Ransomware: A Major Threat to National Security

Cole Lamers
lamecv19@uwgb.edu

Eric Spoerl
spoeer08@uwgb.edu

Garrit Levey
levegd06@uwgb.edu

Abstract

A staggering 550,000 ransomware attacks were recorded daily during the year of 2020 netting cybercriminals an immense amount of capital estimated to be over 1.5 trillion dollars. Ransomware is malicious software which encrypts a victim's data, preventing access to files, systems, or networks, until a specified amount of untraceable currency is paid as a ransom. Owing their success to aging infrastructure and lack of defensive funding, hacking groups have employed ransomware to entirely shut down critical infrastructure such as medical equipment, gas, and oil pipelines, as well as communication systems in the fields of healthcare, the military, and key spheres of industry around the world. This presents a large challenge for organizations when determining how best to protect themselves against these popular and devastating attacks. Fortunately, the increase in ransomware attacks has caused a resurgence in cybersecurity, specifically, ransomware mitigation strategies and software which are designed to detect and prevent ransomware attacks before they can cause damage. In this paper we will address the techniques and tools used to create and deploy ransomware, the historical effects of ransomware in large scale, global events, and the most effective techniques organizations can adopt to mitigate and prevent ransomware attacks. Through continual understanding of the nature of ransomware, we aim to educate end-users and organizations alike about the capabilities of ransomware as well as the protection strategies available in an effort to support the evolving and relentless fight against ransomware.

1 Keywords

Ransomware; Encryption; Security Awareness; Cryptocurrency; Internet of Things, Phishing; Social Engineering; Supervisor Control and Data Acquisition; Industrial Control Systems; Worm

2 Introduction

Ransomware is an extremely lucrative criminal activity netting an estimated 20 billion dollars worldwide. (House of Representatives, 2021). Attributing much of its success to easy distribution and large attack surface, ransomware continues to plague businesses big and small. According to Trend Micro research, 2016 saw a record 400 percent rise in new ransomware families being created (150 new families) indicating that this threat has not been contained and continues to gain momentum under inadequate antiviral solutions (TrendMicro, 2016). Traditional ransomware places an emphasis on locking down files and systems which prevent users from accessing them. In critical sectors such as healthcare and agriculture, this can have serious long-term effects. New variants of ransomware are designed with an additional threat, exfiltration of data which goes beyond simply locking users out of files and systems by also extracting and posting sensitive information on sites which hackers can purchase and use maliciously.

3 Notable Ransomware Events

3.1 AIDS Trojan 1989

The first documented ransomware incident occurred in 1989 and targeted the healthcare industry by infecting 20,000 attendees of the World Health Organization AIDS conference with ransomware. The AIDS ransomware was developed by Dr. Joseph Popp and was named PC Cyborg Trojan (Salvi and Kerkar, 2016). It was created as a proof of concept to expose unknown capabilities of cryptography in computing. The ransomware was loaded onto 20,000 5.25-inch floppy disks and was distributed to researches from 90 different countries. Dr. Popp claimed that there was a questionnaire on each floppy disk which tempted users to insert it into their systems (Cohen, 2021). Dr. Popp used social engineering as a means to infect thousands. Social engineering is the act of tricking someone into divulging information or performing an action Pilette:21. The ransomware itself worked by replacing the AUTOEXEC.BAT file found in Windows systems and would then count the number of times the machine had booted. After the machine had booted 90 times, the ransomware would hide directories and encrypt the names of all the files in the C drive making the system unusable. To pay the ransom, victims were required to mail a letter containing 189 dollars to a specified P.O. box in Panama. Although a very minimal ransom amount compared to today, The PC Cyborg Trojan set the stage for future ransomware variants.

3.2 WannaCry

Ransomware titled WannaCry was developed in 2017 and resulted in the infection of over 200,000 computers in 150 different countries (Trautman and Ormerod, 2018). WannaCry was distributed to victims via phishing emails containing malicious links or file attachments. Phishing emails use social engineering tactics to trick users into clicking malicious links or file attachments. This ransomware variant was especially difficult to protect against due to its ability to spread to other computers without the need for human interaction. Ransomware with this ability is categorized as a worm. WannaCry relied on the ability to exploit two popular vulnerabilities in Windows machines: EternalBlue and DoublePulsar (Akbanov et al., 2019). Both vulnerabilities, if successfully exploited, allowed remote attackers to execute arbitrary code on the machine leading to an overall system takeover. Systems were vulnerable to EternalBlue if they were running a specific configuration of Server Message Block (SMB) which was used to transfer network packets between multiple computers (Mago and Madyira, 2018). The DoublePulsar vulnerability originated as a tool developed by the National Security Agency (NSA) intended to be used as a backdoor into systems to perform updates. These vulnerabilities were primarily exploited in unsupported versions of Windows XP. The widespread ransomware incurred nearly a billion dollars in damage to victim companies. The ransomware attack took place over a small time period of less than 9 hours. It ended quickly because British security researcher, Marcus Hutchins was able to reverse engineer the ransomware and disable it by activating the kill switch. The ransomware was designed to connect and resolve a specified domain name. If the domain was resolved, the ransomware would stop the entire encryption process and become disabled. The domain used was ”www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com” which Hutchins registered to halt the WannaCry attack (Mackenzie, 2019). WannaCry's success lead to other variants of ransomware, most notably Petya, targeting the same vulnerabilities (Aidan et al., 2017). Patching of unsupported systems as well as user awareness of phishing emails could have drastically prevented these devastating ransomware attacks.

3.3 Colonial Pipeline incident 2021

As the United States continues to go through repetitive years of record-breaking amounts of ransomware attacks, it was only a matter of time until an eye-opening attack happened which affected thousands. On May 6th, 2021, the Colonial Pipeline, used for transporting critical oil across the United States was attacked by ransomware. This monumental attack allowed overseas cyber criminals to penetrate a major utility with significant impacts to the entirety of the United States eastern seaboard economy and also make off with 2.3 million dollars. The colonial pipeline was a significant event for ransomware publicity in recent times due to its impact on East Coast market forces. Gas prices rose due to fear of a gas and oil shortage as a result of the cyber attack. The entity responsible for the attack was DarkSide, an eastern European ransomware group. Their ransomware explicitly targeted non-ex-Soviet countries and also particularly non-essential facilities such as hospitals, schools, and non-profit organizations, and government agencies. This contentious attack, along with their demands of 2 million dollars in bitcoin shows the fuel that is continually adding to the fire (Vaas, 2021). Many worldwide ransomware actors have turned to the use of crypto currency when demanding ransom payments because of crypto's explosive growth in value as well as being very difficult to trace.

4 Creation,Deployment, and Payment

4.1 How Ransomware Works

Ransomware is designed to lock down critical files and systems. Ransomware uses a series of complex mathematical algorithms called ciphers to create a key, the key is then applied to a file which scrambles the data rendering it unreadable unless the same key is applied to the original data. After the encryption has been completed, the original data is locked and inaccessible. Out of all of the potential malware attacks that are employed on the internet, the usage of locker and crypto type ransomware has been proven to be the most destructive. Ransomware kits normally use strong encryption algorithms to encrypt system data to a state that is nearly impossible to crack and has a very low probability of restoring 100 percent of system data.

4.2 How Ransomware is Delivered

Ransomware, although complex in design, is relatively simple to deliver to victims. According to IBM's X-Force Threat Intelligence Index of 2021, 33 percent of cyber attacks used phishing as an initial attack vector (Singleton et al., 2021). Phishing attacks take advantage of end user error and trick users into clicking links or attachments within seemingly legitimate emails which begin malicious downloads and infect the user's system or the entire network. This reliance on human intervention with computers remains a primary attack vector for distributing ransomware (Fanning, 2015). Malicious websites can also be used to distribute ransomware. Malicious websites can contain drive-by-downloads which is malware installed on a user's computer without their knowledge when they browse to a compromised website (O'Gorman and McDonald, 2012). A typical drive-by-download starts with a user visiting a certain website which has been previously compromised by an attacker who inserted a hidden redirect in the form of an inline frame or malicious advertising links. When a user connects to the compromised site, their web browser connects to the visible website but also connects to the hidden malicious website which downloads an exploit kit. The exploit kit determines if the user's browser has any known vulnerabilities, and if it does, exploits them to download ransomware. Throughout the entire process, the user is unaware of anything being downloaded onto their system. A less popular but still common ransomware distribution method is through exploited vulnerabilities within operating systems. MacOS and Linux saw major families of ransomware in 2015 targeting GNU and *nix systems. The usage of social engineering techniques has been the standard method of payload delivery for a large share share of all ransomware attacks in the United States.

4.3 How Ransom is Paid

Once the files are encrypted, ransomware will notify the victim that their machine has been compromised by providing a pop-up message. The message includes the ransom payment requested, a deadline for payment, and instructs the victim how to pay the ransom. Ransomware primarily requests payment in the form of cryptocurrency such as Bitcoin. Crypto currency has received popularity and widespread adoption due to its limited traceability and it's explosive increase in monetary value. Although cryptocurrency transactions are not entirely anonymous. They can be linked with public keys associated with payments. However, public keys can be circumvented with various software that provides further encryption of this data which ultimately strips any legitimate means of identifying a specific user to various transactions. Coupled with utilizing Tor, it makes it almost impossible to monitor. This is leading to significant difficulties for most law enforcement agencies in that transactions cannot be tracked, digitally or physically. The hope behind paying a ransom is that the original data becomes decrypted and is restored to the user. However, paying the ransom does not guarantee the restoration of data. A study conducted by (Cartwright, 2019), found that 50 percent of ransomware payouts returned/decrypted the user data. This trend has continues as ransomware vendors find that their system has become a legitimate business model that can ensure them longer term gains. While early on with regards to US Federal Policy, the government does not encourage paying the ransom. Currently that is still the policy and is backed by the Cyber Security Infrastructure Security Agency (CISA) (CISA, 2020) Ransomware payments are extremely profitable. A 2012 report from Symantec showed that, from a single ransomware variant charging 200 dollars in ransom and infecting over 5,000 computers every day, over 30,000 dollars can be made daily if just 2.9 percent of the infected victims choose to pay the ransom (O'Gorman and McDonald, 2012). The trend is that cryptocurrencies are the predominant form of payment for ransomware becoming the adopted method of conducting transactions illicit activities (Kshetri, 2017) Within the last 10 years, ransomware payouts have varied but the most targeted platform remains to be Windows machines (Zimba and Chishimba, 2019).

5 Key Industries

5.1 Healthcare

Healthcare organizations have become highly targeted by cyber criminals who wish to disrupt critical services and steal valuable sensitive data. A 2020 report concluded that 94 percent of healthcare organizations have experienced some form of data breach (Bhuyan et al., 2020). A data breach occurs when sensitive information is accessed by unauthorized personnel. For a hospital, a data breach compromises the personal and financial information stored digitally for patients. Healthcare organizations store thousands of patient records known as protected health information (PHI). PHI includes patient names, date of birth, social security numbers, payment information, etc. This information is crucial for healthcare organizations to provide the best quality of care to patients. Due to the sensitive nature, this information is very valuable to legitimate healthcare organizations and malicious actors alike. When cyber criminals steal PHI, they will sell it on the Dark Web. Due to providing online anonymity, the Dark Web has become a hub for cybercriminals to purchase and sell victim's sensitive information. Social Security numbers are worth up to 5 dollars each, credit and debit cards are roughly 100 dollars each, and driver's license information sells for about 20 dollars. Complete patient files containing multiple sensitive fields can sell for 1000 dollars each. Considering healthcare facilities store thousands of PHI records, a cybercriminal can make a lucrative amount of money on the Dark Web after a successful ransomware attack. Healthcare organizations have a large attack surface. During the COVID-19 pandemic of 2020, Internet-of-things (IoT) devices were used to track patient temperature data for use in predictive analytics to predict where virus outbreaks would occur throughout the world. IoT devices refer to physical objects that contain sensors, processing ability, software, and operating systems that collect data and exchange it over the networks. Unlike traditional technology, IoT devices require little to no user intervention making them excellent at monitoring and collecting data constantly. IoT devices are often designed for a single purpose and are widely diverse. Other uses for IoT devices in healthcare include pacemakers, drug infusion pumps, and x-ray machines. The adoption of IoT devices has allowed the healthcare industry to better serve its patients through continuous monitoring, accurate data collection, and medical technology that leads to more positive patient outcomes. Unfortunately, the rapid adoption of IoT devices has caused difficulty in balancing usability, performance, and safety resulting in organizations sacrificing security in exchange for ease of connectivity. The healthcare industry uses many technologies to provide critical patient care. These technologies often use outdated or unsupported operating systems or applications which contain vulnerabilities which can expose the system and the organization to cyber-attacks. Outdated systems and software are referred to as legacy. Legacy systems include physical equipment and software that no longer receive support from the vendor in the form of updates and patches. Due to a lack of support, these legacy systems are left exposed to multiple vulnerabilities and are difficult to protect. Healthcare organizations often lack the resources and funding necessary to adequately defend themselves against cyberattacks. In 2018, healthcare providers spent approximately 5 percent of their IT budgets on cybersecurity (Garrity M., 2019). In comparison, banking and the financial sectors spend over 7 percent and retail and wholesale spend 6 percent. A survey conducted in 2018 revealed that 39 percent of healthcare IT staffs consisted of fewer than 10 people (N.A, 2018). Due to the importance of maintaining the confidentiality and integrity of PHI, policies and regulations have been created to protect it. The US Department of Health and Human Services (HHS) issued the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a law that requires healthcare organizations to follow and maintain strict national standards to protect sensitive patient health information. New variants of ransomware are designed with an additional threat, exfiltration of data. Exfiltration of PHI will likely result in a HIPAA breach. A breach under the HIPAA Rules is defined as, " . . . the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." (Silver-Malyska et al., 2020). A HIPAA breach is very costly to healthcare organizations as it results in hefty fines, damaged reputation, and large administrative overhead so it is crucial that organizations create policies and procedures which define how to safely access and store PHI.

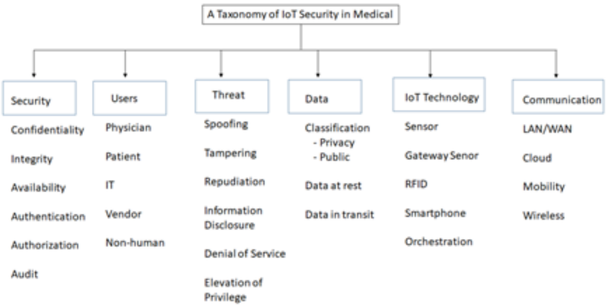

Figure 1: IoT Security Taxonomy

5.2 Military and Government

A research study was conducted to determine how effective ransomware was in the government sector of the United States. Results from the study concluded that between the years of 2016 and 2019, there were a reported 169 different attacks that targeted some type of government entity using ransomware. Of the 169, 24 of the attacks were against colleges and smaller local schools. Most, if not all of the attacks were conducted against a "soft target" or an entity that had little to no funding to combat this type of threat to the data that was being housed (Liska A., 2019). To further strengthen the defense in the 2020 fiscal year, the United States spent 17.4 billion dollars on cybersecurity-related activities. Of the 17.4 billion, 8-10 billion dollars was injected into the Depart of Defense to protect critical domestic infrastructure, 2 billion went to the Department of Homeland Security's Cybersecurity and Infrastructure Security Administration (CISA) (Reeder et al., 2021). CISA's main role is the protection of critical infrastructure to include the energy and food supply chains that were targeted. The United States already has an extensive system of legislature that has been created in the past to address emerging threats to cybersecurity vectors such as frequency, impact, and the sophistication of the attack on information systems. Although these frameworks have served well to protect the country in the past, a great deal of revision is required to address new threats as they emerge. Currently there are more than 50 statutes that address various aspects of cybersecurity, be it directly or indirectly, unfortunately these statutes follow no overarching framework. Although the most recent of these laws have seen some type of revision since their creation, there has been no major cybersecurity legislation enacted since 2002. In response to the lack of action, recent legislative proposals have focused on a multitude of issues to include national strategy and role of government, reform of the Federal Information Security Management Act, protection of critical infrastructure, information sharing and cross-sector coordination, breaches, cybercrime, electronic commerce privacy, international efforts, research, and development, and also creating a cybersecurity workforce (Fischer, 2013). Although no new law has been enacted since 2002, the Cybersecurity Act of 2012 introduced purposing regulatory frameworks and organization changes with the addition of a few recommendations from the House Republic task force to include incentives for improving private-sector cybersecurity. This bill would go on to see a handful of refinement cycles and later debated on the Senate until it failed to achieve two cloture votes. It was only until major ransomware attacks began to occur at increasing frequency that the legislative branch was forced to refocus attention back to this topic and begin to draft major bills in 2020.

5.3 Industrial

Supervisory Control and Data acquisition (SCADA) systems are the predominant networks running the majority of all US based utilities and industrial systems. 80 percent of utilities in the US utilize SCADA systems (Slay, 2008). SCADA systems predominantly run on Windows desktop operating systems. This has been proven to be a major issue when hardware, operating systems, and software are not appropriately upgraded, leading to intrusion vectors that can result in significant events such as the growing threat of ransomware attacks. SCADA systems are vital to the everyday infrastructure and operations of most major companies. Typically they are involved in factory or major companies with large scale supply chains required to operate with automated measurement processes (such as scales, temperature, pressure, voltages, input/output). These allow for verification of what is occurring in real time without requiring a person physically present to do so. Over time this grew into working over a network giving these workers the ability to check this information remotely as opposed to the physical location of the systems. This is possible by using data transfer protocols such as TCP/IP. This remote data transfer is the primary vector which ransomware vendors target within SCADA systems. Some major vulnerabilities that exist within SCADA are non-isolated networks, older hardware/software or operating systems, legacy tech and patch handling, and little to no network encryption. The affects of ransomware on SCADA systems as a whole can be temporarily catastrophic, such as when the city of Atlanta had power grids and a few servers locked down. The ransom payment demanded was 52,000 dollars; they rejected the payment and thus incurred 2.6 million dollars in recovery costs. For SCADA systems, the recommendations to prevent these issues involves isolating networks, scaling back privileges for users allowing minimal acess, latest patches, and altering credentials for imperative systems (Ibarra et al., 2019). SCADA systems are typically written using low level programming languages such as C or C++. These languages require direct access to the memory allocated within the computer. The usage of these low level programming languages correlates with the trend of using buffer overflow attacks to be the predominant attacks against SCADA systems. A buffer overflow occurs when memory is written which exceeds the bounds and spills over into other memory buffers. This error may force the program into a state which allows the attacker to inject malicious code and compromise the system. Historically, most SCADA systems utilized closed off software from outside interaction meaning the only way to access them was to physically be present at the system. This has changed dramatically as IoT usage has grown. Aspects related to pipeline operations have now been able to provide status updates to an employee remotely. As networks needed to provide this info, they establish more points of contact that a ransomware vendor can investigate. In 2019, the President of the Interstate Natural Gas Association of America made a statement that they are now worried about the "threat from sophisticated, well-resourced nation state actors." (Congressional, 2021) This was foreseen in the Colonial pipeline with the speculation by the FBI of the DarkSide group targeting them.

6 Prevention and Mitigation

To promote security best practices, healthcare facilities can reduce the risk of ransomware attacks by allocating more of their IT budget towards cybersecurity. An increased budget would allow the IT department to purchase and utilize powerful security tools such as vulnerability scanners and intrusion prevention systems which can detect and respond to ransomware attacks. An increased IT support staff allows an organization more ability to monitor networks and systems and provide training to end users. The overall recommendation now in regard to addressing the ransomware issue is solely a defensive approach, promoting a mix of a proactive measures to minimize the event of an attack, and reactive measures to be prepared in case it does occur. Currently there is no panacea of protecting against ransomware. It isn't just one set of malware, but a tree with varying branches and differentiation between them that even certain approaches to some can be completely ineffective against others.

6.1 Technical Controls

Technical safeguards include regular backups, firewall technology, blocking port access, adopting a least privilege principle, using virus and malware protection programs, encrypting stored and transferred data, and monitoring the network for intrusion attempts (Nifakos et al., 2021) These proactive measures are not simple to implement and require both time and funding. However, the costs associated with falling victim to a ransomware or other cyber-attack far exceeds the cost of implementing the proactive measures.

6.1.1 Software

One way organizations can protect PHI even if it is exfiltrated by a ransomware attack is by using encryption and data masking. Encryption provides confidentiality by rendering data unreadable to unauthorized users. Data masking hides sensitive information such as social security numbers by replacing data with symbols or random values. The two main techniques for securing legacy systems are implementing an intrusion detection system (IDS) and tunnelling insecure communication protocols over a secure channel (Tervoort et al., 2020). An intrusion detection system is a tool that monitors individual devices or an entire network searching for known threats or suspicious activity. There are two main techniques employed by IDS's. The first is knowledge-based which determines if an attack is occurring by using a list of known attack signatures. If activity matches an attack signature, the IDS creates an alert that malicious activity is occurring. However, this technique will not detect unknown attacks. A behavior-based IDS will learn how a system normally operates and then will create an alert if behavior deviates from a known baseline. This is useful for detecting undefined attacks but may introduce a greater number of false positives depending on the sensitivity of the IDS. A network-based intrusion detection systems (NBIDS) is a device connected to the network segment of an organization which monitors traffic flow of network devices, collects data, and determines if network traffic is malicious. They are useful in detecting broad attacks on the network but are insufficient in detecting isolated attacks on individual devices. Contrary to a NBIDS, a host-based intrusion detection system (HBIDS) monitors individual devices. It uses software installed on a device to monitor log and system files, suspicious processes, and user privileges to determine if an attack is occurring. A major drawback of HBIDS is that software is required to be installed on individual devices which is a challenge for large organizations. Regardless of the type of IDS used, they both utilize two different models to detect malicious activity. The most customizable model is statistical-anomaly which creates a profile of normal behavior by analyzing log files, file/folder properties, and traffic patterns. If activity deviates from the normal profile, it indicates that an attack is occurring. This model suffers from a high false positive rate due to the difficulty of defining normal behavior on a system. Another challenge is that the normal profile on the IDS must be maintained regularly to provide accurate detections. Another model used by IDS is rule or signature-based. This model analyzes the sequence of events that take place during an attack and creates a unique signature to identify different attacks. If system activity matches one of these predefined signatures, the IDS raises an alert that an attack is occurring. This model is very easy to implement and maintain and has a low false positive rate. However, it is unable to detect unknown attacks such as zero-days. In (Yadav et al., 2017), the authors propose the use of honeypots to overcome the shortcomings of traditional IDS solutions. A honeypot is a program, machine, or system put on a network as bait for attackers. The authors propose placing a honeypot both in the demilitarized zone (DMZ) between the internet and an organization's local area network (LAN), as well as within the LAN itself. The author's reasoning for this architecture is the honeypot in the DMZ can detect attacks originating from the external internet and the honeypot within the LAN of the organization can detect malicious activity from within the organization's network. The author points out that most attacks in healthcare are performed by insiders (Yadav et al., 2017). The authors propose the use of a Dionaea and Kippo SSH honeypot system. Dionaea's main purpose is to download a copy of the malware requested by the attacker. Once downloaded, it sends the copy to multiple sandbox environments which analyze the submitted malware and can determine what kind of malware it is. Dionaea requires minimal user interaction, so it is a great tool for security personnel to determine which malware they are being targeted with. With this data, they can create security policies to combat these attacks. The second part of the proposed honeypot solution is Kippo. Kippo allows an attacker to remotely log into a system and execute commands in a remote shell. Kippo appears as a legitimate system to the attacker and creates a log of all interactions between the attacker and the shell (Yadav et al., 2017). Kippo can track all activity of the attacker including what commands they execute, what usernames and passwords they attempt to gain access, and what files they attempt to access. Security personnel can read Kippo logs to determine what data the attacker was trying to access as well as what techniques were used. They can then use this information to improve the security posture of the entire organization. The recommendation to circumvent the issues plaguing SCADA systems is for SCADA software to be converted over to the Rust programming language as it is a memory safe (meaning, no ability to perform buffer overflow) language that provides access low level access to memory such as C/C++. Another ransomware prevention tool is the use of a browser plugin that can detect and prevent ransomware attacks. For example, if a user clicked a phishing link or attachment, the plugin would analyze the website or the downloaded file, create a hash value, and then compare the calculated hash value with a database of ransomware hashes. If the hashes match, the plugin would report to the user that the file is malicious and can prevent the execution of the file which prevent the system from getting infected. In (Han et al., 2017), the authors point out shortcomings of their design in that the plugin would not be able to detect unknown or new ransomware variants due to the reliance of a known database of hash signatures. Along with being able to detect malicious downloads, the plugin will also report to the user when a site their visiting online is not using Secure Sockets Layer (SSL) encryption meaning that all data sent to and received from the website can be viewed by unauthorized parties and sensitive information such as credit card numbers, banking information, and social security numbers could be stolen. The hope for the authors is that using the plugin will not only prevent infection from ransomware but also increase user awareness of cybersecurity and form healthy security habits from non-technical users. The first line of defense is using software within firewalls, antivirus, VPN, and operating systems. Firewalls restrict access to the internal network, antivirus can detect infections within systems, VPN should be used for encrypted communication of remote users, and operating systems should be kept up-to-date with the latest patches to mitigate the chance of vulnerabilities. The need for artificial intelligence that can quickly evaluate human behavior will break the cycle of defensive strategies being one step behind the criminals. With the aid of artificial intelligence, the human factor of information security will drastically be reduced and will allow for more resources to be used for network upgrades (Mamedova et al., 2019) MWR has created a state-of-the-art ransomware agent called RansomFlare that uses dynamic (behavioral) analyses and machine learning to quickly understand ransomware. Dynamic-based analysis detection is a system of live monitoring to determine if any processes on a network are behaving in malicious intent and initiates a termination function after the process has been flagged (Nieuwenhuizen, 2017). After RansomFlare has gone through a complete iteration of termination, the software then initiates machine learning to understand the origin, behavior, and mapping of the process. RansomFlare has seen great results and offers and potential solution to the ransomware question.

6.1.2 Patching

Patching remains one of the main sources to prevent ransomware since it fixes existing vulnerabilities within a system or product (Richardson et al., 2017). The spread of malware can be countered through patching. The underlying vulnerabilities exploited by malware can be fixed by installing security patches that immunize the susceptible and potentially remove the malware from infected machines (Eshghi et al., 2014).The desire for constant connectivity of multiple devices as well as the ability to easily manage and control them remotely has resulted in the creation and adoption of Internet-of-Things (IoT) devices. IoT devices refer to physical objects that contain sensors, processing ability, software, and operating systems that collect data and exchange it over the networks. Examples of IoT devices include smart refrigerators, thermostats, security cameras, etc. Unlike traditional technology, IoT devices require little to no user intervention making them excellent at monitoring and collecting data constantly. IoT devices are not only used personally but also commercially as businesses utilize their capabilities to further their mission. IoT devices are often designed for a single purpose and are widely diverse. Due to resource constraints and difficulties in managing thousands of unique devices, traditional security mechanisms are inadequate and often contain vulnerabilities.A study done by Hewlett Packard (HP) in 2014 reported that 70 percent of IoT devices are exposed to attacks (HP, 2014). These vulnerabilities typically exist in the form of backdoors, hardcoded passwords, or unsecure firmware. In 2018, one survey noted that 28 percent of respondents stated that their organization does not scan for cyber vulnerabilities (Black, 2018).

6.1.3 Backups

For backups to be effective, organizations should follow the 3-2-1 rule. Maintain three copies of data, use two different media formats to store the data, and store one of the copies off-site (Spence et al., 2018). If an organization falls victim to a ransomware attack, they may be able to avoid paying the ransom if they have up-to-date and offline backups in place. According to an interview with a cloud backup service company, one of their healthcare customers lost access to 14 years' worth of files in an attack, but, because the victim had backup services, they did not have to pay the ransom and were able to regain access to files to continue operations (Zetter K., 2016). Backing up is the process of making copies of data which can be used to restore to a point in the past (Laudon, 2016). A backup process mainly involves two metrics, recovery point objective (RPO) and recovery time objective (RTO) (Mugoh, 2011). RPO is the point in time where the system will be restored to. RTO is the time it takes to complete a restore. Backups can be incremental, differential, or full. Full backups copy the entire data set which allows for fast recovery but is very time consuming. Incremental backups back up data that changed since the previous backup which allow for fast back up creation. However, each incremental backup depends on the previous one meaning any damage or loss on one of the sets could prevent complete data recovery. Differential backups back up data that has changed since the last full backup. Differential backups restore quickly but take longer to create backups. The backup solutions discussed fall into three categories: traditional backup, replication, continuous data protection (CDP). Traditional backup is the preferred backup solution as it involves copying files on a system and then storing them on an isolated storage medium periodically which is usually daily, weekly, and monthly (Evans, 2014). If the original system is infected, the system can be restored to a healthy state using the backup copy. Unlike a traditional backup, replication involves taking a snapshot of a system keeping a copy of the most recent data and storing it in a geographical area separated from the source system. Replication is not sufficient for ransomware recovery because the ransomware encrypts data on the source and will encrypt data on the replicated system almost immediately. CDP is like replication, but it can copy a much larger amount of data. The main drawback of CDP is that it requires a very large amount of storage making it a very expensive solution. Also, like replication, it cannot be used as a backup since changes on the source system quickly get replicated onto the target which means the CDP system will contain ransomware-encrypted data. Another important consideration businesses should make when designing backup strategies is where backups are stored geographically. If a server hosting normal user file storage gets infected by ransomware and has access to critical backup infrastructure, the backup infrastructure will be encrypted and become unusable for recovery. Therefore, it is crucial that backup solutions are "air-gapped" from the data source so that it will not be reachable by infected network systems. An air gap provides physical and electronic separation of computing systems making them unable to communicate with each other. Of the three proposed backup methodologies, traditional backup is the most effective in combating ransomware. If a system is infected with ransomware and the company doesn't wish to pay the ransom, they can easily search the backup system for a time when it was free of ransomware and restore to that point in time. The authors suggest a backup solution that uses traditional backup methodologies based on full backups with incremental backups completed between the full backup (Thomas, 2018). In addition to air-gapping the backup media, user access to the backup media should be very strict and follow the practice of least privilege allowing only administrative users to read and write to the backup system. Unfortunately, encryption ransomware has evolved to not only encrypt data on the original system, but also extends the encryption to any backups connected to the victim system or network. Some more advanced encryption ransomware will obtain kernel privileges gaining complete control of the victim's operating system and allowing the ransomware to delete and destroy both local and network backups. This makes backups insufficient in protecting businesses from the devastating effects of encryption ransomware. The article proposes the use of a ransomware-tolerant Solid-State Drive (SSD) called "FlashGuard" which allows quick and effective recovery from encryption ransomware without relying on backups (Huang et al., 2017). Hard-Disk Drives (HDD's) physically overwrite data on disks after a logical overwrite occurs which is time-intensive. Unlike HDD's, SSD's utilize out-of-place writes which will write to a free block of storage prior to erasing the original value causing increased performance in SSD's compared to HDD's. FlashGuard leverages these out-of-place writes to maintain a copy of a page that is deleted or modified which allows it to retain copies of data encrypted by ransomware (Huang et al., 2017). FlashGuard was tested using 1,447 ransomware samples encompassing 13 different families of ransomware. In these tests, the authors downloaded 1,447 ransomware samples, and executed them on virtual machines with protection services such as firewall, Microsoft security protection, and user account control disabled (Huang et al., 2017). They also gave the ransomware samples administrative privileges and enabled them to access the Internet to facilitate communications to command-and-control servers used in encryption. The authors observed that the encryption time ranged from 20 minutes to an hour and that most attempted to destroy backups. In testing the effectiveness of FlashGuard, it was noted that restoring the encrypted system was successful and the execution time for restoring ranged from 4.2 to 49.6 seconds. For comparison, the native approach takes 707.7 seconds. Using firmware-level data recovery, businesses can combat the advanced techniques modern encryption ransomware uses to prevent access to crucial data. The second line of defense is backups. Organizations should create backup solutions using both software and hardware and should regularly test the functionality of backups to ensure data is safe, accessible, and redundant. In the event of a ransomware attack that doesn't encrypt backups, devices can be restored to a state before they were infected with ransomware allowing access to critical files and systems.

6.2 Organizational Controls

6.2.1 User Awareness Training

In (Kessler et al., 2020), the authors stated that the majority of data breaches result from employee negligence and/or carelessness surrounding information security, something that cannot be fully mended through legislative or technological remediation. Training the workforce is an effective strategy to prevent ransomware attacks. Organizations can increase organizational awareness by training their users on the indicators of a ransomware attack. Indicators may include clicking a link or opening an attachment within a suspicious email, an extreme increase in usage of the user's central processing unit (CPU), and an inability to access certain files. With proper training, a user can detect and respond to a ransomware attack effectively reducing the potential damage from spreading to an entire network to being contained to a single device. Users should be trained on how to identify phishing emails and instructed not to click on links or attachments within suspicious emails. With sufficient training, end users go from being a weak link in the organization's security, to being an asset in detecting and reporting attacks to technical personnel. In terms of workflow and communication, security personnel should conduct simulated phishing attacks to increase user awareness and test technical personnel's detecting and recovery strategies. Implement internal policies which restrict users' ability to install applications or access personal email accounts. Risk and business impact assessments should also be conducted to identify critical data and applications. Finally, security personnel should monitor network activity to proactively prevent ransomware attacks by identifying indicators of compromise (IOC) before an infection occurs. Typically spread through phishing emails, ransomware can be sent to hundreds of thousands of users within different organizations disguising itself as legitimate email attachments or links within email. Since most if not all users within an organization have access to email, all users of an organization can fall victim to a ransomware attack if they don't have the awareness required to detect and prevent attacks in the first place. Cyber security awareness has a great dependence on human-factor psychology, which is the study of the interaction of people with machines and technology (Elradi, 2021) Humans are the weakest link in the chain of cyber security which means a simple mistake can cause significant damage if they fall victim to a ransomware attack (Young et al., 2018) Educating end users, will likely result in a decrease in the number of cyber security incidents and a large increase in the organization's aptitude to detect and respond to security incidents (Hull, 2019) The end user rescue checklist is a step-by-step guide for users on what to do in the event of a ransomware infection. The four main components of the checklist are: disconnect systems, verify encryption, determine the type of ransomware, and determine the appropriate response. Putting the checklist into practice, the first thing a user should do when they believe their system is infected is to disconnect the device from the network as well as turn off Wi-Fi Bluetooth and Hotspot functionality. In doing so, ransomware on the system will be unable to communicate over the network preventing it from receiving instructions from the command-and-control server. Next, the user should try to access shared folders, network storage devices, attached storage media, and cloud-based storage to determine if any of the data was encrypted successfully by the ransomware. If the encryption was successful, the strain of ransomware should be determined to mitigate the effect of the attack. Currently, the most viable element of informational security to be exploited by potential attackers, is the human element. Not only is this factor the soft spot for most networks, but it is also the most unreliable and uncontrollable in information security. The root of this problem stems from the fact that this type of weakness is mainly caused by a lack of user awareness to the importance of information security or that they don't have a clear understanding of the risk of a potential attack. To combat this issue, corporations, governments, and other large entities have begun to draft and adopt information security awareness programs to better educate their workers on the field of information security. In the hopes of better educating their subordinates in the field, corporations are aiming to reduce the risk to their networks by showing the warning signs and best practices to operate on. The creation of these awareness programs is undoubtedly the correct step in the right direction, but time will only tell if the initiatives bear any fruits. The authors of this article argue that the creation of the plans must be supplemented with continual campaigns to continue to keep the human element in check (Veseli, 2011). The effectiveness of the security awareness programs must be taken seriously and adapted depending on the findings of the campaign. When dealing with thousands of employees, there is no one size fits all approach is it is the responsibility of the chief information officer to create a blended approach that covers all the bases. One of the most difficult challenges that information security specialists have to combat is the usage of phishing in the form of social engineering and the potential for these to cripple their networks with ransomware. Due to the complexity of spear phishing, social engineering phishing attacks, it can be difficult for even trained or tech savvy employees to detect the scheme at hand. It is estimated that 80 percent of all organizations have experienced a phishing attack since transitioning into the digital era (Thomas, 2018). This stat is monolithic in nature and highlights a major problem that businesses, government, and technology sectors deal with. Because the lion shares of all phishing attacks target the user, a high amount of emphasis has been placed to empower the user to have a strong understanding in internet best practices. This article supports the claim to educate the users by highlighting several staggering stats that give perspective to the scope of this problem. The authors argue that the two main focuses for criminals to attacker users is the usage of spear phishing to steal personal identities and capital through ransomware attacks. By providing education on the origin, objective, and ways that ransomware is deployed, a better state of readiness can be achieved (Uandykova et al., 2020) Similar to how major corporations require information technology related "safety classes" it may be necessary for a variety of different learning objects be pushed onto the public in order to promote a more robust understanding of the industry. A cognitive study concluded there are three short term factors the affects the human ability to make right decisions. These three factors are workload, stress, and vigilance (Priestman et al., 2019).

6.2.2 Policies

The Least Privilege Principle is still the most recommended security stance in terms of prevention in a network as it helps defend against unpatched systems and currently unknown vulnerabilities (Ren et al., 2020). (Add info about policies - least access, admin rights, USB access, group policies, etc.) (Frenz, 2017)

6.3 Laws and Regulations

The Chairman of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, Representative Yvette D. Clarke purposed the State and Local Cybersecurity Improvement Act. This act would facilitate the release of 500 million dollars' worth of grants to State, local, territorial, and tribal governments to strengthen their cybersecurity. The overall scope of this act is to encourage all sectors of government to heavily increase their funding for cyber security in their budgets. In addition, this act will also require the Cybersecurity and Infrastructure Agency (CISA) to develop a strategy to improve the cybersecurity of state, local, tribal, and territorial governments, identify and prepare Federal resources that can be quickly made available to these elements, and to also set a baseline objective for state and local cybersecurity efforts (DHS, 2021). Furthermore, this act will require all echelons of government to develop comprehensive cybersecurity plans to guide the use of grant dollars and establish state and local cybersecurity resiliency committee. The creation of this act marks the first major pushback from the federal government against cybersecurity related crimes and it is the first of many steps in the process of defending state and local networks from cyber criminals. Between 2015 to 2019, there were 947 proposed bills on cybersecurity from all 50 states in the hopes of avoiding future attacks (CISA, 2019). Of the 947 bills that were proposed, only 233 were actually passed, a 24 percent success mark. The remaining 714 bills were either paused indefinitely, vetoed by the state governor, or failed to pass through legislation and were nixed(Skertic J., 2021). Interestingly enough, of the 947 proposed bills, 107 originated from the state of New York but only four were enacted, further highlighting the neglect towards cybersecurity related funding. The framework in (Snoke, 2020) outlines a 5-step program that entities operating in the Department of Defense can use to create policy and security plans going forward. The first step is for the entity to identify possible vectors in the network that ransomware can be inject to. To do this, the program recommends performing asset management for physical devices, clients, servers, data, software platforms, and applications. Doing so will ensure that the documentation on hand reflects the current inventory status and includes information about business use and stockholders. Additionally, step one outlines the need for documentation on possible infection vectors, malware propagation mechanisms and access methods for the assets that are public exposed. These assets will then have to be assigned a priority and outline in the continuity plan of the department in case of an attack. The second step of the plan is to protect the assets on the network. This can be done by performing regular backups, validations checks and further encryption of the data on hand. Mitigation of social engineering attacks, especially when attempting to prevent ransomware attacks, remains a large priority and a focus for education initiatives. The agency can also place responsibility on the users of the network to practice proper software hygiene by maintaining user awareness and avoid potentially hazardous websites on the web. The following step in the plan is to create an environment that encourages users to report social engineering events, reconnaissance activity, and ransomware-indicative network activity. Additionally, deploying robust anti malware applications and host-based intrusion prevent software can further supplement the defense of the network. The fourth step of the program outlines the need for a response plan to be drafted in the event of an attack. This continuity plan must accurately guide incident response to protect data integrity and support business continuity. Creating communication channels in which stakeholders can safely express updates and move forward on their piece of the response is also a huge focus of this step. Ideally, the creation of the continuity plan will establish standards that the organization can adopt moving forward. The last step of the program is the recovery plan in case the continuity plan does not accurately address the threat. During this step the backup plans that already have been put into place will be enacted and data backups restored. Lost software will also be restored, and the event logs of the attack will be reported back to the appropriate levels of law enforcement. The trend with cryptocurrencies being constantly used among most hacking groups has not been unnoticed by the US government. Congress has recently passed in the infrastructure bill of 2021 to require reporting requirements for cryptocurrency transactions (Rubin et al., 2021). This is another tool that primarily focuses on domestic utilization of cryptocurrency, however as one of the world powers now attempting to monitor its use, this could likely fall into the trend of other governments following suit as well. A ransomware group cannot properly extort victims if there is a worldwide recognition that all transactions can be traced to a specific individual or entity like how bank transactions work. This is a part of the process to move toward resolving these problems in the world today related to our modern digital world.

7 Conclusion

References

J. S. Aidan, H. K. Verma and L. K. Awasthi 2017 *Comprehensive Survey on Petya Ransomware Attack* International Conference on Next Generation Computing and Information Systems (ICNGCIS), 2017, pp. 122-125

Akbanov, M., Vassilakis, V. G., and Logothetis, M. D. 2019 *WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms.* Journal of Telecommunications and Information Technology.

Bhuyan, S.S.; Kabir, U.Y.; Escareno, J.M.; Ector, K.; Palakodeti, S.; Wyant, D.; Kumar, S.; Levy, M.; Kedia, S.; Dasgupta, D.; et al. 2020 *Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations*. J. Med Syst.

Black, Ryan. 2018 *Vulnerabilities are Surging, and Healthcare Cybersecurity Might Struggle to Keep Up.* Inside Digital Health

Cartwright A and Cartwright E 2019 *Ransomware and Reputation* Games

CISA 2020 *Ransomware Guide* CyberSecurity Infrastructure Security Agency

CISA 2019 *Security Tip (ST04-015): Understanding Denial-of-Service Attacks* Cybersecurity and Infrastructure Security Agency

Cohen, G. 2021 Industrial Cybersecurity Pulse

Department of Homeland Security 2021 *Responding to ransomware: exploring policy solutions to a cybersecurity crisis. serial no. 17-12, 53* Department of Homeland Security

Elradi, M., Mohamed, M., and Ali, M. 2021 *Ransomware Attack: Rescue-checklist Cyber Security Awareness Program* Artificial Intelligence Advances

Eshghi, S., Khouzani, M. H. R., Sarkar, S., Venkatesh, S. S. 2014 *Optimal patching in clustered malware epidemics.* IEEE/ACM Transactions on Networking, 24(1), 283-298.

Evans, C. 2014 *Backup vs replication, snapshots, CDP and data protection strategy* ComputerWeekly

Fanning, K. 2015 *Minimizing the Cost of Malware.* Journal of Corporate Accounting and Finance (Wiley), 26(3), 7–14.

Fischer, E. A. 2013 *Federal laws relating to cybersecurity: overview and discussion of proposed revisions* Library of Congress Washington DC congressional research service.

Frenz, Christopher M., and Christian Diaz. 2017 *Antiransomware guide.* OWASP

Garrity M. 2019 *5 percent of hospital IT budgets go to cybersecurity despite 82 percent of hospitals reporting breaches* Becker's Health IT

Jordan W. Han, Ong J. Hoe, Joseph S. Wing, and Sarfraz N. Brohi. 2017 *A Conceptual Security Approach with Awareness Strategy and Implementation Policy to Eliminate Ransomware.* In Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence (CSAI). Association for Computing Machinery, New York, NY, USA, 222–226

House of Representatives, Congress. 2021 *Cyber threats in the pipeline: using lessons from the colonial ransomware attack to defend critical infrastructure.* U.S Government Publishing Office

Jian Huang, Jun Xu, Xinyu Xing, Peng Liu, and Moinuddin K. Qureshi. 2017 *FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)* Association for Computing Machinery

Hull G, John H, Arief B. 2019 *Ransomware deployment methods and analysis: views from a predictive model and human responses* Crime Science

Ibarra J, Butt U, Do A, Jahankhani H, Jamal A 2019 *Ransomware Impact to SCADA Systems and its Scope to Critical Infrastructure* International Conference on Global Security, Safety and Sustainability pp. 1-12

Kessler, S.R.; Pindek, S.; Kleinman, G.; Andel, S.A.; Spector, P.E.; Kessler, S.R.; Pindek, S.; Kleinman, G.; Andel, S.A.; Spector, P.E. 2020 *Information security climate and the assessment of information security risk among healthcare employees.* Health Inform. J.26, 461–473

Kshetri, N., Voas, J. 2017 *Do crypto-currencies fuel ransomware?* IT Professional Magazine, 19(5), 11-15

Laudon, K. Laudon, J. 2016 *Management Information Systems* Pearson

Liska A. 2019 *Early findings: Review of state and local government ransomware* Recorded Future

Mackenzie, Peter 2019 *WannaCry Aftershock.* Sophos

Mago, M., Madyira, F. F. 2018 *Ransomware software: Case of wannacry.* International Research Journal of Advanced Engineering and Science, 3(1), 258-261.

Mamedova, N., Urintsov, A., Staroverova, O., Ivanov, E., Galahov, D. 2019 *Social engineering in the context of ensuring information security.* SHS Web of Conferences (Vol. 69, p. 00073) EDP Sciences.

Mugoh, L., Ateya, I. L., Shibwabo, B. K. 2011 *Continuous data protection architecture as a strategy for reduced data recovery time* Journal of Systems Integration, 2(4), 54-69.

N.A. 2018 *Hospitals are vulnerable to security risks, putting patient data, care in danger.* Healthcare Business Technology

N.A. 2014 *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack* Hewlett Packard Inc.

Nieuwenhuizen, D. 2017 *A behavioural-based approach to ransomware detection.* MWR Labs Whitepaper

Nifakos, Sokratis, et al. 2021 *Influence of human factors on cyber security within healthcare organisations: a systematic review.* Sensors 21.15: 5119.

O'Gorman, G., McDonald, G. 2012 *Ransomware: A growing menace* Symantec Corporation Arizona, AZ, USA

Pilette, C. 2021 *What is social engineering? A definition + techniques to watch for" NortonLifeLock*

Priestman, W.; Anstis, T.; Sebire, I.G.; Sridharan, S.; Sebire, N.J. 2019 Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ Health Care Inf. 2019, 26, e100031*

Reeder, J. R., Hall, C. T. 2021 Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack

Ren, A. L. Y., Liang, C. T., Hyug, I. J., Broh, S. N., Jhanjhi, N. Z. 2020 A Three-Level Ransomware Detection and Prevention Mechanism. *EAI Endorsed Transactions on Energy Web, 7(27).*

Richardson, Ronny and North, Max M. 2017 Ransomware: Evolution, Mitigation and Prevention *Faculty Publications. 4276.*

Rubin, G. T., and Collins, E. 2021 em What's in the bipartisan infrastructure bill? From amtrak to roads to water systems; roughly 1 trillion dollar proposal is key part of president Biden's agenda. Wall Street Journal

Salvi, M. H. U., and Kerkar, M. R. V. 2016 Ransomware: A cyber extortion. *Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146, 2.*

Silver-Malyska, Tara, and Jason N. Sheffield. 2020 The First Word: The HIPAA Response to Malware Events, Including Ransomware Attacks. *Benefits Quarterly, vol. 36, no. 3, 2020, pp. 44.*

Singleton C, Wikoff A, Eitan A, DeBeck C, Hammond C, Lee C, Sperry C, Kiefer C, Zaboeva C, McMillen D, et al. 2021 X-Force Threat Intelligence Index 2021 *IBM*

Skertic, J. 2021 Cybersecurity Legislation and Ransomware Attacks in the United States *Old Dominion University Digital Commons*

J. Slay and M. Miller 2008 Lessons learned from the Maroochy water breach *Critical Infrastructure Protection*

Snoke, T. D., Shimeall, T. J. 2020 An Updated Framework of Defenses Against Ransomware *Carnegie-Mellon University of Pittsburgh*

Spence N, Niharika B, Paul D, Coustasse A. 2018 Ransomware in Healthcare Facilities:A Harbinger of the Future?

Tervoort T, De Oliveira M.T, Pieters W, Van Gelder P, Olabarriaga S.D, Marquering H 2020 Solutions for Mitigating Cybersecurity Risks Caused by Legacy Software in Medical Devices: A Scoping Review *IEEE*

Thomas, Jason and Galligher, Gordon 2018 Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware *Computer and Information Science, Vol 11, No 1*

Thomas, J. 2018 Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management, 12(3) 1-23*

Trautman, L. J., and Ormerod, P. C. 2018 Wannacry, ransomware, and the emerging threat to corporations. *Tenn. L. Rev., 86, 503.*

TrendMicro 2016 The plateau of ransomware, more business process compromise, and the boom of cyberpropaganda—what big security concerns should we expect in 2017? *TrendMicro*

Uandykova, M., Lisin, A., Stepanova, D., Baitenova, L., Mutaliyeva, L., Yüksel, S., Dinçer, H. 2020 The social and legislative principles of counteracting ransomware crime. *Entrepreneurship and Sustainability Issues, 8(2), 777-798.*

Vaas, L. 2021 Colonial Pipeline's ransomware attack sparks emergency declaration *Woburn: Newstex*

Veseli, I. 2011 Measuring the effectiveness of information security awareness program

Yadav, Aastha, Sarthak Raisurana, and P. Lalitha. 2017 Information security in healthcare organizations using low-interaction honeypot intrusion detection system *International Journal of Security and Its Applications 11.9*

Young, H., van Vliet, T., van de Ven, J., Jol, S., Broekman, C 2018 Understanding human factors in cyber security as a dynamic system *Conference on Applied Human Factors and Ergonomics, pp. 244-254 Springer*

Zetter K. 2016 4 Ways to Protect Against the Very Real Threat of Ransomware. *Wired*

Zimba, A., Chishimba, M. 2019 Understanding the evolution of ransomware: Paradigm shifts in attack structures. *International Journal of Computer Network and Information Security, 11(1), 26.*

2021 Pipeline cybersecurity - federal programs *Congressional Research Service Report Targeted News Service*