https://doi.org/10.48009/4_iis_2016_58-69

Issues in Information Systems
Volume 17, Issue IV, pp. 58-69, 2016

RECOVERING FROM THE NIGHTMARE OF RANSOMWARE – HOW SAVVY USERS GET HIT WITH VIRUSES AND MALWARE: A PERSONAL CASE STUDY

Azad Ali, Indiana University of Pennsylvania, azad.ali@iup.edu
Raj Murthy. Indiana University of Pennsylvania, Raj.murthy@iup.edu
Frederick Kohun, Robert Morris University, Kohun@rmu.edu

ABSTRACT

The purpose of this paper is to describe the ways that savvy computer users unknowingly install malware on their computers and thus infecting and causing damage to their files and computers. In particular, it focuses on one type of malware that is being repeatedly downloaded and installed by users from different levels of expertise in terms of their use of computers. The name of this malware is ransomware. This type of malware is dangerous and is creating havoc in the life of many users. These users include one of the authors of this paper that unknowingly downloaded and installed this malware. It damaged the contents of his family computer that is currently still undergoing reconstruction. The experience of this particular case along with relevant description of the malware and related literature is included in this study.

Keywords: Ransomware, Viruses, Malware, Crypto 3, Computer ransom

INTRODUCTION

> The term *malware* (*mal*icious soft*ware*) refers to a program with malicious intent designed to damage the machine on which it executes or the network over which it communicates. The growth in the complexity of modern computing systems makes it difficult, if not impossible, to avoid bugs. This increases the possibility of malware attacks that usually exploit such vulnerabilities in order to damage the system. Furthermore, as the size and complexity of a system grows, it becomes more difficult to analyze it and prove that it is not infected. Thus, the threat of malware attacks is an unavoidable problem in computer security (Preda et al, P 25:2).

It seems nowadays that getting your computer infected with malware (or virus) is inescapable. No matter how careful we are in working with the computer or browsing and downloading from the Internet, it is not guaranteed that your computer will not get infected. Instead precautionary steps may help mitigate the possibility of downloading malwares but, nevertheless, getting infected with malware seems unavoidable.

One of the most dangerous malware that is widely spreading among computers and devastating the work of many, is called "ransomware." The way that ransomware works is that it installs itself on a computer, it locks the functionality of data or system files on the computer and it asks users to pay ransom in order to return the functionality of their files and systems (Goldsborough, 2016, Shilam, 2016, Touchette, 2016, SentinelOne, 2016)). Ransomware does so by encrypting the files and hold the decryption keys at their server. Once the ransom is paid, the decryption keys are released and then functionality for the attacked system and files are return back to normal for the most part. If the ransom payment is not made within the specified time, then the files remain encrypted and the functionality of the system along with accessibility to the files remain locked (Luo and Liao, 2007).

One of the people hit with ransomware is one of the authors of this paper. Although, this author did not pay the ransom, he along with his family are still suffering from the loss of access to the data files that were encrypted by the ransomware of their computer. This paper, in part, describes the experience in how he unknowingly installed this malware and how he is recovering from this experience. The paper is divided into the following sections:

- The first section reviews most recent literature that points to seriousness of the ransomware problem and the extent in which it causes damage to users

- The second section discusses how ransomware get installed and the cycle that they go through from installation, to receiving/not receiving payment and through recovering the lost functionality
- The third section explains the ways that savvy users unknowingly install ransomware
- The next section elaborates on the experience of the author in dealing with ransomware and is followed by concluding comments about the experience of dealing with ransomware.

THE RISK OF RANSOMWARE – IT IS SERIOUS, IT IS BIG

Reading about ransomware is something, experiencing the effects of ransomware is something different. However, to experience it and then read more about it is a totally different story. Ransomware is a big problem that is invading individual and business computers. It is causing damage to computers large and small and it causing havoc in the life of many parts of the world. It is a serious problem that is not to be taken lightly.

The seriousness of the ransomware problem is illustrated in an article published by Heater (2016). The title of the article demonstrates. the danger of this malware and raises many eyebrows about the risk of this malware. The title reads "How ransomware conquered the world." The picture on the cover page of the same article describes it more visually. It shows two hands bound and chained over a computer keyboard indicating that nothing can be done about it. Figure 1 below shows the image of the cover page of this article.

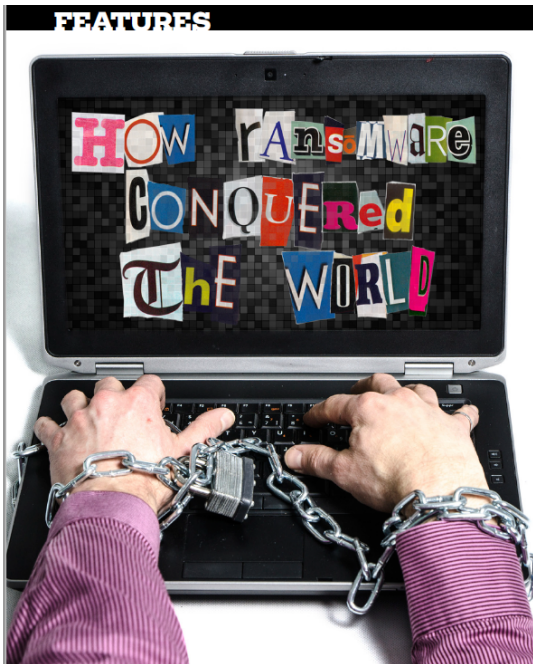

Figure 1. Coverage of Article about Ransomware (Heater, 2016)

While the title and cover page of the article above shows how serious the problem of ransomware is, we undertook a brief literature review that highlights the seriousness of this problem. We list a synopsis of some of these works and associated stories below.

- Everett (2016) noted that ransomware is "Going by reported incidents, it's a $70m per year criminal enterprise, but in reality it looks more like $200m, which is unbelievable" (P. 10).

- O'Gorman and McDonald (2012) reported "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 (2016) called year 2016 as the "year of ransomware" and justified using this name for the year due to increasingly high profit examples of ransomware. The most notable, heater mentioned is the story of Hollywood Presbyterian Medical Center. The computer network of this medical center was brought to a halt as a result of being hit by ransomware. After paying a ransom of $17000, the hospital was able to retrieve the functionality of their computer network.

- Lemos (2015) reported that ransomware is growing fast and stated to invade android users. Lemos explained that four out of five malware that hit Android users are all asking for ransom to pay, so they are ransomware. Lemos also gave an example of a company when hit with a ransomware, they fund 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 and predicted that it will double again in the next year. Everett explained that ransomware are precise in selecting targets. For example, they select florist shops before Valentine's Day because they knew the heavy traffic these shops experience in that period.

- 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).

The stories are abundant, the damages of ransomware are extensive and the prospect of even greater damage from ransomware is real. But to explain how all this, how it works inside the system and how it collects all these ransoms, the next section explains about the life cycle of ransomware.

AN OVERVIEW – THE RANSOMWARE PROCESS

This section reviews literature about the mechanism by which ransomware is installed on computers, the havoc that this installation creates and then how money (ransom) is collected from the victims of the malware. Although similar steps are often followed in the installation of ransomware and the following collection of ransom. Nevertheless, we deemed that explanation of each of the steps involved in this process separately is necessary because some steps are dependent on earlier decisions made by the victims of the ransomware and by the criminals who installed it. Also, some later steps are dependent on earlier steps in the process.

The point to be explained here is that the process is not always straight forward and some people follow different paths in dealing with ransomware. Thus we wanted to illustrate this process pictorially. For this purpose we selected a chart that is too familiar to IT educators. It is called "System Development Life Cycle" or SDLC. Based on the symbols used in SDLC, we draw a parallel chart that represents the ransomware process. Figure 2 below shows pictorial representation of what we have termed here as "The Ransomware Process". Then, the remainder of this section explains what is involved in each steps in the process we illustrated in figure 2.

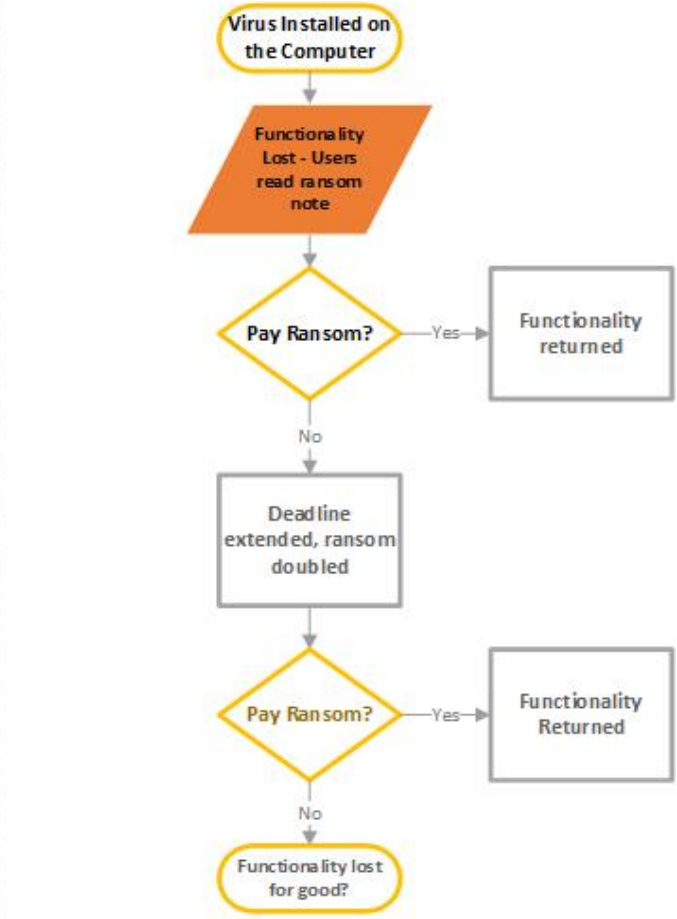

Figure 2. The Ransomware Process

Malware Infects Computer(s)

In this step, the virus infects the computer(s). It could infect one computer or multiple computers. It typically infects one computer but it often spreads across network drives to infect other computers as well. When it infects other computers or invades networked computers, it most often does this quietly and it may take days for it to attach the entire network. Lemos (2015) explained about one company that ransomware got installed on one of their computer from the Internet. Then over the following three days, ransomware encrypted accounting and customer data on their computers and extended to encrypt accounting data on mapped network drive which extended the infection to other computers on the same company network as well.

Functionality Loss/Victims Recognize and Read Ransom

The loss of functionality is most often is related to loss of access to data and data files. It is often this loss of access that makes the users aware that something went wrong on their computers and to begin to investigate the problem. Lemos (2016) explains that a company was made aware of ransomware installed on their network when they lost access to their accounting data. Heather (2016) explained that a lady 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 accompanied by the simultaneous writing of ransom notes. The ransom notes are 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 (2015) explained that after the company lost access to

accounting data, the technical support checked further and found about 200 copies of the same ransom note written on their computer. O'Gorman and McDonald (2016) displayed an example of one ransom note as shown in figure 3 below:

Figure 3. Example of Ransomware Note (O'Gorman and McDonald, 2016)

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 4 below shows a ransom note placed on another computer yet written in different languages as displayed in the article written by O'Gorman and McDonald in four countries: USA, UK, Germany and Austria:

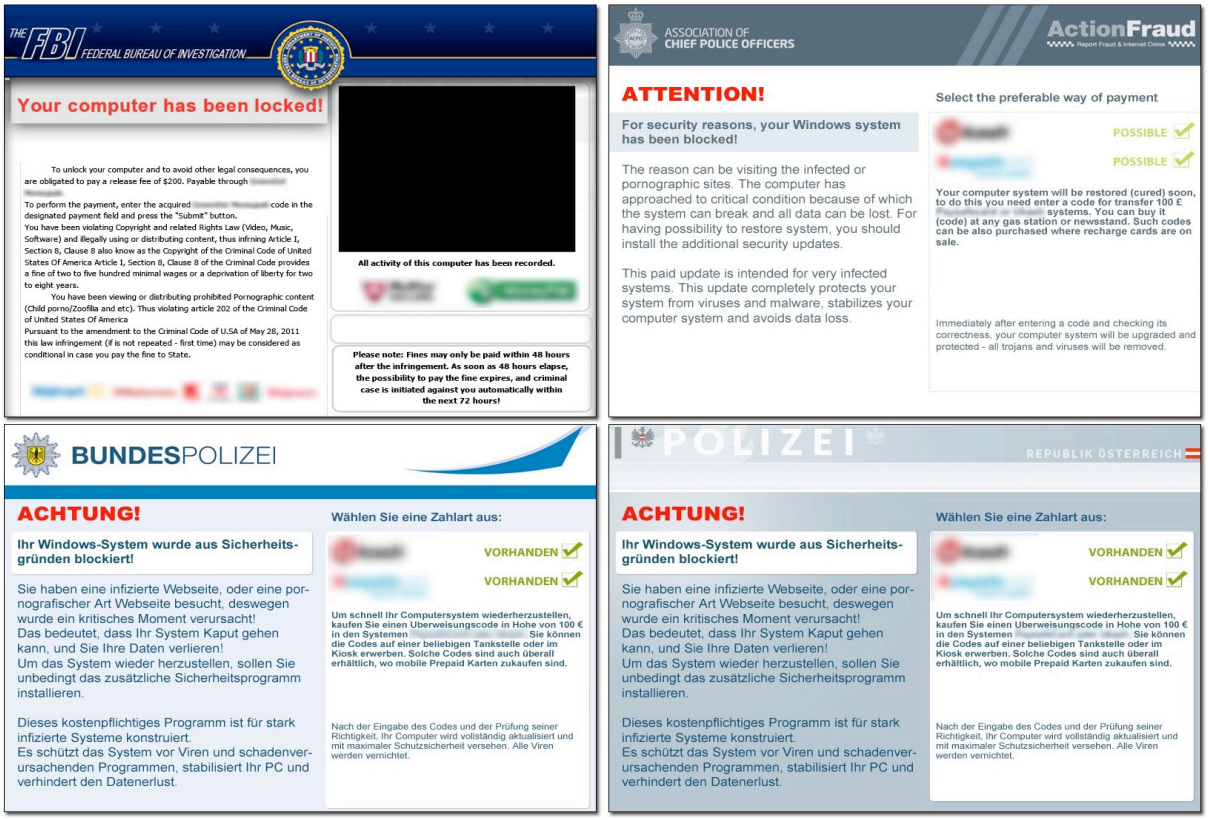

Figure 4. Ransom note written in different languages (O'Gorman and McDonald, 2016)

Victims Decide to Pay/Not to Pay

The next step in the process is for the victims (who their computers were infected with the malware) is to decide whether to pay the ransom note or not to pay it. The ransom note include instructions and specifies 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, the using a "Tor browser" when informing the attackers that payment was made. Tor interfaces are known for their ability of "anonymous browsing (Clark, Oorschot and Adams, 2007). It is often instructed in the ransom note to use this browser when communicating about this ransomware.

The preferred payment method in ransomware is the use of Bit Coin currency. Bit Coin is best described as the "The online currency" and can be exchanged to other currencies later. The ransom note details how to pay the ransom and the language of these instructions are once again – localized. In other words, they are intended to be displayed in the language of the victims. Everett (2016) displayed an example of such a message written in the Spanish language as shown in figure 5 below:

Figure 5. Example of Bit Coin Instructions Written in Spanish (Everett 2016)

A common concern of the victims when deciding to pay or not to pay is their concern that the functionality of their system will not be restored even after paying the ransom. Lemos (2015) reported that after the company paid the ransom, they were able to retrieve their 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 restoring the data on the mapped drive. However the company did not trust that they would. In fact, Lemos reported that the company were more concerned that they will lose more data if they take the offer suggested by ransomware installers..

Extension of Deadline/Ransom Doubles

The original ransom note typically includes a notation that if the ransom is not paid within a specified period time that the deadline may, but at a cost of a higher ransom. Our literature review revealed that negotiation takes place at this time of extension as the second deadline approaches. These negotiations helped to bring down the amount of ransom to be paid in some cases. Everett (2016) for example, reported that after negotiation, a hospital paid $17,000 in return for their data. They negotiated the ransom down from the $3.6 million demanded first. Heather (2016) reported on another kind of negotiation that led to a relatively happy ending. Heather reported that a lady lost access to her files, and she passed the first deadline to make the payment and the fine was about to be doubled. Then, this

lady negotiated and was able to get files back without paying the extra ransom – she paid the original amount of the ransom.

Last Chance

If the second deadline passes without receiving a ransom payment, then it appears that all files and functionality will be 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 negotiate. The original ransom notes also indicate that after the deadline, all encryption and decryption keys will be lost and, as a result, 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.

REASONS USERS DOWNLOAD MALWARE

This section sheds light on different ways that the users unknowingly download viruses on their computers which subsequently may lead to the demand of ransom the havoc associated with it. This may not limited to the installation of ransomware malware, but it may similarly include the installations of any virus. Special focus will be on what we found in installing ransomware.

Drive-by-downloads

Narvaez et al (2010) defined drive-by-downloads in general terms 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 and Seifert, 2011). Similar things happen in terms of ransomware installation. O'Gorman and McDonald (2016) referenced situations when individuals browse the web looking for porn content. When they click on a particular links, the ransomware site then downloads the program that contains 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 seen it hides the program that holds the computer data for virus.

Through clicking on ads

Clicking on a link on the Internet that is hiding a virus is nothing new. This technique is used to spread viruses on the Internet even in 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. However, in regards to ransomware this kind of clicking (and installing the virus) takes on different forms. We report on two incidents that we found in the literature that account for such clicking and the following downloading of the virus for ransomware.

Lemos (2015) reported on a company in New England where the co-owner talked about a "click-happy" employee that ended up downloading a virus for ransomware and that infected the entire system. The virus ended up encrypting data on the compromised system and the company later ended up paying $500 in return for the return of their data.
O'Gorman and McDonald (2012) reported that ransomware criminals often place advertisement on web sites. The ads are for porn sites and the virus is hidden inside the ad. When the user clicks on the ad, the virus spread through their system. This make it more likely that the user will pay the ransom given that the user has visited the porn site and may want to hide this information from others.

Through spam emails

This is a traditional and typical virus propagation technique. It is common among novice users who find attachments within an email, they get curious about the file, they try to open it, and unknowingly, install the virus. This form of

virus proliferation has been in existence for some time and it seems that ransomware gets installed sometimes using these email attachments.

The attachments to spam emails may look like legitimate documents. However, once clicked on, they contain a program that infects the computer with the malware (or ransomware).

None of the above – Acts of frustration

"None of the above" or "others" are categories that educators are familiar with. When an item does not belong to the categories known or listed, or when identification of factors cannot be explained in terms of existing listed categories--the term "none of the above" or "others" are used. In the case of ransomware installation, there needs to be an "others" category because we are not totally certain of all the ways that ransomware infects different computers. Thus we list this category under "None of the above".

One explanation as to how ransomware is acquired may fall under this "Others" category. The explanation for downloading ransomware may be the frustration that some users face with persistent computer problems. This frustration may lead them to search for solution that includes downloading files, patches, repairs and/or links that appear to be able to solve their computer problem and then help with their frustration (Lazar et. al, 2006). These links may be culprit in the spread and infecting computers with ransomware.

THE RANSOMWARE AS IT HAPPENED –OUR CASE

This section explains about the personal experience with installing ransomware and dealing with the aftermath of it. It illustrates how ransomware was installed on the family computer of one of the authors of this paper, how they discovered it and the how they dealt with it afterward. We will divide this discussion according to the steps we followed in the literature review when we discussed the Ransomware Process.

The problem how it happened

The virus was installed based on long frustration with computer problem and a desperate acts to find a solution to the problems. Here is what happened

.

- The computer was very slow (yes very slow)
- It was repeatedly displaying the message "SharePoint stopped working"
- We tried to solve the problem many times, none worked and the problem persisted for long time
- We tried to search the web and Googled the error message
- We came across a discussion board that is talking about this 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 suggested in the link. A "red flag" that was overlooked was the suggestion here is to start the computer in *safe mode.* In hindsight, this allowed the malware to work without interference of any anti-virus software that was present on the computer. What a clear red flag, yet it was overlooked because of the ongoing frustration with the computer problems.

Functionality lost – Reading the ransom note

The family kept complaining that files could not be accessed on the computer. When any Word file was attempted to be opened or an image file was to be viewed, the computer displays strange characters (gibberish characters). When the problem persisted, we checked into the drive and found the following message in all sub folders under "My Documents" folder.

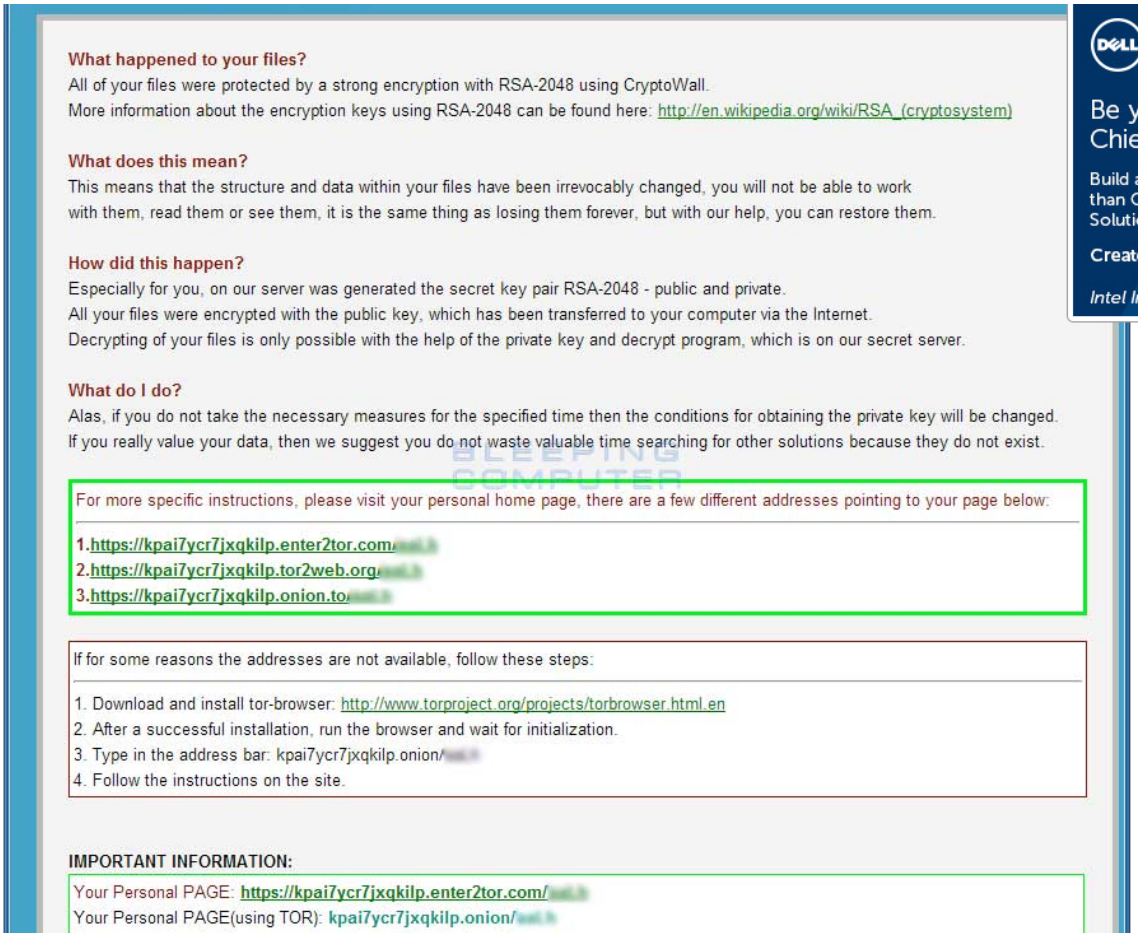

Figure 6. Example of the ransom message the author received

The same message was repeated in all folders and was saved in PDF format as well as JPEG format.

To pay/not pay

By the time we discovered this problem, the first deadline already passed. We began checking for a solution. We thought that this would be temporary, and that we could find a solution. We thought that if we copy the files to another computer, they would open. Possibly, if we updated our Malware Bytes and Sophos software the problem would be resolved.

Additionally, the ransom message was 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, we eventually decided that we would not pay the ransom. The second deadline passed and then ransom note disappeared which made it impossible to investigate how to pay, negotiate and fix the problem if we wanted to. Although we initially made the decision not to pay after the first message, we then decided to consider it. At the end, we were ready to accept the fact that the files we lost may have been lost for good. This included individual document files, vacation photo files, and other miscellaneous files saved under the. "My Document" folder. No system files were affected.

CONCLUDING REMARKS

While there was significant loss from this virus, the problem could have been much worse. The malware as installed in the safe mode could have roamed freely looking for any user name, password, financial, and sensitive information, Thus we are grateful that the damage was not extensive as it had the potential to be. Based on our experience, we provide the following suggestions for dealing with menace 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 became too old, too slow and having a lot of problems.

We learned a big lesson from our experience after being hit with ransomware, we realize that it could have been worse but we are grateful that it was not worse. Thus we explained our experience here and provided suggestions on how to deal with it, we hope it will help others in dealing with this menace of ransomware.

REFERENCES

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.

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

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

Heater , B. (2016). How ransomware CONQUERED The WORLD. PC Magazine, 109-118.

Heartfield, R., & Loukas, G. (2015). A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks. *ACM Computing Surveys (CSUR)*, *48*(3), 37.

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

Lazar, J., Jones, A., Hackley, M., & Shneiderman, B. (2006). Severity and impact of computer user frustration: A comparison of student and workplace users. *Interacting with Computers*, *18*(2), 187-207.

Lemos, R. Ransomware: What one company learned the hard way. *PC World. 33*(5), 45-48, May 2015. ISSN: 07378939

Luo, X., & Liao, Q. (2007). Awareness Education as the key to Ransomware Prevention. *Information Systems Security*, *16*(4), 195-202.LEMOS, R. (2015). 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.

Preda, Mila Dalla, et al. "A semantics-based approach to malware detection." ACM SIGPLAN Isohara, T., Takemori, K., & Kubota, A. (2011, December). Kernel-based behavior analysis for android malware detection. In *Computational Intelligence and Security (CIS), 2011 Seventh International Conference,* pp. 1011-1015. IEEE.

SentenialOne (2016). The Rise of Ransomware & How to Defend Against it. Whitepaper.

Shillam, R. (2016). What If Your Business Was Held To Ransom?. *IS Practices for SME Success Series*, 111 retrieved May 10, 2016 from http://commerce3.derby.ac.uk/ojs/index.php/itpsme/article/viewFile/15/13#page=111

Touchette, F. (2016). The evolution of malware. *Network Security*, *2016*(1), 11-14.

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.