Statement of Adam Meyers

For the Senate Judiciary Committee's Subcommittee on Crime and Terrorism
"Ransomware: Understanding the Threat and Exploring Solutions."

May 18, 2016

Good afternoon. I'd like to thank Senator Graham and Senator Whitehouse, as well as the members of the Committee, for inviting me to present testimony in today's hearing on Ransomware: Understanding the Threat and Exploring Solutions.

I have been involved in the research of cyber adversary activity for well over 15 years. I began my career in the defense industrial base (DIB), where I supported numerous federal customers across the military, intelligence community, and various civilian agencies in information security matters.

Since 2011 I have led the intelligence team at CrowdStrike, Inc., a commercial security technology company headquartered in Irvine, California. In my capacity as the Vice President of Intelligence, I manage a team of more than 30 professionals who conduct research on threat actors operating for Criminal, Espionage, and "Hacktivist" purposes. This team tracks the technical, cultural, and behavioral aspects of these attacks for the purpose of identifying the threat actors, extrapolating how they operate, and determining what can be done to mitigate these actions.

The observations and conclusions I am sharing today in my personal capacity are the culmination of a career spent in cybersecurity protecting a wide range of interests across both the public and private sectors. As it applies to the subject set forth by this committee, I will provide testimony on the origins of ransomware and the manner in which the threat actors executing these malicious attacks operate, as well as discuss what can be done to counteract these threats.

A Brief History of Ransomware

Ransomware is a scourge; it is software designed with the malicious intent to compel a victim to pay a monetary ransom in exchange for access to their own data. Modern ransomware originated in the mid-2000s, and the earliest incidents closely mirror what we see every day—a victim receives an email containing a malicious payload that, when opened, sets off a chain of events that can ultimately cost the victim irreplaceable data, memories, and time. Even more terrifying is the use of "exploit kits" that can deliver ransomware to an unsuspecting victim who simply visits a legitimate website that has been compromised by an adversary.

Historically, there have been two primary modes in which ransomware operates: encryption-based and fear-based. The fear-based model attempts to scare victims into paying a ransom under the threat of prosecution for software piracy, possessing pornographic/forbidden material, or losing access to the victim computer. This ransomware, far more common in the beginning of this decade, would create a warning for the user of a system; often it would purport to be from a law enforcement agency.

Fear-based ransomware, commonly called "scareware", was a successor to fake anti-virus schemes where a victim would become infected, and a message would advise the victim that some threat was detected and that they needed to pay to remove it. These early schemes relied on credit card payments, which would come to be replaced by cryptocurrency as credit card companies were able to interdict these charges.

Some of the more common schemes of fear-based ransomware would accuse the user of accessing child pornography or copyrighted material, and advise them they were obligated to pay a fine. Fear-based ransomware variants have become less common as encryption-based ransomware exploded over the past several years.

Incidents of encryption-based ransomware date back to the mid-2000s. These variants encrypt components of the victim's filesystem using a variety of cryptographic algorithms, leaving behind a ransom note demanding payment for the decryption of these files. A variant known as "Cryptolocker" kicked off the modern ransomware epidemic in 2013. This variant demanded the victim pay several hundred dollars, and it would begin incrementing the price of the ransom over time until ultimately destroying the decryption key.

Cryptography in Ransomware

Early ransomware used flawed cryptographic systems, which security analysts were able to exploit to recover data. The attackers learned from these mistakes and built better cryptography into their tools. Around this time, the attackers learned to target automated backups made by the operating system to further complicate any possible recovery by the victim.

Modern ransomware, which encrypts the victim's data, generally uses a cryptographic system known as asymmetric or public key cryptography. Asymmetric cryptography relies on a key that is split into two components: a public key and a private key. The ransomware initially communicates with the adversary's infrastructure to generate the key pair. The ransomware uses the public key to encrypt the victim's data, which can only be decrypted with the private key that the attacker retains. Once the victim pays the ransom, the attacker provides access to the private key, which can then be used to decrypt the data. In the case of Cryptolocker, the attacker would provide a decryption tool that included the private key; this would be used by the victim to decrypt their data.

Distribution of Ransomware

Cryptolocker was delivered frequently as a secondary payload from a botnet infrastructure known as Gameover Zeus (GOZ), which was used to conduct various criminal activities ranging from Account Clearing House (ACH) fraud, theft of banking credentials, and potentially even to collect documents that appeared to be related to intelligence collection aligned with the interests of the Russian Federation.

In May 2014, in concert with private industry researchers, the international law enforcement community and the U.S. Department of Justice conducted an operation to disrupt both GOZ and Cryptolocker. The effect of this disruption permanently impacted both the distribution mechanism of Cryptolocker and the infrastructure that victim systems would attempt to communicate with to negotiate the encryption key. Although this operation was successful in disrupting Cryptolocker, soon copycat variants emerged. Cryptowall quickly rose to prominence, succeeded by a variety of other variants known by names such as TorrentLocker, Teslacrypt, Locky, Cerber, and numerous others.

The distribution of ransomware relies on other elements of the criminal ecosystem; services such as pay-per-install botnets, loaders, exploit kits, and spam botnets are used to distribute the ransomware for the attacker. These services of course require the ransomware adversary to pay for their use, creating a business cost for the attacker to conduct operations. The relationship between the proprietors of these services and the ransomware actors is symbiotic. In order to monetize their botnets, the botherders (those who operate botnets) need the ransomware actors to pay them, while these services are required to distribute the ransomware to victims.

This is an important relationship to understand. The ransomware does not self-propagate; it rides other services in order to reach its target. Ransomware can also be delivered through affiliate models, known in Russian slang as “partnerkas”; this simply means that the ransomware is built and operated by actors who provide commission payments in exchange for distribution to victims. Partnerkas are a common theme in the interconnected criminal ecosystem; they have been observed in use for everything from online pharmaceutical markets to the distribution of ransomware.

Ransomware Revenue

The revenue generated by ransomware is not insignificant; this is perhaps the biggest challenge with dissuading attackers from continuing to develop and deploy these threats. Open source reporting indicates millions of dollars were paid to the actors behind Cryptolocker, while other sources indicate the Cryptowall actors made significantly more, though this appears to be unvalidated.

Through my team’s own research, we observed as one niche player in three months made $73,000 from their ransomware campaign, and they appear to only be getting started. The attraction for attackers to use ransomware is obvious—it provides huge payoff with little investment.

These attackers have two choices: they can purchase ransomware as a software package, or they can build their own. The sale of ransomware illustrates the breadth of the criminal ecosystem; a relatively novice or unsophisticated actor who finds their way into the right forum can go about buying a ransomware package, enlisting the services of a botherder to distribute their payload and a law enforcement-resistant infrastructure provider to host their command and control systems with relative ease.

Once they have employed these services, they simply watch as the money flows in. The money collected in ransom payments is increasingly using Bitcoin or similar “cryptocurrency”, which can be rapidly used by the attacker or transferred into another currency of their choosing. Some of these actors even factor the volatility of the cryptocurrency into their ransom demand ensuring they don’t lose any profits due to market changes.

The ransomware adversaries have recently taken further actions to complicate the interdiction and tracing of funds by employing The Onion Router (TOR) hidden services, which utilize TOR’s anonymizing capabilities to mask where the command and control infrastructure is housed.

Targeting and Impact

Ransomware is increasingly making its way into the public eye as hospitals, local governments, law enforcement, and schools are forced to pay the ransom in order to recover their critical data. Beginning in 2016, a trend emerged that has become quite common: hospitals across the United States and Europe have been locked out of their own data and forced to pay a ransom. The adversaries behind these attacks and others who are looking to generate revenue have surely taken notice of these increasingly desperate stories, which in some cases even speculate that medical procedures could be delayed by these attacks.

This trend, unfortunately, is not likely to dissipate in the near future. Organizations lack comprehensive protection, fail to ensure they maintain adequate offsite backups, and in general do not have any safeguards or countermeasures to stop ransomware from impacting their operations. While it is true the ransomware does not self-propagate as mentioned earlier, if one person in a large organization infects their computer, and that computer has a shared drive or folder, the ransomware can impact far more than just that one system, encrypting every file in the organization.

Threat actors have likely taken note that victims such as hospitals have paid ransoms in the tens of thousands of dollars in order to recover their data, prompting them to look for other victims who provide critical services to target. At least one actor has begun conducting targeted ransomware attacks. This involves a comprehensive penetration of a victim enterprise, where the attacker achieves administrative access across the entire company, delivering a devastating blow by distributing ransomware across the entire network, effectively crippling the victim.

MItigating Damage and Stopping Ransomware

Ransomware is typically distributed in four ways: email, pay-per-install botnets, exploit kits, and targeted breaches. Email distribution often employs a scare tactic using subjects threatening legal, financial, or employment impact against the victim. These emails will generally deliver a malicious file, which appears to be a legitimate document but in fact it silently installs the ransomware that encrypts the victim's data before delivering a ransom note. In recent months, overlap between spam botnets used to deliver these emails have illustrated the interconnections between the ecosystem of online criminal activity. The similarities between the delivery of payloads such as the banking Trojan Dridex and ransomware packages such as Locky and Cerber demonstrate a deep connection in the underground between spam botnets, loader botnets, and the actual payloads.

Pay-per-install botnets are delivered by a variety of means, but once on a victim system the proprietor of that botnet can sell access to that system to the highest bidder. Exploit kits capture victim web browsers, and subject them to a battery of tests in order to identify a vulnerability. Once a suitable vulnerability is identified, it is exploited and a malicious payload is silently deployed.

Targeted ransomware is currently less common. In this scenario, an attacker with sufficient skills identifies a victim they think will pay, compromises that victim's enterprise, and moves laterally until achieving administrative access that they can then use to deliver the ransomware across every system belonging to the victim.

Individuals and corporations seeking to protect themselves must maintain adequate backups; incremental backups that are routinely stored off the network are essential to recovering from a ransomware attack. Proactive use of threat intelligence can also help organizations mitigate the impact of ransomware that in many cases necessitates the ability to connect to the attacker's infrastructure in order to negotiate the encryption keys before encrypting the data.

Ransomware frequently uses a technique known as domain generation algorithms (DGA) to avoid network-based countermeasures. A DGA creates a dynamic command and control domain based off of an algorithm developed by the attackers. This ensures that if their ransomware is identified and analyzed, an organization cannot simply block the command and control host, which is constantly changing.

Through detailed analysis of this DGA, organizations can predict which domains may be used by the ransomware in the future and proactively block them, preventing the ransomware from negotiating the cryptographic key. While this level of analysis is not plausible for every organization, it can provide the most effective defense against these threats.

Analysis of ransomware can also illuminate potential "vaccination" opportunities. Often during the initial execution the code will check whether it has already run on the victim system, checking for markers that, if present, will signal that it need not continue its routine. By proactively creating these markers, it is possible to prevent the code from ever having the opportunity to encrypt the intended victim's data. Behavior-based security technology can detect the scanning for files and the encrypting of them, as well a other unique aspects of ransomware, which can then be used to prevent the ransomware from successfully deploying to the system.

In closing, ransomware continues to be an attractive tool for criminals who seek to terrorize individuals and businesses in order to extort payment in exchange for sensitive data. Ransomware is continuously being developed in order to improve effectiveness, reach, and impact. These tools are distributed amongst a global criminal ecosystem that exists outside of the purview of law enforcement. Individuals seeking to protect themselves must remain vigilant and ensure they make judicious backups of their data. As long as victims continue to pay these ransoms, these malicious actors will continue to be emboldened to operate.

Thank you for the opportunity to testify before you today. I look forward to your questions and our continued discussion.