Issues in
Informing Science +
Information Technology

An Official Publication
of the Informing Science Institute
InformingScience.org

IISIT.org

Volume 14, 2017

Ransomware: A Research and a Personal Case Study of Dealing with this Nasty Malware

Azad Ali Indiana University of Pennsylvania, Indiana PA Azad.ali@iup.edu

* Corresponding author

NOTE: This paper is a follow-up on an article by Ali, Murthy, & Kohun (2016) that was published in *Issues in Information Systems*.

Abstract

Aim/Purpose Share research finding about ransomware, depict the ransomware work in a format that commonly used by researchers and practitioners and illustrate personal case experience in dealing with ransomware.

Background Author was hit with Ransomware, suffered a lot from it, and did a lot of research about this topic. Author wants to share findings in his research and his experience in dealing with the aftermath of being hit with ransomware.

Methodology Case study. Applying the literature review for a personal case study.

Contribution More knowledge and awareness about ransomware, how it attacks peoples' computers, and how well informed users can be hit with this malware.

Findings Even advanced computer users can be hit and suffer from Ransomware attacks. Awareness is very helpful. In addition, this study drew in chart format what is termed "The Ransomware Process", depicting in chart format the steps that ransomware hits users and collects ransom.

Recommendations for Practitioners Study reiterates other recommendations made for dealing with ransomware attacks but puts them in personal context for more effective awareness about this malware.

Recommendation for Researchers This study lays the foundation for additional research to find solutions to the ransomware problem. IT researchers are aware of chart representations to depict cycles (like SDLC). This paper puts the problem in similar representation to show the work of ransomware.

Impact on Society Society will be better informed about ransomware. Through combining research, illustrating personal experience, and graphically representing the work of ransomware, society at large will be better informed about the risk of this malware.

Accepting Editor: Eli Cohen │ Received: November 29, 2016 │ Revised: January 18, March 2, 2017 │ Accepted: March 28, 2017.

Cite as: Ali, A. (2017). Ransomware: A research and a personal case study of dealing with this nasty malware. *Issues in Informing Science and Information Technology Education, 14,* 87-99. Retrieved from http://www.informingscience.org/Publications/3707

Future Research Research into solutions for this problem and how to apply them to personal cases

Keywords Ransomware, Malware, Crypto 3, Crypto 4, Computer ransom

INTRODUCTION

> If Ron Howard were to remake his 1996 film ransom today, instead of Mel Gibson passionately screaming "Give me back my Son!" in response to the kidnapper's demand, he very well could have Gibson scream "Give me back my files!" in response to cybercriminal's demands for ransom (Solander, Forman, & Glasser, 2016, p. 53).

The quotation above reflects a dichotomy between two kidnapping crimes examples: one happens in the real world and the second take place in cyberspace. Lemos (2015) noted the following about the first type of crime "IN THE REAL world kidnapping is a risky crime – getting paid usually means getting caught" (p. 45). Yet the kidnapping crimes in cyberspace is becoming more popular, it is on a sharp rise in terms on number of attacks and losses they cause and they also *leave* many who were infected with it in chaotic situations (Constantin, 2016, Heater, 2016, Tutle, 2016). This ransomware problem is becoming so severe that many call these the people who infect computers as criminals or cyber criminals (Bhardwaj, Avasthi, Sastry, & Subrahmanyam, 2016) and the whole operation is called by some as "cyber extortion" (Goldsborough, 2016). The point to emphasize is that this problem is becoming big and awareness of this ransomware may be helpful to avoid it.

The author of this paper illustrates his experience in dealing with ransomware after getting one of his family computers infected with the malware and after losing valuable data files. The purpose of this paper is to share knowledge about this malware, raise awareness about the risk of this malware and a hope to find a solution for data our family lost. The remainder of this paper is divided into the following sections:

- The first section explains about Ransomware, the meaning of it, a brief historical background, and some additional information about it
- The second section describes the ransomware process – the steps that it takes from the first time that a computer is infected with a virus to the last step where users pay ransom and get their files back. Often many do not pay the ransom and may end up losing their files.
- The third section illustrates the experience of the author in how he unknowingly downloaded the malware, how it encrypted files, and how he did not pay the ransom and his data files remain encrypted. It also explains the dealing in the aftermath of infected with ransomware.
- The last section provides a summary of the study and suggested cautionary recommendations in dealing with this malware.

ABOUT RANSOMWARE – A LITERATURE REVIEW

This section reviews literature about ransomware, the meaning of it, a brief history on how it developed, and some stories from people who were infected with this malware and additional information. The purpose of this information is to shed light and give basic knowledge about this malware so to establish a basic understanding as we go into the next section when we discuss the ransomware process.

RANSOMWARE AS DEFINED

Ransomware came from two words ransom and ware. Webster's dictionary defined Ransom as "money that is paid in order to free someone who has been captured or kidnapped" ("ransom," 2016) and as "a consideration paid or demanded for the release of someone or something from captivity". At the same time, Webster's dictionary likened the word "ware" with "aware and gave example of their use in a sentence "was ware of black looks cast at me" ("ware," 2016). So the meaning for the word is that someone is holding something, is making others aware that he/she is holding a person, and is making a demand for a payment in order for the person held hostage be released.

This knowledge of the two words (ransom and ware) as understood in life brought into the cyber technology field. Different people have defined ransomware from different points of view and addressed them at various stages. Glassberg (2016), for example, provided a simple definition of ransomware and described it as, "A type of computer malware that uses encryption as its weapon" (p. 22). Although the definition explains an important component in ransomware – that is using encryption – it is not comprehensive enough to provide additional information about holding files, paying ransom, and then possibly returning the functions of the files.

O'Gorman & McDonald (2012) provided a more comprehensive definition as "a category of malicious software which, when run, disables the functionality of a computer in some way. The ransomware program displays a message that demands payment to restore functionality. The malware, in effect, holds the computer ransom."(p. 2). This definition explains ransomware when it disables computer functionality and later called it an "extortion racket" but specific information is lacking here regarding the ransom paying for holding the computer ransom.

Ransomware in other cases can do specific damage to the computer data files. Although it can hit any file on the computer, ransomware often target specific files types. Luo and Liao (2007) explained that ransomware targets files with the following file name extension: .txt, .doc, .rft, . ppt, .cbm, . cpp, . asm, .db, .db1, .db1, .dbx, .cgi, .dsw, .gzip, .zip,, jpeg, .key, .mdb, .pgp, .pdf.

Perhaps, the most comprehensive definition is the one provided by the Cyber Threat Alliance. This alliance is a group of cyber security firms formed in 2014 to keep track cyber threats. In their first report published in 2015, the Cyber Threat Security Alliance (2015) introduced the following definition of ransomware:

> Ransomware is a type of malware that encrypts a victim's files and subsequently demands payment in return for the key that can decrypt said files. When ransomware is first installed on a victim's machine, it will typically target sensitive files such as important financial data, business records, databases, personal files, and more. Personal files, such as photos and home movies, may hold sentimental value to the victim (p. 2)

Ransomware - A Brief History

There are different accounts regarding the dates that ransomware started to infect computers, the shape in which it started, the amount of money they used to charge to give back access to data, and the geographical regions they emerged from. The difference in accounts may largely be because ransomware started small, it emerged in different format than what we witness now, and its' mechanism of spreading and collecting money was different too.

Glassberg (2016), for example, noted that ransomware has been around for many years but did not suggest a date for the starting of this malware. Hampton and Baig (2016) on the other hand explained that although money extortion from users has been evolving for three decades, these activities remained "unsophisticated" until 2011 when cyber criminals learned to lure users to their web sites, download the malware, encrypt files, and then extort money from users. Kharraz, Robertson, Balzarotti, Bilge, & Kirda (2015) explained that that ransomware started to appear around 2004 but the volume of ransomware attacks was not significant until about ten years later when ransomware made major headlines news in 2013.

Salvi and Kerkar (2016) provided more details on the first appearance of ransomware. They explained that extorting money from computer malware dates back to 1989 when the first malware infected computers by replacing the old "autoexec.bat" file with a different file. The new "autoexec.bat" would be waiting for some time before it loced the computer and displayed a message demanding payment. Salvi and Kerkar explained further that the computer would remain locked until a post office box in Panama received a payment and then they sent a floppy disk that contained the solution to the locking problem.

The points that can be concluded from the above is that ransomware started to take the shape that we see now sometime between the years 2012-2014. This evidenced by two reports published by Cyber Threat Alliance (2015) and Cyber Threat Alliance (2016). Both reports suggested that Cryptowall 3 and Cryptowall 4 (variations of ransomware) started to appear in the years 2014 and 2015 separately.

Various reports note differently regarding amount of money gathered from ransomware attacks. The American Bankers Association (2016), for example, estimated that the amount collected for releasing the decryption key from ransomware attacks can range anywhere from couple hundred to thousands of dollars depending on who was infected with the malware. Salvi and Kerkar (2016) provided specific information on the amount charged when cyber extortion first started. They noted that the first ransom collected from victims was in 1989 when they had to mail $189 to PC Cyborg Corp. at a post office box in Panama. That price has changed as communication became easier over cyberspace and different digital currencies have emerged in the exchange of money.

The author found through literature review that in most cases the price asked was equal to one bitcoin (about $500) (Everrett, 2016, Heater, 2016, Hampton & Baig, 2015, Lemos, 2015). Salvi and Kerkar (2016) echoed similar numbers and noted that ransomware attackers demand anywhere from $300-$500 in return for releasing the decryption key and the return the functionality. That asking remained the same even for mac users. Heater (2016) found that ransomware for mac started to appear in the market suggesting a $500 ransom to release the data.

In other cases, there were different extreme numbers that listed as asking price for releasing access to encrypted data. Everett (2016) for example noted that a hospital infected with malware was initially asked to pay $3.5 million in ransom but then the hospital negotiated it down to $17,000.

There were also different accounts on the geographical location ransomware started from and how it spread to different locations. Glassberg (2016) suggested that ransomware was limited first to Russia and Eastern Europe. O'Gorman and McDonald (2012) explained that ransomware first appeared in Russia/Russian speaking countries in 2009, it spread to Western Europe and then to the United States and Canada around 2010. The points above shared one knowledge about the original place where ransomware started from – Russia and Eastern Europe. However, there was a different account about a group that held hospital data hostage. The group claimed that they originated in Turkey (Everett, 2016).

Table 1: Comparison of Top Hit Countries - Source Cyber Threat Alliance (2015)

CryptoWall v3	CryptoWall v4
United States	United States
Canada	India
United Kingdom	Canada
Australia	Mexico
Russia	United Arab Emirates
Germany	France
India	Romania
Italy	Taiwan
France	Jamaica
Netherlands	Bulgaria

Although ransomware may have started invading computers in Russia and Eastern Europe, that has changed. Ransomware attacks are now common in all G20 countries (Glassberg, 2016) and the United States is now the top-targeted nation for Ransomware attacks. The Cyber Threat Alliance (2015) listed the countries that were mostly hit by the two variations of ransomware, CryptoWall 3 and CryptoWall 4. Table 1 shows this list by CyberThreat Alliance:

Stories and Number to Tell About Ransomware

Bhardwadj et al (2016) suggested that ransomware and alike cyber-criminal activities affect end users for digital extortion at a scale never seen before. Nevertheless, the extent of the damage caused by ransomware attacks may be further clarified by reading stories and listing numbers about ransomware. Thus, this section lists below some stories and numbers about ransomware and the havoc they created in the life of many:

- The American Bankers Association (2016) estimated that $18 million was lost to ransomware attacks between April 2015 and June 2016 for individuals and businesses.
- Everett (2016) explained that ransomware based on reporting incidents is about $70 million per year. Everett also predicted that more incidents are not reported, and that taking into considerations both reported non-reported incidents, ransomware is about $200 million enterprise.
- The Cyber Threat Alliance (2015) reported that during the period from November 2015 to June 2016 7.1 million attempted infections spread across the globe. The peak of one day of ransomware hits reached 228,496.
- O’Gorman and McDonald (2012) noted “An investigation into one of the smaller players in this scam identified 68,000 compromised computers in just one month, which could have resulted in victims being defrauded of up to $400,000 USD” (p. 1). The same study noted that a larger gang used a different malware that intended to infect 500,000 computers over a period of 18 days.
- Heater and Baig (2015) predicted that the year of 2016 will be the “year of ransomware” and justified using this name for the year due to increasingly high profit examples of ransomware attacks that took place in the year before.
- Tuttle (2016) explained about a story of high-profile example when reporting on the Hollywood Presbyterian Medical Center. The computer network of this medical center was brought to a halt because of a hit by ransomware. This affected network-related functions, including CT scans, lab work, pharmaceutical activity, and patient records. Only after paying a ransom of $17,000, the hospital was able to retrieve the functionality of their computer network. The paying price negotiated down from millions that initially demanded after the initial ransomware attack.
- Lemos (2015) called ransomware “an escalating epidemic” and reported that between mid-March and August 2014 it infected more 600,000 systems worldwide. Lemos also gave an example of a company when hit with a ransomware. They later found more than 200 ransom notes on different places on their network directing them to pay $500 in order to return the functionality of their system.
- Everett (2016) noted that the number of ransomware attacks were doubled in the past twelve months compared to a year earlier and predicted that it will double again the following year. Everett explained that ransomware is precise in selecting targets. For example, they select florist shops before Valentine’s Day because they know the heavy traffic these shops experience in that period forces them to pay the ransom.

- A study conducted to "look under the hood of ransomware attacks" noted that ransomware attacks increased by 500% in 2013 compared to the year before. It further suggested that this malware infected about 250,000 computers including a police department that ended paying a ransom to decrypt their computers and return their data (Kharraz et al, 2015).

A final note that explains the real risk posed by ransomware is found in the quotation listed by Heater (2016) where it said, "Ransomware can hit anyone, but hackers are increasingly targeting people who are more willing to pay" (p. 1).

Ransomware at Work – The Ransomware Process

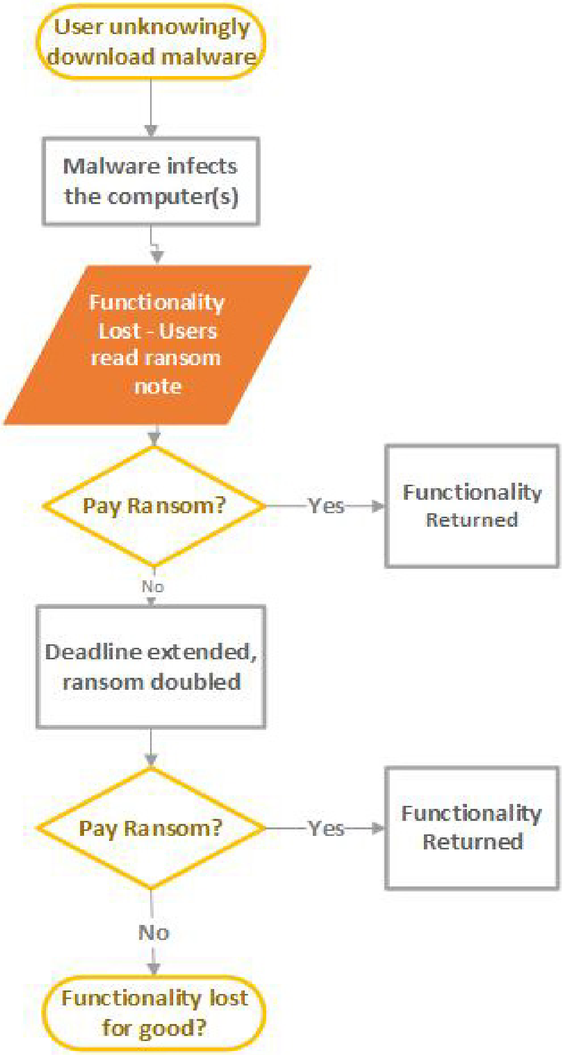

User unknowingly download malware
Malware infects the computer(s)
Functionality Lost - Users read ransom note
Pay Ransom?
Yes
Functionality Returned
No
Deadline extended, ransom doubled
Pay Ransom?
Yes
Functionality Returned
No
Functionality lost for good?

Figure 1 – The Ransomware Process

The ransomware process takes different directions depending on the user action and the path resulting from the criminals after they receive the ransom. Ali, Murthy, and Kohun (2016) introduced a chart that depicts the steps involved in the ransomware process. The following are the steps suggested by Ali et al. in the ransomware process:

1. Virus infects the computer
2. Functionality lost – users read ransom note

3. User decide to pay ransom (or not)
4. Deadline extended
5. User decide to pay after passing of extending deadline
6. Functionality either returned or lost for good depending if paid or not paid

The first listed above is too involved and deserves more attention. In the author's opinion, this step can be clarified more if it is divided into two steps. Thus, we divided this step into two and presented an alternative chart that depicts the ransomware process. Figure 1 is a revised version of the ransomware process that was first introduced:

The remainder of this section explains in more details each of the steps listed in Figure 1.

Users Unknowingly Download the Malware

It is obvious that users do not want to download viruses to their computers. Nevertheless, many users at different levels of expertise unknowingly download malware into their computers and there are different factors that make them do this. Some of these factors include the following. (Heater, 2016):

1. Lack of knowledge
2. Overlook the danger surrounding visiting certain sites
3. Inappropriate anti-virus installations
4. Outdated necessary software (like Java, Acrobat, Browsers, and others)
5. Sticking with old computers
6. Desperate attempts to solve computer problems

The sources where people download and install viruses could be diverse as well. Glassberg (2016) suggested that users could download and install malware on their computer from the following sources:

- Drive by download
- Clicking on a wrong advertisement pop-up link
- Phishing attacks through email attachments

Narvaez et al. (2010) defined drive-by-downloads in general term as "malware that push, and then execute, malicious code on a client system without the user's consent" (p. 1). Given there is no user consent, it makes this process of installing the malware unknown to the user (Zhang, Seifert, Stokes, & Lee, 2011). O'Gorman and McDonald (2012) referenced situations when individuals browse the web looking for porn content. When they click on a particular link, the ransomware site then downloads the malware. It then executes the program to spread the malware on the computer. All this goes on without the knowledge of the users. In other words, the web site may be posing as a porn site, but behind the scene, it hides the program that holds the computer data for virus.

Clicking on a wrong advertisement link may lead to installing the malware as well. This technique been used to spread viruses since the early days of the Internet. Popping screens, multiple animations, and different kinds of flying messages that are designed to divert attention so users click on the link and unknowingly download the virus on the computer. The phishing attacks through email attachments have become more sophisticated as well. Constantin (2016) explained that some cyber criminals send email and pretend to apply for a job. They include malware in the attachment. When the attachment clicked, it installs the malware on the computer. The interesting point noted here is that the applicants (pretenders) study the situation well; they submit something that looks closely similar to a legitimate application, thus increasing the chance that on the other side someone opens the attachment and install the malware.

Malware Infects the Computer

Bhardwaj et al. (2016) talked about the sequence of steps that the malware takes to infect the computers:

- Malware injects malicious code into end user computer
- The malware gets installed in a random location
- Code from the malware then infects users' files and computers

Heater (2016) reported that it typically takes less than three minutes after infecting with ransomware until all intended files are encrypted on the computer. Heather noted further that the encryption of the ransomware is so strong that is considered a "bullet proof" – that is no one else can unlock (other than the attackers) the encryption and thus the files remained encrypted.

Salvi and Kerkar (2016) explained that ransomware affects the work of the computer in three possible places:

- In the Master Boot record (called MBR ransomware),
- In the screen locking category (Called screen locking ransomware)
- In the file encryption categories (called file encryption ransomware)

The master boot record (MBR) is an area in the computer's hard drive that permits the operating system to boot. Constantin (2016) explained that when computers get infected with ransomware, the malware overwrites the existing MBR and replaces it with a different MBR. This will disable logging into the computer until a decryption code is obtained from the criminals who injected this virus.

Locking screen ransomware – This type of ransomware is called WinLocker (Tuttle, 2016). It displays a full screen image that blocks all other windows and demands payment. Information about payment and the transmission of money is displayed on the locking screen.

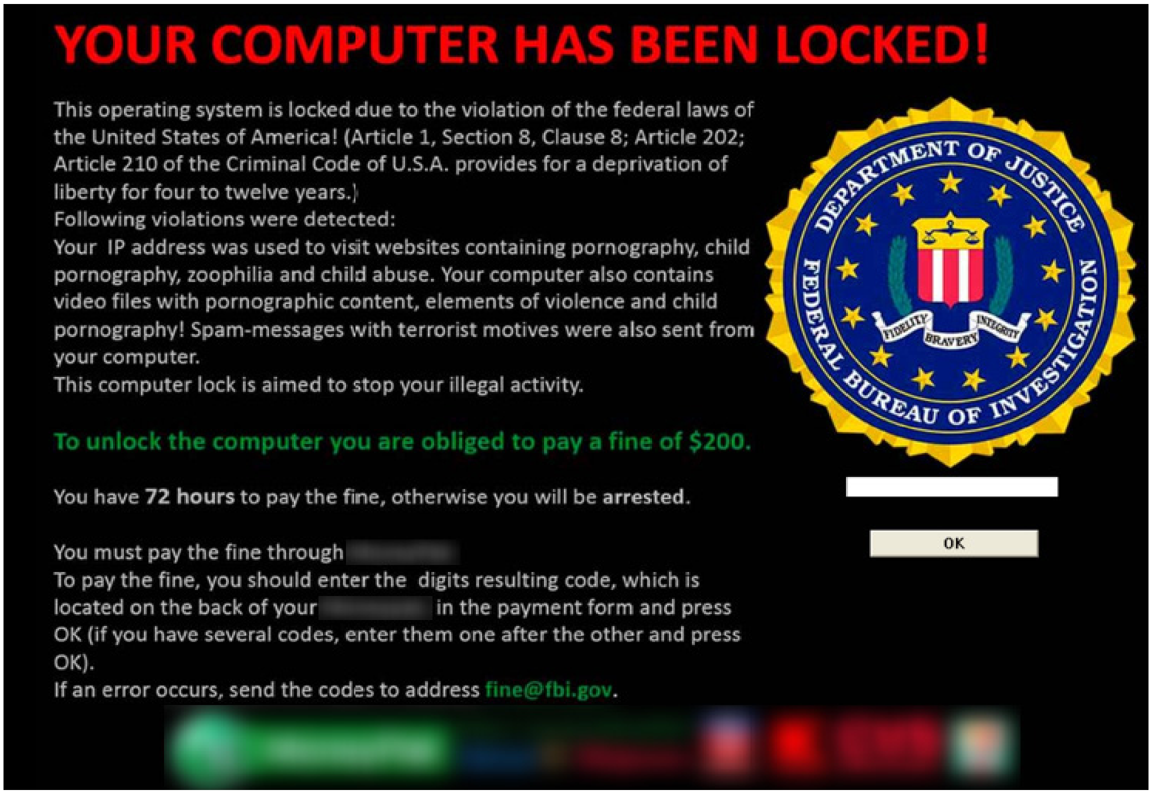
File encryption ransomware – This is the most common form of ransomware. Once the files are encrypted, they will be inaccessible until the ransom is paid. Typically, a text file containing instructions for downloading additional browsers and details of how to pay are left in the same folder.

Functionality Loss/Victims Read Ransom

Victims of ransomware most often notice that something is wrong when they lose access to their data first. Lemos (2016) explained that a company was made aware of ransomware installed on their network when they lost access to their accounting data. Heather (2016) noted that a woman learned about the loss of functionality when she tried to access a file-containing list of guests for a planned party.

The installation of the ransomware is often accompanied by writing ransom notes at the same time. The ransom notes typically written in multiple places so that the users notice them as soon as possible. However, many do not notice the ransom note until after the loss of functionality. Lemos (2016) explained that after the company lost access to accounting data, the technical support group checked further about the loss of data and found about 200 copies of the same ransom note written on their computer. O'Gorman and McDonald (2012) displayed an example of one ransom note as shown in Figure 2.

The ransom note is often localized (that is, written in the local language of the victim). It seems that the language of the ransom is selected based on the location of the IP address of the computer they infect. Figure 3 shows a ransom note placed on another computer written in different languages as displayed in the article written by O'Gorman and McDonald in four countries: USA, UK, Germany and Austria.



YOUR COMPUTER HAS BEEN LOCKED!

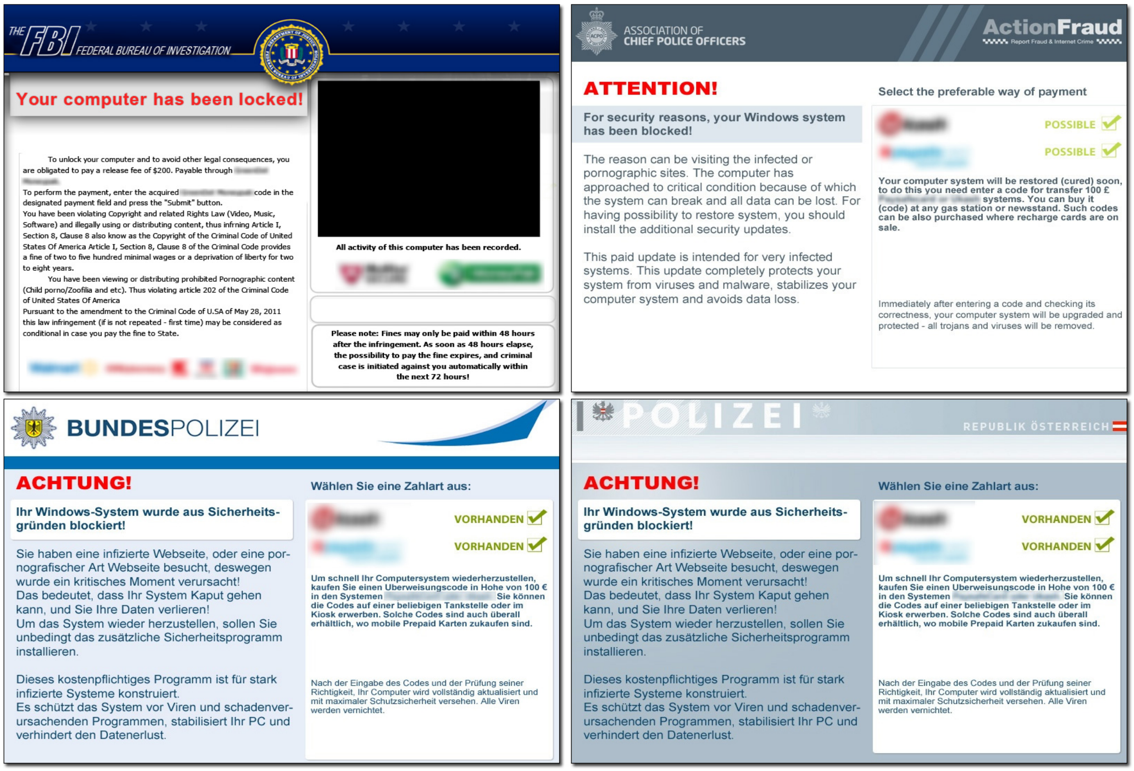
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Figure2: Example of Ransomware Note (O'Gorman & McDonald, 2012)



Your computer has been locked!

To unlock your computer and to avoid other legal consequences, you are obligated to pay a release fee of $200. Payable through [redacted]
To perform the payment, enter the acquired [redacted] code in the designated payment field and press the "Submit" button.
You have been violating Copyright and related Rights Law (Video, Music, Software) and illegally using or distributing content, thus infrning Article I, Section 8, Clause 8 also know as the Copyright of the Criminal Code of United States Of America Article I, Section 8, Clause 8 of the Criminal Code provides a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.
You have been viewing or distributing prohibited Pornographic content (Child porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of United States Of America
Pursuant to the amendment to the Criminal Code of U.SA of May 28, 2011 this law infringement (if is not repeated - first time) may be considered as conditional in case you pay the fine to State.

All activity of this computer has been recorded.

Please note: Fines may only be paid within 48 hours after the infringement. As soon as 48 hours elapse, the possibility to pay the fine expires, and criminal case is initiated against you automatically within the next 72 hours!

ASSOCIATION OF CHIEF POLICE OFFICERS
ActionFraud
Report Fraud & Internet Crime

ATTENTION!

For security reasons, your Windows system has been blocked!

The reason can be visiting the infected or pornographic sites. The computer has approached to critical condition because of which the system can break and all data can be lost. For having possibility to restore system, you should install the additional security updates.

This paid update is intended for very infected systems. This update completely protects your system from viruses and malware, stabilizes your computer system and avoids data loss.

Select the preferable way of payment

POSSIBLE ☑
POSSIBLE ☑

Your computer system will be restored (cured) soon, to do this you need enter a code for transfer 100 £ [redacted] systems. You can buy it (code) at any gas station or newsstand. Such codes can be also purchased where recharge cards are on sale.

Immediately after entering a code and checking its correctness, your computer system will be upgraded and protected - all trojans and viruses will be removed.

ACHTUNG!

Ihr Windows-System wurde aus Sicherheitsgründen blockiert!

Sie haben eine infizierte Webseite, oder eine pornografischer Art Webseite besucht, deswegen wurde ein kritisches Moment verursacht!
Das bedeutet, dass Ihr System Kaput gehen kann, und Sie Ihre Daten verlieren!
Um das System wieder herzustellen, sollen Sie unbedingt das zusätzliche Sicherheitsprogramm installieren.

Dieses kostenpflichtiges Programm ist für stark infizierte Systeme konstruiert.
Es schützt das System vor Viren und schadenverursachenden Programmen, stabilisiert Ihr PC und verhindert den Datenerlust.

Wählen Sie eine Zahlart aus:

VORHANDEN ☑
VORHANDEN ☑

Um schnell Ihr Computersystem wiederherzustellen, kaufen Sie einen Uberweisungscode in Hohe von 100 € in den Systemen [redacted] Sie können die Codes auf einer beliebigen Tankstelle oder im Kiosk erwerben. Solche Codes sind auch überall erhältlich, wo mobile Prepaid Karten zukaufen sind.

Nach der Eingabe des Codes und der Prüfung seiner Richtigkeit, Ihr Computer wird vollständig aktualisiert und mit maximaler Schutzsicherheit versehen. Alle Viren werden vernichtet.

ACHTUNG!

Ihr Windows-System wurde aus Sicherheitsgründen blockiert!

Sie haben eine infizierte Webseite, oder eine pornografischer Art Webseite besucht, deswegen wurde ein kritisches Moment verursacht!
Das bedeutet, dass Ihr System Kaput gehen kann, und Sie Ihre Daten verlieren!
Um das System wieder herzustellen, sollen Sie unbedingt das zusätzliche Sicherheitsprogramm installieren.

Dieses kostenpflichtiges Programm ist für stark infizierte Systeme konstruiert.
Es schützt das System vor Viren und schadenverursachenden Programmen, stabilisiert Ihr PC und verhindert den Datenerlust.

Wählen Sie eine Zahlart aus:

VORHANDEN ☑
VORHANDEN ☑

Um schnell Ihr Computersystem wiederherzustellen, kaufen Sie einen Uberweisungscode in Hohe von 100 € in den Systemen [redacted] Sie können die Codes auf einer beliebigen Tankstelle oder im Kiosk erwerben. Solche Codes sind auch überall erhältlich, wo mobile Prepaid Karten zukaufen sind.

Nach der Eingabe des Codes und der Prüfung seiner Richtigkeit, Ihr Computer wird vollständig aktualisiert und mit maximaler Schutzsicherheit versehen. Alle Viren werden vernichtet.

Figure 3: Ransom note written in different languages (O'Gorman and McDonald, 2012)

Victims Decide to Pay/Not to Pay

The next step in the process is for the victims (whose computers are infected with the malware) to decide whether to pay the ransom or not to pay it. The ransom notes typically include instructions and specify the method of payment and the steps to follow to make the payment. In all the steps for making the payment, the main goal in the message is to protect the anonymity of the criminals who installed the ransomware. This includes, for example, using a "Tor browser" when informing the attackers that payment is made. Tor interfaces are known for their ability of "anonymous browsing (Clark, Oorschot, & Adams, 2007), thus it is often instructed in the ransom note to use this browser when communicating about this ransomware.

A common concern of victims of ransomware when deciding to pay or not to pay is their worry that they will not be able to retrieve all their data even after paying the ransom. Lemos (2016) reported that after a company paid ransom, they were able to retrieve all their lost accounting data. However, they had difficulty retrieving data from the mapped drive. The attackers who installed the ransomware in the first place offered to help with the data on the mapped drive; however, the company did not trust that they would work to retrieve. Instead, they worried that the attackers can cause more damage instead and did not take the offer of help.

Extension of Deadline/Ransom Doubles

The original ransom note typically includes two stipulations about deadlines: First, a deadline is set to pay the ransom. The second stipulation specifies that the first deadline can be extended for a second and last time but the amount of asked ransom will be doubled. Through our literature review, we found that negotiations take place at this time of extension and when the second deadline approaches. Everett (2016) for example reported that after negotiation, a hospital paid $17,000 in return for their data negotiating down the ransom from $3.6m. Heather (2016) reported on another kind of negotiation that led to happy conclusion of paying for ransomware. Heather reported that a woman lost access to her files, and she passed the first the deadline to make the payment and the fine was about to be doubled. Yet, this woman negotiated and was able to get files back without paying the extra money from doubling the ransom – she paid the original amount of the ransom.

Last Chance

If the second deadline passes without receiving a payment by the ransomware, then all encrypted files are going to be lost for good. Also, all functionality lost during the ransomware attack will remain lost. All files remain encrypted, the users cannot retrieve their content, and the ransom notes disappear from the computer. Thus, the victim cannot go back and review the notes, make payment or any other things. The original ransom notes also state that after the deadline all encryption and decryption keys will be lost, and thus the functionality of the computer/files will be lost for good. Our literature review and our experience support this contention that the files are lost for good after the second deadline.

The Personal Case Illustration

This section explains about the experience that the author had with installing ransomware and dealing with the aftermath of it. It is divided similar to the steps we discussed in the section about the Ransomware Life Cycle.

The Problem: How It Happened

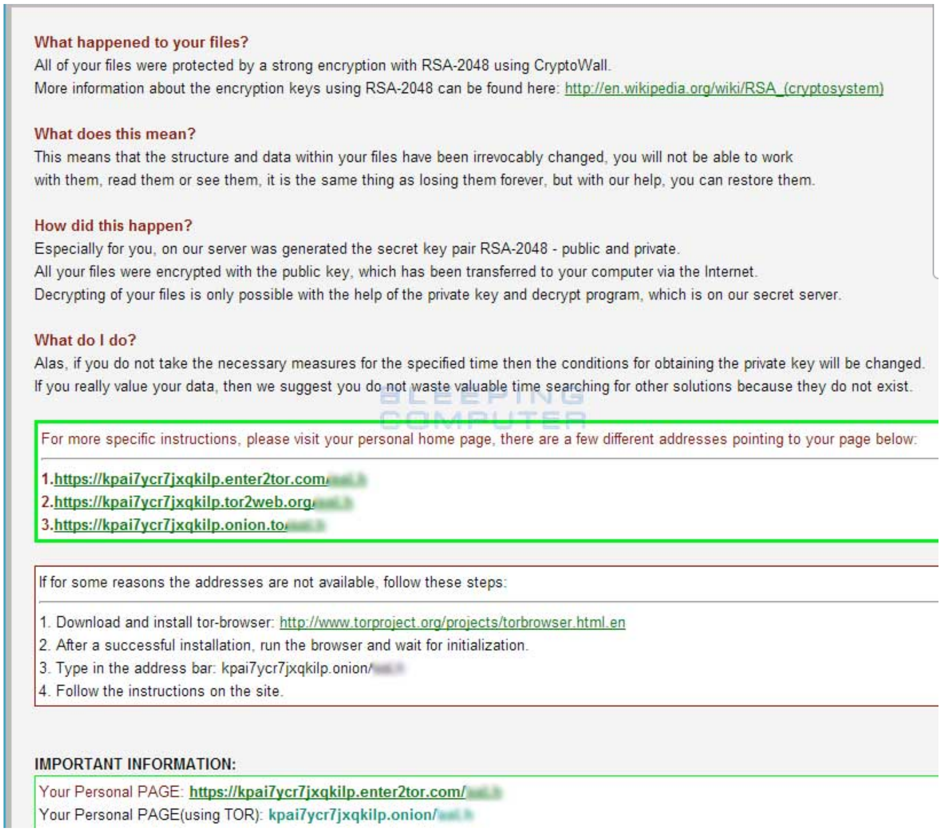
The author unknowingly installed ransomware after a long frustration with computer problems and as a desperate act to find a solution to the problems. The following list describes how it happened:

- The computer was very slow (yes VERY slow)
- It was repeatedly displaying the message "shareware not working"

- I tried to solve the problem many times, none worked and the problem persisted for a long time
- I tried to search the web and googled the error message
- I came across a discussion board that was talking about our error message. One of the discussants suggested to download "Malware bytes" and provided a link to it. It suggested to start the computer in safe mode, then install and run the file indicated in the link – a prime red flag I overlooked in the mix. This red flag was the suggestion to start the computer in *safe mode* so the malware worked without interference of any other anti-virus software I already had on the computer. What a clear message, yet I overlooked it because of the long frustration with the computer problems.

FUNCTIONALITY LOST – READING THE RANSOM NOTE

My wife kept complaining that she could not access the files on her computer. When she opened any Word file or try to view image files, the computer displays strange characters. When the problem persisted, I checked into the drive and found a message in all sub folders under "My Documents" folder. The content of the message displayed in Figure 4.



What happened to your files?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1.https://kpai7ycr7jxqkilp.enter2tor.com/[redacted]
2.https://kpai7ycr7jxqkilp.tor2web.org/[redacted]
3.https://kpai7ycr7jxqkilp.onion.to/[redacted]

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: kpai7ycr7jxqkilp.onion/[redacted]
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
Your Personal PAGE: https://kpai7ycr7jxqkilp.enter2tor.com/[redacted]
Your Personal PAGE(using TOR): kpai7ycr7jxqkilp.onion/[redacted]

Figure 4: Example of the ransom message the author received

TO PAY/NOT PAY

By the time my wife and I discovered this problem, the first deadline had already passed. We began checking for solution. We thought that this would be temporary; maybe we can provide some solutions. We assumed that if we copied the files to another computer, it would open. May be if we update our Malware Bytes and Sophos anti-virus software, it may solve the problem.

The ransom message detailed about how to download the Tor browser and how to submit the payment. However, it did not specify the amount.

The Second Deadline

As we read more about this problem and discussed it with experts in the field, I decided not to pay the ransom. The second deadline passed and then the ransom notes disappeared which made it impossible to investigate how to pay to fix it if we wished to. Although we made the decision not to pay after the first message, we were ready to look more into the subject. At the end, we accepted that the files we lost might have been lost for good. This included individual document files, vacation picture files, and other user files saved under "My Document" folder but no system files.

Summary and Concluding Remarks

This paper was about ransomware – a nasty malware that invades users' computers, encrypt files, disables access to data files and computers, and demands money payment for the return of functionality to the computers and files. The paper started first by explaining about ransomware, a historical background on how the malware developed, and different stories about how ransomware affected the lives of many. It then explained about the ransomware process and depicted its development in a chart to show the relationship between the different steps in this process. The paper then explained in more detail about the personal experience of the author of this paper; how the computer of his family was hit with this malware and the missed signals that led to this download of ransomware.

Although our experience from being hit with Ransomware was painful, it could have been worse. The message we (my wife and I) want to deliver in this paper is that the risk from ransomware is real and the risk is big. In our case, the risk was that the criminals were able to obtain our financial data, our contact information, and more sensitive information we saved on the computer. Nevertheless, we are grateful that the damage was not more extensive than we had, and thus we offer the following suggestions for people in order to mitigate the damage of ransomware:

- Backup, backup and then backup. Flash drive are becoming cheap and have abundant storage that can back up entire "My Documents" folder
- Keep anti-virus software up to date
- Keep other system files (like browser files, Java, Adobe Acrobat) up to date
- Invest in buying a new computer if your computer becomes too old, too slow and is having a lot of problems.

References

Ali, A., Murthy, R., & Kohun, F. (2016). Recovering from the nightmare ransomware – How savvy users get hit with viruses and malware: A personal case study. *Issues in Information Systems*, 17(4), 58-69.

American Bankers Association. (2016). *Ransomware*. Retrieved November 14, 2016 from http://www.aba.com/Tools/Function/Cyber/Pages/Ransomware.aspx

Bhardwaj, A., Avasthi, V., Sastry, H., & Subrahmanyam, G. V. B. (2016). Ransomware digital extortion: A rising new age threat. *Indian Journal of Science and Technology*, *9*, 14.

Clark, J., Van Oorschot, P. C., & Adams, C. (2007, July). Usability of anonymous web browsing: An examination of tor interfaces and deployability. *In Proceedings of the 3rd symposium on Usable privacy and security* (pp. 41-51). ACM.

Constantin, L. (2016). This nasty ransomware overwrites your PC's master boot record. *Pcworld*, *34*(5), 44-46.

Cyber Threat Alliance. (2015). *Lucrative ransomware attacks: Analysis of the CryptoWall Version 3 threat*. Retrieved November 3, 2016 from http://cyberthreatalliance.org/cryptowall-report-v3.pdf

Cyber Tthreat Alliance (2016). *Cryptowall Version 4 threat.* Retrieved November 4, 2016 from https://cyberthreatalliance.org/pr/pr-092616.html

Everett, C. (2016). Ransomware: to pay or not to pay?. *Computer Fraud & Security*, *2016*(4), 8-12.

Glassberg, J. (2016). Defending against the ransom ware threat. *POWERGRID International*, *21*(8), 22-24.

Goldsborough, R. (2016). Protecting yourself from ransomware. *Teacher Librarian*, *43*(4), 70-71.

Hampton, N., & Baig, Z. A. (2015). Ransomware: Emergence of the cyber-extortion menace. *Proceedings of the 13th Australian Information Security Management Conference*, 30th, November 2015 – 2 December 2015 (PP 47-56), Edith Cowan University Campus.

Heater, B. (2016, May). How ransomware conquered the world. *PC Magazine Digital Edition*, 109-118.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. In *Proceedings of the Detection of Intrusions and Malware, and Vulnerability Assessment Conference* (pp. 3-24). Springer International Publishing.

Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. *Information Systems Security, 16*(4), 195-202.

Lemos, R. (2015). How to prevent ransomware: What one company learned the hard way. *PC World*, *33*(5), 45-48.

Narvaez, J., Endicott-Popovsky, B., Seifert, C., Aval, C., & Frincke, D. A. (2010, January). Drive-by-downloads. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference* (pp. 1-10). IEEE.

O'Gorman, G., & McDonald, G. (2012). *Ransomware: A growing menace.* Symantec Corporation.

ransom. (2016). In *Merriam-Webster.com.* Retrieved September 20, 2016 from http://www.merriam-webster.com/dictionary/ransom

Salvi, M. H. U., & Kerkar, M. R. V. (2016). Ransomware: A cyber extortion. *Asian Journal of Convergence in Technology*, *2*(3),

Solander, A. C., Forman, A. S., & Glasser, N. M. (2016). Ransomware--Give me back my files!. *Employee Relations Law Journal*, *42*(2), 53-55.

Tuttle, H. (2016). Ransomware attacks pose growing threat. *Risk Management*, *63*(4), 4.

ware (2016). In *Merriam-Webster.com.* Retrieved September 20, 2016 from http://www.merriam-webster.com/dictionary/ware

Zhang, J., Seifert, C., Stokes, J. W., & Lee, W. (2011, March). Arrow: Generating signatures to detect drive-by downloads. In *Proceedings of the 20th International Conference on World Wide Web* (pp. 187-196). ACM.

Biography

Azad Ali, D.Sc., Professor of Information Technology at Eberly College of Business – Indiana University of Pennsylvania – has 30 years of combined experience in areas of financial and information systems. He holds a bachelor degree in Business Administration from the University of Baghdad, an MBA from Indiana University of Pennsylvania, an MPA from the University of Pittsburgh, and a Doctorate of Science in Communications and Information Systems from Robert Morris University. Dr. Ali's research interests include service-learning projects, web design tools, dealing with isolation in doctoral programs, and curriculum.