Department of Justice

STATEMENT OF

RICHARD W. DOWNING
ACTING DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING

"RANSOMWARE: UNDERSTANDING THE THREAT AND EXPLORING SOLUTIONS"

PRESENTED

MAY 18, 2016

Richard W. Downing
Acting Deputy Assistant Attorney General
Department of Justice

Before the
Committee on the Judiciary
United States Senate

At a Hearing Entitled
"Ransomware: Understanding the Threat and Exploring Solutions"

Presented
May 18, 2016

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 the threat from ransomware, as well as legislative proposals to combat this and other forms of cybercrime. I particularly want to thank the Chair and Ranking Member for holding this hearing. Their continued leadership on these issues is advancing the nation's cybersecurity. We appreciate your work to ensure that the Department of Justice has the tools necessary to address cyber threats.

As the Attorney General has repeatedly said, fighting cybercrime is one of the highest priorities of the Department of Justice. Cyber threats continue to grow more sophisticated and more destructive. It is imperative that we have the personnel, tools, and laws necessary to respond to these threats, including identifying and prosecuting the criminals behind them. Today, I would like to discuss three specific topics: (1) the growing threat of ransomware; (2) the relationship between ransomware and other cyber threats, particularly botnets, which are networks of victim computers criminals control to commit data intrusions, theft, and extortion on a massive scale; and (3) how updating our laws can help law enforcement fight the scourge of botnets.

I. Ransomware

We rely more than ever on computer networks, electronic devices, and the Internet in almost every aspect of our lives and businesses. And just as the importance of these technologies has grown, we also face ever more sophisticated and destructive threats to our personal lives and our businesses from hackers, organized criminal networks, and even nation states. Cybercriminals have targeted the confidential banking information of average Americans, siphoned trade secrets of our largest businesses worth millions or even billions of dollars, and stolen personal information from millions of victims. The crimes they commit put individuals and companies alike at risk of financial ruin and undermine the security of our technological infrastructure.

One increasingly common and destructive cyber threat is ransomware, as it offers criminals an increasingly popular avenue to profit from unlawfully obtaining access to others' electronic devices. Ransomware is malicious software, or malware, that blocks access to a victim's critical data and systems, typically by encrypting files on the computer. According to the Federal Bureau of Investigation ("FBI"), malicious code like ransomware can be delivered through a variety of ways. One frequent delivery mechanism is through "phishing attacks," which involve criminals sending emails, including messages drafted to look like they are from trustworthy senders, containing malicious attachments or links that, once opened or clicked, activate the ransomware. A second common method involves hacking into websites and planting the malware there, infecting the computers of website visitors. In addition, it is not uncommon for criminals to utilize botnet infrastructure and code to facilitate the widespread delivery of ransomware.

Either way, victims frequently discover that they have lost control of their system when the ransomware posts a message on the device's screen demanding payment of a ransom – usually in a very short period of time – in exchange for a key to decrypt the data. Failure to pay the ransom leaves the data encrypted and inaccessible to the device owner. Some variants also try to spread laterally across the victim's network to encrypt files on other computers or servers to which the victim's device has access. And to add insult to injury, certain variants have displayed messages pretending to be from law enforcement that accuse the user of criminal or embarrassing activity and frame the ransom as a demand that the victim pay a fake "fine." Regardless, the ultimate effect is that a single infection can result in an entire organization's network being hijacked and held hostage for ransom, or individual users being deprived of access to their most personal data.

Ransomware is the latest consequence arising from a systematic problem of criminals exploiting flaws in home and business computers. As this Committee knows, for years, the Department has been concerned about the widespread infection of personal computers with malicious software. It is too easy for criminals to infect computers, and it is far too hard to catch those criminals. The consequences that follow from having a computer infected have multiplied. Once a computer is infected, it comes under the control of a criminal, who can make that computer do whatever the criminal wants. From this follows dozens of other crimes: the theft of intellectual property or bank account login credentials, cyberstalking and "sextortion," and, increasingly, ransom demands.

It is hard to overstate the impact ransomware can have on victims or the urgency they feel to get systems fundamental to their businesses and daily lives back up and running. Unfortunately, many victims today lack reliable options for quickly restoring their systems that do not involve paying the ransom. One op-ed in *The New York Times* recounted how the author, whose mother's computer was infected with CryptoWall ransomware, raced around Brooklyn to purchase the $500 worth of bitcoins (a virtual currency) that the criminals demanded to decrypt nearly 6,000 files on her mother's computer before the countdown clock running on the screen ran out.

Earlier this year, we learned that criminals took control of computers at Hollywood Presbyterian Medical Center in Los Angeles until they were paid a ransom of $17,000 in bitcoin. Criminals using the "Locky" ransomware reportedly attacked at least one hospital system – the Methodist Hospital in Henderson, Kentucky – where doctors and nurses could not access patient files. Attacks of this type on medical facilities are particularly concerning if they pose a risk that the facility will be unable to provide critical services to patients.

And the threat is not localized to any particular industry. Dozens of State and local governments, for instance, have also been victimized by ransomware attacks, including at least one police department which paid the demand to regain access to tens of thousands of witness statements, crime scene photographs, and other evidence critical to that office's investigations.

Compounding the harms, according to the FBI, is the fact that not everyone who pays the ransom receives a key to decrypt the data. What's more, victims who have refused to pay the ransom have experienced varying degrees of success in recovering from the loss of data. A Pittsburgh insurance company was eventually able to restore data from a backup, but only after incurring approximately $70,000 in losses and sending employees home during remediation. A Florida company, by contrast, was not successful and lost critical files, resulting in approximately $30,000 in losses. And a North Carolina business, whose main files and backup were both encrypted, lost its files despite engaging a computer forensics firm to try to restore access to them. That company has lost about $80,000, and the owner told the FBI that, as a result, he may have to lay off employees.

The scope of the threat from ransomware is staggering. Between 2005 and 2015, the Internet Crime Complaint Center ("IC3") run by FBI received over 7,600 ransomware complaints, with nearly a third received in 2015 alone. Victims reported losses totaling over $57 million. While the ransom fees are typically between $200 and $10,000, victims' reported losses also included the costs of mitigation efforts, legal fees, and lost productivity. These figures also reflect just incidents reported to IC3. The actual number of victims, and the true cost of ransomware, is certainly much higher.

What's more, ransomware schemes are becoming more sophisticated, with new variants now targeting platforms like smartphones and Mac OS X. One particularly malicious variant copies the user's files, then incrementally deletes the originals *and* the copies to pressure the victim to pay. Another is so personally tailored that the potential victim receives an email containing his or her full name and mailing address.

And the threat of ransomware is not diminishing – ransomware attacks, in fact, increased 35 percent in 2015, according to a leading cybersecurity firm. Several factors appear to have contributed to the growth of ransomware attacks. First, our networks and systems remain vulnerable to intrusions. At a technical level, known but unpatched vulnerabilities continue to provide criminals with too many ways to attack systems. Verizon's 2016 Data Breach Investigations Report found that the top 10 known vulnerabilities account for 85% of successful exploit traffic. Symantec reported that nearly 75 percent of all legitimate websites have unpatched vulnerabilities. At the same time, ransomware schemes succeed in part because end

users continue to fall victim to ever more sophisticated social engineering attacks by, for example, clicking on malware-laden attachments in phishing emails.

Second, cyber threats are scalable and asymmetric. Disseminating large quantities of malware through phishing schemes offers adversaries a low cost, but highly rewarding, way to attack victims. This is particularly true when the criminal has access to a botnet – that is, a network of computers and servers infected by malware that criminals can control to send traffic, such as malicious emails, to victims.

Third, the economics favor the extortionists. In the modern era, the need to maintain access to personal and business data is generally valued more than the size of the ransoms criminals extort from victims. Criminals appear to calibrate the size of the ransom demand to incentivize paying the ransom.

Fourth, technology is providing criminals with highly sophisticated tools to deploy technical infrastructure that is very difficult for law enforcement agencies to take down. For example, criminals executing ransomware schemes often utilize criminal and general-purpose anonymizing proxy networks, such as Tor ("The Onion Router"), to communicate with victims, even going so far as to set up Tor hidden services websites to answer victims' questions and facilitate payment. Use of anonymizing proxy networks interferes with law enforcement's ability to trace these communications and identify the criminals running the ransomware. Further, the criminals frequently require that payments are made using virtual currencies, primarily bitcoin, that make it difficult for law enforcement to track the payments.

Despite these many challenges, law enforcement is actively working to disrupt and defeat ransomware schemes. The FBI currently has over 30 active investigations into different ransomware variants. And this hard work has achieved some notable successes. In 2014, for example, the Department of Justice disrupted a ransomware scheme using Cryptolocker, a highly sophisticated malware that encrypted computer files on more than 260,000 computers around the world. Once infected, victims saw a message on their computer monitors, telling them that their files were encrypted and that they had three days to pay a ransom, usually between $300 and $750, if they wanted to receive the decryption key. By one estimate, more than $27 million in ransom payments were made in just the first two months after Cryptolocker launched.

To dismantle Cryptolocker and the malware that gave it access to victims' computers, the Department led a multi-national action that seized computer servers acting as the command and control hubs for the Cryptolocker malware. The Department also identified victims and, working with our partners at the Department of Homeland Security ("DHS") as well as in foreign law enforcement agencies and the private sector, facilitated the removal of malware from many victim computers.

This is a point that merits emphasis. Our success against Cryptolocker and the associated malware was only possible due to the invaluable assistance provided by technology companies such as Dell SecureWorks, Microsoft, Deloitte Cyber Risk Services, Symantec, Trend Micro, and many others, as well as from universities like Carnegie Mellon and Georgia Tech. The

Department of Justice is absolutely committed to working side by side with all partners to find technical solutions to cyber threats – and especially with cybersecurity professionals who often have specialized knowledge and unique expertise that we need in our efforts to protect the public from cyber threats. Indeed, such collaboration often produces the best solutions and the greatest successes.

Our outreach and partnership efforts extend to partners around the world. Strong international collaboration and coordination are essential to identifying, disrupting, and mitigating the effects of cyber threats like ransomware. Cybercriminals and the systems they use to further their crimes often reside outside the United States. This requires the Department to work with nations where criminal infrastructure, such as command and control servers that send out orders to infected bots, are located. By sharing information and working together against common threats, we can benefit from other countries' domestic authorities to make arrests, execute search warrants and gather evidence, and seize and disrupt command and control servers and other infrastructure. To support these efforts, the Department works closely with the European Cyber Crime Center ("EC3") and partner agencies such as the Australian Federal Police, Germany's Bundeskriminalamt, the Royal Canadian Mounted Police, New Zealand Police, and the U.K.'s National Crime Agency, among many others. The Department provides critical, real-time assistance to foreign counterparts through the 24/7 Points of Contact Network established by the Group of Seven Nations and by the Budapest Cybercrime Convention. The Criminal Division's Office of International Affairs provides invaluable legal support to evidence collection and extradition efforts by both U.S. and foreign law enforcement agencies. The Computer Crime and Intellectual Property Section conducts training programs to help allies develop cyber laws, and our Federal law enforcement partners work with those countries to improve their investigative capabilities. Due in large part to our extensive engagement with, and training of, foreign criminal prosecutors and investigators, we have developed highly productive international relationships that are critical to the successes of our investigations and prosecutions.

As with other cyber threats, defeating ransomware cannot be accomplished by law enforcement alone. Rather, it requires a strategy that encourages the public and private sectors to work together to strengthen and layer our defenses. Ransomware in general is a volume business; it succeeds where large numbers of victims can be successfully infected and have no other recourse to retrieve their data other than paying the ransom. Increasing the costs of this criminal conduct and diminishing the potential illicit profits are both necessary to undermine the profit margins motivating ransomware attacks. And strengthening IT systems to be harder to penetrate and more resilient in case data is damaged or lost does just that. It's imperative, therefore, that we improve our digital hygiene by promptly installing the latest patches against known vulnerabilities and continuously training and educating end users about the threats from malware and social engineering. And we need to encourage the development of incident response plans now – *pre-intrusion* – to mitigate the potential damage to infected systems and accelerate law enforcement's ability to respond and investigate.

Law enforcement has a role in promoting better cybersecurity, too. The FBI regularly shares cyber threat information with DHS and works closely with the National Cybersecurity and Communications Integration Center (NCCIC), housed within DHS, on mitigation efforts related

to ransomware and other malware. In addition to public sector information sharing, the Department has conducted outreach to educate the public about the threat from ransomware, how to avoid becoming a victim, and what steps one can take to mitigate the harm from ransomware, such as staying up to date with patches and making secure back-ups. Outreach efforts include public service announcements, such as a recently published advisory from the Federal Bureau of Investigation providing tips on how to protect systems from ransomware threats and respond to infections. In addition, the FBI has conducted multiple briefings to InfraGard – its partnership with the private sector and State law enforcement – and other government and public sectors groups on the ransomware threat. Similarly, the U.S. Secret Service has provided information and tips on ransomware via its Electronic Crime Task Forces located throughout the country. Likewise, the Cybersecurity Unit within the Criminal Division's Computer Crime and Intellectual Property Section ("CCIPS") has issued guidance for organizations and other potential victims of cybercrime, encouraging them to develop incident response plans that can accelerate and improve notification of law enforcement and mitigate the damage should they suffer an intrusion.

Increasing our collective awareness about these threats – and what we can all do to protect our systems from them – could significantly undermine ransomware's effectiveness.

II. Law enforcement efforts to combat malware, especially botnets

Ransomware is just one strain of malware and, as with other malware, criminals often require a broad and resilient network of computers to execute ransomware attacks. This is where botnets can come into play. As noted earlier, botnets are networks of computers infected with malware that criminals can control remotely. Botnets operate as force multipliers for criminals, giving them control of hundreds, thousands, or even millions of innocent computers and servers to send malware, spam, and commands against targets, or to steal or encrypt victims' data. And the threat from botnets has increased as individual hackers and organized criminal groups have used ever more sophisticated techniques to infect computers, encrypt communications, and avoid detection by investigators. Law enforcement can take action against malware in two ways: by investigating and prosecuting the offenders and by disrupting and, where possible, seizing the infrastructure that supports ransomware attacks.

We have had recent significant successes in both actions. Just last month, two major international hackers – Aleksandr Andreevich Panin, a/k/a Gribodemon, of Russia, and Hamza Bendelladj, a/k/a Bx1, of Algeria – were sentenced to prison terms of over nine years and 15 years, respectively, for their roles in developing and distributing the prolific malware known as SpyEye. This malware infected an estimated 1.4 million computers in the United States and abroad, enabling the criminals to steal confidential personal and financial information, such as online banking credentials and PINs. Panin also sold variants of the malware to over 150 other criminals, including one who set up a botnet that stole over $3.2 million in a six-month period using SpyEye.

We have also worked with our international partners to dismantle other forms of criminal infrastructure that facilitated the spread of botnets, malware, and computer crime more generally.

In July 2015, a coalition of law enforcement agencies from 20 nations—led by the Department of Justice and the European Cybercrime Center ("EC3")—worked together to take down the Darkode hacking forum. Darkode served as an online underground marketplace where hackers congregated to buy, sell, and trade malicious software, botnets, and other tools to facilitate computer intrusions, as well as stolen personal information. The coordinated law enforcement action led to the search, arrest, or charging of 70 Darkode members and associates around the world.

But there are times when it is not yet possible to arrest the offenders, either because they have not yet been identified or because they currently reside in a country from which it is impossible to extradite them. Law enforcement must then attempt to disrupt the infrastructure. Despite the technological complexity of botnets, the Department has moved successfully in recent years to disrupt botnets and free victim computers, starting with the Department's coordinated takedown of the Coreflood botnet in 2011. Coreflood infected computers with keylogging malware that stole usernames, passwords, and other private personal and financial information from unsuspecting computer users. Once in possession of that information, the criminals running Coreflood used it to steal funds. To dismantle the Coreflood botnet, the Department obtained court orders authorizing the government to seize the servers controlling the botnet and replace them with government-controlled servers that instructed infected computers to stop running the malware. Our Coreflood response demonstrated that the government could disrupt a botnet using a combination of court authorized seizures, forfeitures, restraining orders, and other civil and criminal processes.

Since Coreflood, the government has taken action against other botnets. One particularly pernicious botnet was Gameover Zeus, a global botnet containing between 500,000 and one million victim computers infected with malware. Criminals used the malware to steal millions of dollars from businesses and consumers, causing more than $100 million in total financial losses. Considered one of the most sophisticated botnets in existence before it was disrupted, Gameover Zeus was used to steal login credentials, passwords, and other personal information when the users attempted to access legitimate websites. The botnet also was used to infect computers with Cryptolocker, the ransomware I described earlier. Under the leadership of the Department of Justice, a broad partnership – including U.S. law enforcement, foreign partners in more than 10 different countries, and numerous private sector entities – mounted joint operations to obtain court authorization to wrest control of the Gameover Zeus botnet away from criminals, disable it, and start to repair the damage it had caused.

A common thread through these and other cases of crime over the Internet is that criminals now have ready access to criminal and general-purpose sophisticated anonymizing technologies, like Tor, to conceal their identity and location. Because criminals hide behind proxy networks designed for online anonymity, searches by remote access are often the only mechanism available to law enforcement to identify and apprehend them. But, current law presents challenges when the government wishes to apply for a search warrant that would authorize that remote search. It assumes that the government knows, physically, where the property to be searched is, and requires the government to apply for a search warrant in that judicial district. Additionally, in certain circumstances it may be preferable for the government

to seek a warrant to take action online to clean up botnets—for example, by preventing the bot code from operating or otherwise severing its connection to the criminals who control it. Under current rules, the government might have to apply for near-identical warrants in 94 different courthouses. In a positive development, the Supreme Court has transmitted to Congress an amendment to Federal Rule of Criminal Procedure 41 that will address both problems. It clarifies which judges can issue warrants in both cases, providing a much-needed update of old law to a new technological reality. Importantly, the amendment does not change any of the traditional protections and procedures, such as the requirement that the government establish probable cause. The amendment would not authorize the government to undertake any search or seizure or use any remote search technique not already permitted under current law. Rather, the amendment would merely ensure that *some* court is available to *consider* whether a particular warrant application comports with the Fourth Amendment.

III. Action by Congress

As cyber threats grow more sophisticated and, unfortunately, more destructive, Congressional action is vital to ensure that our laws are up to date and that the Department has the resources necessary to disrupt cyber threats, mitigate the harm of intrusions, and identify and prosecute those who threaten the public. While the Administration has advanced several legislative proposals to enhance available legal authorities to fight 21st Century cyber threats, two deserve two particular attention in the context of fighting ransomware and botnets.

The first is expanding courts' authority to issue injunctions to shut down botnets and widespread ransomware schemes. Current law provides Federal courts with the authority to issue injunctions to stop the ongoing commission of only a narrow set of crimes involving fraud or illegal wiretapping. Botnets though have been used for many other types of illegal activity, including spreading ransomware, stealing sensitive corporate information, hacking other computers, and denial of service attacks against websites. Yet these criminal schemes may not constitute fraud or illegal wiretapping, depriving courts of statutory authority to issue injunctions similar to those successfully used to incapacitate the Coreflood and Gameover Zeus botnets.

The Administration supports an amendment to fill this gap by authorizing courts to issue injunctions that prevent ongoing hacking violations involving 100 or more victim computers. Using this authority, courts could enjoin the creation, maintenance, operation, or use of a botnet or other widespread, coordinated 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 in Coreflood and Gameover Zeus – would also apply here. Before an injunction may issue, the government must file a civil lawsuit against the defendant and demonstrate to a judge's satisfaction that it is likely to succeed on the merits, and that the public interest favors an injunction. The defendants and enjoined parties have the right to notice and a hearing before a permanent injunction is issued. Further, the defendants and enjoined parties may move to quash or modify any injunctions that the court issues.

The second proposal is to amend the Computer Fraud and Abuse Act ("CFAA") – the primary Federal anti-hacking statute. 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 and have included safeguards for legitimate security research in our proposal. . 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.

Getting ahead of cyber threats requires not just new authorities, but ensuring the Department has the resources necessary to investigate ransomware schemes, disrupt botnets that span the globe, and prosecute those who create, disseminate, and monetize malware. The Department's FY2017 Budget provides $121 million in additional funding against cyber threats. The global cost of cybercrime estimated in the hundreds of billions of dollars. In addition, cybercrime is not limited to malware and botnets; it includes the significant risk of foreign actors stealing hundreds of millions of dollars of American intellectual property, critical to our country's economic and national security interests as well as the health and safety of the American people. Safeguarding the trade secrets and protecting the copyrights and trademarks of virtually every U.S. industry are essential to ensuring American innovation and creativity. To strengthen our response to this threat, the Department has requested a funding enhancement to place International Computer Hacking and Intellectual Property ("ICHIP") Attachés overseas to fight transnational crime with a particular emphasis on transnational cybercrime and IP matters. The Department looks forward to working with the Committee to guarantee that the government has the right funds in place to protect and safeguard the public from cyber threats.

*** * ***

In conclusion, thank you again for your leadership on fighting these threats. The Department is committed to partnering with you to develop the right legislative response, and I look forward to answering any questions you might have.