Ransomware and Its Impact on Modern Society

Charles Jones Jr.
Department of Computer Science
Hampton University
charles.jones2@my.hamptonu.edu

Jean Muhammad
Department of Computer Science
Hampton University
jeana.muhammad@hamptonu.edu

ABSTRACT

This research project discusses a common threat that is consistently present in the world that we live in today on the front of cybersecurity as well as cyberspace. Among all of the various cyber-attacks that exist in our world today, Ransomware has taken a front seat when discussing the different types of threats that create the potential to harm us users on a day to day basis. This form of threat is something that has been plaguing users for years and has caused financial manipulation for hospitals, businesses, and private citizens as well. This research project will discuss the threats that have been present in the past 5-10 years and will provide an in depth study of what occurred and what could have been done in order to prevent this type of attack from happening. The topic of risk assessment and vulnerability will be analyzed as well.

CCS CONCEPTS

• **Security and privacy → Software and application security** → Software security engineering; • **Software and its engineering**

KEYWORDS

Ransomware, Malware, Security

ACM Reference format:
C. Jones, J. Muhammad. 2017. Ransomware and Its Impact on Modern Society. In *Proceedings of 2017 ADMI Symposium*, Virginia Beach, Virginia USA, March 23-26, 2017.

1 INTRODUCTION

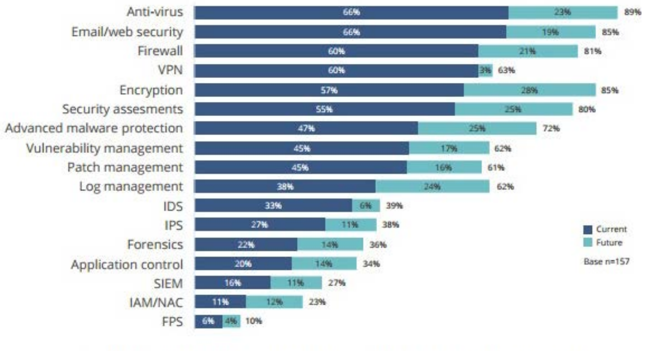
Ransomware is a pedigree of malicious software that has been around for decades. As a matter of fact, one of the first ransomware attacks originated back as early at the 1980's. Most of these attacks occur when dealing with public places of business as well as federal governments. One of the most common organizations that are victims to ransomware attacks are public hospitals and health systems across the United States.

Ransomware, malicious software or applications that make threats both idle and actual towards users of a particular application or service. This malicious software demands the targeted user and or entity to pay an enormous sum of money in return for the release of their personal documentation and or records back to them. These forms of attacks occur frequently in the United States and across overseas as well. The primary targets of some of the most recent attacks are primarily hospitals and personnel management offices as well as public record entities as well. There have been a total of 53,000 ransomware attacks in March 2016 alone according to Symantec. This number fluctuated a lot in the early months of January and February but since the appearance of "Locky" in email chains and messages, the number has increased. Symantec classifies "Locky" as a family of malware that is facilitated within ransomware to help steal and scam money from un-suspecting users.

In Quarter 1 alone of this year, $209 million dollars was paid to ransomware criminals. The average ransom demand this year is $649 which is significantly higher than the average figure in 2015. With the nature of these ransomware attacks happening all over the world, the question of security and recovery come into account. According to Barkly, less than half of ransomware victim's backup their data on a regular basis. Most backups fail because they are either unmonitored, the backups fail for unspecified reasons and loss of encrypted backup drives. Of the 100 percent of ransomware victims, only 5 percent of those attacked actually consider paying the ransom as an option to recover their stolen data.

2 BACKGROUND

Ransomware is common malicious software that can be used to exploit money from other users and it doesn't determine who is a potential victim or who isn't. Everyone can be a victim and everyone can be a potential target of ransomware. Most ransomware is implemented using some sort of advertisement or some form of spam attachment added onto an email that the user is most commonly unaware of. The attachments and advertisements make it difficult because we see advertisements every day whether it is on YouTube or just on the internet. We as users often overlook advertisements because they are tailored to us the user so that we can continue to use the online application or service for free and not have to forfeit a monthly payment or a yearly payment.



Which of the following other security services do currently invest/do you plan to invest in in the next 12 to 24 months?

Figure 1: Security Services Used by Healthcare Organizations

Figure 1 is a current bar graph of what companies and organizations are doing in order to protect themselves from ransomware attacks. The darker blue bar illustrates current strategies where the light blue bar represents future implementations/course of action that these same companies plan on taking in the upcoming months and or years.

The following categories consist of: Antivirus, Email/web security, Firewall, VPN, Encryption, Security Assessments, Advanced Malware Protection, Vulnerability Management, Patch Management, Log Management, IDS, IPS, Forensics, Application Control, SIEM, IAM/NAC, and FPS.

Table 1. Overall percentages of Current and Future Implementations.

Implementation	% Current	% Future
Anti-virus	66	23
Email/Web Security	66	19
Firewall	60	21
VPN	60	3
Encryption	57	28
Security assessments	55	25
Advanced Malware Protection	47	25
Vulnerability Management	45	17
Patch Management	45	16
Log Management	38	24
IDS	33	6
IPS	27	6
Forensics	22	14
Application Control	20	14
SIEM	16	11
IAM/NAC	11	12
FPS	6	4

These are just some of the basic/advanced techniques that companies and organizations use to protect themselves from daily threats on their networks and classified files. There are a variety of other protection methods as well but these are some of the most popular across the board.

With ransomware, the question comes into account of just how much ransomware truly exists and where does it stem from in terms of topology and hierarchy? There are a variety of ransomware families that currently exist and are on record in today’s society. The most known families of ransomware include:

ACCDFISA stands for Anti Cyber Crime Department of Federal Internet Security Agency Ransom. This particular type of ransomware encrypts files into a password-protected; Cybercriminals behind this ransomware asks payment thru Moneypak, Paysafe, or Ukash to restore the files and unlock the screen; Known as a multi-component malware packaged as a self-extracting (SFX) archive.
What this means is that your information is taken from your computer and encrypted with a password that only the malicious user knows and uses faulty payment methods to demand the money or monetary funds from the user.

ANDROIDOS_LOCKER was the first ransomware spotted in the mobile arena. This software uses a service known as Tor that allows for both private and anonymous server connections. This ransomware also leaves hidden files on your mobile device that can render your mobile device useless as well as the important data contained on it useless as well.

CRIBIT is also known as BitCrypt uses RSA encryption algorithms to and adds the string bitcryp to the file that it has infected. CRIBIT is also an extension/variant of CRILOCK ransomware family.

CRILOCK employs a DGA (Domain Generation Algorithm) server connections. This ransomware is also known as CryptoLocker. Further investigation found that this ransomware was found to be a part of spam mail that downloads another form of ransomware knowns as ZBOT.

CRITOLOCK uses a cryptosystem that writes the word Cryptology in the infected users wallpaper and changes code to change the users wallpaper at any given point in time.

CRYPAURA encrypts files and attaches email addresses and contact information for decryption. The common email address associated with this ransomware is paycrpt@aol.com

CRYPCTB encrypts files and ensures that there is no way to recover encrypted files by deleting traces of itself copies. Most common in spam emails in the form of an attachment. Prime user of social engineering to trick users into opening the attachment.

CRYPDEF short abbreviation for CryptoDefense. Unique version of ransomware that demands the users to pay the money that is being requested to be paid using bitcoin currency.

CRYPTCOIN demands users to pay in bitcoin in order for the files to be decrypted. One free test is offered to the users in order to decrypt their files.

CRYPTFILE utilizes public key RSA encryption and demands 1 bitcoin to obtain the private key in order to decrypt the files.

CRYPWALL sent through email and is contained within spam attachments. This ransomware also comes equipped with multiple versions of spyware attached to it. This type also follows an updated ransom note.

CRYPTROLF displays a troll face post encryption of your files.

CRYPTTOR changes the wallpapers on desktops to illustrations of walls and then prompts the user to pay the ransom in order to pay the amount that the user is asking for.

CRYPTOR is a batch file type ransomware that possesses the capabilities of encrypting user files using an application known as Privacy Guard.

DOWNCRYPT comes to the user via spam email that creates decoy documents to persuade the user that none of their documents have been stolen or tampered with.

VIRLOCK tampers with document files, user archives, batch files and media files such as images and photos.

PGPCODER first ransomware discovered back in 2005. Also the first ransomware that was seen by enforcement.

KOLLAH encrypts files using certain extension names; Target files include Microsoft Office documents, PDF files, and other files deemed information-rich and relevant to most users; Adds the string GLAMOUR to files it encrypts

KOVTER attack launched from ads that are embedded on YouTube advertisements lead to a Sweet Orange exploit kit.

MATSNU asks for ransom upfront by locking the screen and possesses other screen locking capabilities as well. This form of attack is a backdoor attack.

RANSOM generic detection for application that prevent users from fully accessing their workstations or systems. Encrypts some files and demands money in order to decrypt files and or unlock the infected machine.

REVETON this ransomware is also known as Police Ransom. Locks the screen using a faulty display that displays a dialog box that the user has violated or broken federal law. Determines that the IP address of the victim’s machine has been identified by the Federal Bureau of Investigation and that the user has visited websites that have illegal content on them.

LOCKY Renames encrypted files to hex values; Attaches .locky to files it encrypts; Arrives via spam with macro-embedded .DOC attachment, similar to the arrival of other forms of ransomware also. One of the most common forms/variants of ransomware that are seen in today’s society.

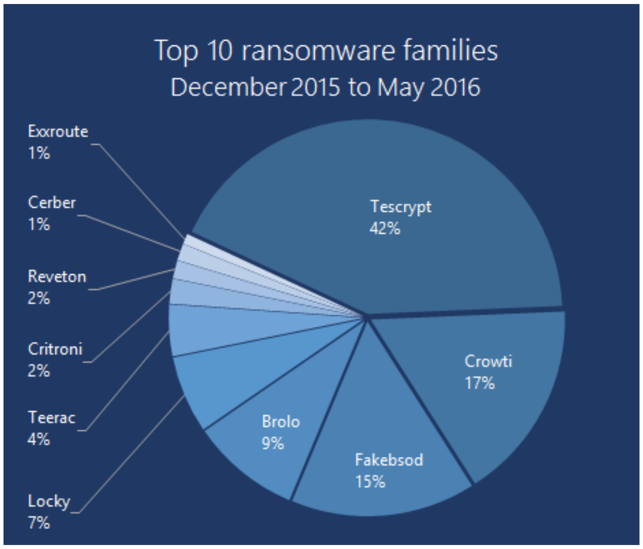


Figure 2: Top 10 ransomware families December 2015 to May 2016 [3].

According to Figure 2 [3], the Top 10 most common ransomware families from December 2015 to May 2016 were:

- Tescrypt – 42%
- Crowti – 17%
- Fakesbsod – 15%
- Brolo – 9%
- Locky – 7%
- Teerac – 4%
- Critroni – 2%
- Reveton – 2%
- Cerber – 1%
- Exxroute – 1%

This pie chart illustrates the Top 10 most common used ransomware families and types. There are a variety of types and variants of ransomware that are openly utilized and accessible to the general public but these just mentioned are the ones that are commonly used by malicious users according to Microsoft.

With these different types of Ransomware that are stealing information from others. The question comes to mind of what larger scale companies do to protect themselves from Ransomware attacks and threats. The answer to this question is

Risk Assessment. With Ransomware comes a huge emphasis on Risk Assessment in which the methodology focuses heavily on analyzing potential risk factors of day to day activities and operations within an organization or department.

Most organizations use it when working with the Software Development Life Cycle. The reason for this is to protect the assets that the company has when developing new software or application. By putting a strong emphasis on Risk Assessment, this ensures that proper measures are taken when sharing information back and forth between employees and other departments involved when dealing with the Software Development Life Cycle. According to the National Institute of Standards and Technology (NIST), Risk Management Guide for Information Technology Systems, Risk is defined as Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. The risk assessment methodology consists of nine steps that can be outlined below:

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

3 SYSTEM CHARACTERIZATION

The first step of the System Characterization consists of inputs and outputs along with the rest of the steps. The inputs for this step consist of Hardware, Software, System interfaces, Data and information, people, and system mission. These key factors inputted into this step yield the output of System boundaries, System functions, System data and criticality and System and data sensitivity. In addition to the inputs and outputs when assessing risk, it is important to define the scope of the effort. Boundaries are established as well as resources and information that will constitute the system as a whole. Additional information used at an operational capacity consists of functional requirements, users of the system, system security policies that govern the overall Information Technology system, System security architecture.

In addition to this is the current network topology, information storage protections that provides the safeguards. Flow of information pertaining to the system, technical controls used for the system, management controls, operational controls, physical security environment and environmental security that is implemented. System Characterization also comes with Information-Gathering Techniques which include Questionnaire and On-site Interviews. These two techniques give a good snapshot of the security of the system and if it's really performing to its highest level. When this information is collected it then proceeds to Document Review which is done by using legislative documentation and directives. Use of Automated Scanning Tools is useful as well in this situation because even without the paper-gathering techniques, it is still possible to gather information on a system that they are responsible for.

4 THREAT IDENTIFICATION

The inputs for this step include the History of system attack and Data from intelligence agencies. The output is the Threat Statement. A threat is the potential for a threat-source to successfully exploit vulnerability. Vulnerability is a weakness or flaw in a system that can be accidentally triggered. When considering risk, it is important to determine thereat-sources, potential vulnerabilities in place and existing controls and protocols. A threat source is identifying as either (1) intent and method targeted at eth intentional exploitation of vulnerability or (2) a situation and method that may accidentally trigger vulnerability. The next major component of this process is the Threat Source component. The threat source component is about circumstances or events that can harm an Information Technology System. There are 3 categories of threat sources.

- Natural threats which are classified as floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, etc.
- Human Threats which are enabled by human beings inadvertently entering data to sabotage an Information Technology System, malicious software upload, unauthorized access, etc.
- Environmental Threats such as power failure for a long period of time, chemicals, pollutions or a leakage of liquid.

Humans are a potentially risky threat source because humans are motivated by threat environments and customizing human threat statements. Utilizing threat reports to determine and potentially predict threat behavior is something that has come in handy when dealing with this step.

5 VULNERABILITY IDENTIFICATION

There are a variety of vulnerability identification factors that are seen as critical. The types of vulnerabilities associated with the Information Technology System depend on the nature of the system itself. Certain rules govern what action should be taken in this step. If the system has not yet been designed, the search for vulnerabilities should concentrate on the security policies of the organization, security procedures, system requirement definitions, vendor and developer's product analysis. If the system is being implemented the identity of vulnerabilities should to expanded to include more specific information including security features described in the security documentation and results of the security certification test and evaluation. If the system is up and running, then the analysis of the IT system security features and security controls, technical and procedural should be used to protect the system. A table of Security Criteria can be found in Table 2:

Table 2: Security Criteria

Management Security	• Assignment of responsibilities • Continuity of support • Incident Response Capability • Risk Assessment
Operational Security	• Control of air-borne contaminants • Controls to ensure electrical power supply • Humidity Control • Temperature Control
Technical Security	• Communications • Cryptography • Discretionary access control • Identification and authentication • Object reuse • System audit

When this process is complete, a security requirements checklist is created. However, with this security checklist comes with directives and government regulatory sources that have to be adhered to when developing such a document. The following examples of government regulatory include:

- Industry practices
- Security Policies, guidelines and standards
- Privacy Act of 1974
- OMB November 2000 Circular A-130
- Federal Information Processing Standards Publications
- CSA of 1987

The Questionnaires and information gathering documents are very important because they provide accurate information about the security of the system and where improvements can be made to prevent further intrusions and remediate certain vulnerabilities within a system. The inputs for this step include reports from prior assessment of risk, audit comments, security requirements, and security test results. From these four categories of inputs for the Vulnerability Identification step a list of potential vulnerabilities can be compiled and adhered to in order to prevent certain vulnerabilities from occurring.

6 ANALYSIS

6.1 Control Analysis

The primary objective of this step is to analyze controls that have been implemented or are in the process of being implemented. This is to eliminate threats exercising a vulnerability system. This leads into the next category known as control methods. Security controls utilize both technical and nontechnical methods. Technical controls serve as safeguards that are implemented into computer hardware, software, or firmware. Nontechnical controls serve at more of a managerial and operational capacity for instance security policies, operational procedures, physical and environmental security as well as personnel. Control categories for technical and nontechnical are categorized based off of control categories. These two categories are known as Preventive and Detective.

- ***Preventive*** controls attempt to violate security policy and controls to access enforcement, authentication, and encryption.
- ***Detective*** controls are used to provide alerts for violations of attempted security policy and include audit trails, detections methods, etc.

6.2 Likelihood Determination

The ***likelihood determination*** indicates overall probability of how often vulnerability is going to happen in an associated threat environment. These overall determinations are based off of the following factors:

- Nature of Vulnerability
- Threat motivation and capability
- Existence and effectiveness of current controls

Likewise, the likelihood definitions are based upon three categories which are known as Low, Medium, and High. Each quality is known by overall motivation and capability.

- Low: threat source lacks capability and proper controls are in place to prevent or impede the vulnerability
- Medium: Threat source motivated and capable but controls are in place to impede successful exercise of the vulnerability.
- High: Threat source highly motivated and prior existing controls are in place but aren't proving to be effective.

6.3 Impact Analysis

This step of the Risk Assessment process elaborates on security goals and the potential consequences that a company can face if they are not met when dealing with vulnerabilities. The three goals that serve as significant importance are:

- ***Loss of Integrity***: Requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
- ***Loss of Availability***: If a mission-critical Information Technology system is unavailable to its end users. Loss of system functionality and operational effectiveness, may result in loss of productive time, thus hindering the end users' performance of their functions in supporting the organization.

- ***Loss of Confidentiality***: System and data confidentiality refers to the protection of information from unauthorized users. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Table 3. Severity when each security goal was not met:

Level	Severity
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Attacks of 2016. According to the figure below provided by Symantec, there has been a significant in Ransomware infections from January 2015 to April 2016. In January 2015, there were approximately 40,000 infections and in February of 2016 that number increased to almost 60,000 ransomware infections.

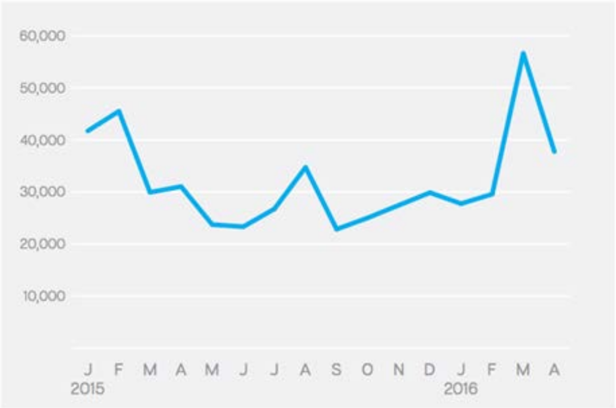


Figure 4: Overall Ransomware Infections by Month from January 2015 to April 2016.

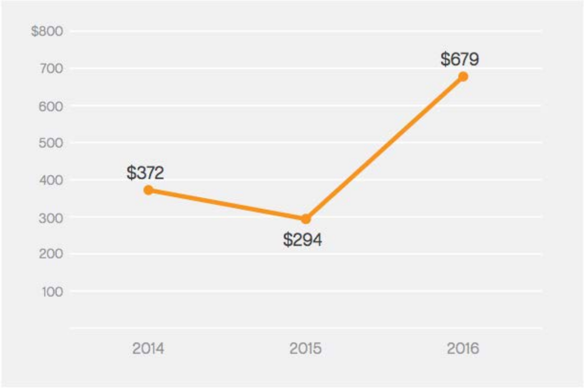


Figure 5: Average Ransom Amount in US Dollars by Year

According to the Figure above, in the year 2014, the average of a typical ransom was $372 and that number steadily decreased to $294 in 2015 and then more than doubled in 2016 at $679 as the average amount per ransom.

Most Used Form of Delivery. Ransomware has been found to ultimately be used by email and by attaching the ransomware to the attachments and to advertisements. Osterman Research conducted a statistic on the Applications by Which Ransomware Entered the Organization. According to their research, 31% of ransomware comes from being embedded in Email links, 28% in email attachments, 24% from a Web site or Web application other than email or social media, 4% from social media, 3% from USB stick, 1% from Business applications, and 9% from unspecified anomalies.

6 CONCLUSION AND RECOMMENDATION

When it comes to Ransomware, it is very essential that we continue to educate students and that we as modern day users of technology continue to emphasize the importance of ethics within our colleges and universities and professional conduct within the workplace. A main characteristic is personal ethics and the act of trusting people with sensitive information at both the classified and proprietary levels and ensuring that the information that is being released is going through the proper channels.

At Hampton University, we reached out to a systems administrator for the computer center on campus as to what measures the university takes towards preventing Ransomware and they stated: "*We do not use Ransomware software for an anti-virus on campus, we only use windows defender and Symantec Endpoint for malware and anti-virus software*."

In addition to the Systems Administrator at Hampton University, we also received feedback from Dr. Danny T. Barnes of the Computer Science Department at Hampton University stating that: "*There is not much that can be done in regards to Ransomware. One critical precaution that needs to be taken when dealing with Ransomware is ensuring that your system is backed up properly and frequently*."

Some of the preventive measures that have been proposed and implemented by the Federal Government have been:

- Awareness Training Program
- Strong spam filters on email traffic and file sharing.
- Scanning incoming and outgoing email traffic
- Proper configuration of firewalls used to block malicious IP addresses.
- Proper patch management on operating systems and firmware updates of business applications.
- Anti-Virus and Anti-Malware programs for conducting regular scans.
- Managing privileged accounts: ensuring that those users who need administrative access and elevated privileges have that access and don't abuse that access for personal gain.

Acknowledgement
This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program under grant no. DGE-1303409 (PI/co-PI: Dr. Chutima Boonthum-Denecke, Dr. Jean Muhammad).

REFERENCES

[1] Incidents of Ransomware on the Rise. (2016, April 29). Retrieved December 12, 2016, from https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

[2] Snell, E. (2016, May 19). Healthcare Ransomware, Connected Devices Top Security Issues. Retrieved December 12, 2016, from http://healthitsecurity.com/news/healthcare-ransomware-connected-devices-top-security-issues

[3] Ransomware. (n.d.). Retrieved December 12, 2016, from https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

[4] Risk Management Guide for Information Technology Systems[PDF]. (2002, July). Gaithersburg, MD: National Institute of Standards and Technology.

[5] Ransomware What It Is and What To Do About It[PDF]. (n.d.). U.S. Department of Homeland Security.

[6] How to Protect your Networks from Ransomware[PDF]. (n.d.). Department of Justice.

[7] Understanding the Depth of the Global Ransomware Problem[PDF]. (2016, August). Black Diamond, Washington: Osterman Research.

[8] An ISTR Special Report: Ransomware and Businesses 2016 [PDF]. (n.d.). Symantec.

[9] Ransomware. (n.d.). Retrieved December 12, 2016, from http://www.trendmicro.com/vinfo/us/security/definition/ransomware

[10] Goldsborough, R. (2016). Protecting yourself from ransomware. Teacher Librarian, 43(4), 70

[11] Anonymous. (2016). Ransomware: Threat and response. Network Security, 2016(10), 17-19. doi:10.1016/S1353-4858(16)30097-6

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

[13] Everett, C. (2016). Ransomware: To pay or not to pay? Computer Fraud & Security, 2016(4), 8-12. doi:10.1016/S1361-3723(16)30036-7

[14] Anonymous. (2016). Hospitals become major target for ransomware. Network Security, 2016(4), 1-2. doi:10.1016/S1353-4858(16)30031-9

[15] Kenyon, B., & McCafferty, J. (2016). Ransomware recovery. Itnow, 58(4), 32-33. doi:10.1093/itnow/bww103