Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Ransomware: Hostage Situation

CAPSTONE REPORT

Khuram Abedin
Jr. Systems Administrator
Millennium Space Systems

University of Oregon
Applied Information
Management
Program

Spring 2018

Continuing and Professional
Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Kara McFall
Director, AIM Program

Ransomware: Hostage Situation

Khuram Abedin

Millennium Space Systems

Abstract

In this digitized world, data is accessible at the fingertips 24/7 and has improved the way people live and productivity and efficiency within organizations. However, security concerns have also taken a toll on reliability and sociability. Cyberattacks such as ransomware – malware, Trojans, phishing, spam, and viruses – cause organizations millions of dollars in damages and productivity loss. This annotated bibliography explores literature on the issues of malware and how to recover from and prevent disastrous attacks.

Table of Contents

Introduction to the Annotated Bibliography

Problem Description

Gómez-Hernández, Álvarez-González, and García-Teodoro (2018) warn that ransomware has become "a pandemic that affects both individuals and organizations all over the world" (p. 389). Ransomware is the process of kidnapping private data or access to equipment by securing it against all who had access and offering to sell access data back to the user (Allen, 2017). Ransomware is known to attack users in many different ways such as infected emails, opening email attachments, clicking on bad links in social media posts, and in instant messenger chats (Allen, 2017). "They all work to stop you from using your computer normally" (Allen, 2017, p. 66). Because email attachments are common sources of ransomware, Information Technology (IT) leaders recommend that users never click on email attachments unless they know the senders (Goldsborough, 2017).

Ransomware has been around for almost 30 years and is becoming increasingly popular due to the large payouts hackers receive (Goldsborough, 2017). Goldsborough (2017) cites security provider Sonicwall's findings on the recent rapid increase of ransomware attacks: "The number of ransomware attacks jumped from 3.8 million in 2015 to 638 million in 2016, an increase of 167 times" (p. 61). Goldsborough (2017) cites Intel Security in noting that there were more then 400 different types of ransomware in 2017, a number that is growing on a daily basis.

One area where ransomware is predicted to experience rapid growth is in connected devices collectively known as the Internet of Things (IoT) (Yaqoob et al., 2017). "According to recent market data, the IoT security market is expected to rise to $28.90 billion by 2020, which indicates that high -security threats are expected to rise substantially in the foreseeable future" (Yaqoob et al., 2017, p. 444). The damage from a ransomware attack in IoT can be more

widespread than a traditional malware attack because it may result in not only financial losses, but also critical information breaches (Yaqoob et al., 2017).

Choudhary (2016) notes that ransomware attacks are worldwide and are affecting businesses and individuals. Ransomware has become a multimillion dollar crime and since its inception has hit large corporations, casinos, hospitals, schools, and churches on a global scale (Allen, 2017). “It’s such a profitable scheme that experts say traditional cyber thieves are abandoning their old ways of making money – stealing credit card numbers and bank account credentials – in favor of ransomware” (Allen, 2017, p. 65). The main motivation for these hackers is maximizing monetization using malware (Choudhary, 2016). “The malware encrypts data on infected machines and demands a ransom from their users before they can get their files back. The ransom is paid in bitcoins” (“CryptoLocker success”, 2014, p. 20). One highly publicized attack was against Hollywood Presbyterian Center in California where hackers breached the hospital’s systems; the hospital ultimately ended up paying roughly $17,000 worth of bitcoins so they could regain access to their network (Young & Yung, 2017).

Ransomware is classified into three basic categories: crypto, locker, and hybrid (Yaqoob et al., 2017). Crypto ransomware applies encryption and decryption algorithms on data devices; typically the data is encrypted using public keys and users are provided with the private keys to decrypt their data (Yaqoob et al., 2017). Locker ransomware is completely different because it restricts user access to device and system functionalities (Yaqoob et al., 2017). In the case of IoT devices, locker ransomware may even alter the functionality of the devices as the means used to convince the owners of the devices to pay the ransom (Yaqoob et al., 2017). The last type of ransomware attack is a hybrid attack. “Hybrid ransomware attacks that enable encryption and locking mechanisms are more dangerous because the device data and functionality could be

compromised" (Yaqoob et al., 2017, p.444). Hybrid attacks target both front-end and back-end infrastructure, increasing the risk of complete paralysis of an entire IoT network (Yaqoob et al., 2017). However, hybrid attacks are more difficult to launch because of device heterogeneity and ownership and the multilayer department of loT systems (Yaqoob et al., 2017).

The potential for ransomware to pose a global threat is real (Young & Yung, 2017). The May 2017 WannaCry attack locked up more than 200,000 computers in 150 countries (Young & Yung, 2017). The attack was noteworthy not just because of the extent of the victims, but also because it exploited a vulnerability that the United States National Security Agency (NSA) had already identified but chose not to report; once whistleblowers exposed the NSA's knowledge a patch was released (Young & Yung, 2017). Young and Yung (2017) worry that despite past global ransomware attacks such as WannaCry, the threat of a severe worldwide attack is being overlooked, noting "those who cannot remember the past are condemned to repeat it" (p. 26).

Purpose Statement

The purpose of this annotated bibliography is to present literature that addresses the problem of ransomware, the damage caused by ransomware attacks, and best practices in avoiding these ransomware attacks.

Research Question

What are best practices for organizations in avoiding ransomware attacks?

Audience

The primary audience members for this annotated bibliography are leaders in information security departments such as Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), and Information Technology (IT) program managers. Information security department leaders will be interested in this information because they will be able to stay

informed of any high-security and high-risk situations related to ransomware and will be able to delegate the work to prevent ransomware attacks from the top down. CIOs will be interested in this information because ransomware attacks threaten the structure and integrity of the organizations they are responsible for overseeing. CIOs will be able to make informed and often crucial decisions regarding the security of their IT infrastructure in a timely manner. Lastly, IT program managers can use this information to learn from previous mistakes related to ransomware, devise plans to address the ransomware threats directly, and implement the plans.

In many cases Chief Executive Officers (CEOs) will also find the information on ransomware and how to prevent attacks useful due to the risk posed by ransomware to organizations large and small. This annotated bibliography contains information that is useful to those parties stated above whose job responsibilities include protecting the organization's assets, data, security and private information.

Search Report

Search strategy. The search strategy I employed involves the use of Google Scholar and the University of Oregon Library, which provided access to research databases like EBSCOhost. I started the search by using keywords such as *technology*, *business*, and *cryptocurrency*; I then narrowed the search to *ransomware amongst organizations*. The most reliable and trusted databases that provided significant information regarding ransomware were EBSCOhost and ScienceDirect. I found several relevant journal articles and other scholarly sources by searching within these two research databases. Because *ransomware* is a fairly recent phenomenon occurring amongst various industries and organizations, I narrowed the date range of the searches to the last few years, ranging from 2015-2018. The search also resulted in articles about ransomware that is present in various industries including healthcare and both the private and

government sector. Even though ransomware has only become a widely discussed subject in the last few years, the search resulted in a plethora of informative articles and real-life examples.

Libraries and search engines. I used the following library and search engines in searching for research materials required for this Capstone:

- UO Library.
- Google Scholar.

Databases. I used the following databases for research:

- Torrance Public Library.
- Academic Search Premier.
- ScienceDirect.
- Ebscohost.
- University of Derby database.
- ProQuest.

Key words and phrases. I used the following keywords to search for appropriate reference sources:

- Ransomware.
- Cybersecurity.
- Bitcoins.
- Malware.
- Virus.
- Cyberattack.
- Corporate cyber-attacks.
- Business cybercrime.

- Trojan attacks.
- Enterprise cybercrime.
- Cyber worm.
- Computer virus.
- Backup encryption.
- Ransomware amongst organizations.

Documentation Methods

Documentation approach. The most active method I used to document my research was using Microsoft Word to track all relevant and substantial sources and their citations and links. I documented all sources in American Psychological Association (APA) format for proper citation later in the annotated bibliography. I alphabetized each reference for easy retrieval later. This Microsoft Word documented provided a clean, efficient, and effective way to manage multiple sources and links to those sources.

Reference Evaluation

Reference evaluation criteria. The literature for this annotated bibliography were evaluated using the criteria defined in the Evaluating Information Sources documentation published by the University of Florida Center for Public Issues (2014), which provides five criteria for the evaluation of information sources.

- *Authority*. Although the research topic is widely discussed via journals, magazine articles, websites, etc., scholarly and peer-reviewed articles took precedence over the more popular sources to ensure the author's research and claims were validated by professionals in the field.

- *Timeliness*. Timeliness was a very important factor for this subject since the research area has only recently gained traction and attention from professionals in the field. Thus, scholarly references were selected that had been published within the last five years.
- *Quality.* I assessed the quality of potential sources based upon a number of criteria including correct use of grammar, punctuation, and spelling. I sought sources of a scholarly nature and ensured that articles were written professionally.
- *Relevancy*. The research question delved into a multidimensional topic. To ensure relevancy I carefully considered each article, study, and journal and selected sources that were directly applicable to the research question.
- Lack of *bias*. To ensure unbiased sources, I selected references that offer various perspectives and opinions. I also avoided sources published by individual vendors selling a product or service to ensure the impartiality of the material.

Annotated Bibliography

The annotated bibliography is comprised of fifteen different references that fall into three different categories: history of ransomware, damage to organizations from ransomware, and best practices to avoid ransomware attacks. The following references provide an understanding of ransomware; the damage it can cause to an organization, its employees, and affiliates; and lastly, the evolving nature of ransomware and the steps to combat it.

Each annotation consists of three elements: (a) the full bibliographic citation, (b) an abstract, and (c) summary. The summaries focus on elements that are relevant to the research focus of best practices for organizations in avoiding ransomware attacks.

History of Ransomware

Choudhary, M., Zavarsky, P., Lindskog, D. (2016). Experimental analysis of ransomware on Windows and Android platforms: Evolution and characterization. *Procedia Computer Science, 94*, 465-472. https://doi.org/10.1016/j.procs.2016.08.072

Abstract. The focus of the paper is on providing insights on how ransomware have evolved from its starting till March 2016 by analyzing samples of selected ransomware variants from existing ransomware families in Windows and Android environments. Seventeen Windows and eight Android ransomware families were analyzed. For each ransomware family, at least, three variants belonging to the same family were compared. The analysis revealed that ransomware variants behave in a very similar manner but use different payloads. Our analysis shows that there has been a significant improvement in encryption techniques used by ransomware. The experimental results in Windows environment demonstrate that detection of ransomware is possible by monitoring

abnormal filesystem and registry activities. In Android environment, our analysis reveals that likelihood of ransomware attacks can be reduced by paying a closer attention to permissions requested by the Android applications.

Summary. The researchers in this study analyzed cases of ransomware within both Microsoft and Android operating systems. They provide real world examples of different levels/cases of ransomware within both environments. Windows examples include devices which go through various stages of ransomware acquired via a malicious website, email attachment, or link on a program. The authors describe how once a Windows device is infected it contacts the control server, sends the victim's machine information to hackers, and generates a random key. The key is then generated and starts to encrypt all files and folders, sometimes attempting to encrypt all disk and network drives as well. The authors also provide an example of ransomware for Android operating devices where the ransomware focuses on an xml file called AndroidManifest.xml. This file is embedded in apps which are downloaded by users. Once the app is downloaded it asks for administrator privileges; if a user clicks *Agree* the ransomware spreads through the device.

The authors note that ransomware has become more and more sophisticated and has evolved. For example, current ransomware will delete all the restore points, volume copies, and backup folders. To avoid ransomware, the authors recommend using a PEiD tool to detect packers, cryptors and compilers which are found in Portable Executable (PE) files. In addition, they recommend using RegShots, which takes snapshots of all register values before and after any installation of programs.

This article is important for this study because it discusses the impact of ransomware but more importantly, how it lives and evolves in both Microsoft and Android environments. The researchers also discuss ways in which ransomware can be detected and prevented under both systems.

Green, A. (2017). Ransomware and the GDPR. *Network Security, 2017*(3), 18-19. https://doi.org/10.1016/S1353-4858(17)30030-2

Abstract. Ransomware is a unique form of hacking that leaves data intact but still disrupts enterprises around the globe. This special malware encrypts computer files, network file shares and even databases, thereby preventing user access. To release the files, the victim is asked to pay a ransom to the cyberthieves. It is completely diabolical and you would think with such brazen criminal activity, there would be relevant data security laws that would kick in. And there are.

Summary. The author of this article takes a deep dive into the details surrounding ransomware attacks, its nature, how it differs from other hacking methods, and its ramifications. The author describes data security laws pertaining to ransomware, including general data protection regulation (GDPR) and data protection directive (DPD). The (GDPA) law requires organizations to report any data that has been encrypted by ransomware. The (DPD) basically covers personal data collected by companies for consumers. The author also provides recommendations for how organizations can avoid falling into a hacker's trap; key recommendations include next-generation firewall, IDS, security information, and event management alerts which detect infected computers.

This article is important for this study because it provides an expert's view on how severe a ransomware attack can be and provides examples of well-known corporations such as Microsoft who have fallen victim. The author also provides recommendations to help organizations ensure they do not become victimized by a ransomware attack. This article is important for this study because it discusses how ransomware is affecting the corporate world and what corporations are doing to prevent disasters.

Hampton, N., Baig, Z. & Zeadally, S. (2018). Ransomware behavioural analysis on windows platforms. *Journal of Information Security and Applications, 40*, 44-51. https://doi.org/10.1016/j.jisa.2018.02.008

Abstract. Ransomware infections have grown exponentially during the recent past to cause major disruption in operations across a range of industries including the government. Through this research, we present an analysis of 14 strains of ransomware that infect Windows platforms, and we do a comparison of Windows Application Programming Interface (API) calls made through ransomware processes with baselines of normal operating system behaviour. The study identifies and reports salient features of ransomware as referred through the frequencies of API calls.

Summary. This article provides an introduction to ransomware, how its level of sophistication has increased and in turn, how much more damaging it is today than it was in the past. This is mostly due to technological advances and a 500% growth in the different strains of ransomware now being used. The authors describe a ransomware attack to be categorized into four stages: infection, data encryption, demand and outcome. The authors provide data to experimental tests where they test certain operations (i.e. running PowerPoint) and then notate the description of events that take place after the

baseline operation. The significance behind this testing was to find a confirmed way to identify ransomware/malicious activity without identifying code signatures. These tests help to determine what the strain of ransomware is actually doing and in turn, provides research that would help the creation of anti-virus software. This article is important for this study because it discusses how ransomware is evolving in the Windows environment and what steps to take to be prepared for such an attack.

Mansfield-Devine, S. (2016). Ransomware: Taking businesses hostage. *Network Security, 2016*(10), 8 – 17. https://doi.org/10.1016/S1353-4858(16)30096-4

Abstract. Cybercrime has its fashions. As technologies evolve and defenses improve, so hackers and cyber-criminals modify their methods of attack. We're currently seeing a burgeoning in the use of ransomware, the digital form of blackmail in which your computer is effectively taken hostage. And both the nature of the chief targets and the ways in which they are being attacked are changing quickly as criminal's spot new opportunities for extorting money.

Summary. The author discusses how hackers are getting smarter and improving their means of hacking as defenses increase from the end-user. The author notes the rise of ransomware in recent years has dramatically increased, citing a 2016 report from Intel Security that described a 127% increase in the rise of ransomware over the past two years. Cyber thieves have used the approach of mass phishing and spamming campaigns to push out attacks, but now have also gone to the next level by exploiting social engineering, often via spear-phishing attacks. Spear-phishing attacks are email-spoofing attacks that target companies or individuals in an attempt to gain access to sensitive information. After the ransomware hits botnets spread through the back end of the

systems to take demand ransoms to be paid using Bitcoins. This form of cyberattack has been extremely profitable for hackers; Intel Security reported one of the hackers made $94 million in just six months. The CryptoWall malware attack generated $325 million in just two months.

Hackers are basically going where the money is and have picked up on how large companies are very reluctant for their own data to be stolen. Attacks have been targeted against the healthcare industry, government agencies, and large organizations that analyze valuable data such as financials, human resources, and health records. Ransomware is so powerful that it has the ability physically harm people if it hits a medical institution. The author cites Intel's Security report which suggested 24 attacks were targeted at hospitals in 2016. One of the biggest attacks was in California where the ransom demand was $5.77 million.

Government agencies have also been targeted because hackers are aware of their old and outdated equipment and know that the government sector has a strong impact on people's lives. The author notes that the scope of the problem is not just Windows platforms; Apple macOS and mobile devices have also faced similar problems. A popular bittorrent client transmitted ransomware onto macOS computers by bypassing macOS gatekeeper protection and infecting the machines. Mobile devices have also been targets of malware, mainly on Android devices. Quick Heal Technologies reported a 200% increase in ransomware attacks on mobile devices during the second quarter of 2016.

This article is important for this study because it discusses how ransomware is evolving as security measures get tougher and what new approaches hackers are taking to stay invisible.

Young, A. L., & Yung, M. (2017). Cryptovirology: The birth, neglect, and explosion of ransomware. *Communications of the ACM*, *60*(7), 24-26. doi:10.1145/3097347

Abstract. Note: this abstract was written by the author of this annotated bibliography in the absence of a published abstract. The authors discuss vulnerabilities that make systems susceptible to ransomware in relation to the concept of cryptovirology. The authors describe the relationship of cryptovirology to both malware and cryptography, specifically the threatening nature of cryptoviruses and the level of damage they can cause. The authors of the article go on to describe the extent and level of sophistication ransomware has reached, to the point that cryptovirology tools are being sold to hackers/extortionists.

Summary. The authors of this article describe cryptovirology as a virus that inhabits its host and spreads the infection. Crytovirology started at Columbia University out of scientific curiosity. Cryptovirology was first released as a form of protection allowing users to hide the content of messages, secure data, and authenticate users. But over time the code was discovered by hackers and used in conjunction with ransomware. The author mentions the famous WannaCry attack which used cryptovirology in May 2017 and locked up more than 200,000 computers in over 150 countries. The same attack also exposed secrets from the NSA that were ultimately exposed to the world.

The authors stress the level of damage that a cryptovirus can have and urge their target audience to become more knowledgeable and aware of its threatening nature. The authors' research found that the attacks are not just limited to businesses, but individuals, hospitals, and government agencies are also rapidly becoming victims. The authors note that news coverage of ransomware attacks such as the Hollywood Presbyterian Medical

Center, an attack where the hospital was forced to pay a heavy ransom in order to regain access to their network, has stirred conversation amongst the public and eventually led to the enactment of new laws within the state of California.

This article is important for this study because it discusses the vulnerabilities within organizations which are allowing hackers to gain access to and attack companies and also details how corporations are dealing with such treats.

Damage to Organizations from Ransomware

CryptoLocker success leads to more malware. (2014). Network Security, 2014(1), 20. https://doi-org./10.1016/S1353-4858(14)70012-1

Abstract. The CryptoLocker ransomware has proven to be hugely successful, and has recently evolved in order to snare even more victims, according to researchers. And it may soon have a successor.

Summary. The author discusses the success of CryptoLocker ransomware and how this success is leading to more ransomware attacks. This new form of malware has evolved as a worm and is able to spread through USB-connected devices such as memory sticks and hard drives. Data on an infected device is encrypted, and the hackers demand a ransom paid in bitcoins before users can retrieve their files. Analysis performed by Dell SecureWorks predicted that 250,000 infections could have taken place in the first 100 days since the launch of this ransomware, resulting in ransomware payments from a minimum of $380,000 to millions of dollars.

This article is important for this study because it gives one example of a successful ransomware attack, including its means of propagating and the ransom demanded by the cyber-thieves who launched the attack.

Malicious-advertising attacks inflict ransomware on victims. (2014). *Computer 47*(12), 16. https://doi.org.10.1109/MC.2014.362

Abstract. Note: This abstract was written by the author of this annotated bibliography in the absence of a published abstract in the source. Malvertising is a term coined by the author to describe malicious advertising is a form of ransomware attack on unassuming users who visit websites and clicking on advertisements that then attack their browsers and hard drives.

Summary. This article presents a unique and dangerous form of malware that infects a user's hard drive when the user clicks on innocent looking advertisements on popular websites. With malvertising, the user clicks on an advertisement from a popular website, malware is distributed to their hard drive, and the hard drive is encrypted. Examples of such malvertising have occurred on popular websites with large amounts of traffic such as Yahoo Finance, AOL, and Match.com. This article is important for this study because it discusses how malvertising is changing one way hackers are attacking users and covering their tracks.

Ransomware claims more victims. (2016). *Network Security*, *2016*(12), 2. https://doi.org/10.1016/S1353-4858(16)30110-6

Abstract. San Francisco's Municipal Railway (Muni) has become the latest high-profile victim of ransomware. It was a very public attack as the usual notification screen that

tells the victim that the machine has been infected and demands the ransom ended up being shown on computer displays at Muni stations.

Summary. This article provides an example of a ransomware attack on a public transportation system: San Francisco's Municipal Railway. Not only did this massive attack affect the organization, but it also affected the general public, in this case the riders who commuted on the railway system. This attack was noteworthy for the delivery of the ransom demand; rather than showing up on the screen of an individual device, the demand was displayed on the computer displays at the Muni stations. The attack resulted in the infection of roughly 900 devices, including office computers, computer aided design (CAD) workstations, laptops, payroll systems, email and print servers, databases, and station kiosk personal computers. Muni refused to pay the ransom demand and was forced to open fare gates, thus allowing riders to ride for free; the estimated lost fares were $50,000.

One other unique feature of this attack was the fact that someone hacked an email account and then used the account to notify the San Francisco Municipal Transport Agency (SFMTA) that he had stolen 30 GB of data and would dump the data on the Internet unless a ransom of 100 bitcoins was paid, a claim that was denied by a SFMTA spokesperson. The email account was hacked when the cyber-criminal guessed the security question for the account.

This article is important for this study because it provides an example of how ransomware hackers took control of the systems of an organization that is made up of hundreds of employees, managers, executives and the general public who use the mass transportation service.

Best Practices to Avoid Ransomware Attacks

Allen, J. (2017). Surviving ransomware. *American Journal of Family Law, 31*(2), 65-68. http://link.galegroup.com/apps/doc/A503308994/AONE?u=s8492775&sid=AONE&xid=c4edc6d7

Abstract. Note: This abstract was written by the author of this annotated bibliography in the absence of a published abstract in the source. The article offers information on ransomware, a type of malicious software that blocks access to the victim's data or threatens to publish or delete it until a ransom is paid. The author discusses the use of new technologies by lawyers in the U.S. and how lawyers can safely employ technology in law practices to protect the confidentiality of clients, ways to protect against ransomware attacks including password protection, anticipating an attack, and using Mac and Windows backups.

Summary. The author describes a recent significant ransomware attack which occurred at the San Francisco Muni Metro systems. The attack caused a breakdown in its operations by shutting down the computers of 900 employees, the Muni email system, and the time-tracking element of its payroll systems; a ransom demand was made to free the affected systems.

The author breaks down ransomware into three classes of malware: screen locking, encrypting, and false threats. The author defines screen locking ransomware as locking a computer screen and displaying a warning with instructions on how to resolve the ransom to unlock the screen. Ransomware that encrypts files does so without notification or warning for the end-user. False threats are described as warnings or notifications to the end-user without any real threat.

The author provides an in-depth analysis of how people and firms can protect themselves from ransomware attacks, including equipment protection and password protection. The author provides examples of equipment protection such as not leaving a device unattended at random locations and making sure the equipment is locked when away from the computer. The author reveals problems with ordinary passwords, including weak passwords that do not contain a minimum of eight characters. As a result, the author recommends biometric access to systems that use facial recognition.

The author also discusses the procedures a user can take to anticipate an attack, including keeping systems and servers up-to-date with patches and updates, making sure data is backed up regularly to the cloud and tapes, also using different types of backups in case one of them gets encrypted.

This source is relevant for this study because it provides details on the best practices for avoiding ransomware and how a user can protect against ransomware attacks.

Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. *Network Security, 2016*(9), 5-9. https://doi.org/10.1016/S1353-4858(16)30086-1

Abstract. Over the past three years, ransomware has become one of the biggest cyber scams to hit businesses. Indeed, the FBI estimates that losses incurred in 2016 due to ransomware will top $1bn. Ransomware is malicious software that allows a hacker to restrict access to an individual's or company's vital information in some way and then demand some form of payment to lift the restriction. The most common form of restriction today is encryption of important data on the computer or network, which essentially lets the attacker hold user data or a system hostage.

Summary. The author discusses how ransomware has become one of the biggest cyber scams to hit businesses. He notes that the FBI estimated losses connected to ransomware in 2016 to top $1 billion in damages. Ransomware becoming an even more lucrative business because hackers are now targeting larger corporations that have bigger budgets to pay more ransom and more important files to hold hostage.

The author provides recommendations for how to avoid a ransomware attack which are categorized as preparation, detection, containment, eradication, and recovery. First, a user must be prepared by eliminating all vulnerabilities by making sure all servers are patched with the latest security updates and system patches. By eliminating all vulnerabilities, a user lessens the chances of the ransomware spreading. Second is detection; companies can detect an attack early using special software that has alarms set for any intrusion, which can minimize the damage. The third step is containment, which involves containing an attack that has already hit an organization to prevent the attack from spreading so network files are not affected. The forth step is eradication, which occurs after a ransomwares event has been acknowledged and controlled and results in the eradication of the malicious code from the network. The authors recommend replacing a unit rather than just cleaning the device. The last step is recovery, which is includes restoring drives and servers from local or cloud-based backups.

This article is important for this study because it discusses what methods corporations can take to detect, prevent, and cure attacks.

Goldsborough, R. (2017). The increasing threat of ransomware. *Teacher Librarian, 45*(1), 61. http://teacherlibrarian.com/2017/

Abstract. Note: this abstract was written by the author of this annotated bibliography in the absence of a published abstract. The article offers information on ways to prevent the threat of ransomware attacks. Among the suggestions include practicing safe computing such as avoiding opening a strange email attachment, utilizing quality security software like Symantec's Norton Security, and providing back up of critical files.

Summary. The author reports the increase in ransomware attacks over the years, noting that from 2015 to 2016 the number of ransomware attacks grew from 3.8 million to 638 million. The author asserts that it does not matter if a user is using Microsoft Windows, Macintosh, Linux, or other platforms: every device is at risk for a ransomware attack. The author suggests taking certain steps to prevent ransomware attacks:

- Do not click on an email attachment unless you know the user; if unsure, phone the sender to verify that he or she sent the attachment.
- Keep software versions and patches up to date. The author recommends enabling automatic updates when available, and periodically checking for updates when the automatic option is not available.
- Install good security software such as Symantec’s Norton Security and Kapersky Internet Security. The author notes that fee-based security programs are typically more robust than free tools.
- Use virtual private network (VPN) software such as Hotspot Shield or TunnelBear when connecting vial public wi-fi.
- Use a secure password manager like KeePass or Lastpass.
- Turn off unneeded software and macros.

- Back up critical files; options include using cloud backup services such as Mozy, cloud storage services such as Dropbox, an external hard drive, USB flash drive, rewritable optical disc, or backup tape.

For those who have found themselves the victim of a ransomware attack, the author notes that sometimes the best option is to begin fresh by wiping the hard drive, reinstalling the operating system and programs, and restoring data from the most recent backup.

Gómez-Hernández, J. A., Álvarez-González, L., and García-Teodoro, P. (2018). R-Locker: Thwarting ransomware action through a honeyfile-based approach. *Computers & Security,* (73), 389-398. https://doi.org/10.1016/j.cose.2017.11.019

Abstract. Ransomware has become a pandemic nowadays. Although some proposals exist to fight against this increasing type of extortion, most of them are prevention like and rely on the assumption that early detection is not so effective once the victim is infected. This paper presents a novel approach intended not just to early detect ransomware but to completely thwart its action. For that, a set of *honeyfiles* is deployed around the target environment in order to catch the ransomware. Instead of being normal archives, honeyfiles are FIFO like, so that the ransomware is blocked once it starts reading the file. In addition to frustrate its action, our honeyfile solution is able to automatically launch countermeasures to solve the infection. Moreover, as it does not require previous training or knowledge, the approach allows fighting against unknown, zero-day ransomware related attacks. As a proof of concept, we have developed the approach for Linux platforms. The tool, named *R-Locker*, shows excellent performance both from the perspective of its accuracy as well as in terms of complexity and resource

consumption. In addition, it has no special needs or privileges and does not affect the normal operation of the overall environment.

Summary. The authors describe the hackers behind ransomware attacks as extortionists and propose solutions to thwart attacks that use *honeyfiles*. Honeyfiles are defined as bait files that are intended for a hacker to open to set off alarms. The authors describe the two main types of ransomware, which are *locker* and *crypto*. Locker ransomware locks the display or keyboard of the user. Crypto ransomware blocks access to information on end user devices by ciphering the user's files and documents. For both types of ransomware, a ransom must be paid before the victim can access the devices or archives.

The authors provide suggestions on how to thwart each attack, including using restoration techniques and tools. However, they note that crypto ransomware is more powerful and nearly impossible to recover from if the ransom is not paid. The main point that the authors attempt to make is the importance of prevention, including user training and education, avoidance of pirated software, maintaining software updates, backing up data, and managing user privileges.

The authors also describe means of detecting ransomware if prevention measures have been unsuccessful, including deploying detectors of filesystem activities, application program interface (API) calls, registry access, command and control (C&C) communications, and encryption procedures. The authors note however that all of these approaches rely on early detection of the malware.

The authors propose the use of honeyfiles to detect and thwart ransomware. The authors note that the benefits of using honeypots include the fact that the ransom attempt is completely blocked when the trap files are accessed, the response is automatic, and the

low complexity of the solution. In their testing of the proposed tool, the authors found it effective in blocking ransomware attempts, but note that cyber defense is an area that is still being developed and recommend more research to fully develop an advanced line of defense against ransomware attacks.

This article is important for this study because it describes a new means of thwarting ransomware.

Orman, H. (2016). Evil offspring-Ransomware and crypto technology. *IEEE Internet Computing, 20*(5), 89-94. https://doi-org./10.1109/MIC.2016.90

Abstract. Note: this abstract was written by the author of this annotated bibliography in the absence of a published abstract. Crypto ransomware is increasingly clever. For anyone contending with crypto ransomware, it helps to know the options available to the malware writers and how they might be tripped up or deflected. It is an interesting new crime, one enabled by asymmetric cryptography, block-chaining systems, a large network of botnets, and the fact that no matter how much we may wish otherwise, the software that drives our computing devices always has exploitable bugs.

Summary. The author explores the history of ransomware and cryptography, and the evolution of the anonymity of the perpetrators who hide behind the attacks. The main recommendation the author provides to avoid ransomware attacks is making and storing offline backups . To avoid or thwart ransomware, the author recommends being wary of emails that can contain malware and using offline backup systems that do not overwrite the data for serval weeks, as this prevents the ransomware from infecting the backup. The author cautions against traditional on-premises backups because ransomware can encrypt any onsite storage solution.

The author posits that runtime execution monitors could be used to sample command traces in real time to determine if encryption was happening in anything other than SSL or other approved encryption programs and, if this occurred, look at the open file description to see if it is indeed ransomware and then notify the user.

This article is important for this study because it provides recommendations on how to avoid and thwart ransomware.

Parkinson, S. (2017). Use of access control to minimize ransomware impact. *Network Security, 2017*(7), 5-8. https://doi.org/10.1016/S1353-4858(17)30069-7

Abstract. The potential for financial gain has resulted in the establishment of a multi-billion-dollar ransomware industry founded on exploitation. Those with weak, unprotected systems, as well as those with little security-specific knowledge, are more likely to fall victim. Such users may not be able to adequately assess the potential risks and may be caught unaware. Those with the most to lose – for example, users who are heavily reliant on their IT system and its data for undertaking their daily business – heighten the potential for exploitation.

Summary. The author of this article discusses how damage is done while ransomware is in progress of encryption. Ransomware goes through a cycle in which applications are opened, modified to overwrite the original with an encrypted version, and stored. The author discusses how ransomware is executed on one of three ways: (a) by modifying the reference monitor, (b) by achieving privilege escalations and operating at maximum permission levels, or (c) by executing using end user credentials and depending on users with high level permissions.

The author provides recommendations for preventing ransomware, including giving end users less privileges, instituting separation of duty, auditing IT infrastructure, and control structure implementation. Giving end users low access and less administrator privileges would ensure less damage to the overall system if the user was hit by ransomware attacks. Separation of duties works by limiting the access users have to the access required to fulfill their duties; an example is making sure employees in accounting have access to accounting folders but do not have access to IT or engineering folders. This separation of duty helps to limit the damage caused by ransomware and makes diagnosing the cause and spread of ransomware easier.

Auditing involves removing old permissions when a user no longer needs them. The author notes that permissions are rarely checked or changed and notes that when employees leave or roles are changed those permissions are often left untouched. Auditing a system and re-evaluating policies and permissions can avoid potential exploitation during a ransomware attack.

Control structure implementation is the last and most important ransomware protection technique. Control structure implementation is conducted within the directory structure hierarchy; it ensures that data is restricted within the pyramid tree.

This article is important for this study because it offers in-depth and technical explanations of how to thwart ransomware.

Yaqoob, I., Ahmed, E., Rehman, M. H. U., Ahmed, A. I, A., Al-garadi, M. A., Imran, M., Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks, 129*(2), 444-458. https://doi.org/10.1016/j.comnet.2017.09.003

Abstract. With the increasing miniaturization of smartphones, computers, and sensors in the Internet of Things (IoT) paradigm, strengthening the security and preventing ransomware attacks have become key concerns. Traditional security mechanisms are no longer applicable because of the involvement of resource-constrained devices, which require more computation power and resources. This paper presents the ransomware attacks and security concerns in IoT. We initially discuss the rise of ransomware attacks and outline the associated challenges. Then, we investigate, report, and highlight the state-of-the-art research efforts directed at IoT from a security perspective. A taxonomy is devised by classifying and categorizing the literature based on important parameters (e.g., threats, requirements, IEEE standards, deployment level, and technologies). Furthermore, a few credible case studies are outlined to alert people regarding how seriously IoT devices are vulnerable to threats. We enumerate the requirements that need to be met for securing IoT. Several indispensable open research challenges (e.g., data integrity, lightweight security mechanisms, lack of security software's upgradability and patch ability features, physical protection of trillions of devices, privacy, and trust) are identified and discussed. Several prominent future research directions are provided.

Summary. The authors of this article discuss IoT or the Internet of Things and stress the fact that as society becomes more heavily reliant on its smartphones and technology, the IoT has grown to encompass applications beyond smartphones and into every aspect of the average citizen's life, making them more vulnerable and susceptible to ransomware. The IoT includes wearable technology, voice assisted applications, smart cars, smart homes, and health monitoring. The authors note that hackers can hack into personal devices and lock the devices until the victims pay the ransoms, the same way that hackers

penetrate a computer system and ask for a ransom from a single user or an entire organization. The basic underlying statement is that IoT is also extremely susceptible to malicious ransomware attacks and therefore, every user with a smartphone should be wary especially considering the copious amounts of private data kept on our personal devices. The authors make the point that IoT not only includes the devices users rely on every day, but also other machines and systems that are imperative to organizations such as life-support machines, manufacturing machinery, industrial robots, smart airplanes, smart cars, and smart railways.

The authors provide multiple solutions to mitigate ransomware:

- Immediately engage incidence response teams to limit the damage. The teams should immediately notify users and turn off infected devices.
- Deploy a backup device to run the network.
- Train users on how to respond to a ransomware attack.
- Make sure users install and update reliable security scanning software.
- Continuously back up IoT data to back-end servers.
- Prepare a backup of application and device configuration files.
- If the data is valuable, sometimes a ransom must be paid. On rare occasions, the device owner may negotiate with the hackers for a release of less data for a smaller payment.

This article is important for this study because it discusses how the connectivity of smartphones, tablets, sensors, and home devices are a concern for security threats and have the ability to start a ransomware attack if proper security techniques are not taken.

The authors also provide suggestions for how to thwart and respond to ransomware attacks on IoT devices.

Conclusion

Introduction

Ransomware is a specific type of malware (Green, 2017). Ransomware is the process of kidnapping private data or access to equipment by securing it against all who have legitimate access and offering to sell a key to restore access to the user (Allen, 2017). Activity related to ransomware is increasing; from 2015 to 2016 the number of ransomware attacks grew from 3.8 million to 638 million (Goldsborough, 2017). Since its establishment, ransomware has become a multimillion dollar crime and has hit large corporations, casinos, hospitals, schools, churches, and other organizations on a global scale (Allen, 2017). Ransomware has become a global threat; the May 2017 WannaCry attack locked up more than 200,000 computers in 150 countries (Young & Yung, 2017).

This annotated bibliography includes sources and research that help to identify best practices for organizations in avoiding ransomware attacks. Information is provided in the following categories: (a) history of ransomware, (b) damage to organizations from ransomware, and (c) best practices to avoid ransomware attacks.

History of Ransomware

Ransomware is a form of malware has been around for the past 30 years (Goldsborough, 2017). Young and Yung (2017) claim credit for the birth of ransomware arising out of a union formed by “a former hacker placed in a room with a cryptographer, both given ample time with which to contemplate the dystopia of tomorrow” (p. 24). Young and Yung (2017) presented what they claim is the first secure data kidnapping attack, which they named cryptoviral extortion, at the 1996 IEEE Security and Privacy conference. Since that time Young and Yung (2017) note

that the model they presented at the conference has grown into an estimated $1 billion annual industry known as ransomware.

Hampton, Biag, and Zeadally (2018) describe the four stages of ransomware as:

- *Infection*, where the victim's machine is infected when a compromised website is accessed or attachment is opened from a spam message.
- *Data encryption*, where the user's files or devices are locked down via cryptographic keys that utilize the Public Key Infrastructure (PKI) on either the infected machine or Command-and-Control server.
- *Demand*, where the ransomware software displays a message demanding payment of a ransom in order to release the locked data or files.
- *Outcome*, which is based on the actions taken by the victim. One potential outcome is that the victim does not pay the ransom but is able to eliminate the ransomware and recover the locked data or files. Another potential outcome is that the victim pays the ransom through anonymous channels such as Bitcoin and, hopefully, receives the key to unlock the data or devices. The final outcome is nonpayment of the ransom and subsequent destruction of the data or files; without a backup, the victim will suffer permanent loss.

Allen (2017) identifies three classes of malware: screen locking, encryption, and false threats. He defines screen locking ransomware as locking a computer screen and displaying a warning with instructions on how to resolve the ransom to unlock the screen. Ransomware that encrypts files does so without notification or warning for the end-user (Allen, 2017). False threats are described as warnings or notifications to the end-user without any real threat (Allen, 2017).

Hackers learn from experience and technological advances (CryptoLocker, 2014). Ransomware has been evolving into more advanced viruses which are becoming difficult to prevent (CryptoLocker, 2014). Ransomware is advancing into new ways of attacking users other than using email attachments and links; for example, a new form of malware has evolved which is being spread by USB-connected devices such as memory sticks and hard drives (CryptoLocker, 2014).

The popularity or ransomware is due to the ability of cyber thieves to determine new ways to make money from this type of malware (Goldsborough, 2017). Goldsborough (2017) notes that in 2016 there were 638 million ransomware attacks, with 400 different types of ransomware identified in 2017 – a number that is growing. Mansfield-Devine (2016) notes that ransomware attacks have shifted from targeting individuals to targeting businesses, since a business offers a greater potential ransom. Choudhary, Zavarsky, and Lindskog (2016) mention how attacks are evolving from different platforms and are no longer just focused on Windows; ransomware attacks have also been launched against Android devices.

As ransomware attacks continue to increase, governments have responded by creating regulations and laws to help protect citizens (Green, 2017). Green (2017) identifies regulations in the European Union (EU) that target cyber thieves, including the Data Protection Directive (DPD), which covers personal data collected by companies from consumers, and the General Data Protection Regulation (GDPR), a uniform law across EU that requires companies to notify victims of any data breaches within 72 hours. In response to multiple ransomware attacks within California, Young and Yung (2017) note a new law aimed at controlling the ransomware epidemic, “SB-1137 Computer crimes: ransomware,” which amends Section 523 of the Penal

Code. The law specifically outlaws the introduction of ransomware into any computer system with the goal of extorting money.

Damage to Organizations from Ransomware

One of the largest attacks to date was the San Francisco Municipal Railway (Muni) attack (Ransomware, 2016). This was a very well-known attack because it was conducted on a public transportation system for a popular city, and ransom demands were displayed on computer displays at Muni stations. The city lost an estimated $50,000 in fares because the Muni system was locked up and the organization was forced to open several fare gates, allowing riders to ride for free (Ransomware, 2016).

One famous attacks took place in Hollywood Presbyterian Center in California when hackers breached the hospital's servers and computer systems and locked the network down (Young & Yung, 2017). The hospital ended up paying $17,000 worth of bitcoins to regain access to their networks (Young & Yung, 2017). The WannaCry ransomware, which was a recent worldwide attack, affected 200,000 computers in 150 countries (Young & Yung, 2017). This attack also hurt the American government by exploiting a vulnerability that the United States National Security Agency (NSA) had already identified but chose not to report; once whistleblowers exposed the NSA's knowledge a patch was released (Young & Yung, 2017).

Another type of ransomware is delivered by clicking on advertisements (Malicious, 2014). One such *malvertising* campaign infected users with the CryptoWall ransomware who clicked on a malicious advertisement from such sites as Yahoo Finance, AOL real estate, and Match.com, exposing up to 3 million people per day to the attack and generating $25,000 per day for the cyber thieves (Malicious, 2014).

Ransomware attacks can net large sums very quickly (CryptoLocker, 2014). The CryptoLocker ransomware not only achieved 250,000 infections within its first 100 days, but estimates of damages range from $380,000 to millions of dollars (CryptoLocker, 2014). Brewer (2016) notes that the FBI estimates that 2016 losses associated with ransomware were $1 billion.

Best Practices to Avoid Ransomware Attacks

Allen (2017) provides a detailed description of how companies and everyday home computer users can protect themselves and their families from ransomware attacks. His recommendations for how to avoid ransomware include protecting equipment by not leaving devices unattended at random locations and making sure the equipment is locked up when away from the device (Allen, 2017). Allen (2017) notes issues with traditional passwords such as weak passwords that contain less than eight characters. To combat these weaknesses, Allen (2017) recommends the use of biometric access and facial recognition access.

Various procedures can help to avoid ransomware attacks; the simplest is to ensure users do not click on attachments unless the user is known (Goldsborough, 2017; Gómez-Hernández et al., 2018; Orman, 2016). Other recommendations include keeping systems and servers up-to-date with patches and updates (Allen, 2017; Brewer, 2016; Goldsborough, 2017; Gómez-Hernández et al., 2018), installing robust virus and malware protection software on all on-premise company servers and end user computers (Goldsborough, 2017), and controlling the use of macros and unused software (Goldsborough, 2017). Ensuring data is backed up regularly to external sources such as the cloud and tapes (Allen, 2017; Goldsborough, 2017; Gómez-Hernández et al., 2018; Orman, 2016), selecting offline backup systems that do not overwrite the data for several weeks (Orman, 2016), and using different types of backups in case one of them gets encrypted (Allen, 2017) are other means of avoiding the ill effects of a ransomware attack.

In addition to prevention, Brewer (2016) provides recommendations for how to detect, contain, eradicate, and recover from a ransomware attack. Brewer (2016) explains that companies can detect an attack early using special software that has alarms set for any intrusion so that the damage caused can be minimized. To contain ransomware, Brewer (2016) recommends having an endpoint protection system that can detect and kill ransomware that has already infected a device; these systems work by disabling network connectivity to prevent encryption of files on the network. Once a ransomware event has been acknowledged and contained, Brewer (2016) recommends eradicating the malware by replacing infected machines rather than attempting to clean them because residual files may still be hidden, waiting to re-infect devices. The last step is recovery, which includes replacing or cleaning systems and restoring drives and servers from local or cloud-based backups. Brewer (2016) also recommends conducting a full investigation after the attack to determine the specific type of ransomware and the vulnerabilities in the system that were exploited to allow the infection.

Gómez-Hernández et al. (2018) identify a honeyfile solution which blocks ransomware. Gómez-Hernández et al. (2018) define a honeyfile as a bait file that is intended for a hacker to access that then triggers an alarm. Once the trap files are accessed, countermeasures are automatically launched to block the infection. The honeyfiles also trigger alarms that notify systems administrators who can launch appropriate responses to the attack. Orman (2016) takes a different approach by suggesting that runtime execution monitors could be used to sample command traces in real time to determine if encryption is happening in anything other than SSL or other approved encryption programs and, if so, examine the open file description to see if it is indeed ransomware, notifying the user of verified infections.

Parkinson (2017) recommends preventing ransomware attacks by giving end users less privileges, ensuring separations of duty by limiting the access individual users have to only what is required, auditing IT infrastructure to remove outdated permissions, re-evaluating permission policies periodically, and implementing control structures within the directory hierarchy to ensure that data is restricted within the pyramid tree.

Yaqoob et al. (2017) focus on the special case of ransomware that targets Internet of Things (IoT) devices. Yaqoob et al. (2017) provide multiple solutions to mitigate ransomware:

- Immediately engage incidence response teams to limit the damage. The teams should immediately notify users and turn off infected devices. Additionally, a backup device should be deployed to run the network.
- Train users on how to respond to a ransomware attack.
- Make sure users install and update reliable security scanning software.
- Continuously back up IoT data to back-end servers.
- Prepare a backup of application and device configuration files.
- If the data is valuable, sometimes a ransom must be paid. On rare occasions, the device owner may negotiate with the hackers for a release of less data for a smaller payment.

Wrap Up

This annotated bibliography provides sources of recent, academic literature to advise the research questions of: What are best practices for organizations in avoiding ransomware attacks? This study focused on the history of ransomware, damage ransomware caused organizations, and best practices to avoid ransomware attacks. Ransomware has been in existence for almost 30 years and is gaining popularity due to the large payouts hackers receive (Goldsborough, 2017).

Ransomware attacks are worldwide and are targeted at both businesses and individuals (Choudhary, 2016). Attacks such as the worldwide WannaCry ransomware and the ransomware suffered by local Hollywood Presbyterian Center have cost organizations and individuals millions of dollars in damages (Allen, 2017). While the types of ransomware attacks are changing and becoming more sophisticated, there are also approaches that are offered to avoid attacks (Allen, 2017; Goldsborough, 2017; Gómez-Hernández et al., 2018; Parkinson, 2017; Yaqoob et al., 2017) and respond once infected (Allen, 2017; Brewer, 2016; Goldsborough, 2017; Orman, 2016; Yaqoob et al., 2017). The experts in this study were unanimous in noting that a passive approach to ransomware poses too great of a risk given the potential losses that may be incurred with a ransomware attack; both organizations and users must proactively plan to prevent and respond to ransomware attacks (Allen, 2017; Brewer, 2016; Goldsborough, 2017; Gómez-Hernández et al., 2018; Orman, 2016; Parkinson, 2017; Yaqoob et al., 2017).

References

Allen, J. (2017). Surviving ransomware. *American Journal of Family Law, 31*(2), 65-68. http://link.galegroup.com/apps/doc/A503308994/AONE?u=s8492775&sid=AONE&xid=c4edc6d7

Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. *Network Security, 2016*(9), 5-9. https://doi.org/10.1016/S1353-4858(16)30086-1

Choudhary, M., Zavarsky, P., Lindskog, D. (2016). Experimental analysis of ransomware on Windows and Android platforms: Evolution and characterization. *Procedia Computer Science,* 94, 465-472. https://doi-org.libproxy.uoregon.edu/10.1016/j.procs.2016.08.072

CryptoLocker success leads to more malware. (2014). Network Security, 2014(1), 20. https://doi-org/10.1016/S1353-4858(14)70012-1

Green, A. (2017). Ransomware and the GDPR. *Network Security, 2017*(3), 18-19. https://doi.org/10.1016/S1353-4858(17)30030-2

Goldsborough, R. (2017). The increasing threat of ransomware. *Teacher Librarian, 45*(1), 61. http://teacherlibrarian.com/2017/

Gómez-Hernández, J. A., Álvarez-González, L., and García-Teodoro, P. (2018). R-Locker: Thwarting ransomware action through a honeyfile-based approach. *Computers & Security, (73),* 389-398. https://doi.org/10.1016/j.cose.2017.11.019

Hampton, N., Baig, Z. & Zeadally, S. (2018). Ransomware behavioural analysis on Windows platforms. *Journal of Information Security and Applications, 40,* 44-51. https://doi-org/10.1016/j.jisa.2018.02.008

Malicious-advertising attacks inflict ransomware on victims. (2014). *Computer, 47*(12), 16-20. https://doi.org./10.1109/MC.2014.362

Mansfield-Devine, S. M. (2016). Ransomware: Taking businesses hostage. *Network Security*, *2016*(10), 8 – 17. https://doi.org/10.1016/S1353-4858(16)30096-4

Orman, H. (2016). Evil offspring-Ransomware and crypto technology. IEEE Internet Computing, 20(5), 89-94. https://doi-org/10.1109/MIC.2016.90

Parkinson, S. (2017). Use of access control to minimize ransomware impact. *Network Security*, *2017*(7), 5-8. https://doi.org/10.1016/S1353-4858(17)30069-7

Ransomware claims more victims. (2016). *Network Security*, *2016*(12), 2. https://doi-org/10.1016/S1353-4858(16)30110-6

Yaqoob, I., Ahmed, E., Habib ur Rehman, M., Ahmed, A.,Al-garadi, M., Imran, M., Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of things. *Computer Networks*, *129*(2), 444-458. https://doi-org/10.1016/j.comnet.2017.09.003

Young, A. L., & Yung, M. (2017). Cryptovirology: The birth, neglect, and explosion of ransomware. *Communications of the ACM*, *60*(7), 24-26. doi:10.1145/3097347