Prepared Testimony and
Statement for the Record of

Jeff Greene
Senior Director, Global Government Affairs & Policy
Symantec Corporation

Hearing on

"Empty Threat or Serious Danger: Assessing North Korea's Risk to the Homeland"

Before the

United States House of Representatives
Committee on Homeland Security
Subcommittee on Oversight and Management Efficiency

October 12, 2017

Chairman Perry, Chairman McCaul, Ranking Member Correa, Ranking Member Thompson, my name is Jeff Greene and I am the Senior Director, Global Government Affairs and Policy at Symantec. I am responsible for Symantec's global public policy agenda and government engagement strategy, and represent the company in key public policy initiatives and partnerships. I also serve as a member of the National Institute of Standards and Technology's (NIST) Information Security and Privacy Advisory Board (ISPAB), and recently supported the President's Commission on Enhancing National Cybersecurity. I have worked on the House and Senate Homeland Security Committees, and immediately prior to joining Symantec I served as Senior Counsel with the Senate committee focusing on cybersecurity and Homeland Defense issues.

Symantec Corporation is the world's leading cybersecurity company, and has the largest civilian threat collection network in the world. Our Global Intelligence Network™ tracks over 700,000 global adversaries and is comprised of more than 98 million attack sensors, which record thousands of events every second. This network monitors over 175 million endpoints located in over 157 countries and territories. Additionally, we process more than 2 billion emails and over 2.4 billion 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.

Symantec has been tracking the Lazarus group for over five years, and we have watched as their targets have evolved and their technical skills have improved. Over the years we have linked numerous attacks to Lazarus, including the attack on Sony Pictures, the Bangladesh Central bank heist, and the recent WannaCry ransomware outbreak. The United States government has publicly attributed the attack on Sony to the Democratic People's Republic of Korea.

In my testimony I will provide an assessment of the Lazarus group's technical capabilities and provide an overview of several attacks that we have connected to them. As an initial matter, however, I want to offer a few high-level observations on Lazarus:

- First, their attacks are unusual both in the breadth of their targets and the goals of their attacks.
- Second, Lazarus shows little hesitation to engage in activity that might give other attack groups pause.
- Finally, Lazarus targets a variety of disparate sectors, many simultaneously, and is very quick to move from target to target.

Lazarus' technical capabilities have improved dramatically in recent years, and we now view them as above-average in overall skills, and expert in some areas. In particular, Lazarus has shown excellent skills when conducting reconnaissance and researching operations, and over the past three to four years the quality of the malware they are producing has increased dramatically. Higher quality malware is harder to detect, and this coupled with Lazarus' improving operational security steps could make it harder to connect future attacks with the group. The group is also a prolific developer of malware – while other highly sophisticated attack groups have a tendency to rely on a single malware family for a sustained campaign, Lazarus is more likely to use a unique (but less complex) piece of malware for each effort without concern for it being discovered within a shorter timeframe so long as they achieve a specific end.

In other areas, Lazarus has shown a lack of overall ability that has at time hampered its ability to complete an operation successfully. Specifically, the WannaCry attacks yielded no apparent financial gain because the collection component was not set up properly, and the attack on the Bangladesh Central Bank was discovered and halted due to a typographical error. Unfortunately, these are relatively

simple errors to correct and given Lazarus' ability to adapt and improve in recent years they are unlikely to repeat them in future operations.

Lazarus has been connected to attacks on a wide variety of sectors – from the entertainment industry to critical infrastructure to government systems to the financial sector. And unlike other groups that have been publicly connected to nation states, Lazarus has attacked individual end-users of the internet. Lazarus' methods have also run the gamut, and include denial of service attacks, highly targeted (and highly sophisticated) intrusions, destructive attacks, and the use of ransomware. Below I will address three specific campaigns.

Bangladesh Central Bank Theft

In early 2016, Lazarus stole $81 million from Bangladesh's central bank – and but for a typographical error might have made off with as much as $1 billion. They exploited weaknesses in the bank's security to infiltrate its network and steal its Society for Worldwide Interbank Financial Telecommunication (SWIFT) credentials, allowing them to initiate fraudulent transfers (it is important to recognize that SWIFT itself was not compromised; the attackers used stolen credentials to initiate fraudulent transactions).

This was a well-planned, sophisticated attack: in order to cover their tracks, the attackers used malware to doctor the bank's printed confirmation messages to delay discovery of the transfers. They also began their attack at the start of a long weekend to reduce further the likelihood of a quick discovery. Once they obtained the bank's SWIFT credentials, the group made several transfer requests to the Federal Reserve Bank of New York for it to transfer the Bangladesh bank's money, primarily to locations in the Philippines and Sri Lanka. Four requests to transfer a total of $81 million to entities in the Philippines went through, but a request to transfer $20 million to a non-profit "foundation" in Sri Lanka raised suspicions because foundation's name was spelled incorrectly.

The transfers were suspended and the fraud was uncovered when the Bangladeshi bank was asked for clarification on the Sri Lankan transfer. By then $81 million had been transferred, primarily into accounts related to casinos in the Philippines. One casino returned $15 million to Bangladesh, but the rest had disappeared. The methods used in this attack – in particular the in-depth knowledge of the SWIFT systems and the steps taken to cover tracks – evidence Lazarus' growing technical skills.

Our analysis of this attack found code sharing between the malware and other unique tools used by Lazarus in other attacks, including some in the financial sector. Additionally, some of the tools used in the attack are connected to Lazarus. We have also seen this malware deployed against banks in the Philippines and Vietnam.

WannaCry Ransomware

Though the WannaCry outbreak became a global story on May 12, 2017, our analysis has revealed that an almost identical version of the ransomware was used in a small number of targeted attacks in February, March, and April of the same year. The key difference between the earlier versions of WannaCry and the one that became a global event was the method of propagation – the early version used stolen credentials to move through infected networks, while the May 12 version included the ability to self-propagate (known as a "worm") that led to its rapid spread.

In fact, within hours of the first detection, the May 12 version disrupted Britain's National Health Service 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, effectively halting the initial outbreak and preventing it from becoming a significant event in the United States. Still, over the course of three days (May 12-15), we blocked WannaCry more than 22 million times on more than 300,000 devices. We were able to prevent WannaCry infections because we had already implemented protections for the underlying vulnerability.

The May version of WannaCry was unique and dangerous because of how quickly it could spread. It was the first ransomware-as-a-worm that has had 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 ransomware package that 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 (in this case, $300 the first week; $600 the second week).

WannaCry spread largely to unpatched computers. Though Microsoft released a patch for the SMB vulnerability for Windows 7 and newer operating systems in March, 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.

The May version of WannaCry was very effective at infecting computers and encrypting the data on them, but it also contained flaws that prevented the authors from collecting their ransom. Specifically, the ransomware was not coded correctly to allow the attackers to collect bitcoin payment from thousands of victims. Interestingly, the authors quickly recognized their error and released a corrected version 13 hours after the outbreak began, but that version did not spread widely before the infection was largely halted.

Our analysis found numerous links between WannaCry and known Lazarus operations. The ransomware shares some code with previous malware used by Lazarus as well as some custom tools connected to the group. Additionally, we found three pieces of malware linked to Lazarus on the network of the target of the very first WannaCry attack in February, at least one of which was used in the Sony Pictures attacks.

Sony Pictures Entertainment

In 2014, Sony was preparing for the holiday release of "The Interview", a film depicting the fictional assassination of North Korean leader Kim Jong-un. On November 24, Sony experienced a cyberattack that disabled its information technology network, destroyed data, and stole emails that were then leaked to the public in an effort to embarrass company officials.

Individuals claiming to be the hackers then sent emails threatening "9/11-style" terrorist attacks on theaters scheduled to show the film, leading some theaters to cancel screenings and for Sony to cancel its widespread release. Much of the media and public attention revolved around the free speech implications of the attack, as well as the release of salacious emails between Hollywood executives and celebrities as well as the salaries paid to different movie stars. But from a cybersecurity standpoint, the "big" story of the attacks was the permanent destruction of computers and data – by one report, impacting as much as three quarters of the computers and servers at Sony Pictures headquarters. Many were damaged by "wiper" malware known as "Destover," a particularly destructive variant which erased all the data on the machines, damaging them beyond repair.[1] The attacks reportedly had cascading effects that went well beyond the computers themselves — hampering essential administrative functions like employee payroll, insurance, and contracts. The destructive element of the Sony attack is what sets it apart from most cyberattacks.

[1] https://www.symantec.com/connect/blog/collaborative-operation-blockbuster-lazarus

On December 19, the FBI and the Director of National Intelligence (DNI) attributed the cyberattacks to the North Korean government based on a number of factors, including technical analysis on the wiper malware which included similar codes, encryption algorithms, and deletion methods to previous attacks linked to the North Korean government. Further, the FBI observed significant overlap in the infrastructure used to conduct the Sony attack and previously known North Korean command and control infrastructure. Lastly, many of the tools and tactics used in the Sony attack had similarities to a cyber attack in March of 2013 against South Korean banks and media outlets, which was carried out by North Korea.[2]

Conclusion

Lazarus is an aggressive and increasingly sophisticated attack group that has a demonstrated willingness to disrupt networks, steal money, and destroy computers and data. They learn from their mistakes and move rapidly from target to target. Unlike other major attack groups which typically focus on one sector or even one industry, Lazarus has no shown such limitations. This means that all industries and sectors, and all governments, have to assume that Lazarus may target them, and must prepare accordingly. Symantec continues to monitor Lazarus' activities and will continue to share information with our government partners as well as publish reports of the activity we observe. Thank you for the opportunity to testify, and I would be happy to take any questions that you may have.

[2] FBI National Press Office, "Update on Sony Investigation," December 19, 2014 https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation