THE ICIT RANSOMWARE REPORT

2016 WILL BE THE YEAR RANSOMWARE HOLDS AMERICA HOSTAGE

AUTHORS:

JAMES SCOTT (ICIT SENIOR FELLOW – INSTITUTE FOR CRITICAL INFRASTRUCTURE TECHNOLOGY)

DREW SPANIEL (ICIT VISITING SCHOLAR, CARNEGIE MELLON UNIVERSITY)

ICIT | Institute for Critical Infrastructure Technology

Expert research contributed by the following ICIT Fellows:

- Danyetta Magana (ICIT Fellow – President, Covenant Security Solutions)
- Igor Baikolov (ICIT Fellow – Chief Scientist, Securonix)
- Brian Contos (ICIT Fellow – Vice President & Chief Security Strategist, Securonix)
- John Menkhart (ICIT Fellow – Vice President, Federal, Securonix)
- George Kamis, (ICIT Fellow – CTO, Forcepoint Federal)
- Stacey Winn (ICIT Fellow - Senior Product Marketing Manager, Public Sector, Forcepoint)
- Thomas Boyden (ICIT Fellow – Managing Director, GRA Quantum)
- Kevin Chalker (ICIT Fellow – Founder & CEO, GRA Quantum)
- John Sabin (ICIT Fellow – Director of Network Security & Architecture, GRA Quantum)

Contents

Introduction:

2016 is the year ransomware will wreak havoc on America's critical infrastructure community. New attacks will become common while unattended vulnerabilities that were silently exploited in 2015 will enable invisible adversaries to capitalize upon positions that they have previously laid claim. "To Pay or Not to Pay", will be the question fueling heated debate in boardrooms across the Nation and abroad. Ransomware is less about technological sophistication and more about exploitation of the human element. Simply, it is a digital spin on a centuries old criminal tactic.

Early in the evolution of structured path systems, the most direct roadways that connected civilization were predominantly used by more privileged members of society and armies. Eventually those who could afford horses or carriages used the roads to travel and merchants used the roads to transfer their wares. Both parties had the money of their birth or labors. Consequently, the roadways became prey to travelling footpads referred to as highwaymen. Modern stories have romanticized these figures into gentlemen thieves who shouted slogans such as "your money or your life" prior to robbing their prey. The culprits were ransoming their prisoners with a choice. Either pay a "travelers fee" or suffer the consequences imposed by a masked adversary. Provided that the thief was honorable enough to allow his victims to live, authorities had a difficult time investigating the crimes and apprehending suspects because the adversaries were mobile. Consequently, culture had to adapt in response to the threat in order for any meaningful change to occur. Carriages began employing guards. People began travelling in groups and travelling at reasonable hours. As roadways became more traversed, highway crime decreased because the risk of getting caught began to outweigh the reward.

The internet is not unlike the aforementioned roadways. Initially, only a privileged few such as security researchers, the military, and a rich few, had access. Attackers could have made money from exploiting the sparse number of victims, but it was not until a greater influx of unwary victims began moving about that real profit could be realized. Ransomware threat actors adopt the highwayman mentality by threatening the lifeblood of their victims – information – and boldly offering an ultimatum. Despite recognition of the threat, the adversaries remain a numerous and nebulous bunch. Law enforcement has neither the time nor the resources to track down the culprits. Only a societal cybersecurity reformation in user awareness and training will deter the attackers.

Security firms like Kaspersky, Covenant Security Solutions, Forcepoint, GRA Quantum, Trend Micro and Securonix predict a dominant resurgence of ransomware attacks in 2016. Already, healthcare organizations, who were previously off-limits targets among ransomware threat actors, have been brutally and relentlessly targeted with inbound attacks intent on leveraging patient lives against the organization's checkbook. This shift may be largely backed by the more sophisticated Advanced Persistent Group Threat actors who are entering the stage because ransomware attacks are under-combated and highly profitable. According to Brian Contos, ICIT Fellow and VP & Chief Security Strategist at Securonix, attackers are pivoting to ransomware because "[It] is a volume business. It's simple, relatively anonymous and fast. Some people will pay, some will not pay, so what. With a wide enough set of targets there is enough upside for these types of attacks to generate a steady revenue stream." Ransomware has been

around since 1989 but its popularity decreased in favor of other malware because the number of internet enabled victim devices was not exceptionally beneficial to the adversary's profit margin. Now, with prevalence of mobile devices and the looming shadow of the internet of things, the potential threat landscape available to ransomware threat actors is too tantalizing a target to ignore. Danyetta Fleming Magana, ICIT Fellow and President and Founder of Covenant Security Solutions elaborates that "The world is a living and breathing digital planet, and over the past decade is has accelerated into a gorgeous global information field. The internet remains the single most common vehicle for billions of communications and business transactions on a daily basis. As new technology becomes available, more and more people and businesses will be connected to the internet in a variety of ways, making most of them prime candidates for a cyber-attack." Society now relies on constant access to the vast stores of data gathered from constant communication of people, devices, and sensors. Information security specialists and the technical controls that they implement must become adaptable, responsive, and resilient to combat emerging threats.

Ransomware cyber-criminals occupy a unique niche in the attack surface. Unlike hackers who attempt to exfiltrate or manipulate data where it is stored, processed, or in transmission, ransomware criminals only attempt to prevent access to the data. Aside from Advanced Persistent Threat groups, hackers, in general, worry about what they can steal. Ransomware criminals concern themselves with what they can disrupt. As harsh as it sounds, businesses can easily continue operations after a data breach. Customers and end users tend to be the long-term victims. The same cannot be said for an active ransomware attack. Business operations grind to a halt until the system is restored or replaced. Moreover, unlike traditional malware actors, ransomware criminals can achieve some profit from targeting any system: mobile devices, personal computers, industrial control systems, refrigerators, portable hard drives, etc. The majority of these devices are not secured in the slightest against a ransomware threat.

One reason that ransomware is so effective is that the cybersecurity field is not entirely prepared for its resurgence. Attacks are more successful when effective countermeasures are not in place. Information security systems exist to detect and mitigate threats, to prevent data modification, to question unusual behavior, etc. After it is on a system, ransomware bypasses many of these controls because it effectively acts as a security application. It denies access to data or encrypts the data. The only difference is that the owner of the system does not own the control. That is not to say that ransomware goes unchecked. Many security applications detect ransomware based on its activity or the signature of the variant. Security firms are consistently developing and releasing anti-ransomware applications and decryption tools in response to the threat. However, solutions do not always exist because some encryption is too difficult to break without the decryption key. For variants of ransomware that rely on types of strong asymmetric encryption that remain relatively unbreakable without the decryption key, victim response is sharply limited to pay the ransom or lose the data. No security vendor or law enforcement authority can help victims recover from these attacks.

As with any cyber-crime, law enforcement's response to ransomware is limited by their constraints (training, personnel, budget, etc.). The FBI leads the effort to prevent the spread of ransomware and respond to incidents. Their Internet Complaint Center allows victims to report ransomware attacks for investigation. In some cases, such as with Cryptolocker, the FBI has partnered with foreign law enforcement to neutralize a threat. Similarly, the Department of

Homeland Security (DHS) devotes resources to analyzing and responding to ransomware threats through U.S. CERT. Whenever an attack is reported to law enforcement, more information is gathered about the ransomware and the attacker's tools, tactics, and procedures. The information is aggregated and used in operations, such as Operation Tovar, to dismantle ransomware operations at the source and recover decryption keys from the captured servers. These large efforts are scarce because most ransomware attacks come from a distributed number of script kiddies and second-hand adversaries who purchased the malware. These more numerous attackers are one of the main differences between ransomware campaigns and APT attacks. There is no central command or primary adversary to focus countermeasures upon.

The other reason that anti-ransomware efforts are stunted is that the opposition is not unified in a response procedure. Most security vendors advise the public (who are not yet victims) to never pay the ransom and to focus on mitigation efforts instead. Mitigation is excellent so long as one negligent employee does not mistakenly compromise the entire system by opening an email. Afterwards, reality sets in. Victims have to make a very difficult decision. Either pay the ransom without knowledge of who receives that money and what further harm is done with it or to lose all of their data behind a layer of encryption. Larger agencies, such as the FBI and DHS have the resources and technical expertise to respond to cyber-attacks in a responsible and rational manner. Smaller law enforcement organizations, such as local police forces, might lack the resources necessary to respond appropriately. Consequently, on a few occasions, police forces have paid the ransom demand to free their systems and resume critical operations. Now, law organizations would only have paid the ransom after exhausting all other options. However, the decisions invoke a feeling that law enforcement bodies may not be the singular solution to the threat. Brian Contos remarks, "If they can't protect themselves adequately we shouldn't expect them to solve all our problems for us." Further, ransomware attacks, especially those against individual users, only demand a few hundred dollars at most from the victim. In comparison to the APT threats and other forms of cyber-crime costing millions of dollars per incident, it seems unlikely that agencies will devote significant resources to investigating individual attacks. From law enforcement's perspective, a home burglary results in greater loss than a singular ransomware attack. Executives at Forcepoint contends that, "The FBI, one of the leading law enforcement agencies tasked with pursuing cybercrimes, has stated that they will assist victims with traditional hacks. In cases of ransomware; however, they are working out the best response approach for victims of these types of attacks." In point of fact, in October 2015, Joseph Bonavolonta, the Boston-based head of the FBI's CYBER and Counterintelligence Program, said, "To be honest, we often advise people just to pay the ransom." In response to pressure from Senator Ron Wyden, the FBI clarified that its position was only to pay the ransom if mitigation steps failed and the only other option was to lose the files. More or less, victims' response amounts to reporting the incident to the FBI and hope that the threat actor is eventually caught. The victim will never recover their ransom (if they paid). Despite increased ransom demands, the response for businesses is not exceptionally better. According to Symantec, "Information security researchers, however, suggest that some cybercriminal extortionists have found $10,000 to be the sweet spot between what organizations are willing to pay and what law enforcements are reluctant to investigate." Again, this response may be justified in that the FBI and DHS also must handle significantly larger incidents. As the internet has no borders, in many cases these agencies do not even have the authority or capability to respond even if the attacker was a known entity.

Cyber-crime is a shared problem that the public and private sector need to collectively address. Ransomware, as a fraction of cyber-crime, is no different. Collaboration and collective cybersecurity improvement is the best strategy for mitigating the ransomware threat and reducing the impact of successful attacks. As initiatives to increase societal cybersecurity training and awareness improve, the attack surface and profitability of ransomware and other malware campaigns will decrease. Imagine how few malware attacks would succeed if no one opened their email! At the same time, public and private sector solutions to malware attacks will improve through shared information to address these problems at their source.

Origins of Ransomware:

The first ransomware, the AIDS trojan, was originally developed by biologist Joseph Popp. Popp passed 20,000 infected floppy disks out at the 1989 World Health Organization's AIDS conference. An accompanying leaflet warned that the software on the disk would "Adversely affect other program applications" and that "you will owe compensation and possible damages to PC Cyborg Corporation and your microcomputer will stop functioning normally." Nevertheless, users booted the disks and infected their own machines. To their credit, malware was relatively scarce at that time because significantly fewer users had access to computers. Similar to some modern ransomware, the AIDS trojan displayed a pretentious display message, chastising the mistakes of the user and eventually informing them to send $189 to PC Cyborg Corporation's P.O. box in Panama in order to free their system. The AIDS trojan counted the number of times that the computer was booted. When the counter reached 90, the malware would hide the directories and either encrypt or lock the files on the C drive. The AIDS trojan ultimately failed because it had a limited number of targets and because a decryption process was quickly developed. Strikingly, the two derivative ransomware variants, crypto ransomware and locker ransomware, follow the same tactics as Popp's 1989 campaign. Even more surprising is that the ransom has not significantly increased for the average user. Instead, global economics, the advent of the internet, and the reliance of technology has expanded the threat surface to include international organizations that are better resourced than the average user. Modern malware evolved to target people and organizations in economically developed nations because their reliance on technology allows it to succeed and to spread. Throughout the nineties, malware was predominantly used for pranks, vandalism, or to gain notoriety. Then, in the early millennium, the threat landscape shifted and attackers began to develop and deploy sophisticated malware to steal secret information, to inflict physical harm on remote systems, or to financially profit. Advanced Persistent Threats (APTs) usually developed for the former two categories while ransomware evolved under the latter motivation.

Ransomware reappeared around 2005 in the form of fraudulent applications, fake spyware removal tools (SpySheriff, etc.), and malicious "performance optimizer" applications (PerformanceOptimizer, RegistryCare, etc). These campaigns targeted Windows and Mac personal computers. Warnings of corrupt files and unused registry entries were used to panic home users into paying $30-90 for a license to a tool that often did nothing for the system. Also in 2006, a forerunner to modern crypto ransomware surfaced as the Trojan.Gpcoder family of malware. Gpcoder used weak symmetric encryption algorithms and was easily decrypted.

Nevertheless, by 2006, other attackers saw the potential of emulating Gpcoder. Trojan.Cryzip and Trojan.Archiveus appeared in 2006. According to Symantec, "Cryzip copied data files into individual password-protected archive files and then deleted the originals." Cryzip was disarmed when researchers discovered that the passcode was embedded in the trojan's code. Archiveus emulated Cryzip except that it asked victims to purchase medication from specific online pharmacies and submit the order identification number instead of asking for a cash transfer. Researchers believe that the developers of Archiveus earned commission from the online pharmacies to which victims were directed. After 2006, the attack surface shifted and caused malicious adversaries to develop ransomware in different ways.

In 2008, users began to recognize the threat landscape and the necessity of fundamental information security applications such as firewall and anti-virus applications. In response, attackers began to develop and deploy fake anti-virus programs, which mirrored the form and function of legitimate applications. The fraudulent programs performed illusory scans and claimed to have found a significant number of threats to the system. Victims were then prompted to either pay for a license or subscription or to pay a flat fee ($40-100) to "fix the problems." As awareness of the scams increased, users began to ignore the applications (both when prompted to download or after the fact) or to remove the applications altogether. The underlying problem in the attack vector was that it relied on user attention to initiate the download or respond to the advert and it depended on user panic and response to receive payment. After developing and deploying the application, the adversaries had no further leverage to entice users to pay.

By late 2008, Trojan.Ransom.C, the first locker ransomware emerged. Locker ransomware locks the user interface of the host machine, thereby disabling the victim's access to their system, often by disabling control of the mouse, some of the keyboard, and other system components. Locker ransomware spread like malware, often through malicious emails and driveby downloads. Ransom.C spoofed a Windows Security Center message, locked the host, and prompted victims to call a premium-rate phone number to reactivate a license for security software. Victims could not ignore locker ransomware. If they wanted to regain access to their system, then they had to either enter a payment voucher number or they had to wait for a vendor solution and learn to deploy it. Keep in mind, that mobile devices were not as capable or as prevalent in 2008 as they are now. Many victims did not have another system on which they could access the internet to search for a vendor solution, let alone have the know-how to decrypt their own systems. Consequently, attackers increased the ransom accompanying locker ransomware by 200-300% to $150-200 per infection.

By 2012, locker ransomware surpassed fake applications because it did not require conscious user action to infect a system. Locker ransomware campaigns became more blunt, telling users about the infection and about their inability to use the system unless a ransom was paid in the desired digital currency. Attackers optimized their social engineering endeavors and the display prompt to incite the most panic in victims in order to minimize victim's ability to react rationally. Attackers posed as law enforcement, claiming on the realistic prompt displayed on the locked screen that the system was locked because the users had pirated music, movies, or software or because the user had accessed illicit content such as child pornography, human trafficking sites, etc. Naïve victims believed that they were paying a fine instead of paying the licensing for a fake service or a ransom. The success and profitability of locker ransomware campaigns declined between 2012 and 2014 because calls to law enforcement and efforts of

security researchers increased the awareness of the scams and the availability of vendor solutions. Further, the prevalence of APT activity has resulted in an increased awareness of social engineering tactics. Rather than adopt more sophisticated tactics, ransomware groups began to shift their development to crypto ransomware.

Since 2013, attackers have been migrating back to crypto ransomware, similar to Popp's AIDS trojan and Ransomware.C, except with stronger encryption algorithms. Crypto ransomware evolution has accelerated over the few years since is reemergence because cyber-criminals have copied each other and adapted upon successful and failed strategies. Successful attackers typically rely on industry standards of encryption, such as RSA, triple Data Encryption Standard (3-DES), or the Advanced Encryption Standard (AES). Crypto ransomware is even more blunt than locker ransomware; often, presenting the intention of the malware and the demand for payment without pretense. Because the malware is more expensive to develop, more sophisticated, and more difficult to remove, attackers increased the average ransom to about $300 per infected host; however, targeted attacks against businesses and critical systems have led to significantly higher ransom demands. As of 2016, ransomware is mutating again to be more vicious and less predictable than in the past. This transition may be the result of adoption by more knowledgeable and ruthless adversaries, such as Advanced Persistent Threat groups.

Overview of Ransomware:

If you wanted to secure the valuables in a room, you could adopt one of two basic approaches. You could lock the valuables in container (a safe, a chest, etc.) so that only those with the key could access them or you could lock the door so that no one could access the room. Analogously, there are two types of ransomware, crypto ransomware and locker ransomware. Crypto ransomware encrypts personal data and files so that the victim cannot access those particular resources unless they pay the ransom. Locker ransomware prevents the victim from using the system at all by locking components or all of the system. Generally, ransomware is profitable because it leveraged society's digital lifestyle against itself. Ransomware locks the devices and data that some value more than their real world interactions. Ransomware depends on the majority of users reacting out of ignorance, fear, or frustration. The most internet dependent nations, United States, Japan, United Kingdom, Italy, Germany, and Russia, are also the most targeted by ransomware. The average ransom for either ransomware is around $300, as of 2015. One might notice that $300 might be significant for an individual; however, the average includes attacks on commercial businesses. In some cases, users might be charged less. In any case, $300 is less than half the price of a new laptop or mobile device; which is critical to the nature of the attack. Adversaries must keep the ransom proportional to the value of the infected host and the ability of the victim to pay. Cybercriminals choose which type of ransomware to deploy based on their skill set, the specifications of the target system, and their prediction of how each type might affect the target victim. In the former analogy, you might have decided that the best approach was to secure the valuables in a safe and then to lock the door. Luckily, a hybrid ransomware has not yet been popularized; however, with more sophisticated adversaries entering the arena, the development of more sophisticated or hybrid ransomware is only a matter of time.

Types of Ransomware:

Locker Ransomware:

Locker ransomware is typically spread through social engineering, phishing campaigns, and watering-hole sites. According to Symantec, about 36% of binary-based ransomware detected in 2014-2015 was locker ransomware. Computer lockers restrict user access to infected systems by either denying access to the user interface or by restricting the availability of computing resources. Certain capabilities, such as numeric keyboard functionality, might remain unlocked while the rest of the keys and the mouse are locked. This design increases user frustration while restricting user action to following the attacker's instructions. This type of ransomware is akin to the locked door in the earlier analogy. Locker ransomware usually leaves underlying files and systems unaffected; instead, it only restricts access to the interface. This design also means that locker ransomware can often be removed easily by restoring the system to a restore point or by deploying a commercial removal tool. In the previous analogy, this is akin to removing the door to access the contents of the room.

The contents of a room tend to remain unharmed if a door is either knocked down, unlocked, or if it is gingerly removed at the hinges. Because the computer locker can be removed without harm to the valuable data, locker campaigns depend on inciting panicked irrational thought in victims. In unsophisticated campaigns, a display page or a banner tells the user that the system will be unlocked if a fine (~$200) is payed, usually through payment vouchers. Victims can purchase vouchers from local stores, credit shops, or "loan outlets." Locker ransomware relies on vouchers because the victim cannot access a cryptocurrency market to purchase Bitcoins because the user interface is disabled.

More sophisticated schemes strongly incorporate social engineering into the scam to pressure the user into paying the fee. The tactic exploits the victim's trust in law enforcement, the need to obey the law, and the fear of the consequences, by invoking imagery and wording reminiscent of law enforcement. For example, a display page might claim that the FBI has locked the computer in suspicion of downloading child pornography or pirating movies. The page will offer to unlock the system if a fee is paid by inputting a numeric code (usually an account number or voucher) into the page or by calling a listed phone number. Any rational user would realize, at the very least that:

A. (Hopefully) The user was not engaging in the alleged illegal activity.
B. It makes no logical sense for the FBI to remotely lock down a computer instead of just showing up and arresting a suspect.
C. The FBI (or whomever) would not accept a "fee" to ignore due process.

Nevertheless, locker ransomware has proven a profitable attack vector, likely because of the victim demographics of its infection vectors. How many senior citizens, who have flawlessly obeyed the law for their entire lives, will input their credit card or financial information into a page telling them that a law enforcement organization will arrest them if they do not immediately pay the fine? Even if they understand that the ransomware is malware, how many sheepish teenagers would use their parent's credit cards to pay the fine to not have to explain that they how they infected their computer on an adult web site?

If the victim was actually engaged in the illicit activity described on the ransom demand, then they might be more likely to pay it, even if they suspect that it is a scam. For instance, many young people visit adult websites and digital piracy websites, through which locker ransomware is known to be distributed. Because the victim already feels guilty or ashamed, they are less likely to think rationally or to seek outside help. Here, the threat actors are leveraging human nature against the victim to achieve their desired outcome. As knowledge of locker ransomware increased, the pool of victims and the profitability diminished.

Attackers abandoned locker ransomware in favor of its more robust counterpart, crypto ransomware. Locker variants are still developed, but they are less numerous than crypto ransomware families. However, 2016 may be the year that locker ransomware reemerges because locker ransomware can infect emerging technology such as mobile phones, wearable devices, and systems connected to the "internet of things". Unlike personal computers, these alternative devices might lack system restore capabilities. User options might be limited to: pay the ransom, pay for a vendor tool to remove the ransomware and then figure out how to deploy and operate the tool, or to restore the device to factory default (if the option remains unlocked). Even in large campaigns, adversaries tend to scale the ransom to the victim demographics' ability to pay. What if the ransom to unlock an IPhone or smart watch is significantly less than cost of the vendor solution? What if the ransom is low enough (say $0.99) that users are willing to pay the ransom because it is more convenient than finding a software solution and then learning how to deploy it on the locked device. Those readers with social media may be familiar with the Facebook scams (offering cheap sunglasses, life-hacks, etc.) that appear when a profile is compromised. The victim's profile propogated the malicious attachment or url to their contacts by either posting on their page or by privately messaging their friends. Now, imagine if locker ransomware spread in the same fashion, texting a malicious link to every device in the victim's contact book. Even a low ransom (less than $0.99) could be extremely profitable if the ransomware is propagated from every infected device.

Crypto Ransomware:

Instead of restricting user action by denying access to the user interface, Crypto ransomware targets the data and filesystems on the device. The critical system files and functionality tend to remain unaffected. The victim can use the computer to do anything except access the encrypted files. Crypto ransomware often includes a time limit, after which the decryption key may or may not actually be permanently deleted if the victim does not pay the ransom on time. People do not think rationally under time limits; as before, the cyber-criminals are compensating for a lack of technical sophistication by leveraging human behavior against the victim. The victim is subject to the anxiety of the ticking clock, the fear of the consequences of making the wrong decision, and the fear of regret if the data is lost forever.

In 2014-2015, crypto ransomware accounted for 64% of the binary based samples of ransomware detected by Symantec. Attackers usually ask for ~$300 USD in bitcoins to unlock the encrypted files. Unlike locker ransomware, crypto ransomware still allows users to access the internet to purchase cryptocurrencies. Some variants of crypto ransomware even provide users with a site to purchase Bitcoins and articles explaining the currency. Interestingly, as Law

Enforcement Agencies and security researchers buy out digital currencies, such as Bitcoins, average users have to pay the price of inflation of the decreased commodity.

Crypto ransomware did not popularize until 2013 because attackers failed to realize that successful crypto ransomware attacks rely on current strong encryption algorithms and proper management of the accompanying cryptographic key. Prior to that, variants failed to be more profitable than locker ransomware because attackers stored the key on the host or within the malware. For some variants, the key was even the same across all samples, which means that once one person had unlocked their system, they could just post the key for any other victim to use to unlock their system.

According to information security researchers at Symantec, the current crypto ransomware threat landscape is still fragmented into new entrants into the market and mature criminal groups. Both types of attackers try to employ industry-standard encryption algorithms, such as RSA, Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES) with a suitably large key in their ransomware; however, entrants tend to lack technical skills and the operational tactics, techniques, and procedures associated with mature groups. Entrants often store encryption keys in the ransomware or they fail to fully disable a system to prevent user action. In contrast, mature cyber criminals generate a unique asymmetric key for each infected system and they wipe the session key from memory when they are finished with it. These dominant cybercriminals combine strong public/private encryption with their established operational procedures to limit victim response to paying the ransom or losing their data. Entrants operate to make a profit from naïve victims, while mature cyber criminals operate to hold hostage systems belonging to users and businesses, and to not be identified by law enforcement. To this end, the community relies on Tor, proxies, and crypto-currencies, such as bitcoins to remain anonymous.

In this digital age, the vast majority of personnel and people digitally store data vital to their profession and personal life. Only a small percent of users regularly backup all of their essential data or all of their essential systems. Crypto ransomware is often spread through Tor, botnets, or other malware. Crypto ransomware is as simple as weaponizing strong encryption against victims to deny them access to those files. After the initial infection, the malware silently identifies and encrypts valuable files. Only after access to target files has been restricted does the ransomware ask the user for a fee to access their files. Without the decryption key held by the attackers, or in some cases, a vendor decryption solution, the user loses access to the encrypted files. Even if the user regularly backs up their data, the crypto ransomware might still be effective if the user does not have the time to revert to the backup or if the user has not backed up their data frequently enough. For example, a medical organization might be a target if they need real time access to their data while a college student might be a target if they have not backed up the term paper that they are rushing to finish for the following morning. Crypto ransomware incites panic in users, but it relies more on their desperation. Because different user worry about different things (documents, photos, servers, etc.) and because cryptographic algorithms are numerous, a plethora of crypto ransom variants target the attack surface. Nevertheless, due to a lack of personal sophistication, the majority of threat actors rely upon or adapt a few successful variants.

Active Examples of Crypto ransomware:

Locky:

On February 5, 2016, medical systems belonging to Hollywood Presbyterian Medical Center were infected with the Locky ransomware. Healthcare data remained unaffected but, computers essential to laboratory work, CT scans, emergency room systems, and pharmacy operations were infected. The email system was taken down, but it remains unclear whether the system was infected or if the system was taken down to preserve indicators of compromise or to prevent further phishing emails. While media outlets reported that the adversary demanded a ransom of 9000 Bitcoins ($3.6 million), President and CEO of HPMC Allen Stefanek said that the accounts were inaccurate. After almost two weeks, the hospital paid a ransom of 40 Bitcoins ($17,000) to unlock their machines, despite ample assistance from the FBI and LAPD, because paying the ransom was the quickest and most efficient way to restore their systems. Stefanek does not believe that the hospital was specifically targeted. He argues that the attack was the result of a random malicious email. In contrast to this assertion, the attackers did not demand the typical user ransom of $210-420.

The novel Locky ransomware is not any more sophisticated than other ransomware applications, but it is rapidly spreading to victim systems. Forbes claims that the Locky ransomware is infecting approximately 90,000 systems per day and that it typically asks users for 0.5-1 Bitcoin (~$420) to unlock their systems. Locky encrypts files with RSA-2048 and AES-128 ciphers. Victims are presented with links to payment landing pages and instructions to install Tor. Security firm Proofpoint asserts that Locky was developed and deployed by the Dridex criminal organization. The Dridex criminal group is the most prominent operating banking malware. Locky is disseminated through spam emails containing Microsoft Word attachments. Each binary of Locky ransomware is reportedly uniquely hashed; consequently, signature based detection is nigh impossible. After infection, the malware deletes backup shadow copies of the operating system. Encrypted files are renamed with the .locky extension and the victim is presented with the ransom demand. Palo Alto Networks, who also connected Locky to Dridex, believes that the group has already raised several hundred thousand dollars from Locky ransoms.

TeslaCrypt/ EccKrypt:

TeslaCrypt infects systems through the Angler exploit kit, which leverages vulnerabilities in Adobe Flash (such as CVE-2015-0311). Silverlight and Internet Explorer may be exploited in absence of Adobe Flash. Angler is injected from an iframe on a compromised website. The victim is redirected to a landing page, where anti-virtual machine checks, antivirus assessments, and host analysis tools are systematically run. If all the checks succeed, then the Flash exploit is used to download the ransomware payload into the victim's temp folder. The Xtea algorithm is used to decode the payload and the ransomware is written to disk.

The TeslaCrypt binary is compiled in Visual C++. The ransomware code is encoded within the binary. After the code is decrypted into memory, TeslaCrypt overwrites the MZ binary

onto itself. The malware copies itself to %appdata%, where it also stores a SHA-256 key (key.dat) and a log file listing the files found through directory enumeration and encrypted. Encypted files feature the additional extension names of .encrypted, .ecc, .ezz, .exx, and recently, .mp3. The malware runs a few threads: a file encryption thread, a thread to monitor and terminate .exe, .msconfig, .regedit, .procexp, and .taskmgr processes, a thread to delete backup shadow files using vssadmin.exe, and a thread to contact the command and control server to communicate the sha-256 value of the key generated from key.dat, the Bitcoin address, the number of files encrypted, and the victim IP address. Although it resembles Crytolocker in design and appearance, they do not share source code. After infection, victims are presented with a pop-up window informing them that the files have been encrypted and directing them to the TeslaCrypt website, directly or through a Tor2Web proxy.

Initially, TeslaCrypt used symmetric encryption; however, after researchers from Cisco's Talos Group released a decryption tool (the Talos TeslaCrypt Decryption tool), the authors reconfigured TeslaCrypt to use asymmetric AES encryption. By late 2015, Kaspersky labs had released another decryption tool, the TeslaCrypt Decryptor. By January 2016, the threat actor had remedied the flaw in their malware and released a third version that appends the .mp3 extension to encrypted files.

TeslaCrypt originally targeted 185 file types related to 40 computer games (Call of Duty, Skyrim, Minecraft, etc.) on Windows systems. The malware capitalizes on how much victims' value the time spent in artificial realities and the intangible assets collected there. Newer variants also encrypt Word, PDF, and JPEG files. Overall, the ransomware is particularly devastating to college aged young adults. Victims are prompted to pay a ransom of ~$500 (in Bitcoins, PaySafeCard, or Ukash). Victims may decrypt a single file for free as a show of good faith.

Cryptolocker:

Cryptolocker is a crypto ransomware trojan that began infecting Windows systems in September 2013 through the Gameover ZeuS botnet, and encrypting the host data with RSA public-key encryption. The private key needed to decrypt the data was stored in the malware's command and control servers. The ransomware also spread as a malicious email attachment (a .ZIP file containing an executable with a PDF icon). Cryptolocker installs in the user profile folder and adds a key to the system registry so that it runs at startup. Next, it connects to one of its C2 servers and generates a 2048-bit RSA key pair, stores the private key on the server, and sends the public key back to the victim machine. The trojan encrypts document, picture, and CAD files on the local hard-drives and mapped network drives with the public key and logs each encrypted file as a registry key.

The vast majority of victim systems were located in the United States and Great Britain. Victims were presented with the demand that unless a 0.3-2 Bitcoin or cash voucher payment was made within 72-100 hours, the private key would be deleted and the data would be forever encrypted. Sometimes, if payment was not received by the deadline, the attackers would offer a new deadline at a higher price, marketing it as an online removal service. In November 2013, this after-the-fact service was offered as a stand-alone website. The site claimed that the private

key would be sent to the victim within 24 hours of a 10 Bitcoin payment. Even if the ransom was paid, some attackers did not decrypt the files. Cryptolocker can be removed from infected systems, but files still cannot be decrypted without the private key.

Cryptolocker and the ZeuS botnet that it relied upon were taken down in the May 2014 Operation Tovar. Afterward, the private keys saved on the servers were converted into an online file recovery tool. Overall, in its 6-month operation, attackers used Cryptolocker to extort over $3 million from victims. Security researchers estimates that only 1.3-3% of victims chose to pay. As a result of its success, numerous rebranded variants appeared on the market.

Cryptowall/ CryptoDefense/CryptorBit:

The Cryptowall family of ransomware first appeared in early 2014 and became popular after Operation Torvar dismantled the Cryptolocker network. Cryptolocker is spread through various exploit kits, spam emails (with attached RAR files that contain CHM files), and malvertising pages. When the malware is delivered, the binary copies itself to the %temp% folder. It then launches a new instance of the explorer.exe process, injects the unpacked Cryptowall binary, and executes the injected code. The malware uses the vssadmin.exe tool to delete shadow copies of files. Afterwards, it launches the svchost.exe process with user privilege and injects and executes its code in the process. Next, It tries to connect to the I2P proxies to find a live command and control server using a hash value that is created by taking a randomly generated number followed by a unique identification value. This is generated using system-specific information such as computer name, OS version, processor type, volume serial number, and other identifiers. The server replies with a unique public key and delivers ransom notes in the language based on geolocation of the machine IP address. Notes are placed in all directories where victim files are encrypted and then Internet Explorer is launched with a display page of the ransom note.

Current variants of the malware (such as Cryptowall 3.0) use I2P network proxies to communicate with their C2 infrastructure and they use the Tor network to collect Bitcoin payments from victims. Initial variants encrypted victim files with RSA public-key encryption; however, the malware has now (Cryptowall 3.0) evolved to use the AES 256 algorithm. Further, the AES decryption key is stored on the C2 server and encrypted with a unique public key. The malware includes a service to decrypt a few randomly selected files as a demonstration that the rest of the files will be decrypted if the 1 Bitcoin ransom is paid. Unlike Cryptolocker, the Cryptowall malware targets Windows systems globally; though, the United States (13%), Great Britain (7%), the Netherlands (7%), and Germany (6%) were the most affected.

CTB-Locker:

The "Curve-Tor-Bitcoin-Locker" (CTB-Locker) is a PHP based trojan that was publicly analyzed by security researcher Kafeine in mid-2014. CTB Locker is essentially a ransomware as a service (RaaS), where the attackers outsource the spread of the malware to a number of script kiddies and botnet operators (often referred to as affiliates) for a share of the paid ransoms. This RaaS model was proven and popularized by fake antivirus, click fraud schemes, and other types of malware. Though CTB-Locker remains the most abundant RaaS, other ransomware has begun to adopt the distribution channel. In CTB-Locker's model, affiliates pay the operators a monthly fee to use the malware. In other models, the originator receives a small percentage of each ransom.

Due to the affiliate model, CTB-Locker uses every infection vector imaginable. Mostly, attackers rely on exploit kits (Rig, Nuclear, etc.) and malicious email campaigns. The latter campaigns often use the Dalexis or Elenoocka downloader to deliver the malware. Dalexis is an auto-executable attached to emails as a cab file. Elenoocka and other downloaders are auto-executables hidden in ZIP or RAR archives. CTB-Locker is also available in English, French, German, Spanish, Latvian, Dutch, and Italian to accommodate affiliates and targets from most American and European countries.

The downloader drops CTB-Locker into the temp directory and it creates a scheduled task to enable reboot persistence. The file system is iterated and files that match CTB-Locker's extension list are enumerated for encryption. The background image of the system is changed and the ransom message and a clickable interface overlay the center of the screen. Victims are told that they have 96 hours to pay the ransom (variably determined by the affiliate) and that any attempt to remove the malware will result in destruction of the decryption key.

CTB-Locker uses a combination of symmetric and asymmetric encryption to restrict victims' access to their files. Rather than use RSA, which is based on prime number factorization, like most ransomware, files targeted by CTB-Locker are encrypted with AES and with Elliptic Curve Cryptography (ECC). ECC is a form of public key cryptography based on elliptic curves over finite fields and the strength of the algorithm derives from the elliptic curve discrete algorithm problem. ECC can achieve similar security levels to RSA with a much smaller key. For instance, a 256-bit ECC key provides equivalent security to a 3072-bit RSA key. The malware uses AES to encrypt the files, and then the means to decrypt the files is encrypted with an ECC public key. Consequently, only the attackers, who possess the ECC private key, can decrypt the files.

CTB-Locker is unique among ransomware in that it does not require internet access or contact with its C2 infrastructure to begin encrypting files. Network connection is not necessary until the victim attempts to decrypt their files. Payment communication is carried out over Tor and proxy sites that relay Tor traffic. After the ransom is paid, a decryption block is sent from the C2 server to the victim host.

In February 2016, attackers began to use the CTB-Locker to encrypt websites hosted by Wordpress. This variant of CTB-Locker is referred to as Critroni. The attackers hack an insecure website and replace its index.php file or index.html file with different files that encrypt the site's data with AES-256 encryption. Afterwards, a ransom message is displayed on the homepage. The prompt provides instructions for how to purchase Bitcoins and typically demands 0.4 Bitcoins. In the first week of the attack, around a hundred sites were infected; though no major domains were infected. The victims tended towards those who relied on outdated versions or vulnerable plugins. Even though the ransomware did not infect major sites, the mutation of the malware should be heeded as an indication that the overall ransomware threat is ramping up. Critroni may have just been an experiment or an innovative script kiddie. At the moment, users who navigate to the victim site see the same ransom instructions as the administrator. Consider the implications if the attackers figured out a way to spread the ransomware onto each visitors' machine. The impact of the malware and its profitability would increase significantly.

Hybrid Ransomware:

One of the prevalent malware mitigation strategies is a layered depth. It stands to reason that in accordance with the concept of mutual escalation, attackers will begin to "attack in layers." This behavior already occurs in APT campaigns and in some ransomware attacks, where for instance, the adversary launches a DDoS attack alongside a more concerning attack. In terms of ransomware, it will be interesting to see if locker ransomware resurges with crypto-ransomware running behind the scenes. Layering the types seems unnecessary now, because victims often pay and because neither security researchers nor law enforcement can break the strong encryption used; however, if either of those cultures change, then locker ransomware, which prevents most user action, may return with controls borrowed from crypto ransomware.

Delivery Channels:

Ransomware follows the same distribution and infection vectors as traditional malware. The primary difference is that ransomware threat actors often lack the sophistication to breach modern networks. These criminals either rely on more experienced members or they pay for a malware installation service, which charges by the number of installations.

Traffic distribution system (TDS):

Traffic distribution services redirect web traffic to a site hosting an exploit kit. Often, traffic is pulled from sites hosting adult content, video streaming services, or media piracy sites. Some ransomware groups, especially criminals who purchase their malware instead of developing it themselves, may hire a TDS to spread their ransomware. If the host is vulnerable to

the exploit kit on the landing page, then the malware is downloaded onto the system as a drive-by-download.

Malvertisement:

As with a TDS, a malicious advertisement can redirect users from an innocuous site to a malicious landing page. Malvertisements may appear legitimate and can even appear on trusted sites if the administrator is fooled into accepting the ad provider or if the site is compromised. Malicious threat actors can purchase traffic from malvertisement services. Redirected victims can be purchased according to geographic location, time of day, visited site, and a number of other factors.

Phishing Emails:

As with most malware campaigns, phishing emails and spam email are the primary delivery method of malicious content into a network because users are culturally trained to open emails and to click on attachments and links. Even with training and awareness programs, most organization find it difficult to reduce successful spear phishing attempts to less than 15 percent of personnel. Attackers only need a single user within an organization to click on the malicious link or attachment in order to compromise the network. The larger the organization, the greater the risk of infection through malicious email.

Botnets are used to send spam emails or tailored phishing emails at random or to personnel within an organization. These botnets and email services are a criminal enterprise unto themselves. Botnets and spam clients are comparatively cheap. It is reasonable to assume that many who purchase their ransomware may also purchase botnets and email spammers. According to Symantec, ransomware emails tend to masquerade as mail delivery notifications, as energy bills, as resumes, as notifications from law enforcement and as tax returns.

Downloaders:

Malware is delivered onto systems through stages of downloaders to minimize the likelihood of signature based detection. Ransomware criminals pay other threat actors to install their ransomware onto already infected machines. The other threat actor offers the service because the infected machine may have been an accidental infection, may be a stepping stone infection, or may no longer contain valuable data. If the ransomware threat actor actually decrypts the system, then the ransomware infection could draw attention to the other compromise; however, it could just as easily mask the other malware by focusing the user's attention on certain infected systems. Users may not suspect that there is a deeper infection after they remove the ransomware. Moreover, the ransomware infection provides the initial threat actor an easy revenue stream, even if the system was not valuable. Botnet operators are

especially fond of offering these services to ransomware and malware authors as a means of drawing quick revenue from the easily constructed botnet. Malware groups who conduct widespread phishing campaigns and watering-hole attacks may be equally willing to sell access to the systems that they compromised by accident.

Social Engineering:

Popp's AIDS trojan relied on social engineering, and human ignorance, to generate profit. The only systems infected belonged to users who ignored the plainly worded warning pamphlet. These victims were either brash or curious. In 1989, a decent percent of the 20,000 victims probably had no choice but to pay the ransom. Older ransomware relied on social engineering and illusory pressure to entice users into infecting their own machines. Fake anti-virus applications told users that their computer was at risk of numerous debilitating viruses while performance optimizers persuaded users that their system could achieve better results. Even locker ransomware that appears as a malvertisement on other sites depends on users clicking on the prompt to initiate installation.

Self-Propagation:

Select ransomware variants contain the functionality to self-propagate through a network in a fashion similar to other malware. The majority of these samples are crypto ransomware because locker ransomware is not exceptionally popular at the moment; however, Android variants of crypto ransomware and locker ransomware have appeared in the wild. These mobile applications are either downloaded from an app store or they spread through an initial victim's contact book via SMS messages to other systems. One such variant targeting Windows is the Ransomlock (W32.Ransomlock.AO) screen locker. With the emergence of the internet of things, self-propagating ransomware is likely how the malware will evolve in the future because the greatest number of interconnected devices can be infected for the minimal amount of applied effort. However, this evolution is not without its own problems. As Symantec observes, ransomware that is continuously spreading throughout the network deters victims from paying the ransom because the system will just be infected again. Criminals will have to develop a mechanism to check whether or not a system has already been infected (such as a certificate) and a mechanism to decrypt all systems belonging to a victim who has paid the ransom; otherwise, the entire business model will be upended. This could be accomplished by either simultaneously removing or deactivating the ransomware from all of the victim's systems.

Ransomware as a Service (RaaS):

When malware attacks succeed, less technical criminals try to capitalize on the threat landscape. Sophisticated threat actors can gain notoriety and additional revenue by outsourcing their malware to these script kiddies. These opportunities are also attractive to botnet operators

who do not know how to exploit their zombies. Ransomware is starting to follow the trend of other malware, in the form of ransomware as a service, through which script kiddies can use the ransomware developed by experienced criminals to exploit victims. The applications are designed to be deployed by practically anyone. The script kiddie downloads the client for free or a nominal fee, sets the ransom and payment deadline, and then attempts to trick victims to infect their own systems through phishing emails or watering-hole sites. If the victim pays the ransom, then the original creator receives a fee (5-20%) and the script kiddie receives the rest.

The Reveton ransomware may have been the progenitor of the ransomware as a service model. In 2012, the Reveton actors paid sites to spread the malware. The first free tool was the Tox ransomware, which allowed users to keep 95% of the ransom. The tool, created by a teen hacker by the same name, infected over 1500 systems and demanded a ransom of $50-200. Fearing law enforcement attention, Tox sold his service, the source code, the web domain, a database of infected systems, and the decryption keys, to an unnamed buyer for $5000. RaaS may not always be profitable. In interviews with Business Insider and Motherboard, attacker Jeiphoos admitted that his November 2015 Encyptor RaaS, had made no money, despite infecting around 300 devices. Brian Krebs comments that "Many [RaaS authors] will try but few will profit reliably (and much at that) for any period of time," he continues that those that succeed will be the ones that offer good “customer service” to script kiddies and victims alike.

In theory, it is a mutually beneficial relationship between the actual threat actor and the script kiddie because both parties generate a profit with minimal additional effort. The script kiddies can utilize a tool that they could not have created and the threat actor can focus their time on developing new variants. However, in practice, the threat actor can suffer if the script kiddie does not decrypt the systems of victims who pay the ransom because news will spread and less victims will pay in the future. If the malware becomes too ubiquitous, then security researchers will develop a decryption tool faster and the ransomware will be rendered prematurely obsolete.

Targets for Ransomware:

Unlike APT campaigns, financially motivated cyber threats, like ransomware campaigns, do not care about the individual target. Instead, they target the subset of society believed to be most likely to pay the ransom demand. Ransomware is often spread in mass in the hopes that a portion of the users will pay. Ransomware, whether purchased or developed, is relatively cheap in comparison to APT malware. Delivery is virtually free. Further, if the attacker does not intend to unlock the user system after the ransom is paid, then there is virtually no need to continuously dedicate resources to an individual attack. A small team can easily infect and ransom millions of systems. The attackers only need a few users per million of targets to pay the ransom for the campaign to be successful.

Financially motivated adversaries tend to target the lowest hanging fruit. Because different threat actors have different perceptions of the market and because the willingness to pay ransoms decreases as victim markets become over-saturated and desensitized, the targets of ransomware change according to victim awareness and willingness to pay. Some adversaries

may even widen their delivery vector to encompass multiple demographics to account for market shifts.

The Average User:

In cybersecurity, people are considered the weakest link. They are also both the most abundant resource and the most susceptible target. Individual users who are easily pressured or who are not fluent in technical solutions to ransomware are the most viable targets. As previously mentioned, this tends to include the elderly and teenagers; however, any age group is a viable target if the attacker effectively incites enough panic or fear into the victim to influence them into the illogical decision to pay the ransom. Attackers can increase this pressure by including a timer, after which the user cannot pay to recover their system or data. Even if the user knows that there is a freely available solution, such as the Tesla decoder (which deciphers the TeslaCrypt crypto ransomware), the user may not understand how to employ the solution and may opt to pay the ransom out of frustration and perceived helplessness.

Individual users are targeted because in the digital era, much of our knowledge, work, and personally valuable objects (photos, music, etc.) are stored on whatever internet enabled device we rely on. The majority of users do not consistently backup their data or follow basic cyber hygiene thoroughly enough to mitigate the impact of a ransomware attack. Symantec claims "twenty-five percent of home users did not do any backups at all. Fifty-five percent backed up some files. In terms of backup frequency, only 25 percent of users backed up files once a week. The rest only made backups once a month or even less frequently than that." Ransomware attackers depend on hitting users between backups. Even if the interval is only one day, the work from that day of labor might be worth a few hundred dollars. Further, some of the more complex variants of ransomware delete local backups, remove system restore points, and spread to any connected device (such as a backup drive). Since crypto ransomware in particular remains in the background until target files are already encrypted, external backups might be compromised before the ransom demands are even made.

Businesses:

The American economy is literally built upon intangible goods and services such as information and knowledge. Businesses large and small rely on their systems and the information contained within in order to conduct their day-to-day operations. Very small businesses, such as a mom-and-pop coffee shop might be able to process transactions without access to their POS system, but Starbucks certainly cannot. Businesses are the prime targets of ransomware because their systems are the most likely to house valuable databases, containing sensitive data, important documents, and other information; meanwhile, their systems are the least likely to be adequately secured. Businesses have the greatest access to liquid capital. Further, for many organizations, system downtime equates to loss of income and reputation. Consequently, they are the most likely to pay the ransom in order to resume operations.

The private sector is a prime target because the number of businesses to target is only less numerous than the number of personnel at each business who can be individually targeted with phishing emails and watering-hole attacks. Many organizations have redundancy systems and backup servers in case an attack succeeds; however, an equal or greater number of businesses have neither. It is unrealistic to expect a small to medium size business to have the same infrastructure as a larger business. Sometimes, extra systems such as backup and redundancy servers are simply outside of their budget. Even if the victim organization has the necessary systems, crypto ransomware has evolved specifically to account for complex victim networks. Modern crypto ransomware maps networks, enumerates drives, and spreads onto as many systems as it can before it activates. As a result, numerous systems, including the backup and redundancy systems, may be infected. Not even a large organization can ignore half their systems going offline. The organization will have to react through remediation, surrender, or allowing the loss of the data. Many organizations cannot survive the loss of essential data for an extended period. Without adequate backups, business continuity may be impossible and customers or end users may be affected. Even with a backup server and business continuity plan, a business may be susceptible to attack. Crypto ransomware can target the corporate network or individual user systems and then spread throughout the network. Sophisticated variants, (PHP.ransomware, Tesla Crypt, etc.) may remain silent on the network while they encrypt databases or files before or during backup operations. Further, many organizations have never conducted live testing of their business continuity or disaster recovery plans. What if the reversion time is unacceptable? What if a backup system is no longer operational due to a system flaw? Attackers know of these operational weaknesses. Attackers systematically target these vulnerabilities in the actual business when they make their ransom demands.

Law Enforcement and Government Agencies:

Law Enforcement and Federal Agencies are often targeted with malware attacks in response to their efforts to investigate and apprehend cyber criminals. While large organizations such as the FBI, DHS, and other federal agencies have resources which increase their resiliency, smaller organizations, such as numerous police stations and state/local government offices, have been the victims of ransomware attacks in recent years. Typically, such as the February 2016 ransomware attacks against the police of the city of Durham North Carolina, the authorities ignore this advice, ignore the demand, and revert their system to a recent backup. This decision can have consequences. In late January 2016, 300 systems belonging to the Lincolnshire County Council were infected with ransomware and had to be taken offline in response. The systems are returning to operation in March 2016. Similarly, on March 4, 2016, 6000 files belonging to the North Dorset District Council had been encrypted by ransomware. The infection had been limited by security systems in place and the council has declined to pay the 1 Bitcoin ransom. Still, in other instances, the authorities have paid the ransom in order to resume critical operations. On February 25, 2016 the systems belonging to the Melrose Police Department of Massachusetts were infected with ransomware from a malicious email that was sent to the entire department. The malware encrypted a software tool called TriTech, which police officers use for computer aided dispatch and as a record management system during patrol. The program also enables law enforcement officers to log incident reports. The department paid the 1 Bitcoin ransom on February 27, 2016.

Emergency Services:

DHS and the Multi-State Information Sharing and Analysis Center warn that cyber-attacks against law enforcement, fire departments, and other emergency services are increasing in frequency. Targets such as these, for whom lost access to systems could cost lives, are juicy targets for ransomware threat actors.

Healthcare Organizations:

The healthcare sector was not a traditional target for ransomware attacks. One theory is that attackers did not target systems that jeopardized lives. Recently, that mentality has changed for at least the group operating the Locky ransomware. Around February 5, 2016, systems belonging to the Hollywood Presbyterian Hospital Medical Center was infected with the Locky ransomware. After ten days, the administration paid attackers 40 Bitcoins ($17,000) to release the systems. Later that week, five computers belonging to the Los Angeles County health department were infected with a ransomware variant. The health department refuses to pay the ransom and will restore its systems from backups. Similarly, two hospitals in Germany were infected with ransomware at roughly the same time as Hollywood Presbyterian Medical Center. Both are restoring their systems from backup systems.

Educational Institutions:

Ransomware threat actors may target administrative systems at lower and higher education institutions. General education systems are more likely to be disrupted by a ransomware attack; though, colleges and universities are more likely to have funds sufficient to pay a sizable ransom. In February 2016, at least 2 primary school districts were targeted with crypto ransomware. Horry County school district in South Carolina paid $8500 to decrypt their 25 servers after an FBI investigation yielded no alternative action. The Oxford County school district in Oxford Mississippi was also infected around the same time. Oxford systems are operational again at the time of this writing, though it remains undisclosed whether the situation was resolved by paying the ransom or by reverting the system from backup servers.

Religious Organizations:

Religious organizations' networks are often infected with malware because their personnel are not trained to ignore phishing emails and they are unaware of cyber-threats. In late February 2016, two Churches were targeted with ransomware attacks: the Community of Christ Church in Hillsboro Oregon and St.Paul's Lutheran Church in Sioux City, Iowa. The former was

infected with the Locky variant of crypto ransomware that recently infected the Hollywood Presbyterian Hospital. The Community of Christ Church paid $570 to free their system. Information about the latter incident is more scarce, except that the church declined to pay the ransom.

Financial Institutions:

The banking and finance sector is the frequent target of botnet schemes such as the Dyre, Dridex, and Ramnit botnets. Ransomware often spreads through established bonnets. Further, the Locky ransomware is believed to have been developed or deployed by the Dridex group. Consequently, financial institutions are likely the next major sector to be targeted by ransomware, if their systems have not been infected already.

On February 17, 2016, attackers behind the TeslaCrypt ransomware issued spam emails masquerading as Visa Total Rewards emails. A malicious attachment, claiming to be a white paper containing more information about rewards and benefits, was used to deploy a JavaScript downloader that delivered the TeslaCrypt malware onto victim hosts. Ransoms of 1.2 Bitcoins within 160 hours were demanded of victims. If victims do not pay within the time frame, then the ransom doubles. The United Kingdom (40%) and the United States (36%) were the most targeted.

Target Systems:

Any system valuable to a user is a valuable target for ransomware because the profitability of the attack vector derives from inconveniencing the victim. As technology becomes more ubiquitous and society's dependence on constant access to information becomes more ingrained, the threat landscape of ransomware increases. According to Symantec, the most frequent targets of ransomware are personal computers, mobile devices, and servers and databases. Additionally, IoT devices, and critical systems (PoS terminals, medical devices, etc) are tantalizing targets.

Personal computers:

Personal computers are the current primary target of ransomware campaigns because they are numerous and easily compromised. Users tend to have poor cyber-hygiene and many users can be coerced into infecting their own systems through social engineering. Ransomware actors make less per victim than in attacks on organizations, but average users are more numerous and in general, they are more likely to pay the ransom out of frustration or lack of viable options. Ransomware variants are designed to target specific operating systems because it must leverage system API hooks to restrict victim access to the system. Additionally, some variants utilize native encryption libraries and APIs to perform the encryption and decryption of user data. Most

target Windows, but variants that target Linux, Mac, and Android are also developed. Symantec comments that like malware, most variants target Windows operating systems because Windows systems account for "around 89 percent of the OS share for desktop computers, with Mac OS X and Linux making up the rest." At least one system agnostic variant, the Browlock Trojan (Trojan.Ransomlock.AG), exists. Browlock executes as Javasccript from a web browser. Its goal is to target the segment of the victim pool not saturated with other attackers.

Mobile devices:

We live in the age of constant access to information. When you hear stories of information restriction out of places like North Korea, you probably have some knee-jerk thoughts in reaction to how a people can exist without open access to the internet. According to the PEW Research Center, as of 2016, 72 percent of American adults owned a smart phone. The global median, as of spring 2015, is about 43 percent. Those figures are further increased if one includes tablet devices, mobile game consoles, and other internet-enabled devices. For the most part, sensitive data is not stored on mobile devices. The value is the device themselves and the inconvenience suggested to most users should they choose not to pay. Since many mobile devices now automatically back data up into the cloud, mobile ransomware must heavily rely on social engineering panic in victims; otherwise, the user can just reset their device to factory default and download some or all of their data from the cloud network.

Mobile devices are almost all operated on Android or iOS. Android supports approximately 80 percent of the devices on the market, but iOS devices tend to be more expensive. There are ransomware variants that exploit both flavors of mobile device. Apple restricts the installation of application from outside of the Apple store, so ransomware may be more difficult to migrate onto a non-jailbroken iPhone. According to Symantec, "A ransomware developer who wishes to explore this route would first have to obtain an enterprise developer certificate from Apple, build their app, sign it with the enterprise certificate, distribute it to potential victims, and convince them to install it. The problem for the cybercriminals in this scenario is that their room to maneuver could be highly restricted and Apple could easily shut down their operation simply by revoking the certificate. This makes ransomware development activity for iOS very risky with little prospect of payback." Android devices are more numerous and more susceptible to attack, so the majority of mobile ransomware targets Android devices.

Ransomware targeting Android devices already exists. In June 2013, Android.Fakedefender infected devices by posing as an antivirus program and then locking the system after a fake scam found "critical threats." Victims were then coerced to pay for a fake software license. Other entrants, such as Android.Lockerdroid.E imitated an adult website application. After installation, the victim was threatened with a traditional law enforcement warning message and told to pay a fine to ($500) unlock their device.

Android.Simplocker, a mobile crypto ransomware also appeared in 2014. Since the Android operating system prevents applications from accessing data in other applications, Simplocker encrypted and ransomed external SD card data (which was not protected by the operating system at the time). Additional variants, such as the 2015 "Porn Droid" change the

user's PIN code. The ransomware does this by obtaining administrative privileges by hiding the escalation button under a fake confirmation message.

Servers:

An organization's servers and databases store all of their critical information. Within a server are an organization's documents, databases, intellectual property, personnel files, client list, and other intangible resources. The compromise of one essential server can hobble an organization. Despite their value, organizations regularly fail to secure, update, and patch the systems. This makes servers susceptible to lateral movement and attack. When a server is compromised, the organization goes into a panic. Even if the attack is a ransomware attack, there is concern for reputational harm due to the perception of lost customer data. Even if the organization has a business continuity plan or disaster recovery plan, the amount of time necessary to revert to a redundancy system may be unacceptable. Symantec reports that ransomware forces this opinion by combining attacks on servers with distributed denial of service (DDoS) attacks against the organization's system. The latter attack stresses the network to the extent that the former attack succeeds in pressuring the victim to pay a ransom. Another avenue of attack is to target the server and the redundancy system prior to revelation that the organization is under attack. Since many servers are perpetually connected to backup systems for real-time redundancy, lateral movement across systems is easy. One way or another, once the attacker has removed the safeguards surrounding the servers, they present the organization with a ransom 10-50 times greater than that demanded of individual users. In numerous cases, organizations tend to pay because, for them, every minute of downtime directly equates to lost revenue.

IoT Devices:

Ransomware is effective because it restricts access to information from a society that feels entitled to constant access to information. Many users pay the ransom without exploring alternative options simply because accepting the lost revenue is easier than applying effort. As more devices are connected to the threat landscape referred to as the internet of things, ransomware will have greater power over victims. Imagine the potential impact of a ransomware that infects a digital home temperature system. Given last year's proof of concept of wirelessly hacking a car, how successful do you suspect a ransomware capable of immobilizing a vehicle might be? In either case, and many others, the attacker would need to employ an alternative means of presenting the challenge for ransom and for collecting the payment. Nevertheless, ransomware is better suited for IoT attacks if only because the code is significantly smaller. Sure, some encryption operations will not work on certain devices and some target devices may not have the storage space necessary to encrypt and decrypt large amounts of data; however, that might just mean that attackers become even less likely to return data back to normal after manipulation.

Critical Systems:

Recall the 2013 Target breach in which point of sale (PoS) terminals were infected with malware. Even conservative estimates assess that the breach cost Target well over a billion dollars. A ransomware attack along the same vein would not compromise customer data in the same manner, but it would result in significant loss of sales. Transactions would become nigh impossible if customers had to use cash only or if the resulting delay per transaction caused lines to reach halfway across the store. Since security researchers speculate that the new Locky ransomware hails from the Russian Dridex criminal group (known for targeting banking and financial organization), it is not too farfetched to foresee this evolution of malware. Consider in the healthcare sector, Locky infected critical systems belonging to Hollywood Presbyterian Hospital and made conducting tests and basic procedures impossible without paying the ransom. Organizations backup critical assets such as databases, but they often neglect to do anything to ensure redundancy of critical systems such as payroll, email servers, or the aforementioned devices. Locky indicates how ransomware will evolve when guided by advanced malware threat actors instead of simpler financially motivated criminals.

The Economy of Ransomware:

Ransomware is unique among cyber-crime because in order for the attack to succeed, it requires the victim to become a willing accomplice after the fact. APT campaigns and less sophisticated financial cyber-crime prefer to remain undetected on the victim system because they profit from the data silently exfiltrated from the victim network. In order for ransomware criminals to profit, they again must rely on exploiting human nature rather than technical sophistication. Humans, like electricity, prefer the path of least resistance. If paying a small fee alleviates our workload or suspends our reality, we pay it. This is why home movers and media outlets are profitable enterprises. Even if the user knows that what they are paying for is illusory and will not alter their situation, such as a gym membership, a credit monitoring service, or the lottery, humans tend to pay into it for the peace of mind that they receive. Therefore, the adversary's goal is to convince victims that paying a ransom will relieve them of their current predicament, without drawing attention to the detail that the attacker is the direct force behind the situation. This approach is similar to 1500s Robin Hood-esque bandits along the road or 1920s mobsters. Victims are paying to regain what already belonged to them from an antagonist who offers to go away or in some cases, offers protection from future harm.

The game of ransomware attacks is discovering the right price for the threat landscape and the target economy. The cyber criminals utilize first-degree price discrimination to locate the highest amount that victims will pay without resorting to alternative solutions. Sources are not entirely clear as to why the AIDS trojan charged $189, an oddly specific number, as its ransom; but, the cost has not significantly increased in the 27 years since. According to Symantec, taking into account inflation, the $189 in 1989 was equivalent to roughly $368 in 2015, which is higher than the average of $300. In reality, the cost to users (as of 2015) fluctuated between $21-700 depending on variant, criminal, infected device, and victim demographic. The wide range shows

that some criminals prefer to make a small profit from a large number of victims while other prefer the inverse.

Ultimately, if the campaign is going to succeed, the ransom must be tailored to the victim population and the victim currency. Most variants require payment in the form of bitcoins or credit vouchers in USD; however, victims might be located across the globe. Even though the United States and India are both developed countries with bustling economies, the ability of the individual to pay will differ according to the national economy and the willingness to pay a given price will differ based on culture. Even in the United States, a victim will be more willing to pay $100 to unlock an infected iPhone than they would to unlock a $25 GoPhone. In response, many groups dynamically tailor their ransoms according to geography and infected system. For example, Cryptowall (Trojan.Cryptodefense) alters the ransom amount according to the victim's geographic location. The ransomware does this by matching the IP address to geographic IP lookup table internally or within the command and control infrastructure.

Cyber-criminals also must discriminate based on the type of victim. Individual users have a low ability to pay and cannot be charged more than the cost of the infected system. Businesses on the other hand value their data more than the system that contains it. Especially in the intangible goods market of the United States, data is the basis for modern business. Attackers who target organizations must be more sophisticated in their operation and their ransomware. Consequently, they assume greater risk, expend greater resources in preparation for the attack, and demand greater ransoms. Whether data is related to financial services, healthcare, or other critical systems, it has an associated value. While ransomware actors do not sell the data for its market price, as an APT might, the value of data does reflect in the ransoms demanded of businesses. For comparison, in 2013, polling company the Ponemon Institute claims that each minute of unexpected data center downtime resulted in a loss of $7900. Similarly, Arbor Networks surveyed organizations to estimate that a DDoS attack costs an average $500 per minute. Now unless a ransomware actor is very thorough, their attack will not halt business operations altogether the way a total network outage would. Further, many of their primary targets (financial institutions, Universities, etc.) can resort to paper forms in the interim. Nevertheless, ransomware attacks do have a financial impact because business operations are slowed while critical systems are restored. In some cases, such as healthcare, lives are jeopardized as the timer ticks forward.

Ransomware criminal groups understand and specifically engineer the pressures that victims feel. Attackers set the timer to restrict the ability of incident response teams to respond. Most adversaries set the timer for a few days but, in the future, others might set the timer to be less than the amount of time it takes to get ahold of a vendor and implement a solution. Symantec predicts that the average ransom paid by businesses is about $10,000. Organizations that pay the ransom do not tend to publically report the amount. Estimations can be made from the few empirical examples available. On February 5, 2016, attackers encrypted the email system and patient records of Hollywood Presbyterian Hospital and demanded a ransom of $17,000 in Bitcoins. After almost two weeks, the hospital paid. Healthcare organizations were not a primary target for ransomware attacks prior to 2016; but, the success of the Hollywood Presbyterian attack and the media coverage will ensure that attackers focus on the healthcare sector in the future. For comparison, after U.S. CERT and DHS released a bulletin about the Cryptolocker ransomware on November 5, 2015, police station systems were targeted with ransom demands of

$750. For comparison, the November 2015 Linux.encoder attacks against Linux based websites demanded a ransom of $420. The evidence suggests that the threat landscape is shifting towards more profitable sectors.

Payment Mediums:

The payment method has evolved with ransomware since the AIDS trojan in 1989. Actors no longer ask for checks or account numbers because those transactions take time, and can be easily traced by law enforcement. Instead, some variants, such as the 2009 Trojan.Ransomlock, ask for wire transfers and premium rate text messages while others demand that the ransom be paid with a digital voucher (CashU, MoneXy, MoneyPak, etc.) or in cryptocurrencies. Cryptocurrencies are typically purchased through the dark net accessed through Tor; though, law enforcement, security researchers, and computer enthusiasts also hold part of the market. Bitcoins (BTC) are the reigning pseudo-anonymous decentralized cryptocurrency. Because Bitcoins are steadily becoming more difficult to purchase on the dark net and because the currency is more volatile than it was in the past, some ransomware variants accept Litecoins (LTC) and Dogecoins (DOGE). Cryptocurrencies are mostly anonymous, though a few security researchers are working on models to track transactions. Cyber-criminals likely exchange the cryptocurrencies for their native currency as soon as they can because the volatile nature of the former could result in a loss of the latter.

Threat actors launder payment vouchers through online services such as casinos and betting sites that are hosted in various geographical and legal jurisdictions so that law enforcement cannot track the culprits. The money is then transferred to prepaid debit cards and the funds are withdrawn from ATM machines using human proxies. These proxies, sometimes referred to as “money mules,” withdraw money for criminal organizations for a predetermined percentage. Bitcoins allegedly do not need to be laundered; however, recent efforts to trace Bitcoins have resulted in Bitcoin laundering services. These services essentially toss legitimate and illicit bitcoins into a bag, shake it, and redistribute the coins for a fee. Alternately, Bitcoins can be routed through block transaction wallets or Bitcoin anonymizers to obfuscate the identity of the owner. As previously stated, cryptocurrencies can be subject to volatile market fluctuations. As a result cyber-criminals do not necessarily have the time to fully obliterate their trail. Conveniently (for them), the criminals who receive Bitcoins do not need to entirely hide their trail from law enforcement efforts to remain at large. Instead, they just need to move coins around enough to provide plausible doubt that they were the culprits involved in the ransomware attack. In most cases, obfuscation methods need only disrupt law enforcement efforts long enough for the adversary to convert their ransom into tangible currency.

How Profitable is Ransomware?:

According to Kaspersky, creating a phishing page and setting up a mass spam email costs about $150. A trendy crypto ransomware sells for about $2000 on dark net forums. Locker ransomware probably costs less. This means that an attacker only needs to ransom eight everyday users (at the average $300) to generate a profit. Symantec estimated that in 2009, 2.9 percent of the victims paid the ransom. In 2014, CTU researchers estimated that about 1.1 percent of the Cryptowall ransomware victims paid the ransom (at an average of $500). Despite this seemingly low response rate, the FBI reported that from the 992 related complaints, Cryptowall reportedly netted over $18 million from victims between 2014-2015. Who knows how many infections were not reported? The lesson is that ransomware, while less sophisticated than APT groups and other cyber criminals, is still significantly profitable, even when only a miniscule number of user fall for its scheme.

Mitigation:

As with any cyber threat, preventing infection is preferred over remediation efforts. The first step to mitigating a ransomware threat is to implement a comprehensive cybersecurity strategy. Any organization that marginalizes cybersecurity to the bottom of the budget or that relies on a "silver bullet" technical solution is going to be breached by cyber criminals and advanced persistent threats alike. Software and hardware solutions are necessary, but they are not the only necessity. First and foremost, information security training and awareness must improve. Afterward, organizations can rely on the layered defenses that they have invested in to secure their network.

Have a Dedicated Information Security Team:

An information security team is essential to every organization. The team is not the same as the information technology team, but the two collaborate. The information security team conducts risk assessment on the organization's cyber security posture against its risk appetite to define incident response procedures, business continuity plans, and disaster recovery plans. The information security team teaches cyber security best practices to personnel and monitors adherence to policy and practices. The team ensures that key assets are protected according to their value to the organization. The information security team deploys and configures the security of all devices on the network. In the case of ransomware, it would be the responsibility of the information security team to ensure that all systems were updated and patched (especially browsers and Adobe, Java, Microsoft, and Linux applications) so that threats do not exploit open vulnerabilities, and to ensure that all critical systems were backed up in the event of a successful attack. ActiveX content in Microsoft Office applications should be disabled so that executables

do not run from malicious attachments. Similarly, blocking the execution of binaries from %APPDATA% and %TEMP% paths will prevent some ransomware from executing. It is also the responsibility of the team to map the network and to allow or deny new devices from joining the network. The team must know who and what devices are connecting to the network and for what reason those devices are connecting. Likewise, remote desktop connections to the network should be disabled. Information is key and only known entities should have access to the network.

Cyber threats evolve according to the value of data and the susceptibility of organizations to attack. Personnel on the information security team should remain up to date on sector relevant threats to the organization's cyber security. This means monitoring and profiling advanced persistent threat groups, criminal groups, hacktavists, ransomware criminals, and other threats to the organization. Information about these threats can be found in industry whitepapers, security intelligence bulletins, and on security research blogs.

Training and Awareness:

Personnel need to be trained to recognize and report threats to the organization. Information Security researchers often chime that "humans are the weakest link" in organizational cybersecurity; but, humans are simultaneously the strongest link because your organization is only as aware as your worst employee. The vast majority of breaches and cyber security incidents are directly correlated to the innocuous or malicious actions of personnel. Malicious emails are the favored attack vector of ransomware and other malware alike. Employees should be trained to recognize a malicious link or attachment. There is no justifiable reason that most organizations cannot reduce their personnel's malicious link click rate below 15 percent. A single employee is all it takes for the entire network to be compromised. Teach employees to not click on any links in any emails. It takes barely any more time to type a link into Google as it does to click the link. Personnel should only open attachments from personnel that they trust and only if they are expecting the file. Ultimately, personnel are the strongest and the weakest link in organizational security. If they make a mistake, then the organization has made a mistake. If they fail, the organization has failed.

Layered Defenses:

Organizations should protect their network as if it was a castle under siege. The goal is not necessarily to prevent an attack. Rather, network defense is about slowing the adversary and detecting their presence in time to react to the intrusion. At the very least, an organization should have as many fundamental systems as possible. No single product should be relied upon because there is no single product that provides comprehensive security. White-list firewalls permit only trusted traffic. Explicitly denying all traffic from Tor and I2P can prevent some variants of ransomware from contacting its C2 infrastructure. Intrusion detection and intrusion prevention systems warn the information security team of threats that get past the firewall. Anti-virus, anti-

malware, and anti-ransomware applications protect the network with systematic scans. User Behavioral Analytic (UBA) systems monitor baseline user behavior and notify the information security team of suspicious activity on the network. An endpoint solution incorporates signature based, heuristic based, behavioral based, and reputational based protections into one product. Change management systems prevent unwanted modification or loss of data. When possible, data should at least be encrypted while at rest and in transit. Segmenting and subnetting the network restricts the access of successful attackers. User accounts should follow a least privileged model. Finally, especially with ransomware attacks, it is paramount to have backup and redundancy systems to ensure data confidentiality, integrity, and availability as well as business continuity.

Policies and Procedures:

After personnel are trained and technical controls are configured, administrative policies can help to prevent incidents. Users should know what activities are allowed on the network. They should know how to recognize suspicious activity and to whom it should be reported. It may be beneficial to negotiate a cyber insurance policy that covers ransomware attacks as well as data breaches. Cyber insurance policies insulate the organization from the unpredictability of the cyber-threat landscape. If nothing else, the policy vendors issue minimum qualification guidelines that can help benchmark what the organization's minimum cybersecurity posture should be. These insurance policies help to quantify risk by applying an actuarial value to digital assets. An appraisal may inform the organization of what they should be protecting as well as what others in their sector are protecting. The rate of the policy will inform the organization where it sits relative to the cybersecurity posture of its competitors. Ultimately, though, the cyber insurance policy is valuable because it removes some of the panic surrounding an incident, allowing more rational responses to inevitable incidents.

When Compromises Occur:

Despite even the best information security program, exceptional operational security, and adherence to the most stringent of mitigation procedures, attacks will occur and some will succeed. Responding to ransomware is situational. When mitigation fails, it is important for organizations and individuals to consider all of the possible responses to a ransomware demand. Disengage from communicating with the attacker until the situation is thoroughly assessed and a course of action decided. Since attackers often give victims a time limit, organized response is essential to ensuring rational decision making. The proper response will depend on the risk appetite of the organization, the potential impact of the hostage data, the impact on business continuity, whether a redundant system is available, and the sectorial regulatory requirements.

Option1: Engage the Incident Response Team:

The response to ransomware attacks follows the same form as the response to APT attacks. Incidents response begins when the organization's information security team is informed of the ongoing attack. Incident response should not be spontaneous. The information security team should have planned out a procedure to follow in the event of a ransomware attack, during their risk assessment. Organizations who cannot afford an internal dedicated information security team should consult with vendor organization prior to an event. Any organization that believes that they can get by without an information security team is doomed to exploitation. Their only response will be to pay the ransom and wait to be exploited again by the same criminals, different criminals, or an advanced persistent threat group.

The incident response team should begin by notifying the authorities and applicable regulatory bodies. Ransomware attacks are, after all, a crime. As with traditional breaches, C-level management may be reluctant to report an incident out of fear of reputational harm. However, this mindset fails to consider that a breached system or, in this case, a system permanently held hostage will inevitably result in much greater harm to the organization. A properly trained information security team should have a plan of action in the event of a ransomware attack. They should also have a disaster recovery plan that identifies the organization's recovery time objective (RTO), and recovery point objective (RPO) for data breaches. RTO, RPO, and the risk appetite of the organization (identified in the risk assessment) will better inform the best course of action.

In the event that a backup exists, then cyber-forensic evidence of the incident should be preserved and documented for/ by law enforcement. Afterward, affected systems can be reverted to backup copies. In the event that there are no redundancy systems or if the secondary systems are compromised, then the information security team can find and implement a vendor solution or decryption tool.

Option 2: Try to Implement a Solution without an Information Security Team:

If a victim organization does not have an information security team, then a respondent will have to assume those roles and responsibilities. Knowledgeable users can implement some vendor solutions and decryption tools; however, without training in information security or computer systems, the victim might not be able to remove the ransomware. In many cases, files may be partially corrupted or incompletely decrypted. Even if the vendor solution is a simple executable, the victim may not be able to assure that their system is not still compromised by inactive ransomware, backdoors, or other malware. The initial infection occurred as the result of a human error (clicking on a malicious email) or a pe-existing infection. Without training and awareness or more comprehensive system management, there is reasonable likelihood that the system will be compromised again.

Option 3: Attempt to Recover the Data:

System backup and recovery are the only certain solution to ransomware. If you have a backup system, then recovery is a simple matter of restoring the system to a save point. Otherwise, you could attempt to recover data through shadow copies or through a file recovery software tool; however, many ransomware variants delete shadow copies and some even detect file recovery software. Since many variants infect the registry, system restore from a save point may not be possible even if the recovery point remains unaffected.

Option 4: Do Nothing:

In lieu of an information security team or vendor solution, options are limited to paying the ransom or accepting the loss of the system or data. If the system is backed up, and the backup remains reliable, then the victim can ignore the ransom demand and restore the system according to the backup. If there is no backup, but the ransom outweighs the cost of the system, then the victim may have to purchase a new device and dispose of the infected system with extreme prejudice.

Option 5: Pay the Ransom:

If the culprit actually provides the decryption key, then paying the ransom may alleviate the immediate pressure on the organization. Some attackers may release the system after receiving payment because doing otherwise would reduce the likelihood that other victims will pay. Ransomware is rampant. If paying the ransom is legitimately being debated, then perform a quick internet search on the type of ransomware holding your system. Whether or not criminals who use that ransomware are likely to release data after receiving payment is likely to show up online. As executives at GRA Quantum point out, “It is always a gamble to pay the ransomware as there is no guarantee that the attacker will relinquish the data (i.e. provide the private key to unlock the files) upon payment.” Some attackers recognize this dichotomy of trust. They recognize that if files are never unlocked then no victim will ever pay a ransom. As a result, variants such as CTBLocker (Trojan.Cryptolocker.G) have an option to decrypt a few random files as a gesture of good faith.

GRA Quantum advises that “paying ransoms once also does nothing to prevent future attacks on the same system.” Recognize that you are interacting with criminals. Cyber-criminals do not tend towards honest interactions. If you pay the ransom once, then the threat actor’s logical response after releasing the system would be to strengthen their foothold in hopes that you will pay the ransom again in the future. If the culprit does not decrypt the data, then there

may not be hope of recovering the system without a vendor solution because some variants, such as cryptolocker, employ strong encryption algorithms such as 2048-bit RSA.

Conversely, the industry claim of "never pay the ransom" is unrealistic. Sometimes, no other options exist. If the backup is compromised or if the system is time critical and restoring the system would significantly impact operations, then it might make sense to pay the ransom. For example, if a critical hospital system is compromised and lives are at risk for every minute that the system remains down, then it might make sense to pay the ransom, even if the system could be restored over a longer period of time. The decision makes sense in consideration of the healthcare organization's primary concern: minimizing loss of life at any cost. If the ransom must be paid, then the organization should pay in bitcoins or some tangible asset. Victims should never pay with their credit cards or financial account information. Even when paying for bitcoins or currency vouchers, the organization should not pay with their credit cards or financial account information. If no alternative exists, then the card or account used to pay should be frozen or closed immediately after the transaction to prevent cascading breaches.

Option 6: A Hybrid Solution:

If the ransom is low, say $300 for a multimillion-dollar organization, then it might make sense to adopt a hybrid approach. This could include simultaneous efforts to pay the ransom, to triage the system, and to attempt to restore from a backup server. Organizations devout the effort and resources to a hybrid approach when system downtime is more dire than the consequences of the ransom. A hybrid approach ensures that the system will be operational in some amount of time, no matter what. This option is essential for critical systems, such as medical devices or police databases. To minimize the expended resources and the impact to the organization, hybrid solutions should only be attempted by a trained and prepared information security team.

Conclusion:

The simple and turnkey application of ransomware enables script kiddies the ability to now play in the hacker big leagues. The number of ransomware attack variations is limited only by the imagination and motivation of the attackers. A vigilant cybersecurity centric corporate culture that cultivates an environment of awareness is the most effective means to minimize the attack surface populated by the human element. The enlistment of an information security team whose sole purpose is proactive corporate infosec management is the first step in a companywide security strategy. The InfoSec team's activity should, at a minimum cover: an immediate companywide vulnerability analysis, a crisis management strategy that takes into consideration all know threats, continuous device and application patching, auditing of third party vendors and agreements, organizational penetration testing and security centric technological upgrades. Together, these actions can profoundly minimize a company's attack surface.

Sources:

Ars Technica:

http://arstechnica.com/security/2016/02/mysterious-spike-in-wordpress-hacks-silently-delivers-ransomware-to-visitors/

The Atlantic:

http://www.theatlantic.com/technology/archive/2016/02/hackers-are-holding-a-hospitals-patient-data-ransom/463008/

Bit Defender:

https://labs.bitdefender.com/2016/02/ransomware-and-sms-sending-trojans-top-threats-in-bitdefender-android-h2-2015-report/

Business Insider:

http://www.businessinsider.com/ransomware-as-a-service-is-the-next-big-cyber-crime-2015-12

CryptoCoins News:

https://www.cryptocoinsnews.com/melrose-police-pay-1-bitcoin-to-get-rid-of-ransomware/

Dark Reading:

http://www.darkreading.com/endpoint/ransomware-5-threats-to-watch/d/d-id/1297317

Data Center Knowledge:

http://www.datacenterknowledge.com/archives/2013/12/03/study-cost-data-center-downtime-rising/

Digital Trends:

http://www.digitaltrends.com/computing/ctb-locker-ransomware-encrypts-wordpress-sites/

Forbes:

http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#1d401fe475b0

Forcepoint:

https://blogs.forcepoint.com/security-labs/lockys-new-dga-seeding-new-domains?cmpid=pr

The Hacker News:

https://thehackernews.com/2015/02/cryptoware-ramsomware-bitcoin.html

Healthcare IT News:
http://www.healthcareitnews.com/news/data-center-outages-come-monster-pricetag

HIPAA Journal:

http://www.hipaajournal.com/cyberattackers-demand-3-6m-ransom-from-hollywood-hospital-8313/

Information Management:

http://www.information-management.com/news/security/data-security-threats-growing-putting-projects-and-innovation-at-risk-10028336-1.html

Information Security Buzz:

http://www.informationsecuritybuzz.com/hacker-news/the-rise-of-android-ransomware/

Invincea:

https://www.invincea.com/2016/02/dridex-crew-bets-on-ransomware/

Kaspersky Lab:

https://noransom.kaspersky.com/

https://business.kaspersky.com/cybercrime-inc-how-profitable-is-the-business/2930/

Know Be 4:
https://www.knowbe4.com/aids-trojan

Krebs on Security:

http://krebsonsecurity.com/2015/11/ransomware-now-gunning-for-your-web-sites/

KTVN:

http://www.ktvn.com/story/31274059/hollywood-hospital-victimized-by-ransomware-locky-spreading-fast

LA Times:

http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-storay.html

Lavasoft:

http://lavasoft.com/mylavasoft/company/blog/ddos-report-downtime-cost-companies-over-500minute

PC Magazine:

http://www.pcmag.com/article2/0,2817,2499822,00.asp

PC Risk:

https://www.pcrisk.com/removal-guides/8120-your-personal-files-are-encrypted-virus

PC World:

http://www.pcworld.com/article/2983138/security/android-ransomware-changes-a-devices-pin-code.html

http://www.pcworld.com/article/2600543/cryptowall-held-over-halfamillion-computers-hostage-encrypted-5-billion-files.html

PR News Wire:

http://www.prnewswire.com/news-releases/cyber-threat-alliance-cracks-the-code-on-cryptowall-crimeware-associated-with-325-million-in-payments-300168593.html

The Register:

http://www.theregister.co.uk/2015/11/02/kaspersky_announces_death_of_coinvault_bitcryptor_ransomware/

http://www.theregister.co.uk/2016/03/04/north_dorset_council_ransomware_refusal_payout/

http://www.theregister.co.uk/2016/01/28/lincolnshire_council/

Security Ledger:

https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/

Security Madein:

https://securitymadein.lu/ransomware-campaigns-behind-the-scenes/

Sophos:

https://blogs.sophos.com/2016/01/06/the-current-state-of-ransomware-teslacrypt/

https://blogs.sophos.com/2015/12/31/the-current-state-of-ransomware-ctb-locker/

https://blogs.sophos.com/2015/12/17/the-current-state-of-ransomware-cryptowall/

Symantec:

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf.

http://www.symantec.com/connect/blogs/ransomcrypt-thriving-menace

http://www.symantec.com/connect/blogs/spam-offering-fake-visa-benefits-rewards-leads-teslacrypt-ransomware

Tech First Post:

http://tech.firstpost.com/news-analysis/mobile-malware-tripled-in-2015-ransomware-at-the-helm-kaspersky-301687.html

Top Tech News:

http://www.toptechnews.com/article/index.php?story_id=113001Z7BMY2

Trend Micro:

http://www.trendmicro.com/vinfo/us/security/definition/Ransomware#Known_Ransomware_Families

USA Today:

http://www.usatoday.com/story/news/nation/2014/05/14/ransom-ware-computer-dark-web-criminal/8843633/

Wired:

http://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/

ZD Net:

http://www.zdnet.com/article/ransomware-springboards-from-wordpress-to-joomla-domains/

Appendix A: Ransomware File Extension and Identifiable Notes

File extensions appended to files:

.ecc, .ezz, .exx, .zzz, .xyz, .aaa, .abc, .ccc, .vvv, .xxx, .ttt, .micro, .encrypted, .locked, .crypto, _crypt, .crinf, .r5a, .XRNT, .XTBL, .crypt, .R16M01D05, .pzdc, .good, .LOL!, .OMG!, .RDM, .RRK, .encryptedRSA, .crjoker, .EnCiPhErEd, .LeChiffre, .keybtc@inbox_com, .0x0, .bleep, .1999, .vault, .HA3, .toxcrypt, .magic, .SUPERCRYPT, .CTBL, .CTB2, .locky, .MP3, or 6-7 length extension consisting of random characters.

Known ransom note files:

HELP*DECRYPT.TXT*, *HELP_YOUR_FILES.TXT*, *HELP_TO_DECRYPT_YOUR_FILES.txt*, *RECOVERY_KEY.txt HELP_RESTORE_FILES.txt*, *HELP_RECOVER_FILES.txt*, *HELP_TO_SAVE_FILES.txt*, *DecryptAllFiles.txt DECRYPT_INSTRUCTIONS.TXT*, *INSTRUCCIONES_DESCIFRADO.TXT*, *How_To_Recover_Files.txt YOUR_FILES.HTML*, *YOUR_FILES.url*, *encryptor_raas_readme_liesmich.txt*, *Help_Decrypt.txt DECRYPT_INSTRUCTION.TXT*, *HOW_TO_DECRYPT_FILES.TXT*, *ReadDecryptFilesHere.txt*, *Coin.Locker.txt _secret_code.txt*, *About_Files.txt*, *Read.txt*, *ReadMe.txt*, *DECRYPT_ReadMe.TXT*, *DecryptAllFiles*.txt FILESAREGONE.TXT, IAMREADYTOPAY.TXT, HELLOTHERE.TXT, READTHISNOW!!!.TXT, SECRETIDHERE.KEY IHAVEYOURSECRET.KEY, SECRET.KEY, HELP*DECYPRT_YOUR_FILES.HTML*, *help_decrypt_your_files.html HELP_TO_SAVE_FILES.txt*, *RECOVERY_FILES.txt*, *RECOVERY_FILE.TXT*, *RECOVERY_FILE*[random].txt Howto*RESTORE_FILES*.txt, Howto*Restore_FILES.txt*, *howto_recover_file*.txt, restore*files*.txt, how*recover+[random].txt*, *_how_recover*.txt, recovery*file*[random].txt, recover*file*[random].txt recovery*file*[random].txt, Howto_Restore_FILES.TXT, help_recover_instructions+[random].txt, _Locky_recover_instructions.txt

Appendix B: Locky Domains For February 2016 through March 2016:

ICIT fellow Forcepoint traced the C2 infrastructure of the Locky ransomware and has published the following list of domains that distribute the Locky ransomware. Network administrators and home users can use this information to block access to these domains.

24/25 Feb 2016:

bkadufmdyf[.pm]
kpvoxwgf[.pm]
fysck[.fr]
hsasjielgfkneh[.ru]
qquvjijtvatj[.in]
edmgbqygn[.de]
nbavfpb[.uk]
wyusb[.yt]

26/27 Feb 2016:

yuljfxdf[.pm]
bvtavc[.nl]
ktovxeteqtwtcsh[.yt]
xyfnvvbuovcd[.be]
hwsdymcytd[.yt]
cgwlamg[.pw]
ehfjt[.pm]
nfacehihugohhi[.nl]

28/29 Feb 2016:

cproso[.pm]
lnjrmdjyidprrse[.de]
nortkbiqhtdgd[.de]
ixwllqpbog[.in]
rvkgvjbp[.it]
ficpn[.fr]
ogworigxknalsd[.eu]
qaekmjxgrtcs[.de]

1 March 2016:

prydlvlxw[.be]
rsimigt[.us]
bqvcl[.in]
ovmspedrbkxlj[.ru]
xthppvomcxu[.be]
aupgcrvfm[.us]
uemtsb[.uk]
echmfrnyuwrlmas[.uk]

2/3 March 2016:

jaliqnp[.yt]
ejpmaxavyptyqnc[.pw]
nhkpknfyjnoqp[.ru]
iqountnrqs[.ru]
krpphdlu[.yt]
tpkmyc[.ru]
hubvdqgfcoierc[.pw]
qsaifcyuopyv[.de]

4/5 March 2016:

bxlrnw[.pw]
vhpurxfuohbqso[.fr]
ffkseaisuicb[.eu]
hgspblbnex[.yt]
cppvgch[.in]
lnkva[.pw]
ysbfaksqohpmf[.in]
iqvcaeogjeg[.it]

6/7 March 2016:

spxst[.us]
nycbuwfisadao[.be]
wwpyvxnihcm[.fr]
yxxpmghmx[.uk]
thcfqk[.it]
dfwqdyjrtyiuaij[.pm]
qrokkqdsmtxa[.us]
apgodprqgy[.eu]

8/9 March 2016:

djcbwpykgnsdikb[.pm]
fkkdmvsjnnptv[.yt]
athfaulmew[.pw]
cupggwpf[.pm]
lsotcg[.in]
gcsxwslqsvbhpr[.pw]
ivtlxgqfkiyj[.it]
dfxvcvxfa[.be]

10/11 March 2016:

kfifrxqke[.in]
fogyrq[.uk]
ombqnwvepxjeufs[.tf]
qnjoimqcqkokt[.yt]
lpmxewicfk[.us]
uubnggrp[.in]
woiwpu[.fr]
rxmbadyblcuoat[.in]

12/13 March 2016:

dlhhgett[.us]
mqvubo[.de]
haageiedrybojk[.tf]
jtlqoqfaykdj[.uk]
edpglqefm[.it]
nbdwqkj[.fr]
pcmfx[.de]
klqqvsewphwko[.it]

14/15 March 2016:

vqmkfujpobvu[.us]
xkxapdrojh[.nl]
stckmju[.yt]
uulhq[.fr]
esyjyjiklwnbhd[.tf]
ycdntrbxkuw[.de]
bdlpmukcp[.eu]
vmpthc[.it]

16/17 March 2016:

ddutcdmfvmbaaba[.be]
mbikamdjklmce[.de]
hkmaebphml[.yt]
jetxtfwv[.pw]
enxme[.us]
nllwyhyrvsdodo[.fr]
pmttrjeukjnl[.yt]
kvxcsnink[.yt]

18/19 March 2016:

vopbboe[.tf]
fmktk[.pw]
avppvitupmdtm[.tf]
cwxghlngfxo[.nl]
wguofdum[.it]
yhdrnk[.ru]
ifxjoqrmcmajhjf[.ru]
docniprmgcxm[.be]

20/21 March 2016:

adrefp[.ru]
jinpjwfrsjpmjgu[.us]
ekqmsioexowp[.uk]
glrbxuhejj[.de]
buvpbsq[.pw]
dvehl[.pw]
mtygfrrwfppuvv[.us]
hdvmubmbyxs[.nl]

22/23 March 2016:

radqq[.tf]
bfyilphwkctxdf[.us]
vhcrhadppxa[.it]
xidmofnsc[.ru]
srlkgw[.pw]
ustmanuqnxxhlmj[.pm]
eqplamxxqghrd[.tf]
yamyqrhatl[.de]

24/25 March 2016:

jxeepaassngeetq[.in]
sdsyswxogrhjf[.tf]
nfvdvistdi[.nl]
pgeeucpt[.uk]
yercwd[.nl]
mqjlvimienyxwr[.fr]
voebnwfybwkg[.pw]
qximfakki[.fr]

26/27 March 2016:

xjneysaum[.us]
hhbrghm[.eu]
jijps[.in]
ernthxdqkbuoi[.tf]
npixhjhhmpm[.uk]
burfvaac[.pm]
ksmbxx[.in]
mtuamviphwoapcq[.uk]

28/29 March 2016:

jjrlgvdlqurpa[.pm]
shmcsgbpypg[.fr]
uivmeislw[.eu]
prsobv[.pm]
ypnlcncyegxteub[.in]
bqvjrrodkfhjg[.it]
vaaytyxqyl[.eu]
fxnitwaq[.fr]

30/31 March 2016:

pvmyilqakqqkl[.in]
kfqoruddyo[.nl]
myxmilto[.it]
hicqd[.us]
qnqlfdthdyidbw[.be]
shxppmfnhjao[.pm]
nqcxfhycl[.in]
wowkllj[.it]

Contact Information

Legislative Branch Inquiries:

- James Scott, Senior Fellow, ICIT (james@icitech.org, 202-774-0848)

Federal Agencies, Executive Branch and Fellow Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Links

Website: www.icitech.org

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg