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.