Testimony of

Charles Blauner

On behalf of the

American Bankers Association

before the

Subcommittee on Crime and Terrorism

of the

Committee on the Judiciary

United States Senate

Testimony of

Charles Blauner

On behalf of the

American Bankers Association

before the

Subcommittee on Crime and Terrorism

of the

Committee on the Judiciary

United States Senate

Wednesday, May 18, 2016

Chairman Graham, Ranking Member Whitehouse, members of the subcommittee, my name is Charles Blauner. I am Managing Director and Global Head of Information Security at Citigroup, Inc. In this capacity, I help lead Citi's information security strategy and I am accountable for overseeing information security risk across all lines of business, functions, and regions.

I appreciate the opportunity to testify today at this important hearing, "Ransomware: Understanding the Threat and Exploring Solutions," representing the American Bankers Association (ABA). The ABA represents 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 had the privilege of serving as Chairman of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) from 2012 to 2014. Citi, along with our counterparts in the industry, is extremely supportive of the FSSCC and its sister organization, the Financial Service Information Sharing and Analysis Center (FS-ISAC).

Established in 2002 to focus on operational risks, the FSSCC is the national critical infrastructure protection coordinator for the financial sector. Because the FSSCC fits into a larger network of sector coordinating councils, it is uniquely positioned within financial services to lead the strategic development of improved shared critical infrastructure and homeland security.

Established in 1999, the FS-ISAC is the designated operational arm of the FSSCC. With approximately 7,000 members from 38 countries, the FS-ISAC supports the protection of the global financial services sector by assisting the FSSCC, and US Treasury as well as regional agencies and entities to identify, prioritize and coordinate the protection of critical financial services, infrastructure services, and key resources. The FS-ISAC also facilitates sharing information about physical and cyber threats, possible vulnerabilities, incidents, and potential protective measures and practices.

Representatives of the ABA have been deeply involved in these two organizations since their inception having acted as FSSCC vice chair from 2013 through 2015, and continuing to serve on the FSSCC Executive Committee and FS-ISAC board. Private sector companies and associations taking on these roles are but one example of the high level of collaboration within our sector, which indicates that cybersecurity and critical infrastructure is a top priority for banks and other financial services companies. We invest an enormous amount of time, energy, and resources to assure the highest level of security among all critical sectors, and are subject to stringent regulatory requirements.

As it relates to Citi, we have made a concerted effort to work with federal, state and local officials, as well as their respective staff, about our role in protecting, detecting and defending against cyberattacks. As one of the world's largest financial institutions, Citi has been, and will continue to be, subject to continually evolving cyber security and other technological risks. We continue to devote significant resources to maintain and regularly upgrade our systems and networks. The launch of our Cyber Fusion Center in Warren, New Jersey – which houses cybersecurity experts from more than a dozen disciplines across Citi – is proving to be an excellent resource in addressing, mitigating and fighting criminal cyber behavior.

As the 114th Congress publicly debates the important issue of cybersecurity and cybercrime, we – as an industry – share your concerns to ensure our nation's laws reflect the evolving cybercrime challenge. Historically, the ABA, the FSSCC, and the FS-ISAC have strongly

supported collaborative efforts to protect our sector's – and our nation's – cyber infrastructure from private criminal actors and nation state threats.

The financial sector is an acknowledged leader in defending against such threats. Our efforts are seasoned, well-tested, and increasingly focused on international and cross-sectorial activity enhancing our collective ability to defend against, and respond to, cyber-attacks. That said, we recognize we must continue to remain vigilant because these attacks take many forms, such as attempting to disrupt, or destroy, the systems we depend on, compromising personally identifiable information or stealing intellectual property, and other criminal acts.

We support further enhancing 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. We appreciate the Committee's successful efforts in spearheading legislation last year to prohibit the sale of Americans' financial information and improve the protection of trade secrets. Further, we commend you for introducing the S. 2931, *The Botnet Prevention Act of 2016,* which would provide important, additional protections, and update the criminal code with improved legal tools to stop criminals and foreign agents from leveraging botnets and attacking our critical infrastructure.

There are three points I want to highlight today:

I. **Botnets continue to be a significant threat to our nation's economy and citizens;**

II. **The financial sector, the Administration, and federal law enforcement are taking strong action against botnets and ransomware; and**

III. **Congress can assist by giving prosecutors better tools to stop criminal use of botnets.**

I. Botnets Continue to be a Significant Threat to Our Nation's Economy and Citizens

As the Committee is well-aware, the cybercrime threat certainly knows no national boundaries. The increased activities of nation states and foreign criminal enterprises attempting to disrupt financial services through denial of service attacks, compromising U.S. customer financial data, or stealing corporate and governmental trade secrets signify the challenges we as a nation face in apprehending and prosecuting global criminals.

The sale of the spyware and other tools used to enable these crimes also remains a concern. The challenge is not just the tools themselves, but also the vast botnet armies of infected computers, distributed internationally, attempting to use these mechanisms. Cybersecurity threats to the financial sector, and indeed to our national economy and nation's citizens, come primarily from four groups: hacktivists promoting a sociopolitical ideology; organized criminal gangs committing cybercrime for financial gain; nation states committing industrial espionage; and extremist groups attempting to disrupt financial markets, while also potentially promoting a cause. Regardless of the group or motivation, a common practice of each is to utilize these botnets to deploy traffic or malicious software, also known as malware, to infect our financial customers' electronic devices in order to compromise their personal financial information, hijack their internet banking sessions, or encrypt their important files and then hold these files hostage for ransom, commonly known as ransomware.

During my tenure as the FSSCC Chairman, our sector also experienced extensive use of botnets to execute denial of service or DDoS attacks against financial institutions. These types of attacks create massive internet traffic in an attempt to overwhelm and crash the internet banking site of an institution. Through the FS-ISAC, the financial services sector acted collectively in response to major attacks, and as a result, minimized the destructive effects and contained a potentially damaging cascade. While the FS-ISAC and the member institutions, in concert with the FBI and the Department of Homeland Security, helped to curtail the impact of these attacks, we must continue to take steps to prevent against such attacks.

Most recently, we have seen the rapid evolution of what is called – "general purpose Malware or Ransomware as a Service (RaaS)" – as malware / ransomware developers are offering customized versions of products to other cyber criminals for a percentage of their profits. This market allows developers to pair their technical capabilities with the access to victims possessed by other criminal organizations. RaaS is likely to result in even greater infection rates and improvements in the efficacy of new ransomware variants as this business model continues to draw new participants.

One example of a new piece of adaptable malware, called GozNym, that can drive corporate account takeovers and also act as ransomware. GozNym can be deployed in a number of ways, including botnet-driven spam emails, which can result in either hijacking a customer's online

banking session or encrypting the files on the victim's computer and demand a ransom to unlock them. The ever-more sophisticated nature and global reach of criminals, nation-states and other bad actors requires our nation to move swiftly to ensure that the U.S. criminal code is equipped to meet the ever-evolving cyber-crime threat.

II. The Financial Sector, the Administration, and Federal Law Enforcement Have Taken Strong Action Against Botnets and Ransomware

The use of botnets by criminals and nation states to deploy malware, including ransomware, is becoming more prevalent and complex. In response, the dedicated efforts of the financial sector, the administration, and federal law enforcement to counteract these threats have obtained some significant successes. As bank customers tend to be the targets of these attacks, financial institutions and law enforcement, particularly the FBI, have focused on educating financial services customers on how to protect themselves through proper computer protocol and general threat awareness.

Customers are encouraged to: make sure they have latest antivirus software and update it regularly; automate the installation of security patches for operating systems and web browsers; create strong and varied passwords, use pop-up blockers, download software only from known and trusted sites; and not open attachments or click on an URL in unsolicited or suspicious e-mails, even if it is addressed from friends and family and looks safe. These same precautions apply to customer mobile devices as well as desktop environments.[1]

To prevent the loss of essential files due to ransomware infection, law enforcement and financial institutions also recommend that individuals and businesses conduct regular system back-ups and move back-ups offline. Also effective is encouraging customers to install dedicated endpoint protection that identifies unique malware attributes and then prevents its installation.

In addition to assisting customers, the financial sector and law enforcement work together to counteract the effects of botnet activity. The best example of these counter efforts include the many botnet takedowns over the last five years, including the 2012-2013 takedowns of the Zeus and Citadel botnets, which set the stage for the 2014-2015 takedowns of the Gameover Zeus and Beebone, the primary distributors of Cryptolocker and other ransomwares. These takedowns

[1] "Incidents of Ransomware on the Rise, Federal Bureau of Investigation, April 29, 2016.

represent a broad, coordinated effort that includes the private sector, U.S. government, and foreign authorities.

We also support 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. These sanctions would be imposed on individuals and entities determined 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 a clear statement that sanctions could, in the future, be used against those that enable cybercrimes; another important component of the order is its definition of actions considered to be significant malicious cyber-enabled activities. These activities are:

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

We also applaud the recent indictments of those Iranians alleged to have acted on behalf of the Iranian government to conduct DDoS attacks against our nation's financial institutions. Such indictments make clear that such criminal actions against our nation's critical infrastructure will not be tolerated, regardless of the perpetrators' location.

III. Congress Can Assist by Giving Prosecutors Better Legal Tools to Stop Criminal Use of Botnets.

The fact that attackers are becoming increasingly adept at circumventing cybersecurity defenses underscores the need for industry and government to develop and deploy enhanced measures with greater speed and frequency. While the threat detection, information sharing, and incident response capabilities of our sector make us well-positioned to withstand attacks, we must also increase the likelihood that our attackers will be held accountable and be subject to real consequences.

Nation states generally deny attribution, or if they take credit for an attack, they do not fear the consequences. While the FBI and the Department of Justice have had increasing success in indicting members of foreign criminal networks and partnering with the private sector to disrupt botnets and other malicious activity; generally, the organizations responsible for committing these acts are not fearful of attribution, extradition, and prosecution. It neither impacts their risk/reward calculation, nor is a factor in their individual decision-making.

Although taking down Gameover Zeus, Beebone, and other botnets is admirable, experience informs us that replacement botnets are always in development and awaiting deployment, creating the need to continually enhance the tools we have available to counteract the ransomware deployment with a nationally coordinated response. Additionally, while the executive order regarding sanctions and the Iranian indictments are important, it is widely recognized that Congress also can assist by passing legislation to close important gaps that current law, private actions, or executive orders cannot address.

Through this committee, Congress took important steps last year to prohibit the sale of Americans' financial information as part of the 2015 Omnibus bill and the inclusion of language protecting trade secrets in the *Defend Trade Secrets Act of 2016*. These provisions, both of which were initially included in the *International Cybercrime Prevention Act of 2015,* are to be commended.

The *Botnet Prevention Act of 2016* completes much of the work envisioned in the 2015 cybercrime bill, adding important provisions to assist prosecutors in stopping criminals and foreign agents from leveraging botnets by:

1. **Enhancing Justice Department's Ability to Fight Networks of Botnets.** Under current law, DOJ's authority to shut down botnets through injunctive relief is limited to botnets engaged in fraud or illegal wiretapping. This provision expands DOJ's authority, and allows injunctions against botnets engaged in a broader range of illegal activity, including destruction of data, denial of service attacks, and other criminal acts that cause damage to computers.

2. **Imposing Tougher Penalties on Damage to Critical Infrastructure Computers.** Without imposing mandatory sentences, this provision gives judges the discretion to impose harsher penalties on those knowingly causing damage to computers that control critical infrastructure systems, such as airports, dams, power plants, and hospitals.

3. **Targeting the Trafficking of Access to Compromised Computers Within a Botnet.** Creates new language in 18 USC 1030(a)(8) prohibiting the sale of "means of access" to a compromised computer if the seller knows or has reason to know the buyer intends to cause damage to the computer, use access to commit wire fraud, or violate the criminal spam statute. Under current law, it is difficult to prosecute sellers of access to compromised computers – especially when the seller is not the person who compromised the computer in the first place – because no current criminal law directly prohibits this conduct.

The ABA fully supports the goals of the *Botnet Prevention Act 2016*. Broadening injunctive powers to encompass DDoS attacks recognizes the damage such attacks can inflict. Increasing penalties on damage to computers controlling portions of the critical infrastructure that we all rely on is crucial. Punishing those who would sell access to botnet-based computers limits the availability of destructive botnets.

We look forward to working with Congress, the Committee, and Administration as we collectively improve the legal and operational tools necessary to deter, detect, apprehend, and prosecute those that are using, for criminal purposes, technology designed to create a more efficient and effective global economy.