United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

December 3, 2015

The Honorable Loretta Lynch
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530

Dear Madam Attorney General:

The threat posed by cyber-attacks remains one of our nation's biggest security challenges. As the frequency and severity of cyber-attacks continues to increase, Congress has a responsibility to continue to strengthen our nation's cybersecurity. To address this evolving 21st century threat with a 21st century response, we must equip the federal government with the authorities and resources it needs. Only by staying a step ahead of the threat can we ensure the security of our citizens.

While much must be done to bolster the cyber defenses of our federal agencies, a far larger group, including individual consumers, faces a growing threat from a malicious computer virus known as "ransomware." After infiltrating a person's computer, the virus encrypts a user's files until a ransom is paid, usually in the form of Bitcoin or other difficult-to-track crypto currency.[1] Infected users face the difficult choice of paying the ransom or losing their files forever. The Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) estimate that in less than eight months more than 234,000 computers were infected with a specific type of ransomware named "CryptoLocker." While only about 1.3 percent of victims paid the ransom, the virus has enabled the extortion of approximately $27 million from infected users in two months.[2]

In June 2014, the DOJ, with the assistance of the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center, scored a major victory against ransomware when it announced that U.S. and foreign law enforcement officials successfully disrupted a large network of CryptoLocker-infected computers and seized CryptoLocker's command-and-control servers.[3] Possession of these servers allowed the development of a decryption tool that enabled CryptoLocker victims to unlock their infected machines.

---

[1] Alina Simone, *How My Mom Got Hacked*, New York Times (Jan. 2, 2015).

[2] U.S. Department of Justice, *U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator* (June 2, 2014) (hereinafter "DOJ CryptoLocker Press Release"); Mark Ward, *Cryptolocker Victims to Get Files Back for Free*, BBC (Aug. 6, 2014).

[3] The command-and-control servers were spread across the world in Canada, France, Germany, Luxembourg, Ukraine and the United Kingdom. Matt Apuzzo, *Secret Global Strike Kills 2 Malicious Web Viruses*, New York Times (June 2, 2014); *See also* DOJ CryptoLocker Press Release (June 2, 2014).

However, within a month of this disruption, the FBI's Internet Crime Complaint Center, a partnership between the FBI and the National White Collar Crime Center, identified a copycat virus named "CryptoWall."[4] Between April 2014 and June 2015, the Center received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million.[5]

To understand more about the DOJ's efforts to address the growing threat of ransomware, we ask that you please provide the following information and materials:

1. Since 2005, how many victims of ransomware-related crimes have reported complaints to the Internet Crime Complaint Center? What is the total amount of losses reported from ransomware victims? In addition to the Center's complaint website, does DOJ or FBI use additional resources to track number of ransomware victims?

2. Soon after its disruption, CryptoLocker was quickly replaced by similar ransomware programs, like CryptoWall and CryptoDefense. As of December 1, 2015, how many active ransomware-type viruses is the DOJ or FBI tracking?

3. Both DOJ and DHS, including the United States Computer Emergency Readiness Team (US-CERT) and the United States Secret Service, distribute cyber vulnerability and threat information to individuals, industry, and other stakeholders. How does the FBI share data about ransomware and other cyber threats with DHS? Please describe any joint efforts between DOJ, FBI, and DHS to disseminate cyber threat information.

4. Does the FBI coordinate with the Federal Trade Commission (FTC) to educate the public about how to mitigate the threat of ransomware? If so, please describe any joint efforts with the FTC.

5. In testimony before the Senate Committee on Banking, Housing, and Urban Affairs last year, officials from the FBI indicated that that agency's techniques must evolve to keep pace with increasingly sophisticated botnets that can be used to disseminate viruses like ransomware.[6] What techniques is DOJ using now to combat botnets, how are those becoming less effective, and what new techniques is DOJ considering to improve its ability to combat botnets in the future?

6. Despite the successful disruption of CryptoLocker in May 2014, the ransomware scheme's architect, Evgeniy Mikhaylovich Bogachev, remains at large in Russia.[7] Please describe the

---

[4] Federal Bureau of Investigation, *Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes* (June 23, 2015).

[5] *Id.*

[6] Senate Committee on Banking, Housing, and Urban Affairs, Testimony of FBI Assistant Director, Cyber Division, Joseph M. Demarest, *Cyber Security: Enhancing Coordination to Protect the Financial Sector*, 113th Cong. (Dec. 10, 2014).

[7] Federal Bureau of Investigation, *Wanted by the FBI - Cyber's Most Wanted - Evgeniy Mikhaylovich Bogachev* (accessed Dec. 2, 2015).

challenges of capturing and bringing to justice suspected criminals operating internationally, including in the Russian Federation and other nations.

7. The disruption of CryptoLocker required coordination between DOJ, DHS, and over a dozen international law enforcement and government entities.[8] How can this coordination be improved? Describe the impediments, if any, to further international law enforcement coordination.

8. Recent news reports suggest ransomware attackers are also targeting public safety and law enforcement agencies.[9] Have federal, state, or local governments sought DOJ or FBI's help to remove ransomware from their computers? If so, please describe the nature of any assistance sought, whether agencies have paid ransoms to remove ransomware, and whether DOJ or the FBI was able to decrypt the computer systems.

9. Do DOJ or its agencies operate or utilize any technology that is or can be leveraged to identify ransomware or ransomware attackers' command and control servers outside of DOJ? For example, do DOJ or its agencies operate any signature based detection, stateful packet inspection, or deep packet inspection technologies across one or more networks outside of DOJ? If so please describe those technologies, their capabilities and limitations, and their current and planned applications.

[redacted]

With best personal regards, we are

Sincerely yours,

Tom Carper
Ranking Member

Ron Johnson
Chairman

[8] DOJ CryptoLocker Press Release (June 2, 2014).

[9] ABC News, *Ransomware: How Hackers Are Shaking Down Police Departments* (Apr. 13, 2015).