Computer and Information Science; Vol. 12, No. 3; 2019
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Enterprise Cybersecurity: Investigating and Detecting Ransomware Infections Using Digital Forensic Techniques

Jason E. Thomas[1,2,3,4], Ryan P. Galligher[5], Macalah L. Thomas[6] & Gordon C. Galligher[7]

[1] Bush School of Government and Public Service, Texas A&M University, College Station, Texas

[2] School of Business & Technology, Excelsior College, Albany, New York

[3] Colangelo College of Business, Grand Canyon University, Phoenix, Arizona

[4] President, The Collective Group, Austin, Texas

[5] Erik Johnson School of Engineering & Computer Science, University of Texas at Dallas

[6] College of Engineering, Texas A&M University, College Station, Texas

[7] Vice President of Managed Services, The Collective Group, Austin, Texas

Correspondence: Jason E. Thomas, The Collective Group, 9433 Bee Caves Rd. Bldg III, Ste. 200, Austin, TX 78733.

Received: May 15, 2019 Accepted: May 30, 2019 Online Published: July 25, 2019

doi:10.5539/cis.v12n3p72 URL: https://doi.org/10.5539/cis.v12n3p72

Abstract

As the world continues to grow and embrace technology ransomware is growing problem. When ransomware encrypts storage sytems, systems shutdown, productivity grinds to a halt, and serious long-term damage takes place. As this is a known problem many firms have developed functionality to address ransomware issues in key security technologies such as intrusion protection systems. Many firms, especially smaller ones, may not have access to these technologies or perhaps the integration of these technologies might not yet be possible due ot varying circumstances. Regardless, ransomware must still be addressed as cyber miscreants actually target weak and unprotected environment. Even without tools that automate and aggregrate security capability, systems administrators can use systems utilities, applications, and digital forensic techniques to detect ransomware and defend their environemnts. This paper explores the literature regarding ransomware attacks, discusses current issues on how ransomware might be addressed, and presents recommendations to detect and investigate ransomware infection.

Keywords: cybersecurity, ransomware, digital forencisce, computer security, cyberattacks, data protection, data loss prevention, information systems, systems administration

1. Introduction

1.1 The Ransomware Challenge

Detecting ransomware is a challenge that virtually all organizations worldwide (Brewer, 2017; Thomas J. E., 2018; Thomas & Galligher, 2018; Wilday, 2018). Once miscreants have access to storage devices, they encrypt system data and make systems toally inaccessible (Brewer, 2017; Symantec, 2016). The consequences of this act are tremendous. Businesses cease to operate, consumers lose access to services, and reputations are tarnished.

While not being able to access an organization's data can be a huge problem in and of itself, many other issues arise when storage systems become encrypted (Thomas J. E., 2017). For example, if the primary disk partition of a system becomes inaccessible, the machine becomes unable to boot. Both user and system applications often depend on data availability to operate effectively, and without access to critical or required data, programs may cease to function or may act randomly. And nonfunctionality obviously inhibits the ability to use the system or application for its intended purpose, as well as potentially posing severe consequences for workflow or actions dependent on the system or application.

In addition to functionally losing access to data for processing, there may be far-reaching implications on the organization depending on the underlying characteristics of the data that is effected. Electronic data are used for all manner of essential tasks. Hospitals store personal health information, which is subject to regulatory

restrictions on use and availability and its overall safety (CDC, 2003). Violations of these regulations could cost organizations as much as $50,000 per incident. Likewise, personal financial information is also tightly regulated (FTC, 2013). Losing such information could subject individuals or organizations to significant fines.

1.2 The Problem to be Adressed

The problem to be addressed is ransomware. Ransomware is currently the dominant type of extortion-based malware (Symantec, 2016; Thomas J. E., 2017; Thomas & Gallagher, 2018). Cybersecurity Ventures predicts that 2019 ransomware damages will be as much as $11.5 billion (Morgan, 2017). A ransomware attack targeting England's National Health Service affected 60 health trusts, 150 countries, and more than 200,000 computer systems (Collier, 2017). The WannaCryRansomware attack shocked the world when it demanded payment in Bitcoin and escalated ransom payment request for noncompliance (Langde, 2017). WannaCry is just one example of ransomware attack. Ransomware continues to evolve, and attacks are becoming more frequent and commonplace, including others such as CryptoLock, Locky, and Petya (Manes, 2017). *1.3 Describe*

2. Methodology

The methodology used in this study was a systematic literature review. Literature reviews are often used in social science and business research to explore process, behavioral-based issues, and business problems (Bandi, Fellah, & Bondalapati, 2019; Jensen, Dinger, Wright & Thatcher, 2017; Kwok, 2015; Nicho, Fakhry & Egbue, 2018; Thomas J. E., 2017; Thomas & Hornsey, 2014). Systematic literature reviews entail defining the scope of the literature review by developing questions to guide research and data review to foster efficiency and focus the literature review (Xiao & Watson, 2017). The questions used to guide this study were as follows:

1. What is ransomware?
2. How does the ransomware process work?
3. How can digital forensic techniques be used to detect ransomware infection?

The authors used keyword searches for relevant articles and data from the peer-reviewed body of literature and the Internet. Research sources included online university libraries, databases such as GoogleScholar and ProQuest, and Internet searches. After appropriate data were gathered, the author analyzed the data and summarized the findings.

3. Literature Review

3.1 Ransomware

Ransomware is a form of malware that takes control of system data and makes them unavailable to users, systems, and applications (Brewer, 2017; Fruhlinger, 2017; Thomas J. E., 2018). Ransomware is considered extortion-based malware because once the software makes data unavailable, typically by encrypting data, a notification is sent to demand payment to release the data (Brewer, 2017; Symantec, 2016; Thomas J. E., 2017). According to Symantec (2016), ransomware is the most dominant newly-created extortion-based malware attack, with more significant presence than other extortion-based malware attacks such as misleading applications, fake antivirus, and lockers (Figure 1).

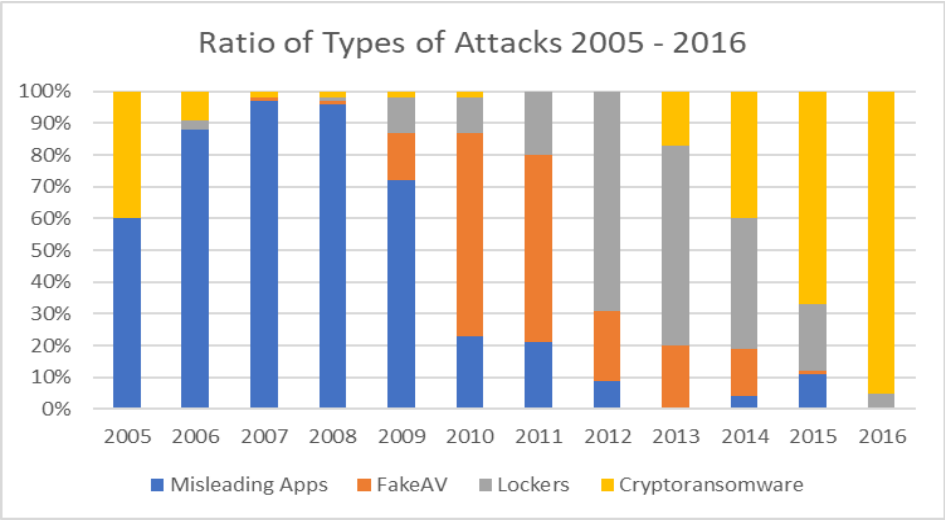

Figure 1. Ratio of extortion-based newly-created malware attacks, adapted from Symantec (2016)

As seen in the Figure, Ransomware is a growing problem. While Ransomware used to be a small component of newly-created malware each year, since 2013 it has grown significantly and, by 2016, has come to significantly dominate the entire sphere of malware that gets created and released each year. A ransomware attack occurs every 40 seconds in the United States (Morgan, 2017). The frequency of ransomware attacks is predicted to increase to every 14 seconds in 2019. Ransomware is growing in prevalence because it targets data that are valuable as both application input and output, making users more motivated to pay for their return. More simply put, ransomware is growing because it is profitable (Thomas, Galligher & Huff, 2018).

Ransomware is so lucrative, in fact, that miscreants now offer ransomware as a service (RaaS) deployed by a portal (Petrasko, 2017). Ransomware affiliates access the portal and deploy the ransomware from a dashboard offering full customization of the ransomware, with options for ransom request and time interval for ransom increase. Often these services are free to deploy and operate using a profit-sharing model, with affiliates making 60 to 80% of the ransom. There are several platforms currently in use, such as Cerber, Satan, Hostman, Flux, and Atom. The number of RaaS platforms on the Dark Web is continuing to grow and is likely powering the increasing number of ransomware attacks. Figure 2 depicts the predicted growth of damages from ransomware attacks. These damages include not simply any ransom that might be paid, but the much more significant amount of effort required by IT organizations to disinfect the environment and, if possible, restore or re-create the information that was lost.

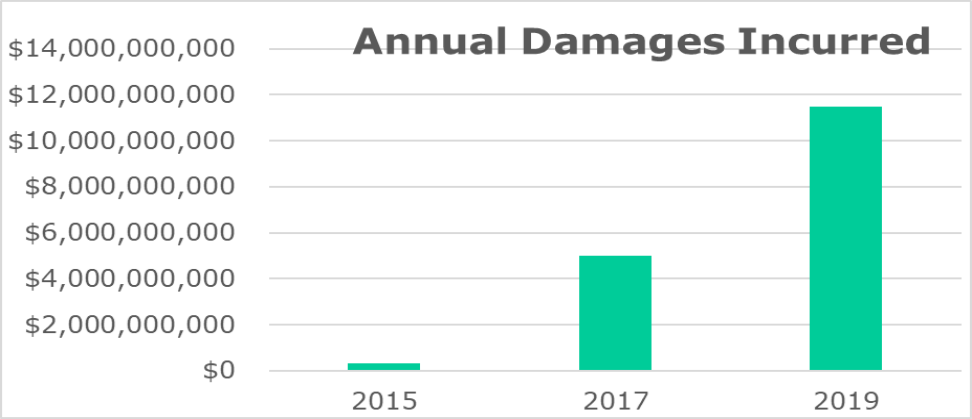

Figure 2. Predicted growth of ransomware attack damages (Morgan, 2017)

3.2 The Ramsomware Process

The ransomware process comprises five phases: (a) infection, (b) delivery, (c) backup attack, (d) encryption, and (e) user notification (Thomas & Galligher, 2018).

During the infection phase, the ransomware implants into the host system. Often the entry point into the system is enabled by a user inadvertently allowing access, such as through a phishing attack or by clicking on a malicious link (Thomas J. E., 2018). This is generally possible because miscreants simply take advantage of user susceptibility to attack due to lack of knowledge of lack or training (Brewer, 2017; Fruhlinger, 2017).

During the next ransomware phase, the infection protocol initiates (Thomas & Galligher, 2018). The ransomware plants an executive file on the host system, and the ransomware embeds itself in the host system. The ransomware alters registry keys to ensure that the infection remains, even after reboot or system reset. At this point, the die is cast, and data encryption will occur according to the established incubation period (Brewer, 2017).

Next, the ransomware seeks to disable the backup system (Thomas & Galligher, 2018). If successful, this will limit the victim's ability to recover. If the attack is successful, more leverage exists to pressure the victim into paying the ransom, and significant damage to business process due to data loss is more likely (Brewer, 2017; Harnedy, 2016).

During the encryption phase, data are encrypted (Thomas & Galligher, 2018). The ransomware establishes an encryption key, with encryption time varying based on factors such as number of connected devices, file size, and network design (Allen, 2017; Brewer, 2017).

Lastly, the ransomware presents a notification to the user (Thomas & Galligher, 2018). The announcement relays the ransom amount and payment instructions. Figure 3 depicts the ransomware infection process.

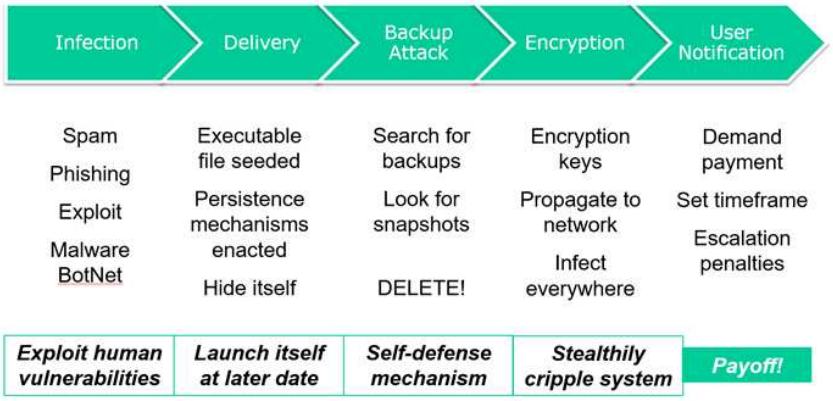

Figure 3. Ransomware infection process, adapted from (Thomas & Galligher, 2018)

3.3 Challenges in Addressing the Ransomware Problem

Addressing ransomware threats is a huge challenge for organizations (Allen, 2017; Brewer, 2017; Fruhlinger, 2017; Symantec, 2016; Thomas & Galligher, 2018). In addition to the technical challenges inherent with ransomware, there are also behavioral and environmental challenges surrounding ransomware. First, ransomware is challenging to detect; few, if any, organizations discover ransomware before infection (Allen, 2017; Brewer, 2017; Thomas & Galligher, 2018; Thomas, Galligher & Huff, 2018)

A fundamental issue underlying these challenges is underreporting due to potential embarrassment, fines, or loss of customer confidence (Langde, 2017; Thomas J. E., 2017; Thomas, Galligher, & Huff, 2018). And in some cases, regulations do not require organizations to report attacks (Meb, 2017). For example, the United States Department of Health and Human Services does not require health organizations to report ransomware attacks.

Another challenge in addressing ransomware attacks is the behavior of the culprits behind the attack. These criminals may not release the data after the ransom is paid. In fact, some may not even have the ability to release the data. Some reports have suggested that one in five victims of ransomware paying ransom is not able to recover their data (Crowe, 2017; Meb, 2017). These companies suffer business losses on top of fees paid to the miscreants, with these business losses rapidly compounding as the companies try to recover what they can, re-create what they must, and live without everything else that was lost.

The most difficult challenge in dealing with ransomware is the people factor. The human members of an organization are the most common attack vector (Thomas J. E., 2018). Employees and team members are subjected to countless attacks such as phishing, spear phishing, social engineering, spam mail, and malicious links (CSO, 2012; Ferrara, 2017; Petrasko, 2017; Thomas J. E., 2018). Currently, a popular distribution model for ransomware is remote desktop (Crowe, 2017; Symantec, 2016, p. 11) .This form of malicious attacking, exploiting protocols such as the remote desktop protocol, is especially insidious as it does not require user involvement. The remote desktop protocol is also commonly turned on by default when enterprise/business systems are added to an Active Directory domain. If a misconfigured firewall allows the specific remote desktop port (3389 TCP) to be accessible from the Internet for any system in an enterprise, then that system can be found and attacked relatively easily (Crowe, 2017).

As discussed, users are a common entry point for ransomware infection (Thomas J. E., 2018). Employees present a constant challenge for information security managers (Komatsu, Takagi & Takemura, 2013; Peltier, 2013). Information literacy skills vary by individual and job role, and information security managers must be diligent to gain mindshare regarding security. Some don't understand the security threat or believe in the probability of real danger. Often security managers try to address this with education (Deceth, 2013; Jensen, Dinger, Wright & Thatcher, 2017; USPS Office of Inspector General, 2015; Thomas J. E., 2018). Adult education, though, requires special skills and assessment techniques tailored to adult learning styles as well as understanding the motivations causing the behavior (Thomas & Hornsey, 2014).

3.4 Digital Forensic Methods

In society today, electronic devices are an integral part of all aspects of life: work, education, play, and relaxation. Digital forensics refers to investigations that involve the use of technology devices such as smartphones, computers, USB drives, and so on (Wiley, 2017). Digital forensic methods are based on traditional forensic methods, but are adapted to technology media (digitalforensics.com, 2018). The basic paradigm for digital forensic investigations is (a) identify, (b) preserve, (c) discover, and (d) present (in more detail: identifying evidence sources, preserving their state, discovering evidence, and presenting the evidence for use by appropriate agencies).

Often this process involves examining storage structures for clues to identify what was stolen or damaged, as well as attempting to trace the source of the criminal activity (Deloitte, 2016). Digital forensic investigators often examine storage systems, file attributes, access logs, and file histories (Bennett, 2011; Chen, 2013; SANS DFIR, 2017). Techniques used to investigate incidents after data encryption may be useful also in detecting ransomware before ransom notification.

4. Discussion

Intuitively, it stands to reason that the techniques used to investigate ransomware incidents might be proactively applied to detect ransomware infection before ransom notification. What follows is a discussion of areas of thought on how digital forensic techniques might be used to detect ransomware infection proactively.

4.1 Opportunities to Detect Ransomware

Ransomware generally gains access to a storage system and encrypts data so that users cannot access data, applications, or systems (Brewer, 2017; Fruhlinger, 2017; Thomas & Galligher, 2018). Ransomware also tends to rename files and their file extensions (Palmer, 2017). Each of these actions creates system changes, particularly in the file system, that can be identified and tracked.

There are several items changed when files are overwritten or modified. Some examples include (a) volume access time, (b) change in file size, (c) change in dedupe ratio, and (d) ransom note files.

When files are accessed and rewritten, the file access time and modified date are changed as a part of normal operating system process (Casey, 2009). Standard digital forensic investigation techniques can be used to detect these changes to file and storage systems. Access and modification of a large number of files within a short time span can be a very good indication of ransomware attack encrypting valuable data or changing settings in order to do things like lock the desktop, steal personal information or hide itself (Kharraz, Robertson, Balzarotti, Bilge, & Kirda, 2015). However, it is relatively easy for ransomware programmers to add in code that gives it the ability to save and modify the access times of files (ShellHacks, 2019). This means that this method of detection does not necessarily to have the ability to catch ransomware.

A large percentage of ransomware will attempt to hold data hostage by either encrypting the information on the computer or by deleting the data (Kharraz, Robertson, Balzarotti, Bilge & Kirda, 2015) When encrypting data, many ransomwares use CryptEncrypt, which encrypts using AES-GCM, AES-256, RSA, or a combination of multiple methods to encrypt and overwrite the files (Kharraz, Robertson, Balzarotti, Bilge & Kirda, 2015). When encrypting files using block ciphers, like the AES and RSA encryption types, padding will be used in order to get the data to be an exact multiple of block size in order to be able to encrypt properly (Obiex, n.d.). Because of this, a large number of files on the system may increasing in size by a very small amount all at once could be a good indication that an encryption-based ransomware has infected the system. Another type of changing file size would be ransomware directly deleting files off of the system until the demands are met. For NTF, the Windows default filesystem, they can go into the Master File Table and clear out the status flag and zero out file information, so that file cannot be seen on the filesystem. However, this does leave the data still on the computer as long as the deleted item is not overwritten on the disk, so it would still be recoverable, and possibly trackable if large amount from generally untouched directories were deleted all at once. (Kharraz, Robertson, Balzarotti, Bilge & Kirda, 2015)

Many network file shares use a process called data deduplication (dedupe), where duplicate information from files is removed and simply have pointers to a single instance of that information in order to save space. However, encryption and dedupe are generally incompatible. This is because dedupe relies upon finding duplications within different files while encryptions remove any discernable patterns within the encrypted file to increase security. (Foskett, 2009). This means that if the file is encrypted first, then the dedupe ratio would plummet to a near 1:1 as there will be near to no duplications in data between encrypted files. Thus, if there is an unauthorized encryption of a system's files, the dedupe ratios would plummet and would be a strong indicator of

encryption ransomware. Lastly, ransomware often leaves behind files in .HTML or .txt format to communicate with victims about the ransomware (Delaney, 2016). Noticeable increases in creation of .HTML or .txt files in directories that generally had low percentages of files of that type beforehand can be a good indicator of ransomware interference.

5. Recommendations to Explore Early Ransomware Detection

Given the nature of ransomware and the footprints it leaves behind, several opportunities exist to monitor systems and achieve early ransomware detection. System administrators and security personnel can conduct manual investigations of systems and storage to look for signs of ransomware. Systems management applications can be applied in alternate ways to help detect these changes. Moreover, file-monitoring applications can be utilized to detect file changes consistent with ransomware infection.

5.1 Manual Investigation.

One way to detect ransomware is to look for file system and storage changes such as last access/modification time changes. Another option is to look for file name extensions associated with ransomware. There are several reliable Internet sources that provide lists of current and historical file name extensions associated with ransomware infection (Delaney, 2016).

Another option is looking at changes in the number of renamed files (Delaney, 2016). While renaming a file is a standard operation on computer systems, it occurs infrequently. Having large volumes of renamed files in a short period of time is a sign that ransomware infection has occurred. Further mass renaming would be easy to detect because systems would stop working.

Security managers have long used the concept of honeypots to deal with intruders and to respond to incidents. Honeypots are dummy systems set up to attract miscreants (Forristal, 2000). Once miscreants take the bait, their intentions are displayed and security teams can take appropriate action. This concept can also be applied to ransomware (Delaney, 2016).

One of the first actions taken by ransomware is to seek out network shares. Often shares are searched in alphabetical order (Delaney, 2016). Thus, one can place a fake or dummy network share for ransomware to target. This share can be monitored, and once the files on it are renamed or encrypted, ransomware can be detected.

As previously discussed, encrypting files and storage systems changes system nature and footprint (Foskett, 2009). In order to track these changes, one must establish a historical baseline. So, another option is to compare existing system state to historical backup and the dedupe system reports.

Systems administrators and security managers can use manual techniques to identify file and storage system changes. Once these processes are established, they can be automated with scripts and batch files, which are common system administration tools. However, more efficiency can be gained using commercial applications.

5.2 Using Applications.

Applications and utilities can be used to detect ransomware. Intrusion detection systems (IDSs) are designed to monitor system activity and report patterns (Peltier, 2013). These systems can be tuned or adapted to detect patterns associated with ransomware such as adding or turning on exploit-detection features (Delaney, 5 methods for detecting ransomware activity, 2016).

Some firms offer anti-ransomware applications (Bust, 2016). These offerings are relatively new, but would seem to have promise in a similar manner to antivirus software. Other products can be adapted or configured to assist in ransomware detection. For example, signature-based (hash) file monitors can be used to identify and track changes to files, and backup applications can be mined for historical data states for comparison with current states to identify changes. For example, a large change in the size of nightly incremental backups could be indicative of ransomware infection (Thomas &Galligher, 2018; Thomas, Galligher, & Huff, 2018).

As stated previously stated, many types of ransomware will attempt to destroy or infect backups that are stored on the infected computer. During the backup attack phase, and around 35% of ransomware will then attempt to extort users into paying a ransome or suffer the conswuquences of losing their data (Kharraz, Robertson, Balzarotti, Bilge & Kirda, 2015). However, using a tradtional backup solution can offer complete mitigation of the threat of these ransomware attacks. This is due to the fact that if the backup program is properly isolated from systems that may be infected the backup system can be used to restore the system to a point in time prior to infection.

Inthis paragraph, also explain any special agreements concerning authorship, such as ifauthors contributed equally to the study. End this paragraph with thanks for personalassistance, such as in manuscript preparation.

6. Conclusion

Ransomware is a significant problem faced by organizations all over the world (Allen, 2017; Brewer, 2017; Thomas J. E., 2017). Once infected, organizations can lose access to data (Collier, 2017; Langde, 2017; Thomas & Galligher, 2018). Because ransomware affects storage and file systems, digital forensic techniques can be applied to identify and track changes in file systems, storage size metadata, and storage system footprint (Bennett, 2011; Chen, 2013; Delaney, 2016; Forristal, 2000; Fruhlinger, 2017). Processes can be applied manually or can be automated by systems administrators. Lastly, third-party applications can be adapted and tuned to help address the ransomware issue.

References

Allen, J. (2017). Surviving ransomware. *American Journal of Family Law, 31*(2), 65-68. Retrieved from https://www.ncbi.nlm.nih.gov/labs/journals/am-j-fam-law/

Bandi, A., Fellah, A., & Bondalapati, H. (2019). Embedding security concepts in introductory programming courses. *The Journal of Computing Sciences in Colleges*, *78*. Retrieved from The Journal of : https://www.ccsc.org/publications/

Bennett, D. (2011, August 22). *The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations*. Retrieved from Forensic Focus: https://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/

Brewer, R. (2017). Ransomware attacks: detection, prevention, and cure. *Netowrk Security, 9*, 5-9. https://doi.org.ezproxy.utica.edu/10.1016/S1353-4858(16)30086-1

Bust, P. (2016, January 25). *Introducing Malwarebytes Anti-Ransomware Beta*. Retrieved from Malwarebytes: https://forums.malwarebytes.com/topic/177751-introducing-malwarebytes-anti-ransomware-beta/

Casey, E. (2009). *Handbook of DIgital Forensics and Investigation.* Cambridge: Academic Press.

CDC. (2003, April 11). *HIPAA Privacy Rule and Health*. Retrieved October 6, 2017, from http://www.cdc.gov/privacyrule/privacy-HIPAAfacts.htm

Chen, B. (2013). Computer Forensics in Criminal Investigations. *Dartmouth Undergraduate Journal of Science, Winder*. Retrieved from http://dujs.dartmouth.edu/2013/03/computer-forensics-in-criminal-investigations/#.WTloN8a1uUk

Collier, R. (2017). NHS ransomware attack spreads worldwide. *CMAJ, 189*(22), 786-787. https://doi.org/10.1503/cmaj.1095434

Crowe, J. (2017, June). *Must know ransomware statistics for 2017*. Retrieved from Barkly: https://blog.barkly.com/ransomware-statistics-2017

CSO. (2012, February 28). *CSO's ultimate guide to social engineering*. Retrieved January 21, 2018, from CSO: https://www.csoonline.com/article/2130996/identity-access/cso-s-ultimate-guide-to-social-engineering.html

Deceth. (2013). *Understanding Computer Security*. Retrieved from Software Engineer Training: http://software-engineer-training.com/understanding-computer-security/

Delaney, D. (2016, May 16). *5 methods for detecting ransomware activity*. Retrieved from NetFort: https://www.netfort.com/blog/methods-for-detecting-ransomware-activity/

Delaney, D. (2016, June 22). *How to generate Ransomware Alerts*. Retrieved from NetFort: https://www.netfort.com/blog/generate-ransomware-alerts/

Deloitte. (2016). *Computer forensics: preserving evidence of cyber crime*. Retrieved from The Wall Street Journal: http://deloitte.wsj.com/cio/2014/12/03/computer-forensics-preserving-evidence-of-cyber-crime/

digitalforensics.com. (2018). *Digital Forensics Corporation*. Retrieved from Digital Forensics Corp: https://www.digitalforensics.com/?utm_source=google&utm_term=computer%20forensics&utm_campaign=AA-DF&gclid=Cj0KCQjwuMrXBRC_ARIsALWZrIjWBkhJSEaPwRCEq-vAxUv4fmD1wStXYX8OPNEHNAsNLTf0cQWhsaoaAgf5EALw_wcB

Ferrara, J. (2017, July 10). *Social engineering: How social media is compounding the threat*. Retrieved January 22, 2018, from SC Media: https://www.scmagazineuk.com/social-engineering-how-social-media-is-compounding-the-threat/article/668589/

Forristal, J. (2000). Luring killer bees with honey -- Attracting hackers to one of your servers may seem foolish, but not if that server is a honey pot. *Network Computing, 11*(16), 100.

Foskett, S. (2009, Februrary 5). *Compression, encryption, deduplication, and replication: Strange bedfellows*. Retrieved from blog.foskets.net: http://blog.fosketts.net/2009/02/05/compression-encryption-deduplication-replication/

Fruhlinger, J. (2017). *What is ransomware? How it works and how to remove it.* Retrieved from CSO: https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html

FTC. (2013, Februrary). *Consumer Sentinel Network Data Book*. Retrieved from Federal Trade Commission: https://www.huffingtonpost.com/2012/02/28/identity-theft-cost-americans-152-billion-2011-ftc_n_1307485.html

Harnedy, R. (2016). *3 better ways to use backup to recover from ransomeware*. Retrieved from Barkly: https://blog.barkly.com/3-better-ways-to-use-backup-to-recover-from-ransomware

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques.*Journal of Management Information Systems, 34*(2), 597-626. https://doi.org/10.1080/07421222.2017.1334499

Jesson, J., Mattheson, L., & Lacey, F. (2011). *Doing Your Literature Review.* Los Angeles: Sage Publications Ltd.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). *Publications.* Retrieved from North Easter Univesrity Systems Security Lab: https://seclab.ccs.neu.edu/static/publications/dimva2015ransomware.pdf

Komatsu, A., Takagi, D., & Takemura, T. (2013). Human aspects of information security.*Information Management & Computer Security, 21*(1), 5-15. https://doi.org/10.1108/09685221311314383

Kwok, A. (2015). The evolution of management theories: A literature review. *Nang Yan Business Journal, 3*(1), 28-40. https://doi.org/10.1515/nybj-2015-0003

Langde, R. (2017, September 16). *Wanna Cry Ransomware: A detailed analysis of the attack*. Retrieved from techspective: https://techspective.net/2017/09/26/wannacry-ransomware-detailed-analysis-attack/

Manes, C. (2017, August 22). *The 10 worst ransomware attacks that ever happened*. Retrieved January 5, 2018, from TechTalk: https://techtalk.gfi.com/the-10-worst-ransomware-attacks-that-ever-happened/

Meb, B. (2017, June 20). *Ransomware attacks can fall below the radar via underreporting*. Retrieved from Healthcaredive: https://www.healthcaredive.com/news/ransomware-attacks-can-fall-below-the-radar-via-underreporting/445351/

Morgan, S. (2017, Novermber 20). *Cybersecurity Business Report*. Retrieved from CSO: https://www.csoonline.com/article/3237674/ransomware/ransomware-damage-costs-predicted-to-hit-115b-by-2019.html

Nicho, M., Fakhry, H., & Egbue, U. (2018). Evaluating user vulnerabilities vs phisher skills in spear phishing.*IADIS International Journal on Computer Science & Information Systesm, 13*(2). Retrieved from www.iadisportal.org/ijcsis

Obiex. (n.d.). *How to calculate the size of encrypted data?* Retrieved from obviex.com: http://www.obviex.com/Articles/CiphertextSize.aspx

Palmer, D. (2017, May 12). *This new ransomware nightmare demands a big payday to decrypt your files*. Retrieved from ZDNet: https://www.zdnet.com/article/this-new-ransomware-nightmare-demands-a-big-payday-to-decrypt-your-files/

Peltier, T. R. (2013). *Information Security Fundamentals.* Boca Raton: Taylor & Francis Group.

Petrasko, M. (2017, March). *Ransomware-as-a-service is booming: Here's what you need to know*. Retrieved from Barkly: https://blog.barkly.com/how-ransomware-as-a-service-works

SANS DFIR. (2017). *SANS Investigative Forensic Toolkit (SIFT) Workstation*. Retrieved from SANS Digital Forensics & Incident Response: https://digital-forensics.sans.org/community/downloads

Shell Hacks. (2019). *Linux Hacks and Guides.* Retrieved from ShellHacks:

https://www.shellhacks.com/fake-file-access-modify-change-timestamps-linux/

Symantec. (2016). *Ransomware and Business 2016*. Retrieved November 28, 2017, from Symantec Website: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

Thomas, J. (2017). Lessons learned in management, marketing, sales, and finance incentive practices a decade after the Subprime Mortgage Crisis. *International Journal of Business and Management, 12*(3), 19-26. https://doi.org/10.5539/ijbm.v12n3p19

Thomas, J. E. (2017, November 6). *Combating ransomware with traditional backup*. https://doi.org/10.13140/RG.2.2.15403.13603

Thomas, J. E. (2017). Exploring buyer motivation to improve management, marketing, sales, and finance practices in the martial arts industry. *9*(2), 14-35. https://doi.org/10.5539/ijms.v9n2p12

Thomas, J. E. (2017, November 30). *Is your backup a real backup? Part II: Combating ransomware with traditional backups*. Retrieved December 5, 2017, from Linkedin: https://www.linkedin.com/pulse/your-backup-real-part-ii-combating-ransomware-backups-thomas-phd/

Thomas, J. E. (2017). Practical application of theory in business. *International Business Research, 10*(11), 10-20. https://doi.org/10.5539/ibr.v10n11p10

Thomas, J. E. (2017). Scholarly views on theory: Its nature, practical application, and relation to world view in business research. *International Journal of Business Management, 12*(9), 231-240. https://doi.org/10.5539/ijbm.v12n9p231

Thomas, J. E. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business and Management, 13*(6), 1-24. https://doi.org/10.5539/ijbm.v13n6p1

Thomas, J. E., & Galligher, G. C. (2018). Improving backup system evaluations in information security risk assessments to combat ransomware.*Computer and Information Science, 11*(1), 14-25. https://doi.org/10.5539/cis.v11n1p14

Thomas, J. E., & Hornsey, P. E. (2014). Adding Rigor to classroom assessment techniuqes for non-traditional adult programs: A liifecycle improvement approach. *Journal of Instructional Research, 3*, 27-37. https://doi.org/10.9743/JIR.2014.3.20

Thomas, J. E., Galligher, G. C., & Huff, B. R. (2018, March 22). *Combatting ransomware with traditional backups and using automation to detect infection prior to ransomware notification.*Texas A & M University, Bush School of Public Service and Administration, College Station.

Thomas, J. E., Wittkopf, A., Dobbins, J., & Rivera, R. (2019). Recommendations to address government concerns regarding intellectual property theft from American research universities by China and other foreign entities while preserving the process of fundamental research. *Research Gate*. https://doi.org/10.13140/RG.2.2.14963.37922

USPS Office of Inspector General. (2015, December 15). *Informaton security awareness training and phishing*. Retrieved January 21, 2018, from USPSOIG.com: https://www.uspsoig.gov/sites/default/files/document-library-files/2015/IT-AR-16-001.pdf

Wilday, T. M. (2018). *Comparing and contrasting how the United States and China address cybersecurity*. Retrieved from ProQuest Dissertations Publishing: https://search.proquest.com/openview/e53c0ca72156227c8d449d451c0855c8/1?pq-origsite=gscholar&cbl=18750&diss=y

Wiley, C. (2017, July 05). *What is the differene between computer forensics & digital forensics*. Retrieved from Career Trend: https://careertrend.com/facts-6733855-difference-computer-forensics-digital-forensics-.html

Xiao, Y., & Watson, M. (2017).Guidance on conducting a systematic literature review. *Journal of Planning Education and Research, 25*(5), 425-427. https://doi.org/10.1177/0739456X17723971