's 18,000 customers and while they chose to only exploit 100 plus the fact that this could have been used not for exploitation and ex-filtration of information but could have been turned they were inside as I think Mr. Mandia so eloquently put it could have been exponentially worse and I think we need to recognize the seriousness of that.

Number two and I think Senator Rubio was raising this as well that while it was a top tier nation-state with their A team and it may be hard for any individual company or public enterprise to totally block that out, we can't default to security fatalism. We've got to at least raise the cost for our adversaries. And whether the items that Mr. Smith just enumerated in terms of better protections even if they get in we can find them and raise their costs if we think through this.

Mr. Smith commented on this but I would like the rest of you for the record to comment on this, this idea around norms and international norms. I use the analogy that in warfare you don't bomb the ambulance. Well should we try to get to a point that you don't bomb the patch? Or that you don't hit the hospital literally? Or the electoral systems? How do we move toward that system of norms?

And finally I think there is a real growing sense and I hear this from industry as well that we need some level of at least information sharing around on a mandatory basis. Again, I want to compliment Kevin's company and Kevin personally for coming forward because but for that effort we might still be, this might still be ongoing. And how we think about that what that reporting to or whom it rep we report to mechanism, I think it's going to require some new creation.

And while I am very open to some level of liability protection, I'm not interested in a liability protection that excuses the kind of sloppy behavior for example that took place in Equifax where they didn't even do the basic cyber hygiene. That if you report that you should not be free of your responsibility if you have been a sloppy player.

So I think there are models. There's FinCEN in the financial sector, there's the National Transportation Safety Board which may be

an even better example. I think Mr. Mandia pointed out within the credit card arena there is this information sharing. Some I know have been thinking about the idea that the cloud service providers, the large enterprises, the first responders a la CrowdStrike and FireEye maybe being co-located at some location with parts of the government.

Because this notion of getting the information out real time, that's not going to happen with all due respect to the great talents that are at the FBI that's not going to happen when it goes to the FBI and they're just not in the business of information sharing. It frankly is probably not going to happen even though CISA's skills continue to be upgraded. We're going to need to think about a different model and I challenge all of you to come forward with that.

I think there's a great deal of appetite bipartisan appetite. I think we realize how serious we were and we potentially dodged a much more serious bullet. And really appreciate all of your participation and it's been constantly mentioned those companies who chose not to participate so far we're going to give them another chance and hopefully they will recognize they have that kind of public service obligation that is reflected by the testimony today.

With that the hearing is in adjourned. Thank you.

[Whereupon at 12:07 p.m. the hearing was adjourned.]

Supplemental Material

Questions for Kevin Mandia, Chief Executive Officer, FireEye, Inc.
February 23, 2021, Hearing: "Hack of U.S. Networks by a Foreign Adversary"

From Chairman Warner and Vice Chairman Rubio

1. What information, as cybersecurity firms, are you required to share with the government when looking at cyber threats? What factors influence your decisions?

We are unaware of any general mandatory disclosure requirement for cybersecurity firms to share cyber threat information with the U.S. government unless the government legally compels a cybersecurity firm to disclose information via a subpoena or another legal mechanism. There are a number of other laws that require disclosure of a cyber incident to the government depending on, for example, the industry, the type of information affected and/or the severity of the cyber incident. For example, there are industry-specific laws such as the defense industry that might require a DoD government contractor to disclose information under certain circumstances pursuant to DFARs. § 252.204-7012.

In the normal course, cybersecurity firms are servicing clients during a cyber incident when gathering cyber threat information and the consent of such client would typically be required before any information is shared. We understand federal legislation and/or other legal instruments are being considered to mandate that certain information be shared with the government during cyber incidents and support those initiatives in order to better protect the Nation and inform the security community at large.

When FireEye chooses to share cyber threat information with the government, it is through our intelligence subscription service with paying (government) customers. We adhere to our Victim Notification program and policy process to protect our government and non-government customers from cyber attacks. It is designed to rapidly collect and analyze relevant and actionable threat intelligence from a variety of FireEye sources and disseminate to potential victims in a secure manner.

Additionally, we may choose to notify certain government partners, including the Department of Homeland Security, the Federal Bureau of Investigation, and the National Security Agency, when we have discovered a major cyber incident, such as recent the recent Pulse Secure, SolarWinds, and Colonial pipeline incidents. Factors for providing notification and/or sharing threat data associated with such incidents include the sophistication of the techniques used by the adversary, the likelihood of the threat actor being a nation state, and/or potential impacts and disruptions to critical infrastructure.

2. Does the Cybersecurity Information Sharing Act of 2015 provide sufficient legal protections for the sharing of information? In what ways could it be improved?

Although the 2015 information sharing law provides liability protections, they do not go far enough. Organizations are hesitant to share data in trusted-group or not-publicly-accessible environments for fear of retribution in the courts; the media; and possibly with shareholders and current and prospective customers.

Current statute provides companies liability protections, but only if *all* the sharing requirements are followed. The law reduces liabilities but does not eliminate them. For example, organizations

Questions for Kevin Mandia, Chief Executive Officer, FireEye, Inc.
February 23, 2021, Hearing: "Hack of U.S. Networks by a Foreign Adversary"

must remove all personally identifiable information (PII) from whatever is shared with the government. This may be easily accomplished for some prior to sharing, but difficult for others. The loss of protections under the law for unintentionally sharing PII is too big a risk for some companies. Updating the sharing program to mitigate against such risks might include the ability to share data anonymously in a repository. Furthermore, using that repository to also analyze and aggregate cyber risks and sharing findings with the security community might incentivize companies to share threat data.

The current information sharing law is challenged beyond limited liability protections. Additional challenges including the following:

- Today's sharing model is voluntary. There are no incentives for a private entity to share information with the federal government, especially for fear of reputational harm; reduction in shareholder value; criticism from the government, the media, etc.
- Participation in the program is low, thus, the information that's shared is minimal and not helpful to the government or participating entities. According to an Inspector General report at the Department of Homeland Security, less than 300 public and private entities were participating in the program as of 2018.
- Cybersecurity workforce issues are not accounted for – if the right cybersecurity experts aren't posted in private entities, they cannot correctly identify or conceptualize what should be shared with the government. There needs to be greater technical assistance from the federal government to help private entities share information.
- Operational capability issues are not accounted for – some companies don't have the capability to make the intelligence actionable or are unable to share intelligence effectively.
- The Department of Homeland Security is not necessarily sharing information back out to the community. Information that is shared is not actionable. The DHS IG report found that the Cybersecurity and Infrastructure Security Agency (CISA) increased the number of participants in the Automated Indicator Sharing (AIS) program and the volume of cyber threat indicators it has shared since the program's inception in 2016, but CISA has made limited progress "improving the overall quality of information it shares with AIS participants to effectively reduce cyber threats and protect against attacks."
- CISA is not staffed appropriately to manage the AIS Initiative, thereby reducing the quality of indicators that are shared back out to the community.
- The AIS technology, as well as relevant standards, are outdated.

We are encouraged by the requirements laid out in the President's recent executive order on cybersecurity, including mandatory disclosure requirements for federal contractors. We look forward to participating in and reviewing feedback and criteria established by DHS to share cyber threat information and to disclose incidents. FireEye maintains that these two activities should not be conflated and requirements surrounding each should be considered separately.

Additionally, CISA should consider (as well as Congress through any compulsory legislative requirements):

- Utilizing "cybersecurity first responders" to assist in identifying, contextualizing, and sharing cyber threat data.

Questions for Kevin Mandia, Chief Executive Officer, FireEye, Inc.
February 23, 2021, Hearing: "Hack of U.S. Networks by a Foreign Adversary"

- Establishing a small group of cyber first responders to prevent or mitigate the impact of cyber incidents through sharing information quickly and confidentially; first responders would include those who assess the events surrounding unlawful access to a network; these first responders would have an obligation to share threat intelligence to a government agency without being concerned about liabilities.
- Ensuring that all shared data is fully anonymized and 100% confidential.

From Senator Wyden

In 2019, FireEye released two free hacking tools, which automated the theft and use of encryption keys from Microsoft's Active Directory Federation Services (AD FS) software to access accounts in the cloud. The Golden SAML hacking technique that these tools automated was used by the adversary in the Solarigate campaign. In January, I wrote to your company to seek information about the steps that FireEye took to protect itself and warn the U.S. government about this hacking technique. FireEye's February response letter did not answer any of the questions I asked. Please respond to the information requests that I made in my January letter. Those information requests are:

3. Please describe and provide a timeline for all efforts by FireEye to warn Microsoft about the vulnerabilities exploited by adfsdump and adfspoof and of the importance of adding defenses against these exploitation techniques to Microsoft's enterprise products. Please provide copies of any relevant communications between FireEye and Microsoft.

4. Please describe and provide a timeline for all efforts by FireEye to warn the Department of Defense, the Office of the Director of National Intelligence, the National Security Agency, and the Cybersecurity Infrastructure and Security Agency, about the vulnerabilities exploited by adfsdump and adfspoof and the importance of the government deploying defenses against these exploitation techniques. Please provide copies of any relevant communications between FireEye and the U.S. government.

5. Please describe and provide a timeline for all efforts taken by FireEye to defend its corporate network against adversaries using adfsdump and adfspoof.

6. Please describe all efforts by FireEye to warn Congress about the need for organizations, including government agencies, to better protect AD FS encryption keys.

With respect to questions 3, 4, and 6, FireEye viewed the activities associated with ADFSDump and ADFSSpoof as a technique versus a vulnerability. As such, as is common practice, we did not disclose these activities via formal channels to any government agencies or the U.S. Congress, as we would through our typical responsible disclosure process for vulnerabilities or incidents. In general, for the latter cases, we use this process to notify vendors, who then in turn notify the appropriate agencies, government entities, etc.

As typically practiced within the security community, we discussed ADFSDump and ADFSSpoof in a number of informal channels:

Questions for Kevin Mandia, Chief Executive Officer, FireEye, Inc.
February 23, 2021, Hearing: "Hack of U.S. Networks by a Foreign Adversary"

- March 2019 – held informal conversations with Microsoft employee about the tool and response of "no feedback" from the ADFS team
- March 2019 – mentioned technique during a talk at a public conference, TROOPERS 19, in Germany
- July 2019 – mentioned technique during an informal "Tech Talk" at Fort Meade
- August 2020 – mentioned technique during a talk at a virtual public conference, Blackhat

With respect to question 5, we followed proper internal security protocols and took appropriate actions to defend and instrument our environment against the technique.

DLA Piper LLP (US)
500 Eighth Street, NW
Washington, DC 20004
www.dlapiper.com

August 5, 2021
VIA E-MAIL

The Honorable Mark Warner
Chairman
Senate Select Committee on Intelligence
703 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Marco Rubio
Vice Chairman
Senate Select Committee on Intelligence
284 Russell Senate Office Building
Washington, D.C. 20510

Dear Chairman Warner and Vice Chairman Rubio,

Thank you for the questions for the record from the Senate Select Committee on Intelligence related to the hearing on February 23, 2021 titled "Hearing on the Hack of U.S. Networks by a Foreign Adversary."

We write on behalf of our client, SolarWinds Corporation ("SolarWinds"), in response to your letter dated April 1, 2021 addressed to Sudhakar Ramakrishna. The enclosed attachment contains SolarWinds' written responses to the Committee's questions for the record on behalf of Mr. Ramakrishna.

Best regards,

John Merrigan

John Merrigan/s

Steve Phillips

Steve Phillips/s

APPENDIX A

Questions for the Record from Chairman Mark Warner and Vice Chairman Marco Rubio, Senators in Congress from the State of Virginia and the State of Florida

1. *Have you determined how the cyber actors gained access to your network? If so, please explain your findings. If not, please explain what factors are impeding your progress in making such a determination.*

   Our third-party forensic investigation firms Crowdstrike and KPMG have assessed that one of the following three vectors likely may have been leveraged by the threat actor(s) as their initial access point:

   - Third party zero-day exploitation
   - Brute force attack on external facing authentication platforms such as VPN
   - Credential compromise via phishing or watering hole attack

   Our third-party forensic investigation firms identified unauthorized access as early as January 2019, but could not identify which of the three above vectors was the initial access method by the threat actor(s) or if any earlier unauthorized access occurred due to the lack of available data dating back to that timeframe.

   While we don't know precisely when or how the threat actor first gained access to our environment, our investigations have uncovered evidence that the threat actor compromised credentials and conducted research and surveillance in furtherance of its objectives through persistent access to our software development environment and internal systems, including our Microsoft Office 365 environment, as early as January 2019.

Questions for the Record from Senator Ron Wyden, a Senator from the State of Oregon

According to a Frequently Asked Questions document published by SolarWinds, the following releases of your Orion product contained the backdoor: 2019.4 Hotfix 5, 2020.2 and 2020.2 Hotfix 1.

1. *Of these versions of your software containing the backdoor, please identify which versions SolarWinds were submitted for testing for Common Criteria certification and for potential placement on the Department of Defense Information Network (DoDIN) Approved Products List (APL).*

   The three product versions of Orion that were found to contain the backdoor, SUNBURST, were not submitted for testing for the Common Criteria certification or DoDIN APL. Prior

versions of Orion were submitted and approved. Evaluations can take up to a year, therefore only some versions go through the process. The SolarWinds Orion Suite for Federal Government must first go through Common Criteria and then is evaluated for DoDIN. SolarWinds Orion Suite for Federal Government version 3.0 completed the evaluation for common criteria and DoDIN APL. SolarWinds Orion Suite for Federal Government version 4.1 is currently under evaluation for Common Criteria.

2. *What were the results of these assessments?*

   See response above for #1.

3. *If these versions were not tested, had they been tested in a manner similar to that used to test prior versions of SolarWinds' software, do you expect that the backdoor would have been discovered? If so, please identify the specific part of the testing process that would have likely resulted in the discovery of the backdoor.*

   We do not believe that the backdoor would have been discovered in the compromised product versions if they had been tested via the Common Criteria certification as this certification only involves "Evaluation Assurance Level 2+" (EAL2+), which does not cover a deep penetration level of testing.

   For DoDIN inspection, we provide the product and DoDIN performs the testing. The detailed test plans are not known to us; therefore, we cannot determine if SUNBURST would have been discovered.

4. *When was SolarWinds first contacted by the FBI? What did the FBI tell your company?*

   SolarWinds' Vice President of Security Architecture was first contacted by the FBI via telephone on December 11, 2020, with notification of an issue about which the Company would be informed at a later time. Later that evening, the FBI sent SolarWinds a *Request for Preservation of Records* via facsimile to SolarWinds' general facsimile line. The request was to preserve for a period of ninety (90) days any and all records and other evidence related to what is now known as the cyber attack.

5. *Since the initial notification by the FBI, how much information has SolarWinds provided to the FBI, and in turn, how much information has the FBI provided SolarWinds? Is SolarWinds satisfied with the amount of information the FBI has shared with it?*

   On December 14, 2020, SolarWinds contacted FBI Cyber Division Assistant Director, Frankland M. Gorham, to provide an update on the cyber attack and to ask for assistance in the investigation. On December 15th, 2020, FBI Cyber Division leadership introduced the

SolarWinds investigation team to the FBI team leading the investigation from the Houston and San Francisco field offices.

SolarWinds is committed to transparency in its engagement with the FBI. SolarWinds has provided terabytes of unique records of information to the FBI, including but not limited to documents, log files, server images, software code, backups, and virtual hard disks. SolarWinds also participates in weekly telephone calls with the FBI and regularly invites its third-party forensic investigative firms to provide briefings to the FBI regarding developments concerning its investigation of the cyber attack.

To date, SolarWinds has received very little information from the FBI to aid in SolarWinds' efforts regarding the cyber attack. SolarWinds respects the confidentiality obligations of the FBI concerning data in its possession, but wishes more information could have been provided (if it existed) such that the company may have been able to conduct a more efficient investigation and work more closely with the government to focus remediation efforts on the customers more likely to be targeted.

Questions for the Record
Senate Select Committee on Intelligence
Hearing on the Hack of U.S. Networks by a Foreign Adversary
February 23, 2021

Questions for the Record for Mr. Brad Smith, President of Microsoft

[From Chairman Warner and Vice Chairman Rubio]

Regarding the ability to misuse identity access tokens described by Senator Wyden:

1. **When did Microsoft first learn of this vulnerability?**

Microsoft, together with other companies, governments, and cybersecurity professionals, first learned of the Golden SAML (Security Assertion Markup Language) post-exploit technique in 2017 when security researchers from CyberArc published[1] a public blog detailing the theory. Their research concluded that it was possible for attackers to "gain access to any application that supports SAML authentication (e.g., Azure, AWS, vSphere, etc.) with any privilege they desire…". Their research further noted that if attackers gained privileges in one environment, such as an on-premises active directory, then they could abuse that access to generate SAML tokens, which could open access to a victim's cloud environment.

In only 15 percent of the recent attacks we saw, the actor used the Golden SAML technique to access Office 365 (O365) accounts. The identity access tokens the actor was able to generate worked as intended – because the actor had first obtained the ability to act as a network administrator in the network and could issue tokens trusted by O365. There was no vulnerability in any Microsoft product or service that was exploited, but the inherent weakness in the SAML industry standard authentication system described in the CyberArc research did provide the actor with this method – among many others – to access other network resources.

Although Office 365 customer data was accessed as a consequence of this attack, we have found no indication that Active Directory (AD) was a vector in this attack – nor that any vulnerabilities in AD were leveraged. There has been speculation that a flaw in AD allowed users to gain elevated access. That is not accurate; the threat actors in this attack used several techniques to escalate privileges and/or obtain privileged credentials that gave them the ability in on-premises networks to act like a system administrator. Our investigations have confirmed several compromise techniques, including password spraying and spear phishing, which enabled the actors to obtain privileged credentials in a customer's environment.

The most advanced threat actors operate with ample patience, time, and resources. In this case, one of the things that the threat actor did extremely well was to appear to stay within the bounds

[1] Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps (cyberark.com)

of how a product or service should be used. The threat actor did not discover or use a new vulnerability in any cloud services that we have seen; rather, attackers took advantage of how a service was implemented in a customer's environment and then leveraged how the service worked to conduct their operation.

2. What steps did Microsoft take to protect against its misuse?

Microsoft advised customers to implement an expanding array of best practices that would help protect against the misuse relating to the Golden SAML post-exploit technique. It's important to emphasize again that use of the Golden SAML technique in the SolarWinds attacks took place *after* an attacker had first obtained the ability to act as a network administrator. Especially given a myriad of potential cybersecurity priorities, the most effective course of action was to prevent an attacker from establishing this ability in the first place.

Microsoft has emphasized five best practices, in particular:

1. Utilize multi-factor authentication;[2]
2. Establish Least Privileged Access principles across your network, and adopt other Zero Trust Principles;[3]
3. Secure the most sensitive credentials of network administrators and others in hardware or in the cloud;
4. Secure devices through Intune;[4] and
5. Use anti-malware tools such as Defender.[5]

We also continued to encourage our customers to move to newer authentication technology, including by moving their authentication practices to the cloud.

The Golden SAML theory that the CyberArc researchers presented would first require an attacker to already have gained a presence in a victim's on-premises network. The attacker would then need to acquire credentials of a network administrator in some manner. Following these steps, the Golden SAML technique could then be executed.

Microsoft's security researchers reviewed this theory, as they do with the thousands of possible attack vectors researchers regularly surface. Given the level of access an attacker would already need to have achieved prior to leveraging this particular technique, coupled with the reality that the initial attack vectors used to gain this level of access were active threats against customers,

---

[2] How to implement Multi-Factor Authentication (MFA) - Microsoft Security; Multi-Factor Authentication (MFA) - Microsoft Security; Set up your Microsoft 365 sign-in for multi-factor authentication

[3] Zero Trust Deployment Center | Microsoft Docs; Zero Trust - Microsoft Security; Using Zero Trust principles to protect against sophisticated attacks like Solorigate - Microsoft Security

[4] What is Microsoft Intune - Azure | Microsoft Docs

[5] Next-generation protection | Microsoft Docs

we prioritized protecting our customers against the initial attack vectors that would lead to multiple potential subsequent threats.

Additionally, our experience shows us that CISOs need to prioritize how they deploy their resources, and even when information about notional post-exploitation techniques is available, combatting such techniques will not necessarily be considered a high enough risk to divert time or resources from other, potentially more important, security efforts.

It's also worth noting that SAML is an old standardized technology that was first introduced in 2002 and subsequently updated in 2005 with SAML 2.0.[6] Given the age of SAML and the limitations of the protocol, we have long encouraged our customers to move to modern authentication technology that is more secure, specifically OAUTH2[7], which we also support in our products. However, many of our customers still require or opt to use SAML, often due to legacy applications that rely upon SAML authentication, making it challenging for them to change. For that reason, cloud providers continue to support SAML authentication, despite its limitations.

We have certainly reflected on what we can do in the future to ensure our customers are better prepared and that we are providing them with the tools they need to better protect themselves. That is why we announced recently that, for the next year, we will make available to government customers our advanced logging capabilities for no cost,[8] as we continue to review our efforts to support customer security. It is also why we continue to encourage organizations to at least move their authentication systems to the cloud. The attack on SolarWinds and its customers shows firsthand how challenging it is for organizations to protect themselves on-premises in today's cyber environment. Regardless of platform or tool leveraged, moving authentication to the cloud is one of the most impactful steps an organization can take to protect itself and its infrastructure.

[From Senator Wyden]

During your opening remarks, you stressed the importance of software security updates and stated that, when hackers tamper with the software updating process, it puts the entire world at greater risk.

3. **Have hackers ever compromised any of the digital infrastructure that Microsoft uses to create, authenticate, and distribute software security updates? If yes, please detail each incident, its impact, and whether Microsoft reported it to the appropriate U.S. government authorities.**

To our knowledge, Microsoft has never been the victim of a successful attack on our software security update channel. In 2012, Kaspersky and CrySys Lab found malware they called "Flame," which impersonated the Windows update channel by appearing to come from

---

[6] What is SAML? How it works and how it enables SSO | CSO Online
[7] An Introduction to OAuth 2 | DigitalOcean
[8] Addressing Audit Log Storage for U.S. Federal Government Customers - Microsoft in Business Blogs

Microsoft—but it did not involve a compromise of our update channel; it involved an imposter. As a result of what we learned from that event, however, we spent significant resources to harden our update infrastructure to prevent an actual compromise from occurring, and we continue to maintain vigilance today.

4. **What security tools or features are included with the E5/G5 license, which is Microsoft's most expensive enterprise software subscription, but not the standard E3/G3 license that might have aided in the discovery or mitigation of the identity compromise at issue in many of the Solorigate compromises or the operation of any subsequent deployed malicious software?**

As explained below, Microsoft's G3/E3 license includes *core* solutions for security, compliance, identity, and management, and the G5/E5 license includes *advanced* solutions. This provides customers with the ability to choose what they want to procure from Microsoft as well as a wide variety of other cybersecurity vendors. And even more important, the effective implementation of the core solutions in the E3/G3 license would absolutely have aided in the discovery or mitigation of the identity compromise at issue in many of the Solorigate compromises, as well as the operation of any subsequently deployed malicious software.

It's worth recognizing that cybersecurity is at an inflection point as threat attack sophistication escalates, digital attack surfaces increase exponentially, and customers navigate different economic constraints and talent scarcity. This environment requires a Zero Trust, multi-tiered security strategy, involving comprehensive protection as well as choice and flexibility based on business requirements and security solutions that organizations may deploy from multiple vendors.

Microsoft's approach to security is anchored in Zero Trust principles, and we provide defense-in-depth security across all layers, from development to operational security and in our baseline security capabilities that are included in our platforms by default. All of our customers benefit from baseline security capabilities, such as our Security Development Lifecycle (SDL),[9] Operational Security Assurance (OSA)[10] practices, Windows Defender Antivirus (AV),[11] Azure Security Center,[12] and Audit Logs for 90 days[13] by default.

In addition, we provide "core" (G3/E3) and "advanced" (G5E5) solutions across security, compliance, and identity management for customers who seek choice and flexibility in the highly fragmented security market, where they procure security solutions from more than 70 different vendors on average. Microsoft security solutions are built to address our customers' requirements and circumstances. We offer multi-platform (i.e., we also support Android, Linux, and iOS) and

---

[9] About the Microsoft Security Development Lifecycle
[10] Microsoft Operational Security Assurance Practices
[11] Next-generation protection | Microsoft Docs
[12] Azure Security Center | Microsoft Azure
[13] Manage audit log retention policies - Microsoft 365 Compliance | Microsoft Docs

multi-cloud (i.e., we also support AWS and Google Cloud), best-of-breed and best-of-integration solutions.

To deliver the best security protection from baseline to advanced, we fiercely innovate, and that requires us to invest across our portfolio of people and technology. Microsoft annually invests more than $1 billion in R&D and security operations, with more than 3,500 people working in security.

CORE (G3/E3) and ADVANCED (G5/E5) SECURITY in Microsoft 365

Most of our enterprise and public sector customers are seeking advanced security and choice in a highly fragmented security market segment with thousands of vendors. Our customers want best of breed as well as best of integration. They want multi-platform and multi-cloud alongside cost savings. Microsoft advanced security was built for customers based on their requests and requirements – to offer them more choice and protection on their terms, customized for their use cases and requirements, depending on what they already own and use.

G3/E3 includes *core* solutions for security, compliance, identity, and management, and G5/E5 includes *advanced* solutions. This allows customers to choose which capabilities are the best fit for their needs at different price points, and it also crucially enables flexibility to purchase and use security products from different vendors consistent with their broader strategies. The ability of our solutions to mitigate any threat or incident response scenario, such as the discovery or mitigation of an identity compromise or the operation of malicious software, depends in part on customer implementation. However, effective use of our core solutions would have aided in the discovery or mitigation of threat activities relevant to the Solorigate compromise.

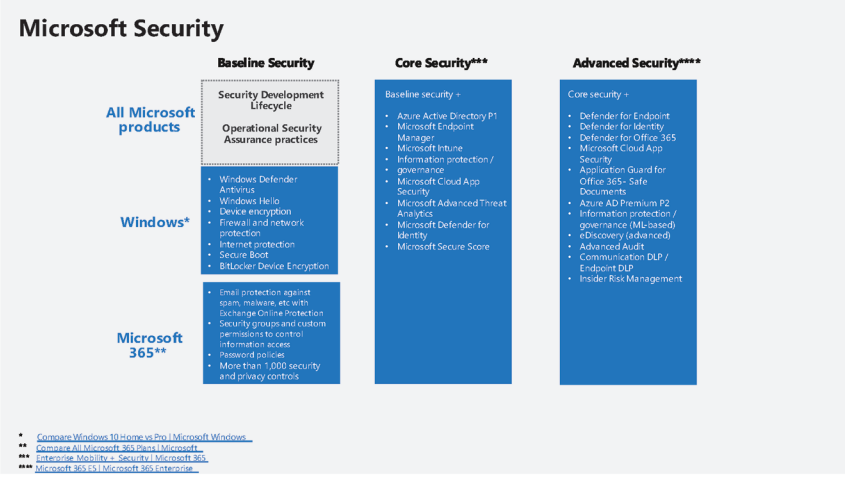
Core (E3/G3) Solutions

- Endpoint and App Management: Microsoft Intune, Mobile Device Management, Mobile Application Management.
- Threat Protection: Defender AV, Defender Firewall, Defender Exploit Guard and Credential Guard, Bitlocker and Bitlocker to Go, Windows Information Protection (these are all part of Windows E3), Desktop Analytics.
- Identity and Access Management: Azure AD Premium – that includes Conditional Access and Cloud App Security Discovery.
- Information governance, information protection and eDiscovery: including manual retention labels, basic policies, sensitivity labels, data loss prevention, office message encryption, content search, litigation hold and basic audit (e.g., out of the box protections such as encrypt-only or do-not-forward policies to sensitive emails with Office 365 Message Encryption).
- Unified Audit Logging (UAL): for M365 E3/G3 and O365 E3 customers, we store Basic Logs for 90 days by default, which provides organizations with visibility into many types of audited activities across many different services in Microsoft 365. Via

the Office 365 Management Activity API, customers can download and store the audit log data on their own for as long as they'd like.
    - For customers who need to retain audit logs for more time, we offer Advanced Audit in our comprehensive E5 offering or via the add-on E5/G5 Compliance SKU (and M365 G5 eDiscovery and Audit), which includes Advanced Audit, and allows customers to store audit logs for up to one year and provides additional capabilities for investigation.
- Microsoft Secure Score: helps customers assess their current state of security posture, improve said posture, and compare with benchmarks.

Advanced (E5/G5)

- Threat Protection: Defender for Endpoint, Defender for Identity, Defender for Office 365, Application Guard for Office 365, Safe Documents.
- Identity and Access Management: Azure AD Premium P2 – including risk-based Conditional Access, Privileged Identity Management, Access Reviews, and Entitlement Management.
- Cloud Security: Microsoft Cloud App Security.
- Information governance, information protection and eDiscovery: rules-based and ML-based retention labels and policies, records management, automatic and ML-based sensitivity labels, communication DLP, endpoint DLP, advanced Office message encryption, Insider Risk Management.
- Advanced Audit: included for M365 G5/E5 and O365 E5 customers, builds on UAL and retains all Exchange, SharePoint, and Azure Active Directory audit records for up to one year (for M365 E5/G5 and O365 E5 customers, we store Unified Audit Logs for 90 days by default, which provides organizations with visibility into many types of audited activities across many different services in Microsoft 365). Retaining audit records for longer periods can help organizations to conduct forensic and compliance investigations by increasing audit log retention required to conduct an investigation, providing access to crucial events that help determine scope of compromise, and faster access to Office 365 Management Activity API. Audit and retention needs are different by customer depending on industry and whether they are using 3rd party solutions. This approach gives customers choice and flexibility on what they pay for in the product, given the storage costs to retain.
    - We also offer customers the option to pay for further retention/storage up to 10 years via different plans based on their needs.



In a blog post published in 2015, a senior Microsoft employee wrote that:

> ***"The token signing certificate is considered the bedrock of security in regards to ADFS [Active Directory Federation Services]. If someone were to get ahold of this certificate, they could easily impersonate your ADFS server."***

In 2017, a researcher demonstrated that these encryption keys could be stolen and used to create tokens that could then be used to log in to accounts with cloud service providers, such as Office 365. The researcher dubbed this attack "Golden SAML." This hacking technique was then exploited by the adversary in the Solorigate incident. Microsoft has confirmed to my office that the company did not warn the U.S. government about the Golden SAML attack because it had not seen hackers exploit it in the wild.

5. **As a general rule, does Microsoft only warn its customers about vulnerabilities that adversaries are exploiting in the wild? If not, please explain why Microsoft chose not to warn its customers about this hacking technique but has opted to warn its customers about other vulnerabilities before they were actively exploited in the wild.**

Microsoft warns customers about hacking techniques in a wide variety of circumstances. It's worth noting once again that the Golden SAML theory became known to cybersecurity professionals at Microsoft and across the U.S. Government and the tech sector at precisely the same time, when it was published in a public paper in 2017.

Microsoft's warnings to customers are based in part on adherence to the principles of Coordinated Vulnerability Disclosure ("CVD"), the goal of which is to provide timely and consistent guidance to customers about vulnerabilities and other issues to help them protect themselves.[14] External researchers or internal Microsoft employees may discover a vulnerability in Microsoft products or services. Under CVD principles, information about the vulnerability is typically not released until an update to address the vulnerability is released. In some instances, even before an update is ready but when it's discovered that attacks using the vulnerability are underway in the wild, we disclose vulnerability information in coordination with the discoverer as appropriate under the circumstances to protect customers.

Again, the hacking technique identified in 2017 as Golden SAML did not involve a vulnerability in Microsoft products or services. The technique was one that demonstrated how an attacker with escalated privileges in a network could take advantage of an industry standard authentication process, SAML, to access other resources. Given that the attack technique did not involve such a vulnerability, the researcher did not report it to Microsoft under CVD principles. Instead, the researcher made the information about the hacking technique publicly available, so that it was equally available to U.S. government agencies, Microsoft and other industry participants.

In some cases, Microsoft shares our own research or amplifies publicly available information about hacking techniques or security priorities. Our customer communication has for years focused on core cybersecurity hygiene that, if properly deployed, would have protected against or minimized the impact of the attack on SolarWinds and its customers. As an industry, we still have work to do to get customers to take basic cybersecurity hygiene steps, which help to defend against and limit the impact of nearly all cybersecurity attacks. As the question notes, prior to the attack on SolarWinds and its customers (in which the Golden SAML technique was not the primary exploit used), there was no evidence that the Golden SAML technique had previously been used in an actual attack in the wild. Additionally, the Golden SAML exploit was not prioritized by the intelligence community as a risk, nor was it flagged by civilian agencies or other entities in the security community as a risk that should be elevated over promoting MFA deployment, combatting ransomware, or undertaking other fundamental security actions. Our experience shows us that CISOs prioritize how they deploy their resources, and even though information about this notional attack vector was available, addressing it was not considered a high enough risk priority to divert time or resources from other potentially more important security efforts.

Customer security is a core priority of ours, and we are constantly reflecting on what we can do better to create a more secure ecosystem. As noted in the question, we prioritize warning customers of vulnerabilities when they are identified and we have a patch or appropriate path to mitigation to share. The Golden SAML technique is different, not only because it was not previously exploited in the wild, but also because it is not a vulnerability but rather a post-exploit attack technique. To use this technique requires an attacker to successfully compromise a network, and then successfully acquire escalated privileges. At that point, as the data from this

[14] https://www.microsoft.com/en-us/msrc/cvd; The CERT Guide to Coordinated Vulnerability Disclosure (cmu.edu)

incident demonstrates, many other approaches to identity compromise are available to an attacker – approaches used by this attacker 85 percent of the time. Prioritizing defenses to this one post-compromise SAML token exploit would not be a good use of an enterprise security resources, not only because it had not been seen in the wild before this attack, but also because an environment would have to be compromised already in order for this attack technique to be deployed. It's also worth noting that SAML is 14-year-old technology. We have counseled our customers to utilize more modern authentication techniques, or to move authentication (and other workloads) to the cloud to maximize security. But many customers use applications in their on-premises environments that rely upon SAML for authentication, so they continue to need us to support SAML in our on-premises authentication products.

The important lesson of Solorigate is that enterprises and government agencies need to improve basic cybersecurity hygiene measures that protect against the most common forms of attack. Those who want the best security should move to the cloud, where advanced security analytics can be provided at scale. The technology industry must work to provide better tools and systems to identity attacks, and Microsoft is working on new ideas to help customers detect sophisticated attacks like this one. The intelligence community will also have a role in helping to identify and defend against the most likely and impactful nation-state attacks against U.S. government infrastructures. And we need to establish internationally enforceable rules of nation state conduct in cyberspace to prevent the most disruptive and heinous forms of attack, including attacks on the software update processes, the primary means by which the industry keeps its technology secure and which customers must be able to trust.

6. **Has any Microsoft penetration testing exercise in the past five years revealed a weakness in Microsoft identity products which could have permitted the creation of new identities, changed user permissions, or led to similar behavior as that observed of the threat actor responsible for the Solorigate incident? If so, what was done to remediate the identified weakness?**

Penetration testing conducted on Microsoft's identity product code over the last five years has not revealed any security vulnerability that could directly lead to identity manipulation. A penetration test that relies on implementation issues specific to an operating environment, including implementation issues revealed by Solorigate, to escalate or modify account privileges or create a new account would not necessarily reveal a risk that can be mitigated by Microsoft identity products. The attacker in the Solorigate incident escalated privileges in customer environments and in a minority of cases managed to compromise the customer's cryptographic secrets used to digitally sign proofs of identity. It is possible for customers to prevent removal of these master secrets from their environments with the use of a Hardware Security Module, as recommended by Microsoft guidance as well as National Security Agency guidance, or through administrative hardening.

According to research published by CrowdStrike, the adversary inserted the first stage of its malware into SolarWinds' software by compromising the company's build server. This server turns the human-readable code written by programmers into code that can be installed on computers. One promising cybersecurity defensive technology to protect against this method of compromise is known as reproducible builds. In short, this technology guarantees that the same code, no matter on which server it is built, will produce the same output. Thus, by comparing the output from several independent build servers, a backdoor inserted by one compromised build server would be easily detected, as the output would differ from the other build servers.

7. Please summarize Microsoft's efforts to date to support reproducible builds.

Microsoft has been pursuing and continues to pursue efforts to support reproducible builds and to address challenges that impact our and others' ability to do so. Generating reproducible builds requires starting with the same source code and other inputs along with consistency across many aspects of the software configuration of the build environment. All of the actions that occur during a build process need to be deterministic and independent of variables that modify the output. Key activities include reading the exact source files used, performing preprocessing with tools, and using a compiler to transform and translate the preprocessed files into a form that can be installed on a computer.

Many conditions, actions, or aspects of input can disrupt the reproducibility of the processes that occur on a build server. A simple example is when a tool inserts the current time into data consumed in an intermediate build step. The consequence will be that the final output then contains a time-based variable. This variable causes the build process to not be reproducible on the same build server as well as on other build servers.

Microsoft recognizes the importance of reproducible builds for software assurance and has publicly acknowledged working towards generating product builds in a reproducible way. In January 2018, we explained that date and time stamps appear nonsensical in some Windows 10 components because setting the timestamp to be a hash in the resulting binary preserves reproducibility.[15]

Language and compilers can also hamper reproducibility. A compiler is a key tool used on build servers to transform human readable code into code that can be installed on computers. If a compiler behaves in a predictable and deterministic way, then it will generate the same output given the same inputs. A deterministic compiler is necessary to support reproducible builds.

Microsoft compilers for C#,[16] Visual Basic,[17] and F#[18] support a compiler option to generate deterministic assemblies. The footnoted feature descriptions identify a list of variables that can

[15] Why are the module timestamps in Windows 10 so nonsensical? | The Old New Thing (microsoft.com)
[16] C# Compiler Options - code generation options | Microsoft Docs
[17] Compiler Options Listed Alphabetically - Visual Basic | Microsoft Docs
[18] Compiler Options - F# | Microsoft Docs

impact reproducibility in addition to the source code itself. For example, different compiler versions can introduce changes in the build output. The deterministic compiler feature for C# and Visual Basic has been available for almost five years and for F# for almost four years. Deterministic build options are not available for other Microsoft compilers (e.g., for the programming language C, assembly, etc.).

Challenges with reproducible builds also exist when software includes external dependencies, which can change as their project's community adds new features and patches vulnerabilities.

To assist developers in locating the exact source files used in a build process, a project called Source Link[19] was transitioned to the .NET Foundation[20] in November 2017. Source Link is supported by Microsoft, and it allows metadata about source control management systems (whether for open-source or propriety software) to be inserted into the output of the build process, helping developers and verifiers trace back the exact source code that was used to generate a build. This is beneficial for general debugging and for making builds reproducible. Microsoft source control products, including GitHub Enterprise, Azure Repos and Azure DevOps Server, all work with Source Link. In February 2021, Microsoft posted guidance on how to generate reproducible builds using Source Link.[21]

8. **Does Microsoft recommend that the U.S. government support efforts to ensure that widely used open source software can be built in a reproducible manner? Does Microsoft have any other recommendations for what the U.S. government should do to increase the security of widely used open source software?**

Yes. Microsoft recommends that the U.S. government support efforts focused on enabling widely used open source software to be built in a reproducible manner, recognizing that realizing that outcome will take significant time – likely several years. Reproducible builds require the entire tool chain involved in the build process to support reproducibility. Example workstreams include keeping track of build inputs (especially the exact source files used in a build), making revisions to source code to remove characteristics that make it incompatible with reproducible builds, and improving available build tools and infrastructure (especially compilers for popular programming languages). Open source software developers use a wide array of languages and tools, and ensuring the entire tool chain supports the efforts of diverse, often community-based projects will be foundational to enabling developers to more seamlessly make changes to support reproducible builds. An informative example of a multi-year effort to enable a large open source project to be built in a reproducible way is here: ReproducibleBuilds - Debian Wiki.[22]

---

[19] GitHub - dotnet/sourcelink: Source Link enables a great source debugging experience for your users, by adding source control metadata to your built assets
[20] https://dotnetfoundation.org/
[21] GitHub - clairernovotny/DeterministicBuilds: Shows how to do deterministic builds with .NET
[22] ReproducibleBuilds - Debian Wiki

Microsoft also encourages the U.S. government to support open source security and broader software security foundations and projects, including the Open Source Security Foundation (OpenSSF),[23] which is carrying forward the work[24] of the Core Infrastructure Initiative and[25] the Open Source Security Coalition,[26] as well as SAFECode[27] and the OWASP Foundation.[28] OpenSSF is particularly focused on improving the security of widely used open source software. For example, this OpenSSF publication, "Threats, Risks and Mitigations in the Open Source Ecosystem,"[29] includes recommended mitigations for improving the security of the open source ecosystem. To further increase the security of widely used open source software, also consider the following guidance: practices for reducing risk when using open source: Microsoft Open Source Software Security;[30] and GitHub code security guidance: Code security - GitHub Docs.[31]

9. **Does Microsoft believe it would be worthwhile for the U.S. government to require that all new software created by or for the U.S. government be capable of being built in a reproducible manner?**

Requiring some software that is created by or for the U.S. government to be built in a reproducible manner would be worthwhile, especially if pursued in a manner reflective of operational challenges and limitations. Factors to be considered include the timing for such a requirement, the availability of support where implementation might be especially challenging (e.g., some open source projects, programming languages without deterministic compilers, etc.), and the ability to appropriately prioritize against other software assurance efforts.

Reproducible builds do increase assurance for a specific step in the software development process, but they do not by themselves guarantee secure software. For example, if the source code contains a vulnerability, then performing a reproducible build and verifying it by repeating the same process in another environment would not identify the vulnerability. Microsoft encourages the U.S. government to use various tools, including its procurement power as well as its research and development, standardization, and center of excellence capacities, to help strengthen software security. Reproducible builds should be considered within a risk-based context as one of numerous technologies that have the potential to increase software assurance and reduce cybersecurity risk. The process and timeline for when such a reproducible build requirement would be feasible, and for what software, merit study, the results of which could

[23] Home - Open Source Security Foundation (openssf.org)
[24] Technology and Enterprise Leaders Combine Efforts to Improve Open Source Security - Open Source Security Foundation (openssf.org)
[25] Home - Core Infrastructure Initiative
[26] GitHub - Open-Source-Security-Coalition/Open-Source-Security-Coalition
[27] Home - SAFECode
[28] OWASP Foundation | Open Source Foundation for Application Security
[29] wg-identifying-security-threats/Threats, Risks, and Mitigations in the Open Source Ecosystem - v1.1.pdf at main · ossf/wg-identifying-security-threats · GitHub
[30] Microsoft Open Source Software Security
[31] Code security - GitHub Docs

lead to worthwhile and deliberative action. The study could take into account possible benefits as well as unintended consequences of such a requirement, such as potentially limiting the diversity of platforms, open source libraries, languages, and toolsets that information and communications technology vendors would be able to use as a result. It could also explore how the U.S. government can help foster ecosystem readiness for such a requirement or advance other software assurance practices that reduce risk.

Questions for the Record
Senate Select Committee on Intelligence
Hearing on the Hack of U.S. Networks by a Foreign Adversary February 23, 2021

Questions for the Record for Mr. George Kurtz, President and Chief Executive Officer of CrowdStrike

[From Chairman Warner and Vice Chairman Rubio]

1. **What information, as cybersecurity firms, are you required to tell the government when looking at cyber threats? What factors influence your decisions?**

CrowdStrike protects public and private sector customers around the globe, including US Federal government agencies. These organizations receive cyber threat information via CrowdStrike's platform and threat intelligence service. The company also engages in cyber threat sharing arrangements where they do not conflict with other legal obligations, such as our customer agreements.

Some CrowdStrike customers are bound by sector-specific cyber incident or data breach reporting obligations. In these instances, CrowdStrike's offerings and service engagements provide customers with relevant information they may need to assess whether or not such notification obligations are triggered. In scenarios where there is no formal obligation to disclose incidents, customers sometimes still elect to disclose information publicly or to Government partners, and we frequently work with them to make sure such disclosures are accurate and actionable.

2. **Does the Cybersecurity Information Sharing Act of 2015 provide sufficient legal protections for the sharing of information? In what ways could it be improved?**

Advocates of cybersecurity information sharing legislation worked for years on concepts that informed the Cybersecurity Information Sharing Act of 2015. The law itself provides certain liability protections for entities that share cyber threat information. That said, many private companies still prefer not to participate in programs like the Department of Homeland Security's Automated Indicator Sharing (AIS) program, for a variety of reasons. Several issues are relevant here:

- **Availability**. There are now a variety of widely-available commercial threat intelligence solutions that provide real-time, accurate protection against cyber threats. When business groups first started advocating that Congress enact information sharing legislation in 2009-10, the state of the field was much less mature. By the time the Cybersecurity Information Sharing Act became law and the Department of Homeland Security created the Automated Indicator Sharing (AIS) program in the 2015-6 timeframe, many companies already consumed commercial threat intelligence.

- **Bi-directionality**. Some public-private sharing schemes mandate that participants provide information in order to receive information. This type of requirement seeks to address the 'free rider' problem and is a sensible requirement for schemes that involve highly sophisticated players (e.g., cybersecurity companies). However, some companies across various industries do not have the capacity to operate in reciprocal arrangements. This can be due to a lack of resources or internal sophistication in identifying and validating indicators.
- **Simplicity and actionability**. The most effective contemporary commercial cybersecurity solutions natively integrate threat intelligence, which provides two key advantages. First, it places responsibility for indicator identification/aggregation on the cybersecurity vendor(s), which often share indicators through commercial or mutual-interest-based arrangements. Second, it simplifies end-users' ability to protect their enterprises by lessening--or obviating--the need to handle raw indicators. This reduces the chances of introducing human errors that lead to distracting false positives or harmful false negatives. This approach often allows the vendor to help inform decisions around the criticality of an identified issue and, in some instances, to automate various responses. The technologies and security practices I outlined in my testimony, including XDR, threat hunting, and metrics, are built upon such innovation.
- **Scale and Context**. We believe modern cybersecurity solutions should leverage the cloud to share threat intelligence and simultaneously protect hundreds or thousands of customers across disparate industry verticals and geographies in real time. This scale would be difficult to replicate by a single government program that requires individual entities to operate as active participants. With respect to context, natively integrated intelligence solutions can allow users to immediately understand whether threat activity observed in their environment is linked to known threat actors. This empowers defenders to act with the deliberate speed needed for ever-evolving threats, a concept I outlined in my testimony.
- **IOCs vs. IOAs**. During the original push for information sharing legislation starting over 10 years ago, there were two central types of information to which organizations sought greater access. The first was contextual information. For example, an indication that there was an active campaign targeting a specific sector like water treatment facilities or the satellite communications supply chain. The second was tactics, techniques, and procedures (TTPs) or data elements like malicious file hashes or other signatures, as well as malicious domains or IP addresses, related to that malicious activity. These sorts of "indicators of compromise" (IOCs) are easily shareable between organizations.

  Today, contextual information is shared by law enforcement organizations, security vendors, and ISAC/ISAO organizations, but it's sometimes less actionable than proponents would hope. Too frequently, the lesson for defenders is that *everyone is attacking you all of the time*. This makes it difficult to adjust threat models and risk areas in response to new information.

  With respect to indicators, IOCs remain important to those defending against malicious activities, but it has become clear that they must be augmented by more subtle "Indicators of Attack" (IOAs). IOAs differ in that they characterize behaviors that, with enough specific reference cases, can be suggestive of malicious activity. For example, a

parent process spawns several child processes, one of which modifies a machine's registry, another of which writes code to disk. Depending on context, this could be part of a safe, normal, and expected business process--or a sign of a ransomware actor preparing an attack. Because of their subtle nature, IOAs are much less straightforward to share.[1]

- **Privacy**. Although various public-private information sharing arrangements include privacy commitments and/or liability protection for sharing information, it is clear that many private sector organizations maintain a cautious approach. In principle, most organizations have no concern with sharing, for example, indicators of malicious activity. In fact, they may even prefer that such information is shared with government entities. But many organizations prefer that such sharing be intermediated through a trusted third party, such as a security vendor, to reduce real or perceived issues about unauthorized disclosures, costly or disruptive follow-up engagements, and misperception about the impact of an indicator.

Information sharing is not necessarily an end goal in its own right--the point is stopping breaches and other malicious cyber activity. There is certainly a role for information sharing, but many of the technologies and strategies I detailed in my written testimony have been embraced by defenders to this end. Further, public and private sector organizations vary so widely in their roles, capacity, and security maturing that we should be skeptical of any one-size-fits-all approach to sharing.[2]

[From Senator Wyden]

3. **In your written testimony, you stated that the "threat actor took advantage of systemic weaknesses in the Windows authentication architecture," using the Golden SAML hacking technique. You also wrote that "this specific Golden SAML attack has been documented since 2017, in a sense it operates as a cloud-scale version of the Golden Ticket attack and similar identity-based attacks I originally wrote about back in 1999." Please detail your firm's efforts, prior to December 1, 2020, to:**
    a. **Urge Microsoft to fix the systemic weaknesses exploited by the Golden SAML technique;**

---

[1] Several additional complications arise with sharing IOAs. First, they may be particular to an organization's specific vantage point (e.g., endpoint solutions may provide a more textured view than, for example, perimeter solutions). Second, vendors within the same category may register IOAs, or the machine events that inform them, differently depending upon how they have instrumented the protected environment. Third, while most organizations are comfortable blocking activities based on IOCs from trusted partners (e.g., blocking traffic to and from a malicious domain), most IOA-based detections and preventions are probabilistic in nature, and organizations should use caution acting on IOAs from a different or untrusted source. Fourth, the rising abuse or misappropriation of commodity IT administration and common ecosystem tools means behaviors that are legitimate and expected in one environment may be malicious in another, and conveying that sort of detail across parties for the purpose of indicator sharing presents an operational challenge.

[2] We note a separate but related policy debate about cyber incident reporting, which this answer does not seek to address.

Since at least 2017, the Golden SAML technique has been well-known in the cybersecurity industry[3] and is the modern, cloud-scale version of authentication attacks rooted in the original Active Directory architecture. As noted in my testimony, I first wrote about Active Directory being used as an attack vector decades ago in the first edition of my book, Hacking Exposed. In subsequent editions, I addressed the threats posed by credential and token compromises, whereas an adversary's ability to obtain initial access enables them to leverage the inherent trust of Active Directory architecture to move laterally in an environment.

b. Warn your corporate and U.S. government customers about these systemic weaknesses and of the need to deploy additional defenses against the Golden SAML technique; and

Although CrowdStrike does operate a threat intelligence function that provides descriptive reports about, among other things, vulnerabilities and exploits, our primary means of delivering protection through our customers is by incorporating actionable detections into our software platform and real-time preventions according to each customer's preference. In so doing, we leverage findings from independent and industry research, threat intelligence collection, and incident response engagements.

Adversaries look to find vulnerabilities to exploit every day, and our focus is to provide technology that protects against threat actors exploiting vulnerabilities before they are known publicly. An example of this can be read in our blog which demonstrates the CrowdStrike Falcon Platform machine learning model, that was in use five months prior to the ostensible beginning of the *StellarParticle* campaign, was able to detect a malicious file leveraged by the threat actor and stop it with no prior knowledge.[4] Further, in December, CrowdStrike released a free tool to help organizations quickly and easily review excessive permissions in their Azure AD environments, help determine configuration weaknesses, and provide advice to mitigate risk.[5]

c. Protect your own IT systems from the Golden SAML technique.

While we cannot in this document disclose specifics about CrowdStrike's security architecture and controls, to include specific dates of implementation, CrowdStrike goes to great lengths to ensure the security of our internal and production environments, including our products. We reference certain aspects of our security program in a December blog post focused on software

---

3 https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps

4 https://www.crowdstrike.com/blog/stellar-performances-how-crowdstrike-machine-learning-handles-the-sunspot-malware/

5 https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/

supply chain issues.[6] Further, we use our own Falcon Platform, including Falcon Identity Protection, and hunt for threats proactively across our enterprise.

###

[6] https://www.crowdstrike.com/blog/crowdstrike-launches-free-tool-to-identify-and-help-mitigate-risks-in-azure-active-directory/.