Prepared Testimony and
Statement for the Record of

Hugh Thompson
Chief Technology Officer

Hearing on

"Bolstering the Government's Cybersecurity: Lessons Learned from WannaCry"

Before the

United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight
and
Subcommittee on Research and Technology

June 15, 2017

Chairman Comstock, Ranking Member Lipinski, Chairman LaHood, Ranking Member Beyer, my name is Dr. Hugh Thompson and I am the Chief Technology Officer (CTO) at Symantec. As CTO of the largest cybersecurity company in the world, I report directly to our CEO and am responsible for Symantec's long-term cybersecurity technology strategy. I have more than 15 years of experience in the security information space and have worked with many of the world's largest organizations and agencies on methodologies to make their systems more secure systems. In addition, I have authored three books and written more than 80 academic and industrial publications on security. For the last eight years I have served as the program committee chairman for the RSA Conference, which is the world's largest information security conference that brings together over 40,000 security professionals across the globe. I hold a Ph.D. in applied mathematics from the Florida Institute of Technology and for many years served as an adjunct professor at Columbia University in New York.

Symantec Corporation is the world's leading cybersecurity company, and has the largest civilian threat collection network in the world. Our Global Intelligence Network monitors over 175 million endpoints located in over 157 countries and territories. Additionally, we process more than 2 billion emails and billions of web requests each day. We maintain nine Security Response Centers and six Security Operations Centers around the globe, and all of these resources combined give our analysts a unique view of the entire cyber threat landscape.

Understanding the current threat environment is essential if we are going to craft good policy and effective defenses. And no recent threat has challenged our collective defenses or is more representative of today's evolving threat more than the WannaCry Ransomware outbreak last month. We are therefore pleased to see the Committee's continued interest in this subject, and appreciate the opportunity to provide our insights.

I. The Current and Emerging Cyber Threat Landscape

Cyber attacks have reached new levels globally. Symantec recently released our 22nd Internet Security Threat Report,[1] which took an in-depth look at threats over the past year. In 2016 we saw explosive growth of ransomware, attempts to disrupt the US electoral process by state-sponsored groups, a record number of identities exposed in data breaches, and some of the biggest distributed denial of service (DDoS) attacks on record powered by a botnet of Internet of Things (IoT) devices. Yet while the attacks caused unprecedented levels of disruption and financial loss, perhaps the most striking feature of the current attack landscape is that in many cases attackers use very simple tools and tactics. During 2016, valuable Zero-day vulnerabilities and sophisticated malware was used more sparingly than in recent years. Instead, attackers increasingly attempted to hide in plain sight. They relied on straightforward approaches, such as spear-phishing emails and "living off the land" by using tools on hand, such as legitimate network administration software and operating system features. Yet despite this trend away from sophisticated attacks, the results were extraordinary, including:

- Over ***1.1 billion*** identities exposed;
- ***Power outages*** in the Ukraine;
- Over ***$800 million*** stolen through Business E-mail Compromise (BEC) scams over just a ***six month period***;
- ***$81 million*** stolen in one bank heist alone;
- A ***tripling*** of the average ransomware demand;
- Average time-to-attack for a newly connected Internet of Thing device down to ***two minutes***.

[1] See *Symantec Internet Security Threat Report*, XXII, April 2017

These shifting tactics demonstrate the resourcefulness of cyber criminals and attackers – but they also show that improved defenses and a concerted effort to address vulnerabilities can make a difference. Attackers are evolving and developing new attacks not because they want to, but because they have to do so. And that evolution comes with a financial cost to the attacker.

Ransomware continues to plague businesses and consumers, and due to its destructiveness is one of the most dangerous cybercrime threats we currently face. During 2016, criminal gangs engaged in indiscriminate campaigns involving massive volumes of malicious emails that in some cases overwhelmed organizations by the sheer volume of ransomware-laden emails alone. Attackers are demanding more and more from victims, and the average ransom demand *more than tripled* in 2016, from $294 to $1,077. The number of new ransomware families also more than tripled to 101, from 30 in both 2014 and 2015. The volume of attacks increased as well. Detections were up 36% percent from 2015, and by December we were seeing almost twice the daily volume that we observed in January.

We are also seeing the emergence of Ransomware-as-a-Service (RaaS). This involves malware developers creating ransomware kits, which can be used easily to create and customize new variants. Typically the developers provide the kits to attackers for a percentage of the proceeds. One example of RaaS is Shark (Ransom.SharkRaaS), which is distributed through its own website and allows users to customize the ransom amount and which files it encrypts. Payment is automated and sent directly to Shark's creators, who retain 20 percent and send the remainder on to the attackers. Our statistics show that, for the most part, attackers are concentrating their attacks on countries with developed, stable economies – 34% of the detections were in the US, and another 39% spread among the United Kingdom, Australia, Germany, Russia, the Netherlands, Canada, India, and Italy.

The world of cyber espionage experienced a notable shift towards more overt activity in 2016, much of which was designed to destabilize and disrupt targeted organizations and countries. We saw:

- a January 2016 attack against the Ukrainian power grid;
- an attack on the World Anti-Doping Agency and subsequent release of test results;
- a widespread, destructive attack on computers in Saudi Arabia; and
- a second attack against the Ukrainian power grid in December of 2016.

In years past, any one of these events would have been the biggest story of the year. But in 2016, we also saw an attack on the US Presidential election, an operation that the Intelligence Community (IC) attributed to Russia. Cyber attacks involving sabotage have traditionally been rare, but 2016 saw two separate waves of attacks involving destructive malware. Disk-wiping malware was used against targets in the attacks on the Ukraine in January and again in December, resulting in power outages. Additionally, a disk-wiping trojan known as Shamoon reappeared after a four-year absence and was used against multiple organizations in Saudi Arabia. Previously, Shamoon was used in highly destructive attacks against Saudi and other Middle Eastern energy companies, and press reports linked it to Iran.

In 2016, cyber criminals expanded their focus from individual bank customers to the banks themselves, sometimes attempting to steal tens of millions of dollars in a single attack. Two groups targeted the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network and stole SWIFT credentials. They used those credentials to initiate fraudulent transactions and covered their tracks by doctoring the banks' printed confirmation messages to delay discovery of the transfers. One group began its attack at the start of a long weekend to reduce the likelihood of a quick discovery.

And while ransomware and financial fraud groups continue to pose the biggest threat to end users, other threats are beginning to emerge. It was only a matter of time before attacks on IoT devices began to gain momentum, and during 2016 Symantec witnessed a twofold increase in attempted attacks against IoT devices. 2016 also saw the first major incident originating from IoT devices, the Mirai botnet, which was composed of routers, digital video cameras, and security cameras. Weak security – in the form of default and hard-coded passwords – made these devices easy pickings for attackers. After compromising millions of devices, the attackers controlled a botnet big enough to carry out the largest DDoS attacks ever seen. In October, the combined power of these compromised devices led to brief outages at some of the most popular websites and online services in the world. Mirai's impact was further magnified when the developer released the source code for the malware, which led to copycat efforts by other groups.

II. WannaCry Outbreak

The WannaCry ransomware outbreak began on Friday, May 12, 2017, and within hours it disrupted Britain's National Health Service (NHS) and Spanish telecom provider Telefonica. After a day, it had infected more than 230,000 computers in over 150 countries. At that point the infection rate plummeted, largely through good luck – a security researcher in the United Kingdom had unknowingly triggered a kill switch when he registered a domain name he found within the code of the ransomware. This prevented the worm from moving laterally, greatly slowing the spread of the infection and effectively halting the initial outbreak over the weekend. Still, over the course of three days (May 12-15), Symantec blocked WannaCry more than 22 million times on more than 300,000 devices. We were able to prevent WannaCry infections because we implemented protections for the underlying vulnerability in April (*See* Attachment for a complete timeline of WannaCry).

WannaCry was unique and dangerous because of how quickly it could spread. It is the first ransomware-as-a-worm that has had scaled global impact; once on a system it propagated autonomously using the Eternal Blue vulnerability in the Windows Server Messaging Block (SMB) protocol. After gaining access to a computer, WannaCry installs a backdoor implant tool called DoublePulsar which transfers and runs the WannaCry ransomware package. The payload works in the same fashion as most modern crypto-ransomware: it finds and encrypts a range of files, then displays a "ransom note" demanding a payment in bitcoin ($300 first week; $600 second week).

WannaCry spread to unpatched computers. Microsoft released a patch for the SMB vulnerability for Windows 7 and newer operating systems in March, but unpatched systems and systems running XP or older operating systems were unprotected. After the WannaCry outbreak began, Microsoft released a patch for XP and earlier platforms. Four days after the initial outbreak these patches were widely applied and new infections slowed to a trickle.

The US government reacted quickly to the outbreak. DHS's National Cybersecurity and Communications Integration Center (NCCIC) held twice daily calls with the private sector to coordinate operational activities. We participated, as did more than a dozen security and IT companies. During these calls, DHS representatives and the private sector shared Indicators of Compromise (IoCs), mitigation techniques, and information on threat vectors. In addition, the NCCIC distributed written analysis on the attack.

Symantec worked closely with the US government from the first hours of the outbreak. We connected DHS researchers with our experts, provided IoCs and analysis to DHS, and received the same from DHS. After the infection waned, we continued our partnership, sharing details about the Lazarus connections (detailed below) that that we were finding. From our perspective, this was one of the most successful public/private incident response efforts in which we have participated.

III. Origins of WannaCry

Tools and infrastructure used in the WannaCry ransomware attacks have strong links to Lazarus, the group that was linked to the destructive attacks on Sony Pictures and the theft of $81 million from the

Bangladesh Central Bank. Our researchers discovered that prior to the global outbreak on May 12, an earlier version of WannaCry was used in a small number of targeted attacks in February, March, and April. These earlier versions of WannaCry used stolen credentials to spread across infected networks, rather than leveraging the Eternal Blue/SMB exploit that caused WannaCry to spread quickly across the globe starting on May 12. Our analysis of these early WannaCry attacks revealed substantial commonalities in the tools, techniques, and infrastructure used by the attackers and those seen in previous Lazarus attacks. This included shared code, reuse of IP addresses, and similar code obfuscation. Thus we believe it is highly likely that the Lazarus group was behind the spread of WannaCry. We do note, however, that the WannaCry attacks are in many ways more typical of a cyber crime campaign than they are of nation-state activity.

IV. Public Private Partnerships

We partner with the US government, and governments around the world, in the fight against cybercrime and cyber attacks. The US Department of Homeland Security works with the private sector through a variety of programs, and has made considerable progress in recent years engaging with industry, especially in the area of information sharing. As noted above, the coordination between government and the private sector was on display during the response to WannaCry.

Some partnership programs are formal, such as the Cyber Information Sharing and Collaboration Program (CISCP). This is DHS's primary structure for private companies to share information about incidents, cyber threats and known vulnerabilities. For example, last October, we used the CISCP program to share a report we published that exposed one of the groups that was trying to steal money from banks by exploiting the SWIFT messaging system. Through CISCP, we passed along our in-depth, technical research to CISCP managers along with a list of indicators including hashes, command and control nodes, and domains. The CISCP team then used our indicators to create an Indicator Bulletin (IB) and pushed it out to all CISCP participants for their use.

In addition to the Department's formal programs, we work with DHS informally. For instance, earlier this year we hosted a group of ten cyber threat analysts at our Herndon Security Operations Center to discuss specific threats and to explore potential areas to coordinate in the future. Among other topics, we discussed Shamoon, a family of destructive malware that we have tracked for years. Shamoon was used in attacks against the Saudi energy sector in 2012 and last year we tracked a fresh wave of attacks hitting the Middle East. The opportunity to sit face-to-face and discuss threats often alleviates a chief concern among many private sector security companies, that too often the information flows just one way – from industry to the government. In-person exchanges often lead to a more complete and bilateral interchange of ideas.

Partnerships can lead to concrete results. One recent example came in December 2016, when Symantec concluded a decade-long research campaign that helped unearth an international cybercriminal gang dubbed "Bayrob." The group is responsible for stealing up to $35 million from victims through auto auction scams, credit card fraud and computer intrusions. Through our research, we discovered multiple versions of Bayrob malware, collected voluminous intelligence data, and tracked Bayrob as it morphed from online fraud to a botnet consisting of over 300,000 computers used primarily for cryptocurrency mining. Over time, Symantec's research team gained deep technical insight into Bayrob's operations and its malicious activities, including its recruitment of money mules. These investigations and countermeasures were crucial in assisting the Federal Bureau of Investigation (FBI) and authorities in Romania in building their case to arrest three of Bayrob's key actors and extradite them to the U.S. They are currently in federal custody awaiting trial.

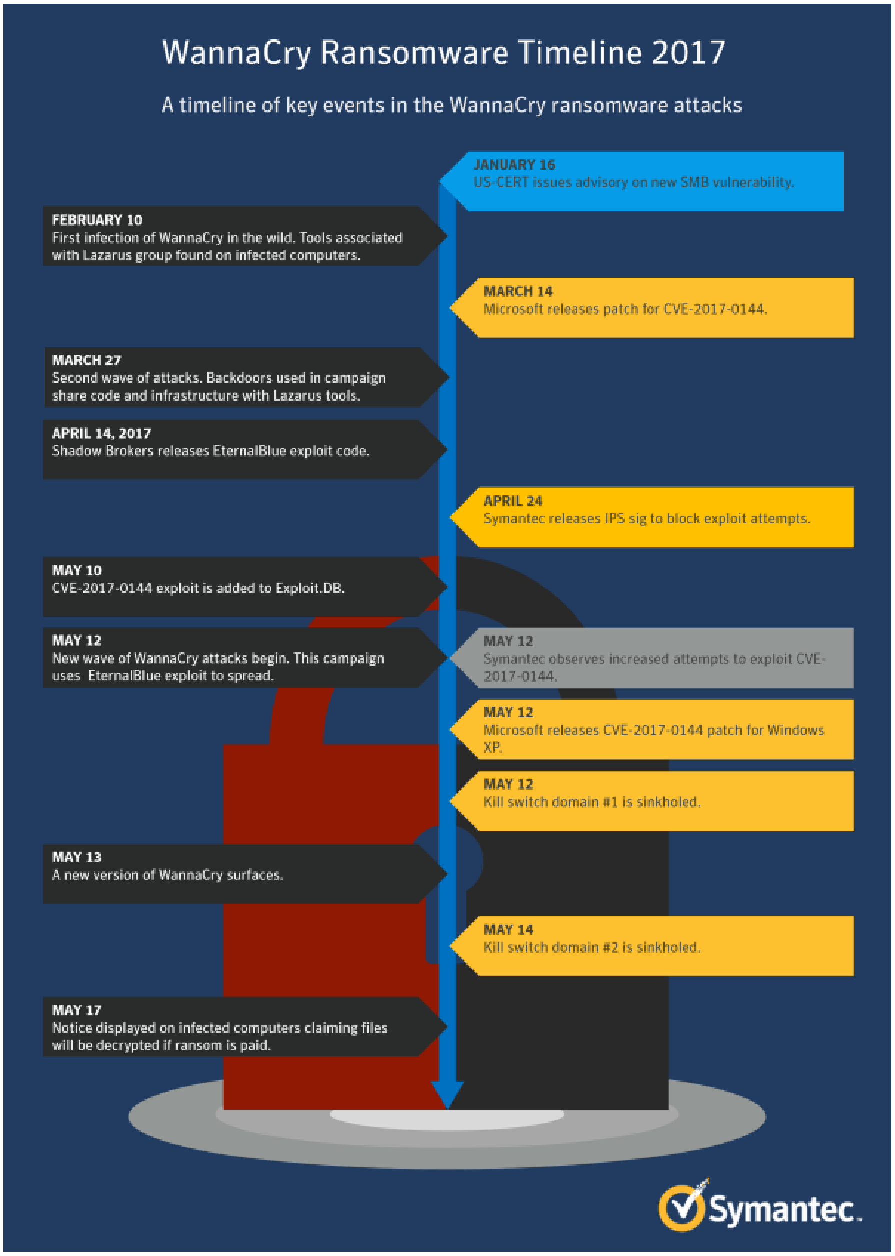
The private sector is also working together to counter cybercrime and industry partnerships have proven highly effective in fighting cybercrime. The Cyber Threat Alliance (CTA) is an excellent example of the private sector banding together to improve the overall safety and security of the Internet. In 2014, Symantec, Fortinet, Intel Security, and Palo Alto Networks formed the CTA to work together to share threat information. Since that time, Cisco and Checkpoint have joined the CTA as founding members. The goal of the CTA is to better distribute detailed information about advanced attacks and thereby raise the situational awareness of CTA members and improve overall protection for our customers.

Prior industry sharing efforts were often limited to the exchange of malware samples, and the CTA sought to change that. Over the past three years the CTA has consistently shared more actionable threat intelligence such as information on “zero day” vulnerabilities, command and control server information, mobile threats, and indicators of compromise related to advanced threats. By raising the industry's collective intelligence through these new data exchanges, CTA members have delivered greater security for individual customers and organizations.

Conclusion

WannaCry was an important event – but it will not be the last of its kind. Thankfully, the outbreak was stopped before it caused major global damage, but this was as much through good fortune as it was through what was a largely effective response. Learning the lessons of WannaCry and improving our ability to respond is essential, because the next attack is coming. We are pleased to help the Committee in doing so, and this hearing is an important part of that effort.

Attachment:



WannaCry Ransomware Timeline 2017

A timeline of key events in the WannaCry ransomware attacks

JANUARY 16
US-CERT issues advisory on new SMB vulnerability.

FEBRUARY 10
First infection of WannaCry in the wild. Tools associated with Lazarus group found on infected computers.

MARCH 14
Microsoft releases patch for CVE-2017-0144.

MARCH 27
Second wave of attacks. Backdoors used in campaign share code and infrastructure with Lazarus tools.

APRIL 14, 2017
Shadow Brokers releases EternalBlue exploit code.

APRIL 24
Symantec releases IPS sig to block exploit attempts.

MAY 10
CVE-2017-0144 exploit is added to Exploit.DB.

MAY 12
New wave of WannaCry attacks begin. This campaign uses EternalBlue exploit to spread.

MAY 12
Symantec observes increased attempts to exploit CVE-2017-0144.

MAY 12
Microsoft releases CVE-2017-0144 patch for Windows XP.

MAY 12
Kill switch domain #1 is sinkholed.

MAY 13
A new version of WannaCry surfaces.

MAY 14
Kill switch domain #2 is sinkholed.

MAY 17
Notice displayed on infected computers claiming files will be decrypted if ransom is paid.

Symantec.