NAVAL POSTGRADUATE SCHOOL CENTER FOR HOMELAND DEFENSE AND SECURITY
HOMELAND SECURITY DIGITAL LIBRARY
SECURING THE HOMELAND THROUGH THE POWER OF INFORMATION

JULY 8, 2015

CYBER CRIME: MODERNIZING OUR LEGAL FRAMEWORK FOR THE INFORMATION AGE

UNITED STATES SENATE COMMITTEE ON THE JUDICIARY, SUBCOMMITTEE ON CRIME AND TERRORISM

ONE HUNDRED FOURTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

MEMBER STATEMENTS:

Sen. Lindsey Graham (R-SC) *[no pdf available, see 20:35 of webcast]*
Chairman, Subcommittee on Crime and Terrorism

Sen. Sheldon Whitehouse (D-RI) *[no pdf available, see 25:55 of webcast]*
Ranking Member, Subcommittee on Crime and Terrorism

WITNESSES:

Mr. David Bitkower *[view pdf]*
Deputy Assistant Attorney General, U.S. Department of Justice, Criminal Division

Mr. Doug Johnson *[view pdf]*
Senior Vice President and Chief Advisor, Payments and Cybersecurity Policy
American Bankers Association

Ms. Jen Ellis *[view pdf]*
Senior Director of Community and Public Affairs, Rapid7

Ms. Bill Wright *[view pdf]*
Director, Government Affairs, Global Cybersecurity Partnerships, Symantec

---

This hearing compilation was prepared by the Homeland Security Digital Library, Naval Postgraduate School, Center for Homeland Defense and Security.

AVAILABLE WEBCAST(S):*

Full Hearing: *http://www.judiciary.senate.gov/hearings/watch?hearingid=1198C2B0-5056-A032-52BF-20253C9AB448*

COMPILED FROM:

http://www.judiciary.senate.gov/meetings/cyber-crime-modernizing-our-legal-framework-for-the-information-age

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

Department of Justice

STATEMENT OF

DAVID M. BITKOWER
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"CYBER CRIME: MODERNIZING OUR LEGAL FRAMEWORK FOR THE INFORMATION AGE"

PRESENTED

JULY 8, 2015

Statement of
David M. Bitkower
Deputy Assistant Attorney General
Criminal Division
Department of Justice

Before the
Subcommittee on Crime and Terrorism
Committee on the Judiciary
United States Senate

At a Hearing Entitled
"Cyber Crime: Modernizing our Legal Framework for the Information Age"

Presented
July 8, 2015

Good afternoon, Chairman Graham, Ranking Member Whitehouse, and Members of the Subcommittee. Thank you for the opportunity to appear before the Subcommittee today to discuss legislative proposals to combat cybercrime. I also particularly want to thank the Chair and Ranking Member for holding this hearing and for their continued leadership on this important issue.

As the Attorney General has made clear, fighting cybercrime is one of the highest priorities of the Department of Justice. Recent revelations about the massive thefts of financial and other sensitive information from both the public and private sector serve as a stark reminder to all of us about how vulnerable we are to those who take advantage of our computer networks to steal our personal and financial information.

Our growing reliance on computer networks and electronic devices in almost every aspect of our lives has been accompanied by an increasing threat from individuals, organized criminal networks, and nation states that victimize American citizens and businesses. Hackers

steal and hold for ransom our most valuable and personal information. They invade our homes by secretly activating webcams. They steal financial information to line their pockets while jeopardizing the financial stability of everyday Americans. A new generation of organized criminals is able to steal the personal information of millions of victims from a computer halfway around the world. These developments also pose a widespread threat to American businesses and the economy. Cyber criminals can orchestrate massive disruptions of businesses and can electronically spirit away trade secrets worth millions of dollars in seconds. Every individual has a stake in protecting computers and computer networks from intrusions and abuse. According to one report, just this past May there were over 44 million new pieces of malicious software — or "malware" — created around the globe. Another report found that in 2014, there were about 24,000 ransomware attacks per day. I'll talk more about ransomware later. A study from last summer estimated that cybercrime costs the global economy approximately $400 billion annually. A study from this past May projects that, by 2019, cybercrime will cost businesses worldwide $2 trillion per year.

An essential part of the mission of the Department of Justice is to protect Americans from emerging criminal threats such as the cyber threats described above and to deter, disrupt, and prosecute the criminals who are responsible for them. These invasions of privacy, for good reason, make us feel vulnerable and unsafe. And that fear is only compounded when we realize that the criminals who hack into our computers often sit on the other side of the world; peddle the stolen information to other criminals; and use the information for financial gain or even to terrorize and extort their victims. As the Deputy Attorney General testified this morning, the Department supports the use of strong encryption to help protect against unauthorized access to

sensitive information. But just as locking your door cannot offer complete protection from crime, cybersecurity cannot provide perfect protection from cyber criminals. That's why the Department's prosecutors, along with agents from the Federal Bureau of Investigation, the United States Secret Service, and other law enforcement agencies, work every day using the legal authorities at our disposal to protect personal information and vindicate the privacy rights of citizens and businesses. But just as our adversaries adapt to new technologies and global realities, so must we. If we want to remain effective in protecting our citizens and businesses, our laws and our resources must keep pace with the tactics and numbers of our adversaries. We ask that Congress continue its support of these critical efforts.

Earlier this year, the President announced new legislative proposals designed to protect the online privacy and security of American citizens and businesses. These proposals include a set of targeted updates to the criminal code to provide additional capabilities to prosecute offenders and deter and disrupt criminal conduct.[1] Some of the proposals will enable the Department to address the growth of specific types of crime, such as the sale of illegal spyware or the use of botnets — networks of victim computers surreptitiously infected with malware. Other proposals address shortcomings in existing statutory capabilities, such as the Government's ability to prosecute cases involving insiders, including Government or corporate employees, who use their access to information systems to misappropriate sensitive and valuable data. The proposals also respond to changes in the threats posed by cyber criminals, such as by adding provisions to enable the prosecution of hacking by organized crime groups and to give

[1] *See* https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat; https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf.

Federal courts the authority to sentence perpetrators of the most significant cybercrimes in line with those who commit similar financial crimes.

Computer Fraud and Abuse Act

One of the most important of the substantive criminal statutes used to bring cyber criminals to justice is the Computer Fraud and Abuse Act, also called the "CFAA." The CFAA is the primary Federal law against hacking. It protects the public against criminals who hack into computers to steal information, install malware, and delete files. The CFAA, in short, reflects our baseline expectation that people are entitled to have control over their own computers and are entitled to trust that the information they store in their computers remains safe.

The law was first enacted in 1984, at a time when the problem of cybercrime was still in its infancy. Over the years, a series of measured, modest changes have been made to the CFAA to reflect new technologies and means of committing crimes and to equip law enforcement to respond to changing threats. The CFAA has not been amended since 2008, and in the intervening years the need again has arisen for the enactment of modest, incremental changes. We support targeted legislative changes to help the CFAA keep up with rapidly-evolving technologies and uses.

Deterring Insider Threats

Ensuring that the law enables us to protect privacy and security without ensnaring harmless or legitimate conduct is particularly important in the context of the CFAA, which protects the privacy and security of computer owners and users. The CFAA applies both to hackers who gain access to victim computers without authorization from halfway around the world, and to those who have some authorization to access a computer — like company

employees entitled to access a sensitive database for specified work purposes — but who intentionally abuse that access. The CFAA needs to be updated to make sure that the statute continues to appropriately deter privacy and data security violations. Targeted legislative changes would maintain the law's key privacy-protecting function while ensuring that trivial violations of things like a website's terms of service do not constitute Federal crimes.

The part of the CFAA that covers the conduct of those who have some authorization to access a computer is the statute that Department prosecutors have used to charge, for example, police officers who take advantage of their access to confidential criminal records databases in order to look up sensitive information about a paramour, sell access to private records to others, or even provide confidential law enforcement information to a charged drug trafficker. We've also used this part of the statute to prosecute a consultant of a health insurer who used his access to the company's sensitive databases to improperly obtain the names and Social Security numbers of thousands of current and former employees.

Unfortunately, recent judicial decisions have limited the Government's ability to prosecute such cases in large parts of the country.[2] As a result of these decisions, insiders may be effectively immunized from punishment even where they intentionally exceed the bounds of their legitimate access to confidential information and cause significant harm to their employers and to the people — often everyday Americans — whose data is improperly accessed.

Let me offer you an example. Suppose a criminal in Eastern Europe hacks into a healthcare database located in California and steals the financial and personal information of millions of Americans. That crime could be charged today under the CFAA because the

[2] *See* http://cdn.ca9.uscourts.gov/datastore/opinions/2012/04/10/10-10038.pdf.

offender accessed the database "without authorization." Now suppose that a customer service employee has access to the healthcare company's records in the ordinary course of the employee's work. Because the database contains sensitive information, the company's rules explicitly state that employees can only access the database for official business. But if the employee intentionally violates those rules, and accesses the private medical records of a political candidate in order to later embarrass that person by publicizing the records, the individual likely could not be prosecuted under the CFAA in one of the affected judicial circuits.

The narrow judicial interpretation of the term "exceeds authorized access" in the CFAA stemmed from the concern that the statute potentially makes relatively trivial conduct a Federal crime. For example, a Federal court feared that the statute could be construed to permit prosecution of a person who accesses the internet to check baseball scores at lunchtime in violation of her employer's strict internet use policy.[3] Or someone who accesses a dating website but lies about his height even though the site's terms of service require users to provide only accurate information.

We understand these concerns. The Department of Justice has no interest in prosecuting harmless violations of use restrictions like these. That's why we've crafted proposed amendments to the CFAA to address these concerns — while making sure thathe law applies to those who commit serious thefts and privacy invasions.

To accomplish this, our proposal does two things. First, it addresses the recent judicial decisions that have posed obstacles to important prosecutions. It does this by clarifying that the definition of "exceeds authorized access" includes the situation where the person accesses the

[3] *Id.*

computer for a purpose that he knows is not authorized by the computer owner. This clarification is necessary to permit the prosecution of, for example, a law enforcement officer who is permitted access to criminal records databases, but only for official business purposes. Second, at the same time, the proposal adds new limitations to make clear that trivial conduct does not constitute an offense. In order to constitute a crime under the new wording, not only must an offender access a protected computer in excess of authorization and obtain information, but the information must be worth $5,000 or more, the access must be in furtherance of a separate felony offense, or the information must be stored on a Government computer.

These changes will empower the Department to prosecute and deter significant threats to privacy and security, but make sure that the CFAA doesn't inadvertently cover trivial conduct.

Sale of U.S. Financial Data Overseas

Another priority in addressing threats to privacy and financial security is shutting down the international black market for Americans' stolen financial information. One of the most common motivations for hacking is the theft of financial information. In recent years, organized, multinational criminal enterprises have emerged that steal large volumes of credit card numbers and other personally identifiable information. Middlemen then sell the stolen data to the highest bidder, often using underground "carding" forums. Statutory reforms should be aimed at making sure that these middlemen — those who profit from the sale of stolen financial data of Americans — can be brought to justice even if they are operating outside of the United States.

Current law makes it a crime to sell "access devices" such as credit card numbers. The law allows the Government to prosecute offenders located outside the United States if the credit card number involved in the offense was issued by an American company *and* meets a set of

additional requirements. In the increasingly international marketplace for stolen financial information, however, these requirements have proven increasingly unworkable in practice. The Government has to prove either that an "article" used in committing the offense moved though the United States, or that the criminal is holding his illicit profits in an American bank. But with the theft of digital data, it's not always clear what "article" is involved. And foreign criminals generally move their money back to their home countries rather than keep it in the United States.

These requirements unduly limit the Department of Justice's ability to prosecute criminals residing outside of the United States who commit crimes that harm Americans. Indeed, law enforcement agencies have identified foreign-based individuals holding for sale vast quantities of credit card numbers issued by American financial institutions where there is not necessarily any evidence that the person selling the numbers is the same person who stole them, and no evidence of "articles" in the United States. The United States has a compelling interest in prosecuting such individuals because of the great harm they cause to U.S. financial institutions and citizens.

A targeted amendment would strike the unnecessary language in the current statute. It would permit the United States to prosecute anyone possessing or trafficking in credit card numbers with intent to defraud as long as the credit cards were issued by a United States financial institution, regardless of where the possession or trafficking takes place. This kind of jurisdiction over conduct that occurs abroad is fully consistent with international norms and other criminal laws aimed at protecting Americans from economic harm. Moreover, in an era of global cybercrime where criminals steal Americans' financial information so that they can traffic it abroad, it is necessary to prevent criminals from victimizing our citizens with impunity.

Botnets

Another striking example of cybercrime that victimizes Americans is the threat from botnets — networks of victim computers surreptitiously infected with malware. Once a computer is infected with the malware, it can be controlled remotely from another computer with a so-called "command and control" server. Using that control, criminals can steal usernames, passwords, and other personal and financial information from the computer user, or hold computers and computer systems for ransom. Criminals can also use armies of infected computers to commit other crimes, such as distributed denial of service (DDoS) attacks, or to conceal their identities and locations while perpetrating crimes ranging from drug dealing to online child sexual exploitation. The scale and sophistication of the threat from botnets is increasing every day. Individual hackers and organized criminal groups are using state-of-the-art techniques to infect hundreds of thousands — sometimes millions — of computers and cause massive financial losses, all while becoming increasingly difficult to detect. If we want security to keep pace with technological innovations by criminals, we need to ensure that we have a variety of effective authorities to combat evolving cyber threats like these.

One powerful method that the Department has used to disrupt botnets and free victim computers from criminal malware is the civil injunction process. Current law gives Federal courts the authority to issue injunctions to stop the ongoing commission of specified fraud crimes or illegal wiretapping, by authorizing actions that prevent a continuing and substantial injury. This authority played a crucial role in the Department's successful disruption of the Coreflood botnet in 2011 and the Gameover Zeus botnet in 2014. These botnets used keystroke logging or "man-in-the-middle" attacks to collect online financial account information, and they transferred

stolen funds to accounts controlled by the criminals. The Gameover Zeus botnet, which infected computers worldwide, was estimated to have inflicted over $100 million in losses on American victims alone, often on small and mid-sized businesses. Because the criminals behind these particular botnets used them to commit fraud against banks and bank customers, existing law allowed the Department to obtain court authority to disrupt the botnets by taking actions such as disabling communication between infected computers and the command and control servers.

The problem is that current law only permits courts to consider injunctions for limited categories of crimes, including certain frauds and illegal wiretapping. Botnets, however, can be used for many different types of illegal activity. They can be used to steal sensitive corporate information, to harvest email account addresses, to hack other computers, or to execute denial of service attacks against websites or other computers. Yet — depending on the facts of any given case — these crimes may not constitute fraud or illegal wiretapping. In those cases, courts may lack the statutory authority to consider an application by prosecutors for an injunction to disrupt the botnets in the same way that injunctions were successfully used to incapacitate the Coreflood and Gameover Zeus botnets.

Appropriate legislative changes would add activities like the operation of a botnet to the list of offenses eligible for injunctive relief. Specifically, our proposal includes an amendment that would permit the Department to seek an injunction to prevent ongoing hacking violations in cases where 100 or more victim computers have been hacked. This numerical threshold focuses the injunctive authority on enjoining the creation, maintenance, operation, or use of a botnet, as well as other widespread attacks on computers using malware (such as “ransomware”).

The same legal safeguards that currently apply to obtaining civil injunctions, and that applied to the injunctions obtained by the Department in the Coreflood and Gameover Zeus cases, would also apply here. Before an injunction is issued, the Government must civilly sue the defendant and demonstrate to a court that it is likely to succeed on the merits of its lawsuit and that the public interest favors an injunction; the defendants and enjoined parties have the right to notice and to have a hearing before a permanent injunction is issued; and the defendants and enjoined parties may move to quash or modify any injunctions that the court issues.

In sum, a targeted amendment would provide the Government with an effective capability to shut down illegal botnets or certain widespread malware, and better match the ways that criminals are using these technologies. It assures that the legal mechanism that has proven effective to date will be available.

Sale of Botnets

The Department has also striven to identify and bring to justice those who create and control botnets. While we have had significant successes to date prosecuting these offenders, we have encountered some shortcomings in the existing law.

Criminals continually find new ways to make money illegally through botnets. Law enforcement officers now frequently observe that those who create botnets not only use the botnets for their own illicit purposes, but also sell or even rent access to the infected computers to other criminals. The criminals who purchase or rent access to botnets then go on to use the infected computers for various crimes, including theft of personal or financial information, the dissemination of spam, for use as proxies to conceal other crimes, or in denial of service attacks

on computers or networks. Americans are suffering extensive, pervasive invasions of privacy and financial losses at the hands of these hackers.

Current criminal law prohibits the creation of a botnet because it prohibits hacking into computers without authorization. It also prohibits the use of botnets to commit other crimes. But it is not similarly clear that the law prohibits the sale or renting of a botnet. In one case, for example, undercover officers discovered that a criminal was offering to sell a botnet consisting of thousands of victim computers. The officers accordingly "bought" the botnet from the criminal and notified the victims that their computers were infected. The operation, however, did not result in a prosecutable U.S. offense because there was no evidence that the seller himself had created the botnet in question or used it for a different crime. While trafficking in botnets is sometimes chargeable under other subsections of the CFAA, this problem has resulted in, and will increasingly result in, the inability to prosecute individuals selling or renting access to many thousands of hacked computers.

We believe that it should be illegal to sell or rent surreptitious control over infected computers to another person, just like it is already clearly illegal to sell or transfer computer passwords. That's why we recommend amending current law to prohibit the sale or transfer not only of "password[s] or similar information" (the wording of the existing statute) but also of "means of access," which would include the ability to access computers that were previously hacked and are now part of a botnet. In addition, the proposal would replace the current requirement that the Government prove that the offender had an "intent to defraud" with a requirement to prove that the offender not only knew his conduct was "wrongful," but that he also knew or should have known that the means of access would be used to hack or damage a

computer. This last change is necessary because, as noted above, criminals don't only use botnets to commit fraud — they also use them to commit a variety of other crimes.

Some commentators have raised the concern that this proposal would chill the activities of legitimate security researchers, academics, and system administrators. We take this concern seriously. We have no interest in prosecuting such individuals, and our proposal would not prohibit such legitimate activity. Indeed, that's precisely why our proposal requires that the Government bear the burden to prove, beyond a reasonable doubt, that the individual intentionally undertook an act (trafficking in a means of access) that he or she knew to be wrongful. And the Government would similarly have to prove that the individual knew or had reason to know that the means of access would be used to commit a crime by hacking someone else's computer without authorization.

This approach makes clear that ordinary, lawful conduct by legitimate security researchers and others is not at risk of criminal prosecution. We want to work with the members of this Subcommittee to make sure any amendment prohibits the pernicious conduct we've described without chilling the activities of those who are trying to improve cybersecurity for all.

Spyware

The widespread use of computers and cellular phones has created a market for malware that allows perpetrators to surreptitiously intercept their victims' communications. For a small fee, people can purchase this software and download it onto a victim's device. Operating secretly in the background, the spyware allows perpetrators to read a victim's email and text messages. They can track a victim's location and listen to their calls. They can even turn on the

microphone in a victim's phone or computer and listen to conversations in the room. They can do all of this from afar and without the victim knowing.

These privacy invasions have far-reaching implications. Spyware can be used by abusive spouses to track, control, and terrorize former partners. Competitors can commit corporate espionage. Spyware can even be used to eavesdrop on law enforcement and national security personnel. As one example, the Department recently prosecuted the maker of a spyware application called "StealthGenie." This application, which was available for the Apple iPhone, Android phones, and Blackberry devices, could surreptitiously record all incoming/outgoing voice calls; it allowed the purchaser to secretly activate the phone to monitor nearby conversations within a 15-foot radius; and it enabled the purchaser to monitor the incoming and outgoing email and text messages. The application was intended for, and I quote from the business development plan: "Spousal cheat: Husband/Wife o[r] boyfriend/girlfriend suspecting their other half of cheating or any other suspicious behaviour or if they just want to monitor them."

The market for this software has made these capabilities widely available to many who would not otherwise have access to them. We need to do more to counter the increase in privacy invasions.

It is already illegal to sell or advertise surreptitious interception devices of this type. Indeed, the Department successfully prosecuted the maker of the "StealthGenie" spyware, and the court fined the offender half-a-million dollars. Yet the people who make and sell these products often reside outside of the United States, making it more difficult to bring them to justice. And they are making millions of dollars of profit selling spyware inside the United

States. These same criminals try to conceal their ill-gotten gains and transfer them out of the reach of law enforcement. Because current law does not authorize the forfeiture of proceeds from the sale of spyware, U.S. law enforcement is unable to disgorge such criminals of the money that they amass.

Our proposal includes an amendment that would expand the scope of the statute that already provides for the forfeiture of surreptitious interception devices themselves to include forfeiture of proceeds from the sale of spyware and property used to facilitate the crime. The proposal includes standard language drawn from other areas of the criminal code regarding the rules and safeguards for civil and criminal forfeiture.

In addition, violators of the surreptitious interception device statute often engage in money laundering by transferring proceeds through multiple overseas accounts to conceal the profits of their criminal enterprise. Because the spyware statute is not listed as a predicate offense in the money laundering statute, however, prosecutors are unable to charge defendants for money laundering activities related to the sale of spyware unless they can link it to some other crime, which will often be difficult or impossible. The proposal therefore adds violations of the spyware statue to the list of money laundering predicate offenses.

Conclusion

I very much appreciate the opportunity to discuss with you the ways in which the Department protects the privacy and security of American citizens and businesses from cyber threats and to discuss targeted legislative changes that would strengthen our ability to counter this increasingly sophisticated threat going forward. We understand how devastating it is to victims of cybercrime who have their personal and financial information siphoned away, whether

by hackers on the other side of the world or by insiders at a company that holds their personal information. The Justice Department is committed to using the full range of investigative capabilities available to us to fight these privacy invasions and protect Americans, and we will continue to use these capabilities responsibly. We appreciate the continued efforts of Congress and this Subcommittee to ensure that statutory authorities to counter cybercrime are updated and effective.

Thank you for the opportunity to discuss this important area of our work, and I look forward to answering any questions you might have.

Testimony of

Wm. Douglas Johnson

On behalf of the

American Bankers Association

before the

Subcommittee on Crime and Terrorism

of the

Committee on the Judiciary

United States Senate

American
Bankers
Association

Testimony of

Wm. Douglas Johnson

On behalf of the

American Bankers Association

before the

Subcommittee on Crime and Terrorism

of the

Committee on the Judiciary

United States Senate

Wednesday, July 8, 2015

Chairman Graham, Ranking Member Whitehouse, members of the subcommittee, my name is Doug Johnson, senior vice president, payments and cybersecurity policy, of the American Bankers Association (ABA). In that capacity, I currently lead the association's physical and cybersecurity, business continuity and resiliency policy and fraud deterrence efforts on behalf of our membership.

I appreciate the opportunity to be here to represent the ABA and discuss the importance of modernizing our legal framework in the current cyber-crime environment The ABA is the voice of the nation's $15 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $11 trillion in deposits and extend over $8 trillion in loans.

I also have the privilege of serving as vice chairman of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and on the board of directors of the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Established in 2002, the FSSCC is the national critical infrastructure protection coordinator for the financial sector, focused on operational risks. Because the FSSCC fits into a larger

network of sector coordinating councils, it is uniquely positioned as the leader within financial services for developing strategies to improve shared critical infrastructure and homeland security.

Established in 1999, the FS-ISAC is the designated operational arm of the FSSCC. The Center supports the protection of the global financial services sector by assisting FSSCC, Treasury as well as regional agencies and entities to identify, prioritize and coordinate the protection of critical financial services, infrastructure service and key resources. The FS-ISAC also facilitates sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures and practices.

As the 114th Congress engages in public debate on the important issue of cybersecurity and cybercrime, we share your concerns regarding the need to modernize our laws to meet the cybercrime challenges our nation faces. The ABA, now through its Center for Payments and Cybersecurity Policy, has historically been very supportive of these collaborative efforts to protect our sector's and nation's cyber infrastructure from private criminal actors and nation state threats. The financial sector is an acknowledged leader in defending against such threats. These efforts are highly mature and increasingly focused on international and cross-sectorial efforts to enhance our collective ability to defend against and respond to cybersecurity attacks that attempt to disrupt or destroy the systems we depend on, compromise personally identifiable information, steal intellectual property, or otherwise conduct criminal acts. We support buttressing our nation's ability to defend against, deter, and prosecute the perpetrators of these acts and will continue to work with Congress and this committee to achieve these goals.

In my testimony I will focus on three main points:

- **The cyber threats we face continue to evolve and become more complex.**
- **Our defenses against these threats continue to mature but challenges remain.**
- **Congress can assist by enhancing the civil and criminal penalties and tools we can use against our attackers.**

I. The Cyber Threats We Face Continue to Evolve and Become more Complex

According to the "Worldwide Threat Assessment of the US Intelligence Community," cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact, and the range of cyber threat actors, methods of attack, targeted systems, and victims are also expanding, highlighting the persistent and ever-changing nature of the threats the private sector faces and will face in the future.[1] Attacks that once were singular in focus, be it a denial of service attack on financial institutions, an attack against merchant point-of-sale devices, or an attempt to destroy or wipe data of an energy company, may now contain a variety of such attack vectors. Such multi-faceted attacks create particular challenges for the victimized company or companies, necessitating the simultaneous maintenance of availability, integrity, and confidentiality of data when formerly a cyber-attack might have impacted only one of these vital data security components.

Attackers of every variety are also becoming increasingly adept at defeating security practices, increasing the velocity with which companies must move to ensure they understand how cyber risks are changing and what mitigating measures are most effective against these risks. It is indeed an arms race. The tools that these perpetrators are using now have the capacity to destroy as well as compromise data, or in the alternative remain on systems for extended periods of time prior to detection.

Another increasing challenge for financial institutions and the private sector generally is the need to digest an increasingly larger volume of cyber threat data. Determining the relevance of a particular piece of threat data, analyzing the magnitude of the threat, evaluating which systems might be impacted, and devising the appropriate course to take to mitigate the threat if necessary has become increasingly difficult.

Who is being attacked is also changing. Prior to 2014, much of the private and public sector cyber security focus was on critical infrastructure and the payments system. Now there is recognition that, given the broader motivations of attackers for conducting a cyber-attack, essentially any company and any sector could be subjected to a significant, highly visible attack.

---

[1] Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, James R. Clapper, Director of National Intelligence, February 26, 2015, available at: http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

The motivations for such attacks are indeed broadening. Nation states are becoming more adept at compromising private and public computer systems for reasons ranging from retribution for perceived wrongs to espionage.

II. Our Defenses against These Threats Continue to Mature but Challenges Remain

The cybercrime threat certainly knows no boundaries. The increased activities of nation states and foreign criminal enterprises attempting to disrupt financial services through denial of service attacks, compromise U.S. customer financial data, or steal U.S. company and governmental trade secrets, point to the challenge we as a nation currently face in reaching overseas to apprehend and prosecute such actors. The overseas sale of the spyware and other tools used to facilitate these crimes is also difficult to prevent. We face vast botnet armies of infected computers, distributed internationally, attempting to use these tools to infect our financial customers' electronic devices, compromise their personal financial information or hijack their internet banking sessions.

The financial services sector's capacity to withstand the direct attack on our critical financial infrastructure as a result of the significant, purportedly nation state-based denial of service attacks demonstrated our sector's capacity to, through the FS-ISAC, act collectively to respond to major attacks and minimize their capacity to cascade through the sector.

Our sector has also initiated civil legal action, in conjunction with the FS-ISAC and Microsoft, to take down botnets responsible for compromising our customer's personal computers in order to extract their financial information. ABA was a declarant in several of the civil suits that successfully seized U.S.-based servers facilitating criminal botnets. These actions also cleansed millions of individual financial customer personal computers that had been infected in order to facilitate botnet traffic.

In April of this year the level of national and international coordination regarding such efforts took an additional step forward in the takedown of the "Beebone" botnet. In this instance, the FBI, the Department of Justice, and the National Cyber Investigative Joint Task Force-International Cyber Crime Coordination Cell (IC4), in coordination with other international law enforcement bodies, coordinated the takedown with the international financial sector. As a result of the court-authorized seizures of over 1000 domains, computers infected with Beebone could no longer report to the criminals responsible for the infection. Instead, infected computers were

redirected to a sinkhole server operated by Europol's European Cybercrime Centre, which is facilitating victim identification and remediation. As was the case with earlier botnet takedowns, as a result of the court-authorized domain seizures, computers infected with Beebone will no longer report to the criminals responsible for the infection. Instead, infected computers will be redirected to a sinkhole server operated by EC3, which will facilitate victim identification and remediation.

We also support recent action by the Administration, through executive order, authorizing the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose sanctions on those individuals and entities that he determines to be responsible for or complicit in malicious cyber-enabled activities that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, economic health, or financial stability of the United States.

In addition to making it clear that sanctions authority will in the future be utilized against those that perpetrate cybercrimes, another important component of the order is the specification of what are considered significant malicious cyber-enabled activities to include:

- Harming or significantly compromising the provision of services by entities in a critical infrastructure sector;
- Significantly disrupting the availability of a computer or network of computers, including through a distributed denial-of-service attack;
- Misappropriating funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain;
- Knowingly receiving or using trade secrets that were stolen by cyber-enabled means for commercial or competitive advantage or private financial gain; or
- Attempting, assisting, or providing material support for any of the harms listed above.

The sanctions executive order sends a strong signal to cybercriminals and foreign entities that America is committed to fighting this increasing threat, and that we share this commitment to working together to help protect our critical infrastructure and the economic security of our country.

III. Congress can assist by Enhancing the Civil and Criminal Penalties and Tools We Can Use Against our Attackers

The fact that attackers are becoming increasingly adept at defeating cybersecurity practices and mitigating measures points to the need for industry and government to develop and deploy enhanced measures on an ongoing basis with greater speed. While the threat detection, information sharing, and incident response capabilities our sector has leave us well positioned to withstand such attacks, we must also increase the potential that our attackers face real consequences for their actions.

Nation states that attack us generally deny attribution, or even if they take credit for the attacks currently do not fear the consequences. While the FBI and the Department of Justice have had increasing success in indicting members of overseas criminal networks and partnering with the private sector to disrupt botnets and other malicious activity, generally the organizations perpetrating these acts are not fearful of attribution, extradition, and prosecution to the degree that it impacts their risk/reward calculation.

While the recent executive order regarding sanctions is also important, it is widely recognized that Congress can also assist by passing legislation to fill important gaps that current law or executive action cannot fill. As such, we support this committee's efforts, as outlined in the recently circulated discussion draft, to propose the "International Cybercrime Prevention Act of 2015," which would:

- Clarify that U.S. economic espionage statutes cover acts committed on behalf of a foreign government;
- Enhance law enforcement tools to prosecute trade secret theft;
- Enhance the ability of trade secret owners to recover damages and keep their trade secrets confidential in court proceedings;
- Ensure our government can prosecute foreign individuals that possess or traffic credit card numbers, regardless of whether that individual is the criminal who stole the numbers in the first place;

- Allow service on foreign defendants outside U.S. jurisdiction. Foreign organizations with no agent or principal place of business within the U.S. should not be immune from service;
- Make the use of surreptitious interception devices a money laundering and RICO predicate and a Computer Fraud and Abuse Act violation;
- Authorize the forfeiture of surreptitious interception devices, proceeds from the sale of spyware, and property used to facilitate these crimes. While current law allows for prosecution of these crimes, cybercrime property and proceeds should not be exempted from forfeiture;
- Attack the use of overseas-controlled botnets by permitting the Department of Justice to seek a civil injunction to prevent ongoing Computer Fraud and Abuse Act (CFAA) violations in cases involving large numbers of victim computers;
- Create a CFAA violation for criminals who knowingly cause damage to a computer that controls critical infrastructure systems; and
- Allow the prosecution of government and corporate insiders that use their access for criminal purposes.

We look forward to working with Congress, this committee, and the Administration as we work to improve the legal and operational tools necessary to deter, detect, apprehend, and prosecute those that are using technology designed to create a more efficient and effective global economy for criminal purposes. We also strongly encourage Congress to act swiftly to enhance our abilities to share critical cybersecurity threat information, as well as to enact a national data security and notification law.

Statement for Hearing on Cyber Crime: Modernizing our Legal Framework for the Information Age

Before the Subcommittee on Crime and Terrorism
United States Senate Committee on the Judiciary
July 8th, 2015

Mr. Chairman, Ranking Member Whitehouse, members of the Committee, thank you for the opportunity to contribute to this hearing. I am the senior director of community and public affairs at Rapid7, a security data and analytics company trusted by more than 3,900 organizations. We are participating in this hearing to represent the perspective of security researchers. I work extensively with researchers, both within Rapid7, and through the Metasploit Framework, which is an open source penetration testing platform driven by contributions from researchers. Metasploit gives organizations the ability to safely test their defenses against the tools and techniques used by cybercriminals in the wild, so defenders can understand whether attacks will be successful, what the impact of an attack will be, and what steps they need to take to protect their organization.

Given the complexity of technology, the pace of innovation, and the potential for human error, we can never expect to build or deploy completely invulnerable systems. Researchers act as independent auditors or antibodies in the digital immune system, mimicking the behavior of cybercriminals in order to test whether computing systems and networks are vulnerable to attack. Once flaws are identified, researchers alert the vendors and technology users, either directly or through a third party, providing the information needed to fix weaknesses and better protect customers and technical systems. Some work for the companies who build and deploy the systems, but many more operate separately. As independent testers, validators, and problem solvers, they are the antibodies of the digital immune system.

According to the Open Source Vulnerability Database, more than 13,500 technology vulnerabilities were disclosed in 2014[1]. This included the Heartbleed vulnerability, which impacted 17% of the secure servers powering the internet, undermining the security of hundreds of thousands of websites, including banking and healthcare sites that deal extensively with confidential personal information.[2] We also saw research revealing a bug in around 5,300 gas station tank gauges across the United States, exposing them to remote attack.[3]
It's clear that research is essential to our safety, yet it is at risk from both current and future legislation. The Computer Fraud and Abuse Act (CFAA) and similar state laws make no distinction between the well-intentioned work of researchers and the nefarious efforts of bad actors. Though they are primarily used to address cybercrime, these laws also deter security research.

Essentially an online anti-trespass law[4], the CFAA is intentionally broad; however, in the 30 years since the law

[1] The Open Source Vulnerability Database: http://blog.osvdb.org/
[2] "Half a million widely trusted websites vulnerable to Heartbleed bug," Netcraft, April 2014: http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html
[3] "The Internet of Gas Station Tank Gauges," Rapid7, January 2015: https://community.rapid7.com/community/infosec/blog/2015/01/22/the-internet-of-gas-station-tank-gauges
[4] "Obama's proposed changes to the computer hacking statute: A deep dive," Washington Post, January 2015: http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/14/obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive/

was first enacted, technology has changed a great deal and the vagueness of the statutory language has become an increasingly big problem for the security research community. Today we see the statute being applied inconsistently by the courts, and unpredictably by prosecutors. The lack of clear definitions and boundary lines creates uncertainty over whether well-meaning research efforts will violate the law. This murkiness deters researchers from engaging in independent research projects, or disclosing accidental discoveries to those who can fix them.

This unfortunate effect is exacerbated by the law containing both criminal penalties and a private cause of action. Technology providers that fear the reputational fallout from a vulnerability disclosure use the threat of a lawsuit as a stick to scare researchers away. This is a worryingly common occurrence as many technology providers focus on the short-term impact to their business, and view independent researchers as trouble makers.

For example, a researcher found a flaw in an interactive toy designed to enable people to communicate with young children. Users were only supposed to be able to communicate with the child once approved by the child's parents, but the bug meant anyone could start talking to the child without their parents' knowledge. In addition, the system would send out information on the child including their name, age and location. When the researcher disclosed his findings to the toy's manufacturer, they threatened legal action. The researcher persevered and eventually the issues were addressed; however, the stress of the experience left the researcher wary of conducting further research.

While the majority of legal threats to researchers come from technology providers, they are not the most frightening concern. A researcher that worked on an internet scanning project that revealed vulnerabilities affecting tens of millions of routers in homes and offices around the U.S. faced the possibility of criminal prosecution. The project involved scanning publicly accessible assets on the internet and revealed important issues such as a bug that could be used to blow up buildings. This was disclosed to the technology vendors and infrastructure operators through the CERT Coordination Center[5] so they could be addressed. Despite the FBI determining that the research project was bona fide and valuable, the prosecutor thought it might be a violation of a state law that is similar to the CFAA. Eventually the prosecutor did drop the investigation; however, facing jail time understandably shook the researcher's confidence, and he ended the project and took a break from research altogether – not an outcome that makes any of us safer.

One of the problems this example highlights is the inconsistency with which these cases are brought, and the challenges presented by the complexity of them. Few prosecutors are actually experts in computer crimes, particularly at the state level, yet cybercrime convictions have become an appealing way to move ahead. This may encourage some to pursue prosecutions that penalize the people who are actually trying to make us more secure.

These are just two example; there are many more. When researchers suffer legal threats, it is not just them or security companies that lose; we all do. I assure you that criminals are looking for these bugs and will take advantage of them, so we need the expertise of researchers to help us protect ourselves. Ignorance is not bliss, it is insecurity. Chilling security research means we won't know what we don't know, and we cannot address issues until we become aware of them.

Yet for all the discussion around cybersecurity legislation, this is not a problem being addressed yet. Most discussions around updating the CFAA focus on extending its application and making penalties more stringent. Penalties are certainly an important part of deterring crime, particularly domestically within the U.S., but they

[5] CERT Coordination Center: https://www.cert.org/about/

are less likely to be impactful internationally when you consider how hard it is to prosecute foreign actors. Studies suggest that people determine whether to commit a crime based primarily on the likelihood of being caught, not the severity of the penalty[6]. This is probably even more the case with large organized crime groups such as the Russian Business Network[7], or state-sponsored hacking groups, such as Deep Panda[8].

This brings me to the Committee's proposed legislation, the International Cybercrime Prevention Act of 2015 (ICPA), which, among other things, would update the CFAA. I'd like to thank the Committee for giving us the chance to comment on the draft proposal. We applaud your emphasis on the prevention of cybercrime. There are a number of things the Bill does well and we were encouraged to see some updates to the proposal we saw from the Department of Justice at the start of the year.

In particular, we are very supportive of the provision intended to shut down botnets and agree this is best undertaken by law enforcement within the checks and balances of a legal framework. We also commend the Bill's focus on protecting critical infrastructure. It makes sense to include the requirement that "the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Our concern with the Bill is that it does not address the issues affecting security researchers. In fact, it could make the situation worse for them. We understand that creating a carve-out is a challenge as often researchers' efforts mirror those of cybercriminals, despite radically-different intentions. We strongly urge the Committee to consider this problem and whether there is a way to create an exemption for research, perhaps based around intent or outcomes.

In addition, clarifying and updating some of the language of the Bill will at least enable researchers to act with more confidence over what is or is not permissible. For example, the statute revolves around the concept of "authorization," but this term is not well defined. Likewise, notions of protected computers and obtaining information are drastically out of date and do not consider the role technology providers and owners may play in exposing data.

Without clarifying the CFAA and creating greater consistency in the way it is prosecuted and litigated, we diminish the value of security research and make it far harder for U.S. organizations and consumers to protect themselves. The reality is that technical systems are complex by nature and will always have bugs that provide opportunities for attackers. The only way to mitigate this is to support a culture where these issues can be proactively identified, disclosed, and addressed. It's not the imperfection of systems that should define us, it's how we respond to the knowledge that they will not be perfect.

Once again, I'd like to thank you for the opportunity of testifying today. I welcome your questions and comments.

---

[6] "Deterrence in Criminal Justice," The Sentencing Project, 2010: http://www.sentencingproject.org/doc/Deterrence%20Briefing%20.pdf

[7] "Shadowy Russian Firm Seen as Conduit for Cybercrime," Washington Post, 2007: http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html

[8] Deep Panda implicated in Athem attack: http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack

Prepared Testimony and
Statement for the Record of

Bill Wright
Director of Government Affairs, Cybersecurity Partnerships
Symantec Corporation

Hearing on

"Cyber Crime: Modernizing our Legal Framework for the Information Age"

Before the

United States Senate
Committee on the Judiciary
Subcommittee on Crime and Terrorism

July 8, 2015

226 Dirksen Senate Office Building

Chairman Graham, Ranking Member Whitehouse, and distinguished members of the Subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Bill Wright and I am the Director of Government Affairs for Cybersecurity Partnerships at Symantec. In this role, I manage a number of global relationships, working extensively with industry, non-profits, and governments to counter cybercrime and improve cybersecurity. I am also responsible for Symantec's global cybersecurity partnership program, through which we partner with governments around the world to raise awareness, mitigate threats, and share cyber threat information.

Symantec protects much of the world's information, and is a global leader in security, backup and availability solutions. We are the largest security software company in the world, with over 32 years of experience developing Internet security technology and helping consumers, businesses and governments secure and manage their information and identities. Our products and services protect people's information and their privacy across platforms – from the smallest mobile device, to the enterprise data center, to cloud-based systems. We have established some of the most comprehensive sources of Internet threat data in the world through our Global Intelligence Network, which is comprised of 57 million attack sensors in 157 countries, recording thousands of events per second. We maintain 9 Security Response Centers around the globe and we process 30 percent of the world's e-mail messages and nearly two billion web requests every day. All of these resources allow us to capture worldwide security data that give our analysts a unique view of the entire Internet threat landscape.

The cyber headlines of the past year have focused on data breaches, cyber espionage and cybercrime. I am pleased that the Subcommittee is again focusing attention on how industry and government can work together to disrupt these threats. In my testimony today, I will discuss:

- The size and scope of the cyber threat landscape, including botnets;
- Successful efforts to disrupt botnets and cybercrime;
- Enhancing cybersecurity through public-private partnerships; and
- Improving laws to fight cybercriminals.

The Size and Scope of the Cyber Threat Landscape

If there is one thing that can be said about the threat landscape, and Internet security as a whole, it is that the only constant is change. The scale of theft of personally identifiable information (PII) is unprecedented – over just the past three years alone, the number of identities exposed through breaches is more than *one billion*. And this is just from known breaches, as many go unreported or undetected. Data breaches touch all parts of society around the globe, from governments and businesses to celebrities and individual households. While many assume that breaches are the result of sophisticated malware or a well-resourced state actor, the reality is much more troubling. According to a recent report from the Online Trust Alliance, 90 percent of last year's breaches could have been prevented if organizations implemented basic cybersecurity best practices.[1] The Center for Internet Security describes these best practices as basic "cyber hygiene." These include creating an inventory of authorized devices, identifying and patching software vulnerabilities in a timely manner, deploying

[1] https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented

strong malware defenses, backing up all systems, and utilizing data loss prevention technology to stop the unauthorized transfer of sensitive data.[2]

Statistics from our 2015 Internet Security Threat Report demonstrate that the cyber threats we are facing on a day-to-day basis are growing. Last year, five out of every six large companies (2,500+ employees) were targeted with spear-phishing attacks, a 40 percent increase over the previous year. Since the beginning of this year, more than 115 million identities have already been exposed, including major breaches in our government, financial, healthcare and educational sectors.[3] These breaches often expose real names, birth dates, and government ID numbers. This stolen data is often sold on the black market for other criminals to exploit (See attachment 1). In addition to their value on the black market, this personal information helps facilitate future attacks by providing cybercriminals a trove of information that can help them create highly customized phishing emails. Some breaches – such as the recent intrusions at the U.S. Office of Personnel Management – also expose other highly sensitive data. While we have not seen this data for sale on the black market yet, it may just be a matter of time.

While the focus on data breaches and the identities put at risk is certainly warranted, we also must not lose sight of the other types of cyber attacks that are equally concerning and can have dangerous consequences. There are a wide set of tools available to the cyber attacker, and the incidents we see today range from basic confidence schemes to massive denial of service attacks to sophisticated (and potentially destructive) intrusions into critical infrastructure systems. The economic impact can be immediate with the theft of money, or more long term and structural, such as through the theft of intellectual property and trade secrets. It can ruin a company or individual's reputation or finances, and it can impact citizens' trust in the Internet and their government. In some cases, cyber attacks can cause physical damage to our critical infrastructure systems and the computers that operate them.

The attackers run the gamut from highly organized criminal enterprises, disgruntled employees, individual cybercriminals, so-called "hacktivists," and state-sponsored groups. The motivations vary – from pure financial gain, to the promotion of a political cause, to espionage (traditional spycraft or economic). These boundaries, however, are not set in stone, as criminals and even state actors might pose as hacktivists, and criminals often offer their skills for hire to the highest bidder. Attribution has always been difficult in cyberspace, and is further complicated by the ability of cyber actors to mask their motives and objectives through misdirection and obfuscation.

Attackers are Moving Faster than Defenses

Vulnerabilities have always been a big part of the security picture, where operating system and browser-related patches have been critical to keeping systems secure. However, the discovery of vulnerabilities such as Heartbleed and ShellShock, and their wide-spread prevalence across a number of operating systems, brought the topic front and center. Within four hours of the Heartbleed vulnerability becoming public, Symantec saw a surge of attackers stepping up to exploit it. Advanced attackers continue to favor zero-day vulnerabilities to silently sneak onto victims' computers, and last year we saw an all-time high of 24 used in attacks. As we observed with Heartbleed, attackers moved in to exploit these vulnerabilities much faster than vendors could create patches, and users could apply them.

---

[2] https://www.cisecurity.org/documents/CSC-MASTER-VER5.1-10.7.2014.pdf
[3] http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

Cybercriminals Are Streamlining and Upgrading Their Techniques

With the glut of personal information on the Internet and black markets, attackers continued to breach networks with highly targeted spear-phishing attacks, which increased eight percent overall. Notably, they were more refined in their targeting than the previous year, deploying fewer emails per attack campaign. Attackers also perfected their use of watering hole attacks. Like the lion in the wild who stalks a watering hole for unsuspecting prey, cyber criminals have become adept at lying in wait on legitimate websites and using them to try to infect visitors' computers. Watering hole attacks compromise legitimate websites that their victims are likely to visit and then modify the sites so that they will surreptitiously deliver malware to targeted companies.

Further complicating organizations' ability to defend themselves was the appearance of "Trojanized" software updates. Attackers identified common software programs used by targeted organizations, hid their malware inside software updates for those programs, and then waited for their targets to download and install that software – in effect, leading companies to infect themselves when they thought they were applying protective patches. Last year, 60 percent of all targeted attacks struck small- and medium-sized organizations. These organizations often have fewer resources to invest in security, and many are still not adopting basic best practices like blocking executable files and screensaver email attachments. This puts not only the businesses, but also their business partners who are often connected via computer networks, at higher risk.

Malware Volume Increases and Becomes More Sophisticated

We also saw the use of malware grow and become more sophisticated. In fact, more than 317 million new pieces of malware were created last year, meaning nearly one million new threats were released into the wild each day. Attackers are also figuring out ways to fashion their malware to avoid detection. In 2014, up to 28 percent of all malware was "virtual machine aware." Virtual Machines (VM) have become a common security tool, as potential malware can be detected, executed and analyzed without endangering the overall system. Unfortunately, this VM-aware malware can recognize that it is on a virtual machine and lie dormant until it determines that it is safe to execute. It can even transmit false data in an attempt to confuse security researchers.

Botnets – Today and into the Future

Much of the cybercrime we see today is facilitated by malicious botnets. They allow cybercriminals to exponentially increase their distribution power and provide a potent tool for any number of crimes.

A "bot" is a type of malware that allows an attacker to take control of an infected computer. Also known as "Web robots," bots are usually part of a network of infected machines, collectively known as a "botnet." These typically are made up of victim machines that stretch across the globe and are controlled by "bot herders" or "bot masters."[4] About half of these bots are what we would call helpful bots, such as the automated web crawlers that check to see that websites are running in good order or that index and update information for search engines. The others are malicious bots.

[4] "Bots and Botnets – A Growing Threat," *Symantec*, http://us.norton.com/botnet/

Botnet Uses

The uses for malicious bots are only limited by the imagination of the criminal bot master. The most common use for botnets is still for Distributed Denial-of-Service (DDoS) attacks. DDoS attacks occur when multiple infected systems are used to overload a website with traffic and render it unable to respond to legitimate requests. Another recent use of DDoS attacks has been to provide cover for other, more sophisticated attacks. Organized crime groups have been known to launch DDoS attacks against banks to divert the attention and resources of the bank's security team while the main attack is launched, which can include draining customer accounts or stealing debit and credit card information.

Another common use for botnets is creating bitcoins, commonly known as bitcoin "mining." The mining process involves compiling information from recent bitcoin transactions and performing complex mathematical computations. Any single computer would take far too long to do the calculations to provide any value, so bot masters co-opt the processing power of thousands of hijacked computers to do so, thus "mining" valuable bitcoins for the bot master. Those bitcoins can then be used to purchase even more powerful cybercrime tools on the black market.

Cybercriminals also use botnets as launch points for attacks or to amplify their own processing power and bandwidth for various criminal activities such as spam generation, malware distribution and click fraud. Bot masters also can rent out their botnets for illegal purposes and can generate hundreds of thousands of dollars by making their botnets available to other users. Harvesting information such as passwords, credit card data, intellectual property, or other confidential information from infected computers is another common use for botnets. When this information is stored on a computer that is part of a botnet, the bot master has access to all of it – in an operational sense, they "own" that device. This information is often then sold to other criminals for fraudulent use.

Efforts to Disrupt Cybercriminals

Every day we read about the impact of cybercrime, but we do not often hear about the successes that law enforcement and the private sector have had in thwarting crime and bringing these criminals to justice. Recently, we have seen a string of successful arrests and prosecutions of some of the most notorious cyber criminals in the world. Earlier this month, a New York judge sentenced Alexander Yucel, the creator of the *Black Shades* Trojan to five years in prison and the forfeiture of $200,000. *Black Shades* was a password-stealing Trojan designed to infect computers and spy on victims through their web cameras, steal files and account information, and log victims' key strokes. Yucel was arrested by the U.S. Federal Bureau of Investigation (FBI) and Europol last year along with dozens of other individuals in the U.S. and abroad. Symantec worked closely with the FBI in this coordinated takedown effort, sharing information that allowed the agency to track down the location of the command and control infrastructure.[5] And just two weeks ago, Ercan "Segate" Findikoglu, the man who prosecutors say orchestrated one of the biggest cyber bank heists in American history was extradited to the U.S. to stand trial for stealing more than $55 million by hacking bank computers and withdrawing millions in cash from ATMs.[6]

---

[5] http://www.wsj.com/articles/blackshades-leader-sentenced-to-prison-1435093984

[6] http://www.nytimes.com/2015/06/25/business/suspect-in-55-million-atm-scheme-is-extradited-to-us.html?_r=0

We have also seen a number of successful takedown operations against prominent financial fraud botnets. In June of 2014, the FBI, the U.K. National Crime Agency, and a number of international law enforcement agencies mounted a major operation against the financial fraud botnet *Gameover Zeus* and the ransomware network *Cryptolocker*. *Gameover Zeus* was the largest financial fraud botnet in operation last year and is often described as one of the most technically sophisticated variants of the ubiquitous *Zeus* malware. Symantec provided technical insights into the operation and impact of both *Gameover Zeus* and *Cryptolocker*, and worked with a broad industry and government coalition during this case. As a result, authorities were able to seize a large portion of the infrastructure used by the cybercriminals behind both threats.[7]

In July 2014, another law enforcement operation targeted the group behind *Shylock*, another dangerous financial fraud botnet, that was was designed to intercept online banking transactions and steal victims' credentials. *Shylock* was responsible for the theft of millions of dollars from victims before the U.K.'s National Crime Agency seized the command and control servers, and the domains that *Shylock* used to communicate between infected computers.[8]

And in February of this year, an operation led by Europol struck against the *Ramnit* botnet and seized its servers and infrastructure. *Ramnit* facilitated a vast cybercrime operation, harvesting banking credentials and other personal information from their victims. The group was in operation for at least five years and in that time evolved into a major criminal operation, infecting more than three million computers.

These law enforcement operations and others have knocked out or severely curtailed the operations of some of the most prominent financial fraud groups in the world. In fact, the number of bots declined by 18 percent in 2014 compared to the previous year. In large measure, this decline is because the FBI, the European Cybercrime Centre (EC3) at Europol, and other international law enforcement agencies, working with Symantec and other technology companies, disrupted and shut them down.

Unfortunately, these successes have led to the emergence of new threats, such as the *Dyre* group. In a very short time, the *Dyre* financial fraud bot has emerged as another dangerous financial Trojan, capable of defrauding customers from a range of financial institutions spanning multiple countries. *Dyre* is capable of using several different types of man-in-the-browser (MITB) attacks against the victim's web browser to steal credentials. One such MITB attack involves scanning every web page a user visited and checking it against a list of sites that *Dyre* is pre-configured to attack. If a match is found, it redirects the victim to a fake website that looks similar to its genuine counterpart. This fake website will harvest the victim's credentials before redirecting back to the genuine website.[9]

Enhancing Cybersecurity Through Public-Private Partnerships

Preventing data theft caused by bots and protecting privacy starts with basic electronic device hygiene such as having security software installed, good patch management practices, using strong passwords, and recognizing suspicious emails. But that is just the start, because as we have seen in these high

---

[7] http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network

[8] http://www.symantec.com/connect/blogs/all-glitters-no-longer-gold-shylock-trojan-gang-hit-takedown

[9] http://www.symantec.com/connect/blogs/dyre-emerges-main-financial-trojan-threat

profile botnet cases, sophisticated and well-funded attackers are persistent and highly skilled. Anti-virus software (AV) should be part of any security program and will stop known malware, but it is just one element in a broad security toolbox.

Today, even moderately sophisticated malware have unique signatures and can slip past systems that are using only AV software. Thus, strong security is layered security – in addition to basic computer hygiene and AV, consumers and organizations need comprehensive protection that includes intrusion protection, reputation-based security, behavioral-based blocking, and data loss prevention tools. These advanced tools look not just for known threats, but they can check the reputation of any file that is loaded on a computer and look for other behavior that could indicate the presence of previously unknown malware.

However, even with modern security suites, there is a risk that your device or network may become compromised. If that occurs, there are a number of things Symantec is doing to assist victims of botnets and other types of cybercrime. It is important to recognize that these are not victimless crimes; at best, owners of infected computers suffer decreased functionality, and at worst they have their identities compromised and their bank accounts raided. Part of our efforts to stop botnets, and indeed cybercrime *writ large*, is helping individual victims.

In April 2014, we partnered with the National White Collar Crime Center (NWC3) to develop an online assistance program, VictimVoice.org, that helps cybercrime victims better understand the investigation process and help prevent future attacks. We also make security tools available to the public to assist them if they are infected by a botnet. For example, we offer free software that allows victims of ransomware and botnets to remove malware from their system.[10]

Because cyberspace is a domain without borders, where crimes are often committed at a great distance, every device in the U.S. is a potential border entry point, making investigation and prosecution of cybercrimes a difficult task. This reality makes international engagement on cybersecurity essential. For example, Symantec recently partnered with AMERIPOL and the Organization of American States to publish a report that provides the most comprehensive snapshot to date of cybersecurity threats in the Latin American and Caribbean region. The goal was to raise awareness of cybercrime issues and promote the importance of cybersecurity throughout the region as a national and economic security imperative.[11] Similarly, Symantec is partnering with the African Union and the U.S. Department of State to develop a report looking at the cybersecurity threats and trends in Africa. That report will be published later this year.

Symantec also maintains close relationships in the U.S. and around the world with international cyber response organizations and law enforcement entities including INTERPOL, EUROPOL, and dozens of national Computer Emergency Response Teams (CERTs) and police forces. Among other things, we share the latest security technology trends, threats, and the techniques that cyber criminals use to launch attacks.

Private to private partnerships have also proven to be effective in fighting cybercrime. An excellent example of the private sector banding together is the establishment of the Cyber Threat Alliance (CTA). The CTA is a group of cyber security practitioners founded in 2014 by Symantec, Fortinet, Intel Security

---

[10] http://www.symantec.com/security_response/removaltools.jsp
[11] http://www.symantec.com/page.jsp?id=cybersecurity-trends

and Palo Alto Networks who share threat information to improve defenses against advanced cyber adversaries across member companies. By sharing detailed security information, we can improve overall protection for our customers. The bulk of information sharing before the CTA was established primarily involved sharing malware samples. The CTA builds upon this foundation to combat advanced attacks by sharing more actionable threat intelligence, including data on zero day vulnerabilities, botnet command and control server information, mobile threats, and indicators of compromise related to advanced persistent threats.[12]

A Path Forward – Improving Laws to Fight Cybercriminals

Symantec welcomes the Subcommittee's sustained interest in fighting cybercrime, and appreciates your efforts to provide additional legal tools to fight this growing threat. We believe there are several areas that Congress could act on to help fight cybercrime and strengthen cybersecurity.

First, Symantec supports amending the Computer Fraud and Abuse Act (CFAA), which is the most important law that prosecutors rely on when taking down botnets. While the CFAA has undergone some changes over the years to keep up with changing technology and evolving threats, more changes are needed. Today, laws allow courts to issue injunctions for crimes involving fraud and illegal wiretapping. Using this law, the Department of Justice has had some notable successes in shutting down botnets. However, botnets also are used for crimes such as DDoS attacks, and for stealing sensitive corporate information. In those cases, an injunction to disrupt a botnet may not be considered by a court due to limits in the existing law. Symantec supports an amendment to the CFAA that would permit judges to issue an injunction against those operating a malicious botnet. This measure would enable authorities to act quickly when a malicious botnet is putting financial or personal information at risk.

Second, we agree with the Department of Justice's recommendation that Congress should modify the so-called "access device fraud statute", 18 U.S.C. § 1029, to allow prosecution of offenders based in other countries who directly and significantly harm individuals or financial institutions in the U.S. This would provide prosecutors the ability to bring charges against foreign criminals that possess or sell stolen credit card numbers, regardless of whether that individual is the one that stole the information in the first place. Prosecutors need this measure in order to pursue the entire criminal chain of individuals that profit from stolen financial information, not just those who conducted the attack.

Third, international cooperation is hampered by outdated legal mechanisms. In order for governments to share cyber information on criminal investigations and prosecutions, we must still proceed through Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory – processes first developed in the 1800s – that take far too long to address the real-time nature of cybercrime. To keep pace with 21st Century threats, the MLAT process should be overhauled and streamlined.

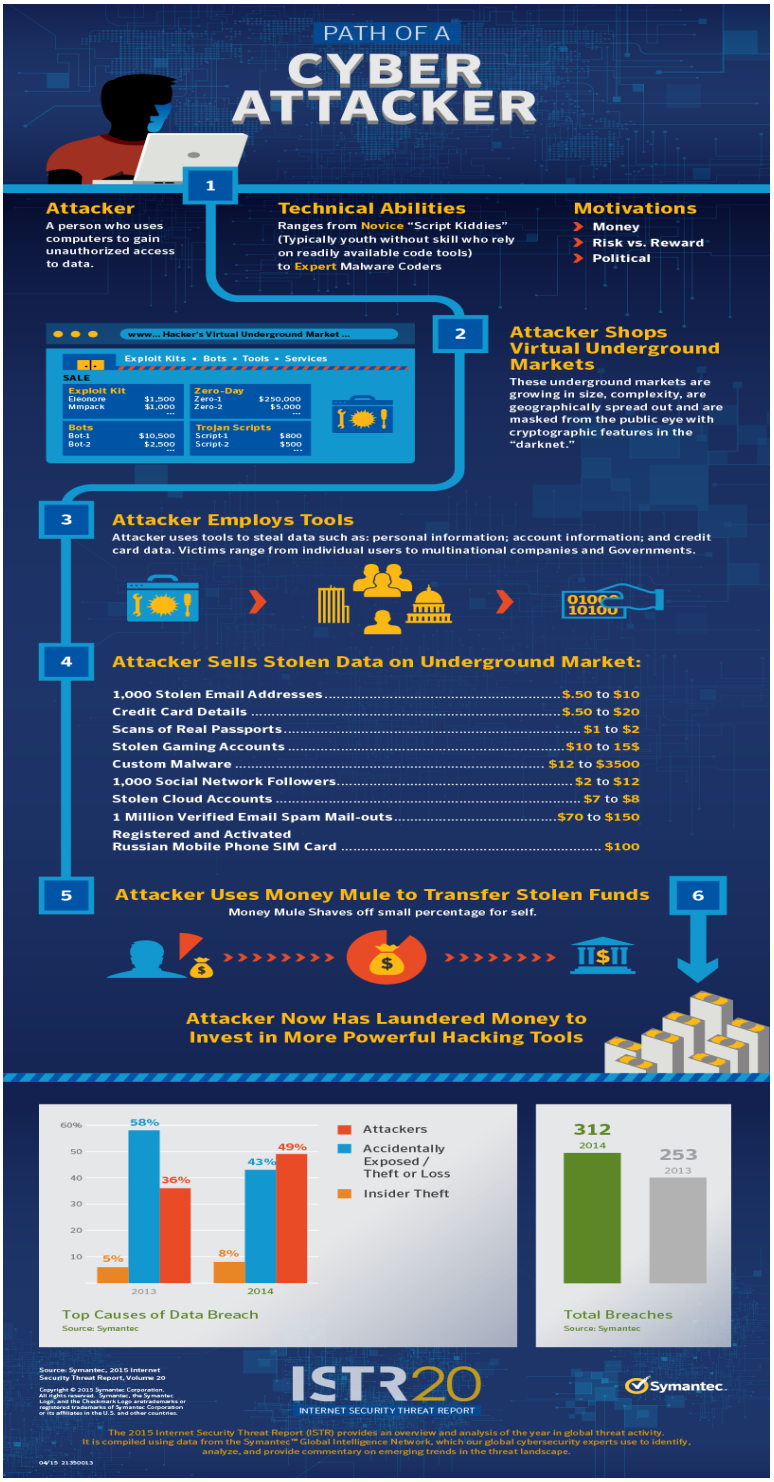
Fourth, intrusions into the computers and systems that run our critical infrastructure are increasing in volume and becoming more sophisticated. For instance, destructive cyberattacks against a power plant or transportation systems could cripple our economy and endanger lives. Symantec supports an amendment to the CFAA that creates a violation and enhanced penalties for criminals who knowingly cause damage to a computer that controls critical infrastructure systems.

[12] http://cyberthreatalliance.org

Last, we should remain vigilant against new laws and regulations that are not properly considered or vetted, no matter how well meaning their intent may be. For instance, last month the Department of Commerce published a proposed rule, stemming from the Wassenaar Arrangement, that imposes strict controls on the export of certain cybersecurity items. Our concern is that, as written, the rule is so vague that it could potentially cover a wider range of cybersecurity products and processes than the Department of Commerce had originally intended. As such, the rule could inadvertently impair security research, damage U.S. security companies, and severely impair our ability to protect our customers around the world.

Conclusion

As this subcommittee knows better than most, we still face significant challenges in our efforts to fight cybercrime and take down botnets. We have made notable progress over the last year but the attackers have evolved and continue to become more sophisticated. Today, both government and industry recognize the imperative for cooperation to fight cybercrime. No single organization can "go it alone" in the current threat landscape. The threats are too complex and the stakes are too high. Ultimately, defeating criminal networks and deterring cybercrime requires strong technical capabilities, effective countermeasures, industry collaboration and smart changes to existing laws that empower law enforcement while still protecting individual rights.

At Symantec, we are committed to improving Internet security across the globe, and will continue to work collaboratively with international industry and government partners on ways to do so. I would also like to commend this subcommittee for its leadership on this important issue. Thank you again for the opportunity to testify, and I will be happy to answer any questions you may have.

Attachment 1