COMBATTING THE RANSOMWARE BLITZKRIEG

THE ONLY DEFENSE IS A LAYERED DEFENSE

LAYER ONE: ENDPOINT SECURITY

APRIL 2016

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:

- Dan Waddell (ICIT Fellow – Director, Government Affairs, (ISC)2)
- Greg Fitzgerald (ICIT Fellow – Chief Strategy Officer, Cylance)
- Rob Bathurst (ICIT Fellow – Managing Director, Healthcare and Life Sciences, Cylance)
- Malcolm Harkins (ICIT Fellow – Global Chief Information Security Officer, Cylance)
- Ryan Brichant (ICIT Fellow – CTO, ICS, FireEye)
- George Kamis, (ICIT Fellow – CTO Federal, Forcepoint)
- 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)
- Rob Roy (ICIT Fellow – Public Sector CTO, Hewlett Packard Enterprise)
- Stan Wisseman (ICIT Fellow – Security Strategist, Hewlett Packard Enterprise)
- Cindy Cullen (ICIT Fellow – Security Strategist, Hewlett Packard Enterprise)
- Stan Mierzwa (ICIT Fellow – Director, Information Technology, Population Council)

Contents

Introduction:

Ransomware attacks have become so commonplace among the general population and critical infrastructure organizations that it's difficult to go a week without hearing about a new variant or victim who has fallen prey to this rapidly evolving mechanism of attack. Malicious actors excel and rule in environments containing Frankensteined, antiquated technologies, finagled to achieve IoT connectivity, operated by cybersecurity novices, who manage environments that lack cyber hygienic and security centric organizational cultures. Ransomware, the weaponization of encryption, has struck fear and confusion into the hearts of PC users and network administrators alike. In order to create a baseline comprehension of ransomware and how to defend against it, we can employ a straightforward illustration using a prototypical 'house'.

Imagine your network as a house: a multistory structure surrounded by a white picket fence. Every door and window is a potential pathway that information (noise, light, etc.), objects (dust particles, baseballs, etc.), or people could use to enter your domicile. Similarly, in Information Security, any system or access point in which data are stored or through which information can enter and leave your network is known as an endpoint. You secure the endpoints of your home with locks, an alarm system, and perhaps a guard dog. Analogously, endpoint security is the practice of employing layers of hardware and software solutions to secure the vulnerable points in your network. As the solutions to secure your home are tailored to the entry point and the scale of the assumed threat, most endpoint security solutions are tailored to protect specific network devices and entry points against specific threats.

The adversaries who target vulnerable networks are similar to home assailants in that a given threat can be measured in severity according to the tools, tactics, and procedures that they adopt and the motive, means, and opportunity afforded to them. A traditional burglary begins with an attacker observing your home from the outside and gleaning what information they can about the defenses, your activities, and the value of the contents in the home. In many cases, context clues, such as mail stacked up in the mailbox, can be employed against you and used to predict a vulnerability in your security; in this case, that the house is currently unoccupied. Next, the attacker moves in closer and tries to use the gathered information to discover a vulnerable entry point, such as an open window or unlocked door. If successful, the attacker enters your home without alerting you or the authorities. Next, the invader evaluates your possessions and decides what is valuable enough and transitive enough to exfiltrate from the home. Finally, the attacker departs with their spoils and leaves you to discover the incident and clean up the mess. The entire attack chain described is characteristic of a typical cyber-threat.

Attackers can conduct similar attacks against your home as those waged against a vulnerable network. Conventionally, the invader can sneak in, steal valuable assets or information, and skulk out. Alternately, the attacker could target your home solely to create chaos. In this manner, teenagers vandalizing a home are no different from the lesser end of the spectrum of script kiddies and hacktavists who deface websites and interfaces for no purpose other than offending the targets. Similarly, an attacker could commit other minor crimes to inundate the victim's entryway with an unexpected influx of visitors. In information security, this form of attack is known as a dedicated denial of service (DDoS). A more malicious adversary could target the victim with more complicated attacks, such as arson, to create chaos, inflict harm, or for ulterior motives such as luring authorities away from another incident. In cyber security, these tangential attacks are characteristic of a sophisticated adversary. Regardless of the form of attack, once the attacker has infiltrated your perimeter, they are in control of the outcome and some amount of your information or assets. In the physical world, we recognize the threats to our homes and we take precautions and set contingency plans. Attackers are prevented from sacking the neighborhood through a standardized set of controls and a common security culture. The field of information security is novel compared to the practice of homesteading. Not every organization recognizes the value of protecting their endpoints with layers of security solutions according to the active threats populating the cyber-landscape. American cyber culture is still lacking in the basic cyber-hygiene and security-centric focus necessary to preclude the cyber-incidents that result from human error. Information about emerging threats or compromised networks is neither shared adequately or equivocally to efficiently benefit the community at large. Policing organizations such as DHS and the FBI are almost always called into respond to the aftermath of an incident instead of summoned to actively apprehend culprits before damage is done. As a result, the network forensics conducted by cybersecurity vendors and law enforcement are used less for attribution or apprehension of a culprit than they are used to notify victims and to attempt to prevent similar incidents in the future. Nevertheless, organizations who employ layered endpoint security solutions and who teach proper cyber hygiene to their employees are finding themselves better defended than their competitors who refuse to invest in cybersecurity based on antiquated excuses like budget constraints or lack of an ROI. These early adopters actively fortify their home network. These networks, properly fortified with layered defense in depth solutions around their endpoints and reinforced with a cyber-hygienic culture, are invulnerable to all but the most sophisticated and targeted attacks. That is not to say that their defenses are impervious. No single solution is a panacea. Silver-bullet solutions that claim to fix everything are embodiments of false hope. Instead, a well-defended network depends on their first line of defense, layered endpoint security solutions, and their internal security solutions to slow the advance of adversaries long enough that either the threat can be reduced or the impact can be mitigated.

Despite the success of endpoint security solutions in reducing an organization's cyber-attack surface and limiting the spread of malware through a network, some organizations have not yet implemented endpoint security solutions. These organizations are inundated by the horde of conventional cyber threats emerging from the cyber landscape and they are desensitized towards the constantly growing list of cyber incidents reported in the media. They ignore the threat posed by advanced persistent threats under the misguided assumption that they are not targets or that their network does not contain valuable data. They fail to realize that in the information age, any organization that stores, processes, or transfers data is a valuable target to bad actors. Contrary to this laissez-faire attitude towards cybersecurity and cyber threats, many of these same organizations have recently become intimidated or targeted by the rising tide of ransomware flooding the internet. Ransomware is a form of malware that an adversary can use to encrypt specific files or file types on a victim machine without the effort and technical knowledge to infiltrate and exfiltrate a system. Most variants spread through malicious links in spear phishing emails or through drive-by-downloads; however, some recent evolutions of the malware such as the Samsam ransomware used in the Medstar Healthcare attacks, were deployed without victim interaction or awareness. After infection, the victim is threatened with the permanent loss of their data unless they pay a predetermined number of Bitcoins. Ransomware attacks are akin to an adversary putting additional heavy locks and security on your home. Notice how much shorter the ransomware attack chain is compared to the chain mentioned in the aforementioned analogy. The attacks tend to occur in a rapid, Blitzkrieg fashion that is designed to disorient and scare the victim as much as overcome their defenses. Most ransomware attackers are script kiddies who tend to not execute reconnaissance or target specific victims. Ransomware attackers do not expend the time or resources sifting through your information and assets to uncover valuable data. They do not worry about entry into your network, about remaining undetected on the network, or about exfiltrating data from the network. Ransomware attackers just deny victims access to their information and systems unless a ransom is paid. Ransomware is rapidly evolving to infect and exploit every device that can run a basic encryption algorithm. Consequently, everyone ranging from average users on PCs to the cell phone addicted millennials, to Fortune 500 corporations are potential victims. If you have data, documents, pictures, music, systems, or devices that you want to operate as normal, then you are a potential ransomware victim. Further, the encryption algorithms often employed, such as AES-256, 3DES, and RSA-256, are functionally unbreakable within the resource and time constraints of the victims that they are targeting.

After a successful attack, victims can lose the data, pay the ransom, or hope that law enforcement and security vendors eventually capture the attacker servers and release decryption keys. Victims are unlikely to want to lose their data and salvage what is left of their system if only because the information might not be replaceable and because admitting defeat in the face of such an unsophisticated adversary could seriously impact employee morale, investor relations and customer perception. Paying the ransom is no confirmation that the data will be released. In many reported instances, the attacker has declined to decrypt the data after the ransom was paid. The payment of ransoms encourages the specific attacker to continue utilizing the attack vector and it encourages new entrants, of varying degrees of sophistication, to conduct attacks. Ransomware is so profitable and effective that sophisticated groups, such as the Dridex criminal organization, and APT’s are entering the threat landscape. These sophisticated adversaries desire the easy economic gains and the chaos created from the effortless attacks. Victims need to realize that they do not know to whom they are paying ransoms or what malicious purpose that contribution will facilitate. In the best of circumstances, a ransom only encourages a script kiddie to attack numerous other hosts. At worst, average citizens and organizations might be actively paying enemy nation states to compromise federal agencies and critical infrastructure systems. In this manner, victims are made accomplice to their own victimization. Lucky victims can decrypt their data with decryption keys or decryptor tools released from information security firms and law enforcement. The release of these solutions is limited to a small subset of victims and the release of keys is increasingly rare.

The only realistic and scalable solution to ransomware is for victims to regularly backup their data and to store that backup in a secure and digitally isolated location. Though a simple preemptive solution, average users and organizations still tend to not regularly backup data. Users fail because either they lack the technical knowledge to create a backup on an external device or they lack the time and energy to create the backup. Organizations fail for the same reasons and because it might be difficult and expensive to regularly backup every device on a network without negatively impacting network performance. Nevertheless, every device in the corporate and home network must be protected from ransomware according to the value of the system and its data because every system in those networks is vulnerable to at least on exploit. Seeing how backups alone are not satisfactory in staunching the flood of ransomware targeting the market, potential victims need to move further back in the attack chain and preempt becoming compromised in the first place. To this end, endpoint security solutions can offer great value and utility to an organization. Endpoint security solutions for each vulnerable network device exist and are easy to deploy. Under the looming shadow of the threat of escalating malware attacks, such as the recent ransomware attacks that threaten every system that stores, processes, or transfers data, that is connected to the internet, organizations can no longer cling to their dismissals of adopting endpoint security solutions.

The Need for Endpoint Security:

Comprehensive, holistic endpoint security solutions exist and are easy for trained information security personnel to implement according to the needs of the organization and according to the threat landscape. According to Stan Mierzwa, an ICIT Fellow and Director of Information Technology at Population Council, organizations often mistakenly believe that, "[implementing an endpoint security solution] has to be more complicated than it is really." Many organizations feel this way because they witness their own networks and networks in their sector repeatedly breached by cyber-adversaries. What these professionals fail to realize is that their underlying assumption, that endpoint security solutions make a network impervious to compromise, is at fault. ICIT Fellow and GRA Quantum CEO remarks, "the biggest misconception of endpoint security is that it is the only solution needed. EPS is but one of the many pieces needed to reduce the potential of a system compromise." Endpoint security is not a silver bullet solution. It will not stop every piece of ransomware or malware from infiltrating the network. A well maintained and managed endpoint security solution will reduce the number of successful attacks by protecting the points that attackers can use to access the network. Organizations often fail to realize that information security is not a static field. It is a process. The threat landscape surrounding every organization that processes, transfers, or stores data, is a constantly shifting and evolving nebulous mist that conceals cyber predators who might be small, large, foreign, domestic, simple, or sophisticated. Do not make the mistake of believing that endpoint security is unnecessary because either you are not worth targeting or because the adversaries are not capable of bypassing your defenses. If you own a system that processes code (so a laptop, desktop, smart phone, medical machine, POS terminal, etc.) then you are a target of uncounted legions of adversaries. Malware is not always focused on compromising your identity or stealing state secrets. Ransomware uses the encryption algorithms that enable modern computing to extort a monetary gain from the victim. Ransoms do not need to be considerable for the attacker to make significant profit because ransomware is so easy to deploy and profit from that an attacker can target thousands to hundreds of thousands of victims without any real investment of time, energy, or computational resources. If only 1% of those victims pay at least $1, then the attacker has likely recovered whatever resources they initially invested in the campaign. Further, even unskilled modern adversaries pose a threat to unprotected organizations. Information is the great equalizer and both sides of the field of information security have felt the joys and sorrows of the age of information. A teenager can spend an hour on YouTube or Reddit and learn enough to successfully breach an unprotected organization. Ransomware can be purchased on dark net for a few hundred dollars by teenagers who download Tor. More sophisticated adversaries are able to breach protected organizations without alerting authorities. The tools purchased or developed by the aggregated community of malicious attackers are often robust and easy-to-use applications focused on exploiting the path of least resistance into a target network. Often the only way to properly observe one of the adversaries is to discover one in your home network or to profile the forensic details left behind after an incident. Endpoint security is an organization's way of locking the windows, bolting the door, and setting alarms against the predators waiting outside. Endpoint security solutions may not be perfect, but operating an organization without endpoint security is the equivalent of living in a cave and hoping that no predators creep in at night.

Of the lines of network defense available to an organization, endpoint security is uniquely capable of stemming the growing ransomware menace. Traditional endpoint solutions, such as antivirus/ malware, firewalls, and IDS/IPS can detect ransomware and the forms of malware that deploy ransomware from entering or operating on the network. Meanwhile, more advanced systems included in vendor endpoint security suites provide the means to react to predictions, rather than detections, and the ability to monitor and manage a vast number of systems from a centralized location. Some bleeding edge solutions even confound ransomware and other malware by exploiting design flaws in the malware and trapping intrusions in perpetual sandboxes. Without endpoint security, the systems on the network are at the mercy of any attacker in possession of malware.

Malware is distributed onto target systems along the path of least resistance. Ransomware tends to infect systems through spear phishing, through drive-by-downloads, through the remote exploit of vulnerable applications, through botnet footholds, and through other malware. If a system can be infected by malware, then it is a target for the smaller and procedurally lighter ransomware attacks. Since recent ransomware, such as the April 2016 CTB-Locker, does not require connection back to a command and control infrastructure, and since ransomware in general can run on more devices than traditional malware, the potential threat landscape of ransomware attacks against organization's devices is rapidly expanding every day. Sophisticated threat actors, such as the Dridex criminal group, renowned for their attacks on the banking industry, have begun to develop and deploy ransomware campaigns for profit and as distractions for their more complicated endeavors. It seems likely that before the end of the first half of 2016, at least one sophisticated threat actor will merge ransomware attacks with data exfiltration campaigns. After all, what is stopping an attacker from exfiltrating your encrypted data while you are waiting on law enforcement or deciding whether or not to pay the ransom? After all, the attacker has the ability to decrypt the data once it is transferred; in fact, most sophisticated APT groups encrypt target data prior to exfiltration as an obfuscation step of the standard attack chain. Integrating ransomware into the campaign would be trivial. The main difference might be that unsophisticated attackers who did not explore the victim network for valuable data ahead of time or who did not target specific victims, might not know if the data encrypted by their ransomware is worth exfiltrating. In perspective of the earlier analogy, this gamble is akin to an antiques speculator paying a lump sum to purchase the unseen contents of a house in hopes that something inside is worth more than the initial investment. To a creative adversary, the stolen data will always be worth exfiltrating. One way or another, ransomware must enter the network through an endpoint and its traffic must leave through an endpoint. Consequently, securing vulnerable endpoints is a critical first step in the battle against ransomware. As shown below, ransomware has already developed to target every major network endpoint; moreover, some novel systems, such as SCADA/ICS systems, POS terminals, and automotive systems are potential targets in the near future.

Vulnerable Endpoints:

Users:

Information Security is only recently beginning to consider users as endpoints. If this notion seems contradictory, consider for a moment, that any insider threat, any social engineering campaign, or most ransomware attacks are dependent on predictable human activity that ignores cyber-hygiene. Organizational leaders need to realize that humans are both the strongest and the weakest link in an organization. They need to adopt a security-centric focus with regards to their workforce. The mistake of a single user, such as clicking on a spear phishing email, can lead to disproportionally large consequences, such as the net $1 Billion loss in the Target breach. Organizations should not assume that their endpoint security solutions are going to be fail-proof, and they should not assume that investing in an endpoint solution would eliminate the risk posed to the organization by average users. ICIT Fellow and HPE Security Strategist Stan Wisseman remarks that, “Many organizations are recognizing that the limitations of securing an endpoint really need focus on securing users ‘access to sensitive data through applications. Applications can be presented through a variety of platforms. But as far as endpoints go – zero trust.” Endpoint security solutions can lend trust to users, applications, and endpoints by serving as a series of controls and sensors. Just as users are the greatest weakness in the organization’s network, they are also the greatest opposition to endpoint security solutions. Many fear that the solution will be unnecessarily complex or that the solution will not be a return on the investment. George Kamis, an ICIT Fellow and the CTO for Federal Markets at Forcepoint responds, “Implementing an endpoint security solution is NOT a technical challenge. It is more of a cultural challenge. Organizations need to change the mind set of IT professionals that endpoint security solutions are required to compliment external cybersecurity solutions. Users pose the highest threat to organizations; companies need to audit and monitor users where they are accessing company/agency information. The endpoint provides an ability to attribute data to specific users prior to encryption and also provides an ability to monitor activity when a user is offline.” Because endpoint solutions lend trust to otherwise ambiguous people, systems, and processes, the return on investment comes from both greater assurance that the network is not compromised and greater confidence that the people, processes, and systems are performing according to their function in the organization.

Ransomware is unique among malware in that it specifically exploits human nature in order to succeed. Ransomware developed from the scareware and fake anti-virus programs of the 1990’s. It depends on catching its victims unawares and then inciting fear and panic to tempt the victim into paying the ransom before they think through the decision. The ideal ransomware victim is a user who is not too tech-savvy, who values what is on their system, and who has not created backups of their valued data on an external device. Many ransomware variants focus on compelling victims to panic and pay.

The Cerber ransomware audibly informs victims and everyone within earshot that the files on the system have been encrypted. The Cerber ransomware surfaced from the Russian underground malware forums around March 4, 2016. Cerber exhibits characteristics of a Ransomware as a Service (RaaS) tool, in which a sophisticated malware developer outsources deployment of their tool for a commission of each paid ransom, to less sophisticated, but more numerous attackers. Though Cerber’s distribution vector is not yet known, RaaS is often distributed through botnets, spam email, and drive-by-downloads.

Cerber identifies the victim’s country of origin (by IP Geolocation). If the victim host is located in one of 12 former soviet nations then the malware terminates itself and will not encrypt data on the computer. Otherwise, Cerber installs itself in %AppData%\{2ED2A2FE-872C-D4A0-17AC-E301404F1CBA}\ folder and names itself after a random Windows executable. The malware sets up an auto-boot registry key and restarts the system. Upon the next log in, Cerber will encrypt the victim files using a JSON configuration file to determine what extensions to target, what nationalities of victims to not target, what files and folders to leave unencrypted, and other configuration information. Cerber enumerates connected drives and systems for files matching certain file extensions, encrypts each file using AES-256 encryption, encrypts the file name, and appends the .CERBER extension to it. Ransom notes, demanding 1.24 Bitcoins (~$500) are placed in every folder containing encrypted data and the audio message begins playing. The ransom doubles if left unpaid for more than a week. Other recent variants, such as Maktub, incite panic by geo-locating or identifying the victim. Maktub spreads through phishing emails that appear as correspondence from a charity, often called Koelster Trust. The links inside distribute the malware and direct the user drop page so that the hacker can collect their credentials, possibly from the browser cache if it is stored. The malware encrypts files and demands 1.25-1.5 bitcoins (~$580-$790) and displays the user’s identity and address with the ransom note. Maktub is nothing more than another twist on the same panic and pay ransomware formula. However, it does demonstrate how attackers are beginning to mimic sophisticated adversarial tactics.

Similarly, sometimes ransomware incites panic by threatening to delete the files or the encryption key if the victim does not pay the ransom within a certain period. The Jigsaw ransomware emerged on in early April 2016 and it improves on that tactic using a ruthlessness characteristic of a more advanced (but not necessarily sophisticated) adversary. Jigsaw encrypts victim files and then demands a payment of $150 in Bitcoin. Every hour that the victim delays paying the ransom, the malware deletes a number of files equivalent to the number of hours that have passed. If the victim shuts down the system in an attempt to halt the timer, the malware deletes 1000 files. The whole time the malware is running, the face of Jigsaw from the Saw horror franchise is staring back at the user beneath a running teleprompter. The malware is clearly meant to disorient and scare the victim into quickly paying the ransom. Luckily for victims of the Jigsaw ransomware, a decryption tool was released soon after the malware was discovered.

Personal Computers:

The vast majority of ransomware victims since the creation of the AIDS trojan in 1989, have been Windows PCs. Personal computers are optimal targets for ransomware because they present the greatest number of open vectors and they are the primary location where average users store, process, and transfer data. Endpoint security solutions are needed to prevent corporate machines from being exploited as well as to prevent employee owned machines (BYOD) from poisoning the network.

Ransomware tends to enter systems through vulnerabilities present in the host operating system or in unpatched applications. In more recent cases, the malware has also been distributed to machines infected by botnets. The code to leverage the exploit and deliver the ransomware is typically delivered through malicious email attachments or through drive-by-downloads. In this manner, the user becomes an accomplice to his or her own exploitation. As with many malware, ransomware attackers seem to prefer to leverage vulnerabilities in Adobe Reader, Flash Player, or Microsoft Word. In absence of these applications, browsers such as Internet Explorer, have been exploited.

One of the numerous ransomwares to target personal computers was the Cryptolocker malware that in many ways set the template for recent ransomware variants. 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. It stores the private key needed to decrypt the data in a remote command and control server. In absence of a botnet, the ransomware spread as a malicious .ZIP file in spam emails. Cryptolocker installs in the user profile folder and adds a boot key to the system registry. 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.

Victims of Cryptolocker 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. Even if the ransom was paid, some attackers did not decrypt the files. 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 estimate that only 1.3-3% of victims chose to pay. In its short lifecycle, Cryptolocker revitalized the ransomware trend that had died off throughout the 1990’s and 2000’s by showing attackers that crime paid. As a result of its success, numerous rebranded variants, such as Cryptowall, Cryptodefense, Torrent Crypt, and many others, appeared on the market.

Interestingly enough, with the sudden horde of ransomware targeting Windows systems with rapid Blitzkrieg attacks, the market has become saturated. Consequently, at least one adversary developed the KeRanger ransomware to target the Apple community. From a holistic information security perspective, Apple products are no more secure than Windows products. Each has their merits and flaws. Apple products have a cultural reputation of "being virus-proof" because it is not profitable for adversaries to target Apple products over Windows products, given Microsoft's significantly greater market share. Conventional attackers also did not develop as much malware for Apple systems because businesses, who are the primary targets of most criminal and espionage campaigns, typically rely on Windows personal computers. Ransomware attackers lack these biases. Any user system that contains data or that can infect other devices through association, is a viable target. If a user would pay any amount of money (even $1) to regain their system, then the attacker has no reason to ignore them.

On March 4, 2016, Palo Alto Networks discovered the KeRanger ransomware in the Transmission 2.90 BitTorrent installer for OS X. Transmission is an open source BitTorrent client bundled with Linux distributions and available for free download online. Attackers infected two Transmission 2.90 installers with infected DMG files in hopes that users would infect their own systems by installing the program from the official website. Approximately 6,500 users obliged them by the next day. According to Transmission representative John Clay, the ransomware was added to the disk-image of the software after cyber-attackers compromised Transmission's main server.

Apple protects its OS X systems with the Gatekeeper security feature which restricts application installations to reduce the likelihood that malware will inadvertently be installed and executed on the machine. The malicious Transmission installers used a valid Apple Developer certificate to bypass the OS X gatekeeper feature. The certificate belonged to POLISAN BOYA SANAYI VE TICARET ANONIM SIRKETI (a Turkish company) with the ID Z7276PX673, which differed from the certificate used on earlier versions of Transmission. The installers were generated and signed the same day as the injection. The malicious files included the traditional Transmission installers, along with an extra file named General.rtf in the Transmission.app/Contents/Resources directory. The code in General.rtf reveals that its main function is to encrypt and ransom user data. While the icon of General.rtf masqueraded as a RTF file, it was actually a Mach-O format executable file packed with UPX 3.91. When users ran the installer, this file would be copied to their ~/Library/kernel_services directory, where it executes as "kernel_service." After the infected application was installed, it ran an embedded executable on the host system to install KeRanger. Upon its initial execution, three files, "kernel_pid", "kernel_time", and "kernel_complete" are created under the ~/Library directory. The current time is written to "kernel_time" and a sleep timer is set to three days. The ransomware is configured to wait three days before contacting its command and control infrastructure over the Tor anonymizer network. The malware collects the host's model name, and UUID and uploads the information to a C2 server. The servers' domains are all sub-domains of onion[.]link or onion[.]nu, which are only accessible via the Tor network. The malware keeps attempting to connect until the server responds with two lines of encrypted data. The malware decodes these two lines, an RSA public key and a line of text written to “README_FOR_DECRYPT.txt”, lines using Base64.

After contact is made with the command and control server, an encryption key is sent and the malware begins encrypting specific file types on the host system. The malware uses a statically linked open source encryption library called mbed TLS (formerly Polar SSL) to encrypt files corresponding to 300 different file extensions found under the /Users and /Volumes directories on the host system. KeRanger begins by creating an encrypted version of each file that appends the .encrypted file extension onto the file name. For example, an encrypted file, test.doc, would become test.doc.encrypted. KeRanger encrypts each file by generating a random number (RN) and encrypting the RN with the RSA key. It then stores the encrypted RN at the beginning of the resulting file. Next, it generates an initialization vecor (IV) using the file’s original contents and stores the IV in the resulting file. The RN and the IV are combined to generate an AES encryption key, which is then used on the contents of the target file and written to the encrypted file. Additionally, developmental features (functions named “_creare_tcp_socket”, “_execute_cmd”, and “_encrypt_timemachine”) in the malware suggest that it also tries to encrypt Time Machine backup files so that users cannot simply avoid the ransom demand by restoring from a back-up point. The victim then receives a ransom demand of 1 Bitcoin (~$420) in order to recover their files. A link in the ransom demand guides victims on how and where to purchase bitcoins, while a separate section directs them to an address (for example “1PGAUBqHNcwSHYKnpHgzCrPkyxNxvsmEof”) to make the payment. Victims attempting to pay the ransom are taken to a page to enter their assigned bitcoin address. After the address is entered, the victim is taken to a page that contains a list of the support requests that were created by the victim. At the top of every page on the payment site is the option to decrypt one file, of the victim’s choice, for free, a reminder of the ransom amount, how much has been paid already, and the bitcoin address to which payments should be forwarded. According to security researcher Lawrence Abrams, the decryption feature is currently non-operational. Victims can also navigate to an FAQ about bitcoins and how to pay the ransom. In the event that the victim pays, a “Download Decryption Pack” button on the page will be enabled so that they can download a decryptor tool unique to their system and files.

As a result of Palo Alto’s discovery, Apple revoked the abused certificate and Gatekeeper now blocks the malicious installers. Additionally, Apple updated the XProtect signatures on all Mac computers to recognize the known variants. If a user tries to open an infected version of Transmission, a warning dialog stating that “Transmission.app will damage your computer. You should move it to the Trash.” or “Transmission can’t be opened. You should eject the disk image.” will be displayed. On March 5, 2016, Transmission removed the malicious installers from the website. Transmission has since increased security on its servers and released two updated versions of the Transmission application. The former, version 2.91 is a clean installation of the application and has since been replaced by version 2.92, which also removes the KeRanger malware.

Servers:

Servers of all varieties are critical to the operation of an organization's network. Productivity can be severely hindered if the email server, DNS server, file server, or any number of other systems are taken offline. Further, despite servers being high-value targets for cyber-adversaries, many organizations irresponsibly leave the devices insecure and unmonitored. Endpoint security solutions can limit access to servers and increase insight into network activity directed at the devices.

On April 15, 2016, the Cisco Talos group revealed that 2100 servers registered to 1600 IP addresses belonging to government entities, schools, aviation companies, and other firms were infected with a backdoor that could be used to deliver ransomware. The attacker could have spread the backdoor to an estimated 3.2 million machines had the infection remained undiscovered. Cisco was investigating the server database as a consequence of the Samsam ransomware attack perpetrated against MedStar Health Networks in late March 2016. Attackers infected MedStar servers by directing an automated exploit tool called Jexboss against the vulnerable JBoss application installed on the servers. The malware then spread to other systems (and possibly other hospitals) on the network. Samsam encrypts victim files with RSA-2048. The evolution of the malware is interesting in that it does not beacon back to command and control infrastructure. Once Samsam is on a host, it is entirely self-sufficient. Because MedStar Health Networks practiced good cyber-hygiene, they were able to restore their systems using system backups and thereby avoid paying the ransom.

Mobile Devices:

Mobile devices used to be frequently targeted by fake applications and scareware at the dawn of the cell phone revolution, but with the advent of vetted application stores, those malware have declined. Mobile devices are everywhere; consequently, it is only a matter of time before ransomware moves to that market in force. One could argue that some devices, such as iPhones automatically back up data to a cloud server and that as a result, mobile devices might not be a huge market because users could just restore the device to factory settings and recover the data. This theory has merit, but it hinges on the assumption that users will recognize that option and the assumption that attackers would only target mobile devices for direct profit. Cell phones connect to other mobile devices, to wireless networks, and to Bluetooth connections. As a result of their ubiquity and their versatility, mobile devices are an optimal stepping stone for ransomware to spread. A given variant could spread through text, email, or recognized device connections and polymetrically increase its distribution with each infection. Endpoint security solutions and coherent BYOD policies can limit the risk that mobile devices present to organizations.

As stated above, mobile ransomware is only recently reemerging. One unnamed variant has been spreading through text message and app markets offering tantalizing adult videos. If a user is careless enough to click on the link or install the app, (and grant it the admin privilege it requests) then a hastily put together site opens and infects the device with android ransomware. The malware takes a picture of the user and threatens to report the victim for viewing kiddie porn, bestiality, or other embarrassing content. The app threatens to spread notice of the victim's activity to contacts, social media, email, and the police unless $15 is paid. So far, the app has infected around 3400 devices that are mostly located in Russia.

Specialized Hardware:

On February 5, 2016 specialized medical equipment belonging to Hollywood Presbyterian Medical Center was infected with the Locky ransomware. The infected equipment, included CT machines, systems essential for laboratory work, and emergency room systems. Despite the assistance of law enforcement and reputable security vendors, after almost two weeks of stunted operations, Hollywood Presbyterian Medical Center paid a ransom of 40 Bitcoins ($17,000) to release their systems. HPMC paid the ransom because continued operation without access to their systems jeopardized patient care. HPMC may have been infected via a phishing email. In these email campaigns, the Locky ransomware masquerades as a Microsoft Word attachment. If opened, Locky encrypts victim data with RSA-2048 and AES-128 ciphers. Encrypted files are renamed with the .locky file extension. Then the malware deletes backup shadow copies of the operating system. Victims are then informed of the infection and directed to a payment page containing instructions to purchase Bitcoins and how to install Tor. Because the malware is uniquely hashed to each victim, conventional signature based solutions are inadequate to detect or prevent a Locky infection.

According to Palo Alto, the Locky ransomware may have been deployed through the Dridex Criminal botnet network. It is likely that Dridex is offering the ransomware as a service to script kiddies. In a ransomware as a service model, a less technical criminal deploys a more sophisticated malware using a prebuilt exploit kit that often includes a GUI. The more sophisticated author of the malware receives a percentage (usually ~30%) of the ransom paid by each victim. According to Forbes, the Locky ransomware was infecting an estimated 90,000 systems per day in February 2016. The attackers usually demanded 0.5-1 Bitcoin (~$420) to decrypt victim systems. The significantly higher demand of $17,000 could indicate that the attack against HPMC was a targeted attack. In an attack that infects specialized hardware, paying the ransomware could seem more financially viable than it might seem. How much money is lost for every hour that a CT machine or MRI is nonoperational? Specialized hardware is uniquely expensive and often complex. While this equipment might not be a sole target of a ransomware attack, its infection does afford the adversary greater leverage over the victim. This may be one reason that the attacker who breached Hollywood Presbyterian extorted $17,000 from his victim instead of the $400-$600 characteristic of the malware. Endpoint security solutions can be used to segment these valuable devices from the network and to secure the devices that do not have the functionality to secure themselves.

Cloud Services:

Cloud Services are employed to reduce the operational cost and increase the resiliency of networks by hosting content on external servers at a remote location. Essentially cloud services allow a firm to lease the maintenance, expertise, and hardware of a service. In January 2016, Brian Krebs reported that the TeslaCrypt ransomware had targeted a Citrix based cloud service provider. When cloud services are compromised, numerous businesses suffer. It is imperative that vendors employ endpoint security solutions on their cloud systems and that clients seek out the vendors who secure their cloud services.

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 Cryptolocker 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.

Potentially Vulnerable Endpoints:

SCADA/ICS

According to an account by Blake Visin in Treatment Plant Operation magazine, in 2013, nine SCADA systems were almost infected with ransomware when a networked system was infected with the Cryptolocker ransomware. Though the spread of the infection was stopped by unplugging the infected control interface, the threat is obvious. Halting any major SCADA or ICS system has cyber-physical implications that dwarf the consequence of a monetary ransom. If a SCADA or ICS system in an Energy, Utilities, or Manufacturing organization becomes infected with ransomware, then lives could be jeopardized in the time it takes to investigate the incident and return the systems to operation. Further, if a system is infected, there is no guarantee that the adversary will provide the decryption key. Since many SCADA and ICS systems are antiquated, they are unlikely to have system backup, fully operational redundancy systems, or technical personnel capable of building the system from a factory reset in a reasonable time frame. These systems used to be protected from malware by their age and by network segregation, such as air gaps. However, ransomware, as weaponized encryption can run on any system with sufficient computational resources and advanced persistent threats developed tactics to infect air gapped systems almost a decade ago. SCADA and ICS systems are already threatened by APT malware such as Black Energy, which threatens to cause physical harm to the systems. While Black Energy has infected American systems, its destructive capabilities have not been unleashed. The threat actor may be withholding the capability in case of the advent of cyber-physical warfare between Russia and the United States. Without an adequate investment in bleeding edge endpoint security solutions, ransomware will likely cause more significant harm much sooner.

IoT Devices:

It is not inconceivable that malware, and ransomware in particular, will eventually target IoT devices. The internet of things is practically an infinite attack surface. Adversaries would have to be extremely risk averse to not develop malware to target the internet of things. IoT devices offer a potential growth bed to any ransomware operation because the devices are interconnected by design and many pointedly lack any form of security. A selection of traditional malware will be too large to ever run on a number of IoT devices, but ransomware, predominantly consisting of a few commands and an encryption algorithm, is much lighter. How much do you predict someone would pay to remove ransomware from a pacemaker? The scenario is not too far-fetched; in fact, it is much more deadly. Many medical devices, such as pacemakers, insulin pumps, and other medication dispersion systems are internet or Bluetooth enabled. Ransomware could utilize that open connection to infect the IoT device. Moreover, according to Cylance's Jon Miller at an ICIT panel in November 2015, placing even light encryption on a pacemaker could decrease its battery life from about a decade to as little as a few years or even a few months because the device is not designed to sustain those operations. The more resource intensive the encryption, the more dire the situation. In some cases, the ransom window might be less than the wait time before a medical team could schedule a surgery to reset or replace the device. The main difficulty that adversaries will have exploiting IoT devices will be how they deliver the ransom demand to the victim and how they collect the payment. Email, text message, or other digital vectors seem most probable since the attacker would want to maintain anonymity.

Cars:

Last year, Charlie Miller and Chris Valasek demonstrated that a skilled hacker could remotely disable a Jeep Cherokee by exploiting vulnerabilities present in the network design, firmware, and CAN Bus of the vehicle. Ransomware would not likely shutdown a car on the highway like the aforementioned hackers did to Wired's Andy Greenberg. Instead, ransomware could be deposited on a victim system through a remote connection, a Bluetooth connection, or through a poisoned software update (similar to the KeRanger ransomware). When the victim attempts to use their vehicle for work or travel, the console display could provide them the ransom note and a method of paying ransom, such as via SMS message. Because encrypting the CAN bus or other systems would disrupt any recent software dependent vehicle, the attack could also be used for ulterior purposes, such as disabling an areas police and emergency response vehicles or conducting a cyber-physical denial of service on a business. Vehicle manufacturers and their firmware/software developers need to seriously consider endpoint security as a necessity by design. The attack surface of ransomware and malware against software driven vehicles will only increase in the years to come as automated vehicles enter the market. If manufacturers delay the adoption of a security-centric culture and the deployment of endpoint security on their software driven devices, then the costs of their inaction could be dire.

Endpoint Security:

ICIT Fellow Malcolm Harkins, the Global Chief Information Security Office at Cylance, contends, “Most malware, such as ransomware, targets the endpoints directly. Knowing that the endpoint is the final target makes endpoint security the most critical part of a layered cyber defense as the vast majority of all compromises begin or end with an endpoint, such as a server or user workstation. Having a robust and intelligent next-generation endpoint security suite allows an organization to stop attacks before they start.” Without endpoint security solutions, your home network is vulnerable to the vast wilderness of the internet. Endpoint security solutions confound adversarial efforts to introduce and spread ransomware through your network. These security solutions are layers of preventative, reactive, and predictive tools that correlate the indicators of suspicious traffic and questionable behavior detected from inbound, outbound, and internal network activity. ICIT Fellow George Kamis, the CTO of Federal Markets at Forcepoint, states, “Endpoint security is essential for identifying behavior associated with malware or APT’s that have evaded external cyber security measures.” Endpoint security solutions prevent adversaries from leveraging exploits on vulnerable endpoints to gain access to the network. Preventative endpoint solutions can scan endpoints for known vulnerabilities and assist the information security team in patching and updating the network. If an attacker penetrates an endpoint and begins to spread ransomware through the network, a reactive endpoint security solution such as IDS/IPS or UBA can issue an alert to the information security team so that they can quarantine the system and contain the infection. Broad endpoint security suites can be used to monitor the macroscopic network for infection. According to Ryan Brichant, an ICIT Fellow and CTO for Industrial Control Systems at FireEye, through an endpoint security solution, “an analyst can proactively search their entire endpoint to quickly identify suspicious activities that may not have reached a critical stage, or to find the source of a breach in order to close that gap in their defense that allowed that attack in the first place. Also, an analyst can determine what the attacker looks like, what they were trying to do, and how they were trying to do it, which enables them to better fortify their endpoints against those attacks.” In short, endpoint security solutions automate the security on endpoints, centralize the threat indicators across endpoints, and serve as the first line of defense to dissuade attackers from moving further into the network.

Endpoints can be characterized according to system endpoints and user endpoints. A system endpoint is an externally accessible system that is traditionally accessed through other systems, such as a remote server or SCADA system. A user endpoint is a human-computer interface through which a human actively processes, transfers, or stores data. For a home user, a system endpoint might be a Bluetooth speaker or external hard-drive, while a user end point would be the laptop, desktop, or mobile device. ICIT Fellow Cindy Cullen, a Security Strategist at HPE, warns readers that, “It is unwise to operate a computer these days without a software based protection in-place. It is vital even for standalone computers to utilize this software.” Readers should recognize that an insecure device, such as a smart phone, could unknowingly infect numerous other devices without the user’s knowledge. How many times has your phone automatically connected to random Wi-Fi networks as you drove or walked around? Ransomware is evolving to spread through any vector. In the case of a phone without security, what is to stop the phone to receive a spoofed “application update” containing ransomware? Endpoint security should be users’ answer to this threat.

Ransomware infections should be prevented according to administrative, technical, and procedural specific to the needs of each endpoint in each category. System endpoints will likely require more technical controls, while user endpoints may be more easily managed through administrative and procedural controls; although, that is not to say that either type of endpoints do not require one or more of the categories of controls. For instance, user endpoints generally have an active external connection, meaning their activity and that of their users must be monitored by endpoint security solutions. Similarly, system endpoints may be subject to administrative and procedural controls, even though system endpoints such as specialized medical hardware, factory ICS systems, or POS terminals predominantly rely on technical security controls. For instance, many of the aforementioned system endpoints lack sufficient internal memory to support native security solutions. Consequently, it is more realistic and efficient to monitor all specialized devices under one master system through the implementation of group policies. When enumerating their network to discover and account for all endpoints, responsible organizations should categorize each endpoint according to its function and then determine technical, administrative, and procedural controls according to device capabilities and the needs of the organization.

Endpoint solutions begin with the foundational security tools such as a whitelisted Firewall, frequently updated antivirus/ antimalware applications, and IDS/IPS. More sophisticated systems such as UBA, anti-spam/anti-phishing, and other tools build upon this foundation. In particular, the spread of ransomware can be limited by configuring the firewall according to an application whitelist, by restricting internet traffic to only trusted sites, and by introducing an anti-spam/ anti-phishing component to the email server. Ransomware is often dropped from other malware as a distraction or as a tangential attack. Anti-virus (AV) and anti-malware can detect the signatures and behavior of these malware before they can drop ransomware onto the system in the first place. According to the socioeconomic theory of the Broken Windows, as more attacks are detected and precluded, other attackers will increase their attacks or enter the threat landscape. As more organizations implement detection tools such as AV, less attackers will see malware and ransomware attacks as profitable and worthwhile. Anti-virus will detect and prevent the activity of known threats; however, ransomware is particularly easy to alter enough to change the signature. Consequently, the AV will not recognize the new variant. Even then, a study conducted by Lastline Labs asserted that only 51% of AV scanners detected a malware sample on the day that the signature was disseminated. After two weeks, only 61% of the AV scanners detected the sample. According to Greg Fitzgerald, and ICIT Fellow and Chief Strategy Officer at Cylance, “The biggest misconception of endpoint security is that traditional anti-virus/ anti-malware solutions are capable of keeping pace with new and advancing attack techniques. Signature and heuristic based solutions require an army of reactive analysts to release new updates after someone has already become the victim. In addition, many endpoint solutions require a large backend cloud infrastructure to maintain their effectiveness, but when the endpoint goes offline, the solution can no longer adequately defend the endpoint." Endpoint security is not perfect, but it is far preferable to the alternative of a total lack of security. Clients need to seek out dependable endpoint security solutions from reputable vendors in order to address the current ransomware threat. The shortcomings of traditional endpoint security solutions such as anti-virus, though discouraging, demonstrates the need for layered defenses. Independent and redundant endpoint security systems that are regularly audited and updated, provide resiliency to the defense strategy to account for the shortcomings of any one system. ICIT Fellow and (ISC)^2 Regional Managing Director, North America, Dan Waddell adds that "When done correctly, each layer of security minimizes the opportunity for a gap to be discovered by hackers and used for subsequent breaches." These redundant systems should not be seen as an excessive investment. Again, think of the walls that protect your home. Chances are, you do not have a single board or piece of plaster between you and the outside world. Your walls are made of layers of panels, insulation, and support beams so that you are best protected from the threats waiting outside. ICIT Fellow Ryan Brichant adds, "A layered security strategy really is about putting security where it can provide the greatest protection, and at endpoints, [which] are the primary target surface that an attacker can identify to initiate an attack. Exposed endpoints are the first place an attack will start and it will radiate from there into the network at large. A layered defense acts like a set of permeable barriers to manage good and bad traffic. This should allow the identification of suspicious traffic so security personnel have access to it along with the time to investigate and act on anything out of the ordinary." Each technical control layered on the end point, surrounds your home network with another wall, through which traffic must pass to access the network. Consequently, in addition to increased security, each technical control both increases your insight into the traffic entering and exiting the network and provides an opportunity to detect and contain malicious activity on the network.

Beneath the technical controls, administrative and policy based controls can shield the organization from ransomware attacks. For instance, a Windows group policy can be used to keep systems updated and secure. Group policies can also be used to restrict activity or access to directories (such as the temp directory) where ransomware and other malware are known to install and operate. On Microsoft Windows, Software Restriction group policies can be used to only allow whitelisted applications to run. Mr. Brichant continues that "Active Malware Policies (AMP) forward deployed to end points provide detection of malware related log entries, processes launching from unusual locations, attempts to establish persistence by unauthorized software, writing of files like autorun.inf, and other behaviors indicative of compromise attempts. Once detected, solutions like detonation chambers can quickly remediate and clean up any residual effects. Should an attack get through the gateway, the next line of defense is the gateway where the ransomware can be quarantined to prevent it from pivoting to other workstations" Group policies can also be used to mandate security on each system on the network and to manage different network segments according to the principles of least privilege and least access.

Selecting an Endpoint Security Solution:

In order to implement an endpoint security solution, an organization must employ information security personnel to conduct a holistic risk assessment of the network. The risk assessment identifies risk appetite, critical systems, and constraints according to a systematic and actionable process. The risk assessment will identify the needs of the organization in consideration of their capabilities. Early in the assessment, stakeholders, critical systems, and risk appetite relative to the threat landscape, should be determined to focus the assessment to the actual needs of the business. For the purpose of endpoint security, the risk assessment also has the added value of necessitating that the information security personnel enumerate and audit the network. How can an endpoint solution be expected to offer any additional level of security or trust if you do not even know what is on your network to secure or upon what foundation your security is built? This process will account for every device on the network, including BYOD, approved USB devices, and other systems. A conservative rule of thumb is if it connects to anything else or plugs into the wall, question whether or not it should be included in the risk assessment. The outcome of the risk assessment is a series of actionable, scenario-based plans and greater knowledge of organizational systems. After the information security team knows the network, then the organization can begin evaluating endpoint security solutions.

Endpoint security solutions are relative to organization size, budget, and assumed risk. In the case of ransomware, every system belonging to every organization is at risk, but not every organization is the likely target of an APT. Controls and implementation of those controls should be assessed according to the risk assessment. Dan Waddell warns, “From a workforce perspective, organizations may lack in-house talent when it comes to designing, implementing, and maintaining a solution – particularly small-medium- businesses (SMBs) and startups. It may make sense for these organizations to partner with a service provider, but it’s important to do your homework and select a trusted provider that has qualified and dedicated resources. For larger organizations that have a dedicated security team, they must account for competing priorities. Often times, their teams are busy putting out fires and dealing with their day-to-day responsibilities. Piling on a big project such as an endpoint implementation may end up ‘robbing Peter to pay Paul’.” As with all information security, resource management is key. A SMB is the viable target for ransomware, but they likely do not need the same endpoint solution as a large Fortune 500 company. Implementation of the solution also depends on trust. The organization must trust the team or vendor designing and implementing the solution to correctly address the threat to the organization.

The vendors worth collaborating with are the vendors who appreciate and understand their clients’ needs. Thomas Boyden, an ICIT Fellow and Managing Director at GRA Quantum comments, “While some endpoint solution providers have better products than others, it always comes down to customer service. The endpoint solution provider that goes above and beyond to ensure that their client/ partner is satisfied will make them stand out from the sea of endpoint solution providers.” Customer service amounts to communication, the ability to meet the needs of the client in an accountable, timely manner, and the benefit presented to the client as a result of their interaction with the vendor. Dan Waddell adds that when evaluating vendors, "Communication stands out as a key differentiator. Providers that communicate with customers on issues/ gaps and continuous evolution of the product and services will add value and contribute greater to an organization's overall return on investment." Communication is the first step to cooperation. ICIT Fellow Ryan Brichant contends that the best vendors are: those who aggregate information from information sharing initiatives and from various endpoints into a complete picture of the threat environment or of an active exploit, those who inspect all aspects of each endpoint to determine if there is suspicious activity or if there is a need for more information, and those who offer visibility into endpoint solutions and who can adapt a defense according to new information or inbound threats. Under the current daily threat of the emergence of a new ransomware variant or a new APT attack, the cooperative characteristics described, communication, transparency, and adaptability, are the hallmarks of reputable endpoint security vendors.

When collaborating with a vendor or hiring information security personnel, trust is built through effective management and clear communication. Jon Sabin, an ICIT Fellow and Director of Network Security & Architecture at GRA Quantum notes, "Organizations should not only be considering the product, but the provider as well. In the current state of cyber security, organizations need a partner to stand by their side, not just a product. Since each organization is unique, the provider and the organization should work hand-in-hand to ensure that the organization is getting exactly what it needs." Vendor agreements, hiring contracts, or task assignments must clearly describe expectations, responsibilities, and penalties for failure to meet the terms specified. Cooperative negotiation, focused around a mutually beneficial relationship and honest about the shortcomings or concerns of both parties, typically yields the most beneficial result for all parties involved. The information security personnel or organizational managers need to maintain visibility into their own endpoints so that they can consistently confirm that the solution meets the needs of the organization. Further, if a partner controls the solution and that partner has access to the network, then the client organization requires visibility into the endpoints of their partner. No organization wants to be the next epic breach as the result of a compromised third party, as was the case with both OPM and Target. The solution implemented needs to be consistently maintained and it needs to add accountability to the network. If an incident occurs, organizations and law enforcement should be able to forensically follow the incident from intrusion to conclusion.

Both parties should test the solution prior to implementation to discover what types of attacks the systems implemented protect against and what types of attacks suggest that additional security solutions are needed. Again, this process must be transparent and open so that both the systems of the client and the reputation of the vendor are protected. Neither party benefits if the vendor claims that a silver-bullet solution covers all attack vectors and the client discovers far too late that the solution only protects against denial of service or ransomware attacks. The capabilities of each tool and system should also be clarified to the client so that the native information security personnel do not misuse the product or have unrealistic expectations. For instance, the client needs to know if the endpoint solution depends on back-end cloud infrastructure or if a power outage at the vendor facility could result in loss of security on the client side. In the case of endpoint security and the growing threat posed by ransomware and other malware, discussion of the specifics is paramount. Vendors should audit and conduct a separate risk assessment on the client network prior to proposing an endpoint solution so that the vendor can provide exactly the services needed by the client. The vendor needs to know the BYOD policy of the client and the client, in turn, needs to seek out services that address the threats presented from personnel devices flooding the corporate environment. The client and vendor should discuss the design, implementation, and maintenance of the solution in terms of its projected lifecycle and the responsibilities and expectations of both parties. Both should determine how preventative or reactive the endpoint solution needs to be in order to address the threats to the organization. Some threats, like ransomware, cannot be responded to with reactive solutions (other than regular backups) and are difficult to prevent with traditional solutions. In the case of these threats, both parties should discuss what predictive or next-generation solutions the client organization can use to protect their systems. As Rob Bathurst, an ICIT Fellow and Managing Director of Healthcare and Life Sciences at Cylance points out, "The truly different and next generation endpoint security solutions focus on preventative actions instead of reacting after a compromise. Leveraging artificial intelligence and mathematical modelling resident on the endpoint is another key differentiator that allows the system to defend itself against new and emerging threats both offline and online with equal effectiveness." Next-generation systems might be more expensive to implement, but the investment will pay for itself over the lifecycle because the system is less likely to become obsolete in the near future.

Vendors and clients will benefit if the terms and the conditions of the agreement are clearly written and flexible enough to adapt to the cyber-threat landscape. After the solution is negotiated and implemented, the vendor should determine if any malicious activity or footholds are already present on the previously insecure endpoints. Again, transparent, cooperative measures such as this will protect both the client systems and the vendor reputation. Whoever manages the endpoint security solution should also collect, share, and utilize threat intelligence to best suit the client and the community at large. Threat intelligence sharing must be a collaborative between the various vendors providing the individual layers of security, while the organization's information security team manages and orchestrates the seamless oversight of the whole.

Conclusion

Combatting the ransomware Blitzkrieg requires the techno-synthesis that only occurs between the layers of a properly customized cybersecurity strategy. The cyber-physical convergence with the internet of things demands a cyber hygienic and security centric counterbalance to the hyper evolving threat landscape. Cyber jihadists, state sponsored APT's, sophisticated mercenary hackers and script kiddies will continue to use ransomware as a monetization tool as well as a mechanism for distraction. The malicious element within the hacker community is collectively migrating toward the ideology of ransomware as an apparatus for distraction, while stealthily exfiltrating and manipulating data that can be monetized for colossal profits on dark web forums.

There will always be new ransomware and malware variants delivered along new and creative attack vectors that exploit recently discovered vulnerabilities in applications, devices and industry niche technologies. Each time this occurs, upstarts and charlatans will attempt to capitalize off of victims by claiming to possess a silver bullet solution; there is no such all-encompassing technology. The only defense is a layered defense, of which endpoint security is an essential layer and can offer a potent ingredient for nextgen cyber fortification.

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

Sources:

Bleeping Computer:

http://www.bleepingcomputer.com/news/security/information-about-the-keranger-os-x-ransomware-and-how-to-remove-it-/

http://www.bleepingcomputer.com/news/security/the-cerber-ransomware-not-only-encrypts-your-data-but-also-speaks-to-you/

http://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/

Cisco Talos:

http://blog.talosintel.com/2016/04/jboss-backdoor.html

CSO Online:

http://www.csoonline.com/article/3040619/security/cerber-ransomware-sold-as-a-service-speaks-to-victims.html

Engadget:

http://www.engadget.com/2016/04/16/jboss-ransomware-exploit/

IB Times:

http://www.ibtimes.co.uk/cerber-terrifying-russian-ransomware-speaks-bitcoin-demand-blackmail-victims-out-loud-1547592

ICIT:

http://icitech.org/publications/

Komando:

http://www.komando.com/happening-now/354996/top-story-new-ransomware-proves-hackers-know-where-you-live-ebay-may-be-to-blame

Krebs On Security:

http://krebsonsecurity.com/2016/01/ransomware-a-threat-to-cloud-services-too/

NDTV:

http://www.ndtv.com/world-news/mac-ransomware-caught-before-large-number-of-computers-infected-1284845

Palo Alto Networks:

http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/

Reuter:

http://in.reuters.com/article/apple-ransomware-idINL1N16F17Q

Slate:

http://www.slate.com/blogs/future_tense/2016/03/07/keranger_ransomware_strikes_mac_os_x_through_transmission_update.html

Tech Crunch:

http://techcrunch.com/2016/04/16/how-to-deal-with-the-rising-threat-of-ransomware/

The Washington Post:

https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html