Prepared Testimony and
Statement for the Record of

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

Hearing on

"Cyber Threats Facing America: An Overview of the Cybersecurity Threat Landscape"

Before the

United States Senate
Committee on Homeland Security and Governmental Affairs

May 10, 2017

Chairman Johnson, Ranking Member McCaskill, 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. Prior to joining Symantec, I served as Senior Counsel with the U.S. Senate Homeland Security and Governmental Affairs Committee, where I focused 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.

Understanding the current threat environment is essential if we are going to craft good policy and effective defenses. We are therefore pleased to see the Committee's continued focus on this subject, and appreciate the opportunity to provide our insights.

I. The Current and Emerging Cyber Threat Landscape - Overview

Cyber attacks reached new levels in 2016, a year marked by multi-million dollar virtual bank heists, 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 2016 attack landscape is that in many cases the attackers used 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***.

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.[1]

[1] *Symantec Internet Security Threat Report* XXII, April 2017 http://www.symantec.com/security_response/publications/threatreport.jsp (Pages 8-10)

II. Targeted Attacks: Subversion and Sabotage Come to the Fore

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

- a January 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.

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. The IC also concluded that the campaign was likely judged a success by its perpetrators, making it likely that these tactics will be reused to influence politics and sow discord in other countries. Indeed, recent public reporting suggests that similar operations may be underway in France and elsewhere in Europe, and just last week FBI Director James Comey said that he expects to see similar attacks in the US before the 2018 mid-term and 2020 Presidential elections.

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, the disk-wiping Trojan 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.

Interestingly, the upsurge in disruptive attacks coincided with a decline or shift in some covert activity, specifically economic espionage, the theft of intellectual property, and trade secrets. Following a 2015 agreement between the US and China, which saw both countries promise not to conduct economic espionage in cyber space, detections of malware linked to suspected Chinese espionage groups dropped considerably. However, we did see some actors who had previously focused on economic espionage shift their focus to what appeared to be more politically motivated targets. Economic espionage did not disappear entirely, and we are constantly looking for indications of a resurgence in economically motivated theft of data.

III. Financial heists: Cyber Attackers Chase the Big Scores

Until recently, cyber criminals mainly targeted on individual bank customers, raiding accounts or stealing credit cards. That changed dramatically in 2016, and we saw a new breed of attacker with bigger ambitions. These groups targeted the banks themselves, sometimes attempting to steal tens of millions of dollars in a single attack. Gangs such as Carbanak have led the way, demonstrating the potential of this approach by pulling off a string of attacks against US banks. Over the past few years Carbanak appears to have targeted hundreds of banks in multiple countries.

During 2016, two other outfits upped the ante by launching even more ambitious attacks. The Banswift group managed to steal $81 million from Bangladesh's central bank by exploiting weaknesses in the bank's security to infiltrate its network and steal its Society for Worldwide Interbank Financial Telecommunication (SWIFT) credentials. It is important to recognize that SWIFT itself was not compromised; the attackers used stolen credentials to initiate fraudulent transactions. In order to cover their tracks, the attackers doctored 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. And while the attackers did make off with $81 million, it could have been much worse as they attempted numerous other transfers that were detected because a spelling error in a recipient's name raised suspicions that led to the transactions being suspended.

Another group, known as Odinaff, also targeted users of SWIFT during 2016. Odinaff's efforts were focused on organizations in the banking, securities, trading, and payroll sectors and like Banswift, the attacks appeared to use malware to hide customers' own records of SWIFT messages relating to the fraudulent transactions. These attacks were highly methodical and sophisticated and required a lot of hands-on involvement. We did not find any evidence linking Odinaff and Banswift.[2]

While Banswift and Odinaff demonstrated some technical expertise and employed tactics associated with advanced groups, much less sophisticated groups also stole massive sums of money. Business email compromise (BEC) scams, which rely on little more than carefully composed spear-phishing emails, continue to cause major losses. Also known as CEO fraud or "whaling," BEC scams are a form of low-tech financial fraud where spoofed emails are sent to an organization's financial staff by scammers pretending to be the CEO or senior management. The scammers then request a large money transfer. Our research found that during the first half of 2016, more than 400 businesses were targeted by BEC scams *every day.* More recently, we observed a new technique – the "hijacking" of legitimate invoices sent by companies so that the account number is changed to that of the scammer.

These scams require little technical expertise but can reap huge financial rewards for the criminals – and significant losses for the companies involved. For example, early in 2016, an Austrian aerospace company fired its CEO after it lost almost $50 million to BEC scammers. And just last week the FBI issued an alert noting that "[b]etween January 2015 and December 2016, there was a 2,370% increase in identified exposed losses" from BEC scams. The FBI estimated that over $5 billion was lost to BEC scams between October, 2013 and December, 2016.[3]

IV. Living Off the Land

Attackers ranging from cyber criminals to state-sponsored groups have begun to change their tactics, making more use of operating system features, off-the-shelf tools, and cloud services to compromise their victims. We call this "living off the land" – making use of the resources at hand rather than malware and exploits – and it provides many advantages to attackers. As a start, identifying and exploiting zero days has become harder as improvements in secure development and bounty programs take hold. Similarly, the use of web attack toolkits dropped, likely due to the effort required in maintaining fresh exploits as well as a backend infrastructure. These shifts could also be an effort to preserve resources – zero days are expensive to find (or to purchase on the black market), and developing new exploits requires an investment in research and development that cuts into a criminal's profit. Finally, "living off the land" attacks are at times harder to detect, as recognizing the malicious use of a legitimate tool can be more complex than identifying malware.

The tools used in these attacks are widely used – completely appropriately. Many are default features of Windows and Microsoft Office, and provide functionality to users and system administrators. But under the control of a criminal, they can facilitate remote access and malware downloads without the use of vulnerabilities or malicious tools. That these tools can be misused is not news; Microsoft Office macros have existed for almost 20 years, and were a common attack vector in the past. For that reason, the overwhelming majority of users have macros disabled by default. 2016 saw the emergence of social

[2] See *Symantec Internet Security Threat Report*, XXII, April 2017 pp. 48

[3] FBI Public Service Announcement, *Business E-mail Compromise – E-mail Account Compromise the 5 Billion Dollar Scam, May 4, 2017;* https://www.ic3.gov/media/2017/170504.aspx#fn3

engineering techniques aimed at tricking users into enabling those macros – and thus opening the door to macro viruses.

The most high-profile case of a "living off the land" attack took place during the US elections – a simple spear-phishing email led to the theft of Hillary Clinton's campaign chairman's emails. This took place *without the use of any malware or exploitation of hardware or software vulnerabilities*. When executed well, these "living off the land" approaches can result in almost symptomless infections, allowing attackers to hide in plain sight.

V. Resurgence of Email as Favored Attack Channel

Malicious emails were the weapon of choice for a wide range of cyber attacks during 2016, used by everyone from state-sponsored cyber espionage groups to mass-mailing ransomware gangs. One in 131 emails sent were malicious, the highest rate in five years.[4] Email's renewed popularity has been driven by several factors – it is a proven attack channel and is not reliant on technical vulnerabilities, but instead uses deception to trick victims into opening attachments, following links, or disclosing their credentials. Malicious emails disguised as routine correspondence, such as invoices or delivery notifications, were the favored means of spreading ransomware. The availability of botnets-for-hire allows criminals to mount massive campaigns pumping out hundreds of thousands of emails daily.[5]

VI. Ransomware Squeezing Victims with Escalating Demands

Ransomware continues to plague businesses and consumers, and due to its destructiveness is one of the most dangerous cybercrime threats we saw in 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.

2016 also saw 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, Italy, and Japan.

VII. New frontiers: IoT Moves into the Spotlight

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

[4] See *Symantec Internet Security Threat Report*, XXII, April 2017 pp. 27-28 (https://www.symantec.com/security-center/threat-report)

[5] *See* Attachment for a compilation of recent prices from the black market to rent botnets, purchase ransomware kits, and buy stolen identities and credit card details. *Symantec Internet Security Threat Report, XXII, April 2017, pp. 51.*

gain momentum, and during 2016 Symantec witnessed a twofold increase in attempted attacks against IoT devices. During peak activity the average IoT device was attacked once every two minutes.

2016 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.[6]

VIII. Successful Disruptions of Cybercriminals

Investigating and prosecuting cybercrime is technically complex, and requires a level of expertise and training that many police agencies and prosecutors are just now beginning to develop. It is also resource intensive – the time and money required to see a case from inception through to a successful conviction is often substantial. The criminals know this, and indeed often count on it. Yet despite these obstacles, law enforcement and the private sector – working together – have made significant progress over the last year and conducted several successful takedowns of prominent cybercrime gangs.

Perhaps the most notable success of 2016 was the arrest and extradition of three Romanian nationals who ran the Bayrob gang. This was the culmination of an eight-year FBI investigation, which we assisted throughout that time. Symantec first exposed Bayrob in 2007, detailing a highly sophisticated eBay scam involving fake auto sales. Despite this public attention the gang continued its criminal activities, carrying out more online auction fraud, as well as diversifying into credit card fraud and recruiting a network of money mules in the US and Europe in order to move nearly $35 million back to Romania. Later, the group turned its attention to building a botnet for cryptocurrency mining, which eventually grew to more than 300,000 computers. On December 16, 2016, the three were indicted in the U.S. District Court in the Northern District of Ohio and are currently in federal custody awaiting trial.[7]

Another major takedown occurred in June 2016 when Russian security forces cracked down on the Lurk group, arresting 50 people in Moscow. The Lurk banking Trojan had targeted Russian financial institutions, stealing more than $25 million. These arrests coincided with a drop in activity from a number of threat groups that focused on financial fraud, including Locky, Dridex, and the Angler exploit kit. Since the Lurk arrests, Angler has disappeared from the threat landscape.

Lastly, the Avalanche botnet takedown dealt a severe blow to cybercriminals across the world. The takedown was a combined effort by multiple international law enforcement agencies and IT organizations, including Symantec. It resulted in the arrest of five individuals and the seizure of 39 servers and several hundred thousand domains, which served as the command and control hub for more than 800,000 compromised computers across the world.

While cybercrime continues to be profitable, the number of significant takedowns and disruptions in 2016 demonstrated that it is no longer a risk-free enterprise. In particular the extradition of the alleged Bayrob masterminds from Eastern Europe to the US sent a strong message that cybercriminals cannot work with impunity from remote locales.

[6] See *Symantec Internet Security Threat Report*, XX!!, April 2017 pp. 68

[7] https://www.justice.gov/usao-ndoh/pr/three-romanian-nationals-indicted-cyber-fraud-case-which-they-infected-60000-computers

IX. Protecting Against an Evolving Threat

Attacks are getting more sophisticated, but so too are security tools. Security still starts with basic measures such as strong passwords and up-to-date patch management. But while these steps may stop some older, simpler exploits, they will be little more than a speed bump for even a moderately sophisticated attack – and will do little to slow a determined, targeted attack.

Effective protection requires a modern security suite that is being fully utilized. An attack requires access, and attackers are increasingly relying on stolen credentials to gain their footholds. Deploying effective multi-factor authentication is essential to denying access to the would-be attacker. To block advanced threats and zero day attacks, sophisticated machine learning and advanced exploit detection and prevention technologies are necessary. This includes tools for detecting encrypted malware, as attackers are increasingly using encryption in an effort to bypass common security tools. Automated security tools learn how to identify attacks, even ones that have never been seen before. It is also increasingly critical to use big data analytics to evaluate global software patterns to create real-time intelligence. Today these analytics are able to identify and block entirely new attacks by evaluating how they are distributed and their relationships with other devices and other files.

Data protection is equally important, and a comprehensive security program includes data loss prevention (DLP) tools that index, track, and control the access to and movement of huge volumes of data across an organization. Perhaps most importantly, DLP tools will prevent that data from moving outside an organization. Organizations should also use encryption technology on particularly sensitive data, which renders it unreadable to anyone who does not have the specific cryptologic key.

Device-specific protections are also important. For example, in the retail world, there are tools that can be applied to point of sale systems that will virtually lock down the system and only allow it to perform those limited functions that are absolutely necessary for completing a sales transaction. In the IoT world, there are authentication, encryption, and endpoint protection tools that are designed to run on small and low power devices. These tools can protect everything from a connected vehicle to the small sensors built into a bridge or that monitor critical machinery. Finally, for the IoT devices that simply cannot be secured – either because they lack the power to run security tools or because it is simply unavailable – we developed Norton Core™, the first router designed specifically to secure IoT devices, whether a connected appliance or a digital video recorder.[8]

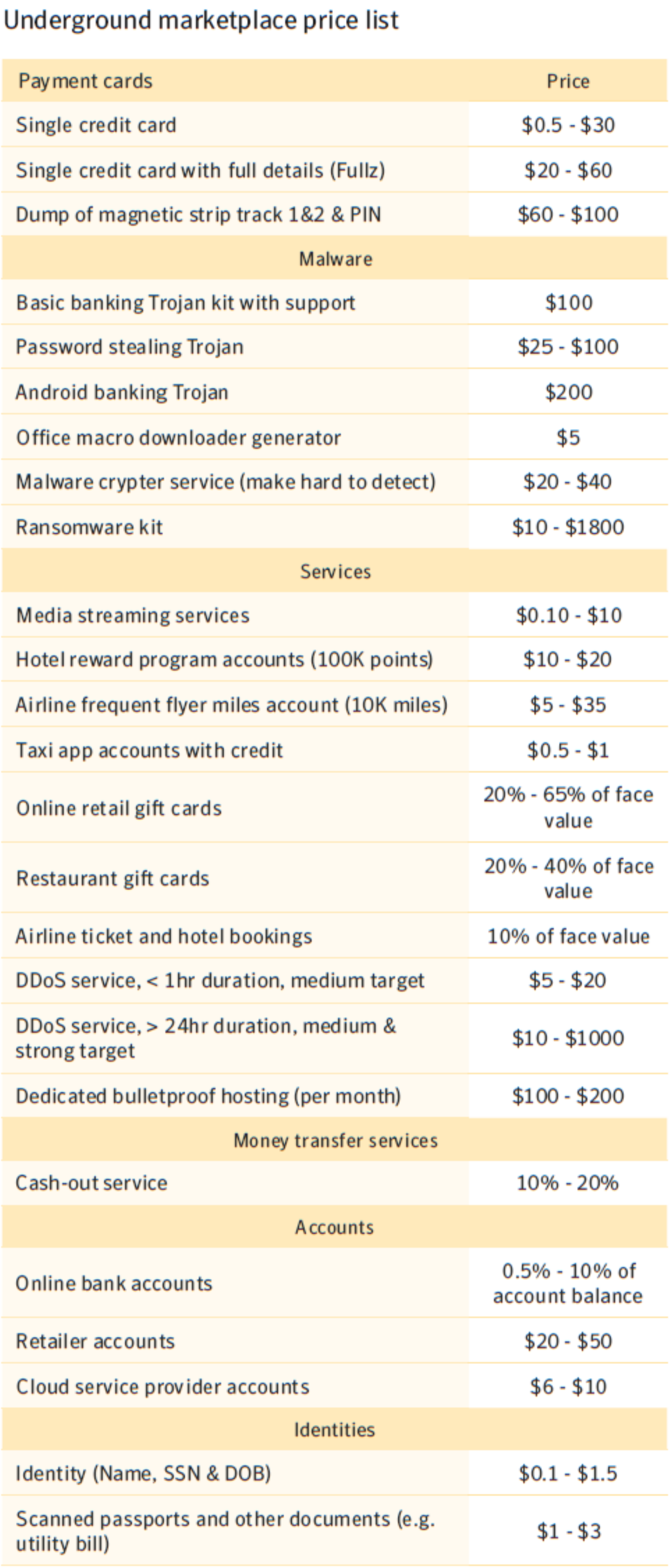
Good security does not happen by accident – it requires planning and continued attention. But criminals will always be evolving, and security must as well.

Conclusion

With the growth of connected devices – from the health trackers we carry in our pockets to the industrial systems that we unknowingly rely on in our daily lives – computer security is now everything security. In 2016, the attacks on the power grid in the Ukraine, as well as the attacks on the US election, drove home this point. But even as attacks morph and improve, so too do defenses, whether technical or through increased awareness. So while it is true that attackers were able to come up with new attack methods that challenged defenders, it is equally true that developing those attacks cost the criminals time, resources, and money. Cybersecurity is the proverbial journey, not a destination. Understanding the threat, how it is changing, and where it is going, is essential if we are going to stay on track in this journey. This hearing is an important step in advancing that understanding.

[8] *See https://us.norton.com/core*

Attachment



Underground marketplace price list

Payment cards	Price
Single credit card	$0.5 - $30
Single credit card with full details (Fullz)	$20 - $60
Dump of magnetic strip track 1&2 & PIN	$60 - $100
Malware	
Basic banking Trojan kit with support	$100
Password stealing Trojan	$25 - $100
Android banking Trojan	$200
Office macro downloader generator	$5
Malware crypter service (make hard to detect)	$20 - $40
Ransomware kit	$10 - $1800
Services	
Media streaming services	$0.10 - $10
Hotel reward program accounts (100K points)	$10 - $20
Airline frequent flyer miles account (10K miles)	$5 - $35
Taxi app accounts with credit	$0.5 - $1
Online retail gift cards	20% - 65% of face value
Restaurant gift cards	20% - 40% of face value
Airline ticket and hotel bookings	10% of face value
DDoS service, < 1hr duration, medium target	$5 - $20
DDoS service, > 24hr duration, medium & strong target	$10 - $1000
Dedicated bulletproof hosting (per month)	$100 - $200
Money transfer services	
Cash-out service	10% - 20%
Accounts	
Online bank accounts	0.5% - 10% of account balance
Retailer accounts	$20 - $50
Cloud service provider accounts	$6 - $10
Identities	
Identity (Name, SSN & DOB)	$0.1 - $1.5
Scanned passports and other documents (e.g. utility bill)	$1 - $3