U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

FEB 0 8 2016

The Honorable Ron Wyden
United States Senate
Washington, D.C. 20510

Dear Senator Wyden:

I am writing in response to your letter dated December 15, 2015, to Director James Comey, regarding your concern about the growing criminal practice of threat actors hacking Americans' devices, encrypting their personal information, and holding it for ransom.

Attached to this letter you will find an Intelligence Memo that answers the questions you posed in your letter. The FBI, in coordination with our federal, international, and private sector partners, is taking proactive steps to neutralize the ransomware threat.

I hope this information will be of assistance to you.

Sincerely,

Donald J. Good
Deputy Assistant Director
Cyber Division

Enclosure

INTELLIGENCE MEMO

FBI Cyber Division

(U) FBI Cyber Division Responses to Senator Wyden's Questions on Ransomware

(U//FOUO) On 15 December 2015 Senator Ron Wyden, Chairman of the U.S. Senate Committee on Finance, submitted a letter to FBI Director Comey regarding ransomware. Below are the questions submitted by Senator Wyden and the responses compiled by FBI Cyber Division:

(U) 1. FBI officials have been quoted as saying the Bureau often advises people "just to pay the ransom." Is this an accurate description of FBI policy with respect to ransomware?

(U//FOUO) The FBI does not advise victims on whether or not to pay the ransom.

(U//FOUO) The FBI advises that the use of backup files is an effective way to minimize the impact of ransomware and that implementing computer security best practices is the most effective way to prevent ransomware infections. 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 would not be a profitable business for cyber criminal actors.

(U//FOUO) If none of these precautions have been taken and the individual or business still wants to recover their files, the victim's remaining alternative is to pay the ransom.

(U) 2. Media reports indicate authorities in the Netherlands, working with an independent cyber security firm, effectively disabled and decrypted two popular ransomware products. What public or private options are available to assist U.S. victims of encryption hacking?

(U//FOUO) 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 the by actors, it is virtually impossible to recover the encrypted files.

(U//FOUO) 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.

(U) The top computer security companies in the world are actively monitoring the latest ransomware variants and identifying vulnerabilities that can be exploited. If a vulnerability exists, these companies publish reports on the vulnerability and in some cases create tools victims can use to recover the encrypted files. While these tools are effective for a short period of time, the cyber criminal actors running the ransomware schemes will publish updates to their infrastructure and code that eliminate identified vulnerabilities and strengthen their operations.

- (U) In April 2015, Cisco created a decryption tool for the Teslacrypt ransomware variant. Researchers were able to identify a vulnerability wherein some cases the master key for decryption was left on victim computers. The file, key.dat, was created by the actors to calculate the decryption key for the victim if the malware was not able to connect to the actor's command and control infrastructure. In July 2015, the actors behind Teslacrypt updated their malware and encryption practices with Teslacrypt 2.0, rendering this tool useless against the new variant.

- (U) In March 2014, a US computer company announced that early versions of CryptoWall created a local copy of the decryption key that was available on a victim's computer, therefore allowing victims to potentially decrypt their files without paying the ransom. As soon as this information was made public the CryptoWall authors fixed the flaw and made improvements to the encryption mechanisms. The actors also began to utilize TOR (The Onion Router) for their command and control infrastructure.

(U//FOUO) 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. There have been recent examples of law enforcement and computer security company solutions in which the actors' private keys were obtained and free decryption tools were created for victims to use to get their files back.

(U) The FBI also makes a concerted effort to proactively share information with private sector partners to assist them in protecting themselves against ransomware and other cyber threats. Specifically, the FBI Cyber Division regularly disseminates FBI Liaison and Alert System (FLASH) reports and Private Industry Notifications (PINs) to private sector partners. These products provide strategic threat actor information, including tactics, techniques, and procedures, to help private sector partners understand the context of the threat. They also provide technical indicators of compromise to enable Chief Information Security Officers (CISOs) and network defenders prevent or detect cyber compromise.

(U) 3. Media reports largely attribute encryption hacking attacks to foreign organized crime groups. Is this accurate?

(U//FOUO) The FBI does not comment on the subjects of on-going investigations. However, most of the top cyber criminal actors that we are aware of are located outside of the United States.

(U) 4. In the nearly 1,000 CryptoWall-related complaints that the FBI has reported on, for what percentage has the FBI have identified a subject?

(U//FOUO) During the course of an investigation into the malicious software Gameover Zeus (GOZ), the FBI observed several correlations between GOZ and a piece of ransomware known as CryptoLocker (a predecessor of CryptoWall). The FBI determined that Evgeniy Bogachev of Krasnodar, Russia had created and managed GOZ and the FBI subsequently indicted the actor and imposed a $3 million reward through the Department of State's (DOS) Transnational Organized Crime Rewards Program for information leading to his arrest.

(U//FOUO) In specific regards to CryptoWall, the FBI cannot comment on any suspects in the case but the FBI believes the main actors behind the CryptoWall operation are located in Eastern Europe.

(U//FOUO) The FBI's investigation to date indicates that CryptoWall is an affiliate-based ransomware operation where the main writers of the ransomware take a cut of the proceeds from individuals who rent the variant to run their own ransomware campaigns. The FBI is working diligently with private sector partners and the Department of Homeland Security to disrupt and dismantle various aspects of CryptoWall infrastructure. Through various investigative techniques, the FBI has identified monikers, hundreds of e-mail addresses, and hundreds of Bitcoin addresses related to distribution of the ransomware and organization of the backend CryptoWall infrastructure.

(U//FOUO) CryptoWall is merely one of many ransomware schemes currently victimizing people throughout the world. While CryptoWall is the most successful and well-known ransomware campaign to date, other variants such as TeslaCrypt and KeyHolder are also encrypting victim's computer files for ransom. Each of these ransomware campaigns are likely organized and executed by different groups of criminal actors.

(U) 5. If the FBI is unable to track the source of the attacks, what is it doing with its substantial experience and abilities in financial forensics to trace the payments and stop these criminal groups from profiting off their scams?

(U) Following the CryptoLocker disruption in May 2014, there has been a shift by cyber criminal actors to receive ransom payments solely using Bitcoin.

(U//FOUO) The FBI is committed to following the money in investigating all crimes with a financial component; ransomware is no exception. Even where payments are collected in cryptocurrencies such as Bitcoin, the FBI analyzes the public blockchain transaction ledger to trace payments. Ransomware perpetrators, however, often use sophisticated techniques to obfuscate their transactions on the blockchain and also gravitate toward complicit exchanges that collect little-to-no information on their customers and operate out of hard-to-reach jurisdictions.

(U) 6. Does the FBI require additional tools or authorities to assist in tracking ransom payments from victims to cyber criminals?

(U) The FBI makes every effort to work closely with the budgetary and legislative processes each year to ensure we are utilizing the full extent of our resources throughout the course of investigations. We also consistently evaluate our tools to see what additional resources we may require.

(U) FBI Strategy and Accomplishments on Ransomware

(U//FOUO) The FBI's strategy to investigate ransomware schemes is typically focused on five areas: subject identification, technical analysis, international cooperation, financial analysis, and outreach and mitigation. Each of these five areas are handled using a whole-of-government approach, sharing information among federal and law enforcement agencies domestically and internationally and partnering with private sector companies who are able to provide additional value.

(U//FOUO) The FBI works very closely with private sector companies and other law enforcement agencies that are monitoring the latest ransomware variants to identify subject identifiers related to ransomware schemes to include: IP addresses, command and control servers, e-mail addresses, Bitcoin wallets, and monikers of individuals that are selling ransomware variants in the cyber underground. The FBI employs numerous investigative techniques to learn more about these indicators and who the individuals are behind the ransomware schemes.

(U//FOUO) The FBI also values the insight that computer security companies provide on the technical aspects of ransomware variants. Cyber criminal actors are consistently improving their operations to make it more difficult for law enforcement to investigate. These actors are using anonymizing services to set up and maintain their infrastructure and are making changes to their ransomware variants on a regular basis. The FBI works closely with computer security companies and other USG agencies to understand the malware's capabilities, how new variants differ, and learn more about the infrastructure being used by the criminal actors. The FBI also does their own analysis on ransomware variants to learn more about the operation and identify investigative leads.

(U//FOUO) As much of the infrastructure being used by cyber criminals is hosted overseas, the FBI regularly works with law enforcement agencies all over the world to gain additional information on IP addresses and servers associated with ransomware schemes. Cyber criminals operating ransomware schemes typically target victims throughout the world, making it a priority for the FBI and international law enforcement agencies.

(U//FOUO) The FBI follows the money in all crimes with a financial component. Even where payments are collected in cryptocurrencies such as Bitcoin, the FBI exploits the public blockchain transaction ledger to trace payments. Ransomware perpetrators often use sophisticated techniques to obfuscate their transactions on the blockchain and gravitate toward complicit exchanges that collect little-to-no information on their customers and operate out of hard-to-reach jurisdictions.

(U//FOUO) As previously mentioned, one of the FBI's main strategies to combat ransomware is focused on outreach efforts to US persons and businesses regarding the importance implementing computer security best practices and routinely backing up computer files. Maintaining regular backup files ensures that data will not be lost in the event a victim experiences a ransomware incident. The use of backups also eliminates the decision a victim has to make on whether to pay the ransom in order to get their files back. If all individuals and businesses maintained backups of their files, ransomware schemes would not be profitable business to criminal actors.

(U//FOUO) The FBI works closely with the Department of Homeland Security/United States Computer Emergency Readiness Team (US-CERT) on mitigation efforts related to ransomware. The FBI routinely shares compromised US 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 their involvement in the remediation of a ransomware variant was the creation of a splash page relating to the Gameover ZeuS/CryptoLocker takedown to provide links to the CryptoLocker Decryption Tool created by Fox-IT.

(U) Accomplishments

(U) The FBI and our federal, international, and private sector partners have taken proactive steps to neutralize some of the more significant ransomware scams through law enforcement actions against major botnets that facilitated the distribution and operation of ransomware. For example:

- (U) CryptoLocker was a highly sophisticated ransomware that used cryptographic key pairs to encrypt the computer files of its victims and demanded ransom for the encryption key. In June 2014, the FBI announced—in conjunction with the Gameover Zeus botnet disruption—that U.S. and foreign law enforcement officials had seized CryptoLocker command and control servers. The investigation into the criminals behind CryptoLocker continues, but the malware is unable to encrypt any additional computers.

- (U) Reveton ransomware, delivered by malware known as Citadel, falsely warned victims that their computers had been identified by the FBI or Department of Justice as being associated with child pornography Web sites or other illegal online activity. In June 2013, Microsoft, the FBI and our financial partners disrupted a massive criminal botnet built on the Citadel malware, halting Reveton's distribution.