William Noonan

Deputy Special Agent in Charge
United States Secret Service
Criminal Investigative Division
Cyber Operations Branch

Prepared Testimony

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

February 12, 2015

Good morning Chairman Ratcliffe, Ranking Member Richmond, and distinguished Members of the subcommittee. Thank you for the opportunity to testify on the Secret Service's progressive efforts to protect our homeland by countering cyber criminal activity.

The cyber crime threats to our Homeland continue to rapidly grow fuelled by the wealth these illicit activities are generating. For over three decades the Secret Service has investigated cyber criminal activity[1] and worked to counter some of the most proficient transnational cyber criminal groups. Based on our experience investigating and apprehending many of the most capable and prolific transnational cyber criminals, I hope to provide this Committee useful with insight into the continued threat our Nation faces from malicious cyber activity.

The Transnational Cyber Crime Threat

Nearly 15 years ago, advances in computer technology and greater access to personally identifiable information (PII) via the Internet created online marketplaces for transnational cyber criminals to share stolen information and criminal methodologies. This has resulted in a steady increase in the quality, quantity, and complexity of cyber crimes targeting private industry and critical infrastructure. These crimes include network intrusions, hacking attacks, and account takeovers leading to significant data breaches affecting every sector of the economy. Recently reported payment card data breaches are examples of this long-term trend of major data breaches perpetrated by transnational cyber criminals who are intent on targeting our Nation's financial payment system for illicit gain.

The wealth accrued by the world's most capable cyber criminals is staggering. Some have become millionaires through their cyber criminal activities, even buying numerous resort properties in tropical locations. More significantly they are reinvesting what they have stolen to develop increasingly sophisticated cyber capabilities and organizations to perpetuate and expand their illicit schemes. The capabilities these criminals develop are increasingly being used by foreign states for intelligence collection or military purposes.

The collaboration amongst top tier cyber-criminals is astounding. These individuals routinely trust one another with millions of dollars as they execute their highly distributed transnational criminal conspiracies. These groups have increasingly segmented their operations, allowing for the development of highly talented specialists in performing each part of the criminal schemes: from gaining unauthorized access to protected computer networks, to engaging in sophisticated frauds, to laundering and distributing their proceeds. These growing specialties raise both the complexity of investigating these cases, as well as the level of potential harm to companies and individuals.

For example, illicit underground cyber crime marketplaces allow criminals to buy, sell, and trade malicious software, access to sensitive networks, spamming services, payment card data, PII, bank account information, brokerage account information, hacking services, and counterfeit identity documents. These illicit digital marketplaces vary in size, with some of the more popular sites boasting membership of approximately 80,000 users and some sites being highly exclusive invitation only associations. These digital marketplaces often use various digital

[1] Congress established 18 USC § 1029-1030 as part of the Comprehensive Crime Control Act of 1984 and explicitly assigned the Secret Service authority to investigate these criminal violations.

currencies, and cyber criminals have made extensive use of digital currencies to pay for criminal goods and services or launder illicit proceeds.

The Secret Service Strategy for Combating this Threat

The Secret Service proactively investigates cyber crime using a variety of investigative means to often infiltrate these transnational cyber criminal groups and counter every element of their criminal schemes. As a result of these proactive investigations, the Secret Service is often the first to learn of planned or ongoing data breaches and is quick to notify affected companies and institutions with actionable information to mitigate the damage from the data breach and terminate the criminal's unauthorized access to their networks. Victim companies rarely identify unauthorized access to their networks; rather law enforcement, financial institutions, or other third parties identify and notify the likely victim company of a data breach.

A trusted relationship with the victim is essential for confirming the crime, remediating the situation, beginning a criminal investigation, and collecting evidence. To foster these trusted relationships, in 2001, Congress directed the Secret Service to develop a national network of electronic crimes task forces, based on our existing New York Electronic Crimes Task Force, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist cyber attacks against critical infrastructure and financial payment systems. Today the Secret Service operates a global network of 38 Electronic Crimes Task Forces (ECTF) as part of this growing network. These ECTFs are the foundation for the Secret Service's investigations of cyber crime and our primary means of sharing actionable information with potential victim companies. For example, in 2014, based on information discovered through just one of our ongoing cyber crime investigations, the Secret Service notified hundreds of U.S. entities of cyber criminal activity targeting their organizations.

The Secret Service also invests in developing the capabilities of our state and local partners. In partnership with the State of Alabama, the Secret Service operates the National Computer Forensic Institute (NCFI) to train state and local law enforcement investigators, prosecutors, and judges in how to conduct computer forensic examinations, respond to network intrusion incidents, and conduct cyber crimes investigations. Graduates of NCFI typically join the Secret Service's network of ECTFs, and have frequently made vital contributions to significant Secret Service investigations of transnational cyber criminals.

As the Secret Service investigates cyber crime, we discover new and emerging cyber criminal methods and share relevant cybersecurity information broadly to enable other organizations to secure their networks while protecting ongoing investigations and the privacy and civil rights of all involved. The Secret Service accomplishes these objectives through contributions to industry-leading annual reports like the Verizon Data Breach Investigations Report and the Trustwave Global Security Report, and through more immediate reports, including joint Malware Initial Findings Reports (MIFRs).

For example, this year UPS Stores Inc. used information published in a joint report on the Back-Off malware to protect itself and its customers from cyber criminal activity.[2] The information in this report was derived from a Secret Service investigation of a network intrusion at a small

[2] *See* http://www.us-cert.gov/security-publications/Backoff-Point-Sale-Malware

retailer in Syracuse, New York. The Secret Service partnered with the National Cybersecurity & Communications Integration Center (NCCIC/US-CERT) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) to widely share actionable cybersecurity information derived from this investigation to help numerous other organizations, while protecting the integrity of the ongoing investigation and the privacy of all parties. For UPS Stores, Inc., the result was the identification of 51 stores in 24 states that had been impacted, enabling UPS Stores, Inc. to contain and mitigate this cyber incident before it developed into a major data breach.[3]

As we share cybersecurity information discovered in the course of our criminal investigations, we also continue pursuing our investigation in order to apprehend and bring to justice those involved. Due to the inherent challenges in investigating transnational crime, particularly the lack of cooperation of some countries with U.S. law enforcement investigations, occasionally it can take years to finally apprehend the top tier criminals. The Secret Service works closely with its partners in the Departments of Justice and State to develop the capabilities of foreign law enforcement partners and to foster collaboration.

For example, in July of 2014 Secret Service agents arrested Roman Seleznev of Vladivostok, Russia, through an international law enforcement operation. Mr. Seleznev has been charged in Seattle in a 40-count indictment for allegedly being involved in the theft and sale of financial information of millions of customers. Seleznev is also charged in a separate indictment with participating in a racketeer influenced corrupt organization (RICO) and conspiracy related to possession of counterfeit and unauthorized access devices.[4] This investigation was led by the Secret Service's Seattle Electronic Crimes Task Force.

In another case, the Secret Service, as part of a joint investigation with U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI) and the Global Illicit Financial Team (GIFT), hosted by IRS-Criminal Investigations, shut down the digital currency provider Liberty Reserve, which was allegedly widely used by criminals worldwide to store, transfer, and launder the proceeds of a variety of illicit activities. In addition, the Treasury Department's Financial Crimes Enforcement Network found Liberty Reserve to be a financial institution of primary money laundering concern pursuant to Section 311 of the USA PATRIOT Act. Liberty Reserve had more than one million users, who conducted approximately 55 million transactions through its system totaling more than $6 billion in funds. The founder of Liberty Reserve, Arthur Budovsky, was recently extradited from Spain to the United States. Mr. Budovsky is among seven individuals charged in the indictment. Four co-defendants – Vladimir Kats, Azzeddine el Amine, Mark Marmilev, and Maxim Chukharev – have pleaded guilty and await sentencing. Charges against Liberty Reserve and two individual defendants, who have not been apprehended, remain pending. This investigation was led by the Secret Service's New York Electronic Crimes Task Force.

[3] *See* UPS Store's press release. Available at: http://www.theupsstore.com/about/media-room/Pages/The-ups-store-notifies-customers.aspx.
[4] *See* http://www.justice.gov/usao/waw/press/2014/October/seleznev.html

Legislative Action to Combat Data Breaches

While there is no technology available to prevent data breaches of U.S. customer information, legislative action could help to improve the Nation's cybersecurity, reduce regulatory costs on U.S. companies, and strengthen law enforcement's ability to conduct effective investigations. In January, the Administration proposed law enforcement provisions related to computer security, highlighting the importance of additional tools to combat emerging criminal practices.[5] We continue to support changes like these that will assist us in countering the rapidly-evolving threat of cyber crime.

Conclusion

The Secret Service is committed to continuing to safeguard the Nation's financial payment systems by defeating cyber criminal organizations. Responding to the growth of these types of crimes, and the level of sophistication these criminals employ, requires significant resources and substantial collaboration among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates significant resources to improving investigative techniques, providing training for law enforcement partners, and sharing information on cyber threats. The Secret Service will continue to coordinate and collaborate with other government agencies and the private sector as we develop new methods for combating cyber crime. Thank you for your continued commitment to protecting our Nation's financial system from cyber crime.

[5] This proposal is available at: http://www.whitehouse.gov/omb/legislative_letters/