U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, D.C. 20530*

MAR 04 2016

The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Senator Carper:

This responds to your letter to the Attorney General dated December 3, 2015, regarding your concern of a growing threat from a type of malicious computer virus known as ransomware. You provided several questions to help the Committee on Homeland Security and Government Affairs' understanding of the Department of Justice's efforts to address the growing threat of ransomware.

To aid in this understanding of our efforts, we have provided 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?**

Since 2005, the Internet Crime Complaint Center (IC3) has had 7,694 ransomware complaints totaling $57,602,032.72. While the ransom fees are typically between $200 and $10,000, victims include additional costs they incurred due to the ransomware incident in their complaints. These additional costs include: network mitigation, network countermeasures, loss of productivity, legal fees, information technology (IT) services, and/or the purchase of credit monitoring services for employees or customers. Additionally, victims sometimes will put a price on the data that was encrypted due to its perceived importance, making it difficult to determine the actual cost to victims associated with a ransomware incident.

It is difficult for the Department of Justice (the Department) to come up with an exact number of ransomware victims. Ransomware variants like Cryptolocker and CryptoWall are used to target victims all over the world. Not all victims report that they are a victim of cyber

crime to IC3. Some victims directly report to their local Federal Bureau of Investigation (FBI) field office or go to their local police department, and some may not report the incident at all. The FBI works closely with the private sector and international partners on many types of ransomware, but an exact number of instances is impossible to determine without gaining access to the criminal actor's infrastructure.

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?**

[redacted]

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.**

The FBI regularly shares information with Department of Homeland Security (DHS) on cyber criminal cases and trends. The FBI Cyber Division (CyD) has FBI employees embedded at DHS and that sit at the National Cybersecurity and Communications Integration Center (NCCIC). The FBI also works closely with multiple agencies that represent DHS through participation at the National Cyber Investigative Joint Task Force (NCIJTF), a cyber threat coordination center that was created to enhance the sharing of cyber threat information among U.S. Government agencies, foreign law enforcement and intelligence partners, and the private sector. One of the entities within the NCIJTF, CyWatch, is a 24/7 watch floor that is responsible for coordinating domestic law enforcement response to criminal and national security cyber intrusions, tracking targeted entity notifications, and managing response to major cyber incidents. CyWatch receives cyber threat and incident reporting, assesses it for action, and engages with the appropriate components within the CyD, FBI field offices, other government agencies, and designated Federal Cyber Centers. The FBI regularly works with the DHS agencies, including Homeland Security Investigations and the United States Secret Service, for case de-confliction at local FBI offices, the NCIJTF, and the National Cyber-Forensics and Training Alliance (NCFTA).

The FBI works closely with DHS/US-CERT on mitigation efforts related to ransomware and other malware variants. The FBI routinely shares information about compromised U.S. based Web sites hosted in the United States with US-CERT for victim notifications and remediation. The FBI ensures that US-CERT is coordinated on law enforcement actions against malware variants and is responsible for coordinating with foreign CERTs for victim notification. An example of the coordination between the FBI and DHS was the mitigation strategy for the Gameover ZeuS (GOZ) / Cryptolocker takedown. The FBI provided a list of all internet protocol (IP) addresses that called out to the malware and passed this information

to US-CERT to share with CERTs in other countries and private industry for malware removal. US-CERT provided a splash page on their Web site to provide victims background on GOZ and Cryptolocker and links to remove the malware from infected computers.

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.**

Most sophisticated ransomware variants use 2048-bit RSA cryptographic key pairs to encrypt victim files. The public key is stored in the registry of the victim computer along with the version number of the malware and a complete list of all encrypted files. Cyber criminal actors hold the private key. When a victim pays the ransom, the actors provide the private key so the files can be decrypted. Without obtaining the private key used by the actors, it is virtually impossible to recover the encrypted files.

Since the most sophisticated ransomware variants are practically impossible to defeat without obtaining the actor's own private decryption keys, the FBI has focused on performing significant outreach to educate the public on ransomware and the importance of keeping backups and maintaining a level of operational security when using a computer. Outreach efforts from the FBI include multiple public service announcements on ransomware, an article on fbi.gov that informs the public on the ransomware threat, providing tips on how victims can protect themselves, and highlighting recent investigations. The FBI has conducted multiple briefings to InfraGard and other government and private sector groups on the ransomware threat. The Cybersecurity Unit within the Department of Justice's Criminal Division has also issued guidance to victims and potential victims of cyber crimes, including ransomware, to assist in their reporting and interaction with law enforcement.

While the FTC primarily brings civil cases on companies engaged in fraud against the consumer, the FBI works closely with the FTC in many investigations and is currently in discussions with the FTC to work closer on leveraging their resources on cyber criminal threats. The Department of Justice has also engaged productively with the FTC on policies relating to cyber crime and strategies for effective protection of personally identifiable information. In February 2014, the FTC posted multiple articles on their consumer information portal about Cryptolocker and best practices to defend against being a victim of ransomware. The FBI is going to engage further with the FTC to leverage their consumer education portal on future threats.

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. 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?**

Each botnet or malware variant is unique and strategies to combat the threat posed by them have to be created on a case-by-case basis. Cyber criminals are consistently evolving to make their infrastructure and malware operations more secure. They are learning from previous law enforcement action on other malware variants and monitor computer security researcher analysis on their operations. Cyber criminals also have secondary infrastructure to prepare for disruptions so when law enforcement takes action, they can continue their fraud schemes with a limited impact to their operation.

As actors become more sophisticated, it has become paramount for the FBI and DOJ to coordinate and collaborate closely with the private sector and foreign law enforcement partners to understand how the variant works, what vulnerabilities exist, what legal options can be utilized, and where the actor's infrastructure is located. This collaboration is also used to prioritize law enforcement efforts and target the highest priority botnets and malware variants.

The FBI has established a precedent for mitigating actions in the face of complex botnets like Gameover ZeuS, Coreflood, and DNS Changer. In the Coreflood investigation, the FBI, working in conjunction with private industry, issued a "stop" command, essentially freezing the activities of the malware. This action protected the victims of the malware from further criminal activity while also being minimally invasive to the user's privacy. Another FBI operation, DNS Changer, resulted in the FBI authorizing industry experts to change settings on criminal DNS servers to legitimate DNS settings, while also rerouting criminal DNS IP blocks.

A more recent example of this cooperation occurred in August-October 2015 with the arrest of the main author of Dridex, Andrey Ghinkul, in Cyprus and coordinated takedown of Dridex infrastructure that occurred shortly after his arrest. The FBI, the United States Attorney's Office for the Western District of Pennsylvania, and the Computer Crime and Intellectual Property Section of the Criminal Division—in coordination with the United Kingdom's National Crime Agency (NCA)—pursued a course of action to sinkhole the Dridex botnet by disrupting the peer-to-peer network (similar to action performed in the GOZ dismantlement). On October 9, 2015, the FBI obtained court authorization to disable remaining portions of the Dridex botnet and the FBI and NCA pursued sinkhole operations in parallel, to achieve the most efficient and effective penetration of the Dridex botnet. A coordinated media campaign among the partners began on October 13, 2015, including a US-CERT Web page listing antivirus tools victims could use to remove the malware.

6. **Despite the successful disruption of CryptoLocker in May 2014, the ransomware scheme's architect, Evgeniy Mikhaylovich Bogachev, remains at large in Russia. Please describe the challenges of capturing and bringing to justice suspected criminals operating internationally, including in the Russian Federation and other nations.**

Many of the most sophisticated cyber criminal actors are located in jurisdictions that do not cooperate directly with the United States. [redacted]

[redacted]

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

There is ample evidence to show that today's cyber criminal threat is truly an international one; where the same tools, techniques, and often criminal groups themselves are impacting multiple countries with the same malware or criminal schemes. Due to the complicated nature of today's cyber criminal threat and the global impact of the most prolific actors, the FBI CyD uses a multipronged approach to strong international engagement.

The FBI CyD engages regularly with international partners through a variety of mechanisms, including: their Legat and Cyber ALAT programs; the newly formed International Cyber Crime Coordination Cell at FBI CyD headquarters; the International Internship held at the National Cyber-Forensics and Training Alliance (NCFTA) in Pittsburgh; bilateral or multilateral investigations; and embedded positions at the international cyber centers at Interpol and Europol.

- Legat and Cyber ALAT programs – Cyber Assistant Legal Attaches (ALATs) have been detailed to Legat offices since 2011 on a permanent and temporary basis to address significant cyber threats. Countries of assignment are based on the cyber threat environment and the host nation's capabilities to engage with the FBI in furtherance of activity to identify, disrupt and/or dismantle cyber threat actors and organizations. The Cyber ALATs seek to expand existing and develop new international cyber partnerships with foreign law enforcement and intelligence services through daily interaction and coordination with those agencies. Every Cyber ALAT is expected to engage with host country law enforcement and intelligence services in furtherance of FBI cases and initiatives, cover leads assigned to the Legat office from Federal Bureau of Investigation headquarters and field offices, facilitate joint investigative activity, operate joint sources where possible and assess the potential of successfully embedding a permanent Cyber ALAT directly within host country law enforcement and/or intelligence services. Cyber ALATs are currently embedded with host country law enforcement/intelligence agencies in Germany, United Kingdom, and South Korea.

- The FBI CyD maintains eight permanent Cyber ALAT positions in foreign countries. Three of these positions were newly established in fiscal year (FY) 2015: London, Ottawa, and Canberra. The already-existing permanent Cyber ALAT locations are The Hague, Bucharest, Kyiv, Tallin, and London. Two Cyber ALATs are assigned in London, one focused on national security computer intrusions and the other focused on criminal computer intrusions. During FY2015, the CyD expanded the Cyber ALAT presence by adding five new temporary locations in Tokyo, Stockholm, Tel Aviv, Prague, and Brasilia. Cyber ALATs are also deployed on long-term temporary assignments to Brussels, Sofia, Paris, Seoul, Berlin/Frankfurt, Rome, and Belgrade.

- International Cyber Crime Coordination Cell (IC4) – The IC4 was created in October 2015 at the FBI CyD to collaborate with our most trusted partners in the fight against major cyber crime. As of January 2016, two international partners and one domestic have embedded personnel within the cell in an effort to tackle the most sophisticated international cyber criminal threats.

- International Internship (ITF) – The ITF, organized by the FBI and hosted at the NCFTA, is an effort to improve collaboration and capacity building with subject matter experts in partner countries through tactical operation, intelligence exchange and training. Since its inception in 2011, the ITF has hosted a total of 22 partner countries, with four new countries planning to attend in 2016.

The FBI CyD is using the above programs to continue to improve operational outcomes where actors, infrastructure, intelligence, and evidence cross international borders. While the CyD has not had success with every country, there has been tremendous growth in the abilities and willingness of countries to help in the fight against major cyber criminal threats.

For example, in 2015, the FBI and 20 international partners effected 70 coordinated searches and arrests targeting members on the online criminal forum, Darkode, under the FBI-led operation Shrouded Horizon. To date, this is one of the biggest international operations targeting online criminal groups responsible for the development and operation of malware-based systems and cyber crime to date.

One of the biggest obstacles with foreign law enforcement cooperation is that cyber crime laws vary by country. In some places, if there is a lack of victims in the actors' home country it is difficult to take any legal action against the suspect. Also, in many countries there are very little personnel and resources devoted to cyber crime, which makes the MLAT process an even slower and lengthier process. The time it takes for these requests to be completed makes solving and sharing of information in a timely fashion difficult, especially when cyber criminals are able to move their schemes and infrastructure quickly.

8. **Recent news reports suggest ransomware attackers are also targeting public safety and law enforcement agencies. 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.

Ransomware actors do not target any one industry. Ransomware victims are targets of opportunity. While ransomware incidents at police departments are very public, there is no evidence to show that they are being sought out by the actors over any other type of victim and the ransom amounts do not differ based on the victim's line of business. There also does not appear to be any correlation between the number of files encrypted and the ransom demand.

The FBI has been contacted by many state and local government victims for help regarding ransomware incidents. As previously described, once ransomware is on a victim's computer, the only way to defeat the encryption of a ransomware variant is to obtain the actual decryption keys used by the actors operating the ransomware.

The actors behind the most sophisticated ransomware schemes are very business oriented and want to make it known that, if victims pay the ransom, they will follow through and provide the private key needed to decrypt the files. Most of the ransomware variants now include the option of allowing the victim to decrypt one file for free to show that the actors do in fact have the ability to restore victims' files. In most instances if the victims do pay the ransom to the actor, the actors will provide the decryption key.

It is up to the victim as to whether they decide to pay the ransom or not. The FBI has focused on doing significant outreach to educate the public on ransomware and the importance of keeping backups and maintaining a level of operational security when using a computer. Individuals or businesses that regularly backup their files on an external server or device can scrub their hard drive to remove the ransomware and restore their files from backup. If all individuals and businesses backed up their files, ransomware that relies on encrypting user files would not be as profitable a business for cyber criminal actors.

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.**

The FBI is using all available tools and outreach methods with private sector partners and foreign law enforcement to identify ransomware actors' command and control servers. Many of the more sophisticated actors are hosting their infrastructure in foreign countries or over anonymizing services, like the Tor Network. These steps can make it difficult for law enforcement to identify the source rapidly. When an actor's infrastructure is located overseas, the MLAT process must be used to request cooperation from foreign law enforcement agencies. Differences in the speed of this process with the speed with which actors can move their infrastructure makes investigations more difficult and less effective.

In order for the FBI to utilize signature- based detection, stateful packet inspection, or deep packet inspection technologies, they would require legal authority, such as consent from a victim or a Title III court order. The collection of this type of data via a Title III order is cumbersome and often not fruitful in uncovering information about the infrastructure the actors are using. At times less invasive investigative methods, such as a pen register trap and trace, can be used to collect information about infrastructure.

The Department, in coordination with our federal, international, and private sector partners, is taking proactive steps to neutralize the ransomware threat.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

Peter J. Kadzik
Assistant Attorney General

cc: The Honorable Ron Johnson
Chairman