United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

December 3, 2015

The Honorable Jeh Johnson
Secretary of Homeland Security
U.S. Department of Homeland Security
Washington, DC 20528

Dear Mr. Secretary:

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 U.S. Department of Justice (DOJ), with the assistance of other law enforcement agencies and 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 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 DHS'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 to DHS? Does DHS track the total amount of losses reported from 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 DHS tracking?

3. DHS, including the United States Computer Emergency Readiness Team (US-CERT) and the United States Secret Service, distributes cyber vulnerability and threat information to individuals, industry, and other stakeholders. Please describe any joint efforts between DHS, DOJ, and FBI to disseminate cyber threat information.

4. Does DHS 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 agencies' techniques must evolve to keep pace with increasingly sophisticated botnets that can be used to disseminate viruses like ransomware.[6] What techniques is DHS using now to combat botnets, how are those becoming less effective, and what new techniques is DHS considering to improve its ability to combat botnets in the future?

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

---

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

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

8. Over the past 12 months, how many instances of ransomware has DHS been made aware of in federal agencies' computers? In which agencies and on what systems was the ransomware located and what was the result? Is DHS aware of instances in which federal agencies have paid ransoms to remove ransomware?

9. How are DHS's EINSTEIN, ALBERT, and Enhanced Cybersecurity Services intrusion detection and prevention systems leveraged to reduce the instances of ransomware on computers at federal agencies, state and local agencies, and critical infrastructure? How can that be improved?

[redacted]

[redacted]

With best personal regards, we are

Sincerely yours,

Tom Carper
Ranking Member

Ron Johnson
Chairman

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