International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 6201-6210

A Review on Ransomware Trend of Attacks and Prevention

Lam Zhanhui, Nor Azlina Abd Rahman

School of Computing and Technology, Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia.

Abstract

Ransomware is an emerging threat to the computer users as well as the organization that denies the user to access the files until the payment is cleared. This research paper will discuss about the evolution of the ransomware with statistics supported and the ways that ransomware can infects the computer systems. Other than that, the recommendations to the computer users when being infected and the preventive measures that can be done to reduce the chances of becoming a ransomware victim are included in the research paper. The objectives of this paper is to enhance the awareness of the computer users, especially in an organizational environment on the attack nature of the ransomware and taking proactive action to deter the ransomware attack.

Keywords: ransomware; evolution; transmission medium; countermeasures.

INTRODUCTION

Ransomware is a form of malware that denying the computer users access to the files and documents in their own system [1]. Apart from encrypting the files of various form in the computer, ransomware has the ability scramble the file names, add extensions to the files, requesting payments in to unlock the computer.

Ransomware infection was first detected in Russia 2006 since the occurrence in 1989 which zipped certain files and requested money from user to get the password to unzip the file [2]. Furthermore, ransomware applies RSA encryption which is much sophisticated compared to its predecessor [3]. Ransomware can be categorized into two major forms which are [4]

i) Locker ransomware which locks down the system

ii) Crypto ransomware which encrypts the files in the system

Symantec's 2015 report has indicated that United States of America is the country that have been most affected by the ransomware in both locker and crypto form. Figure 1 shows the Top 5 countries that are affected by ransomware.

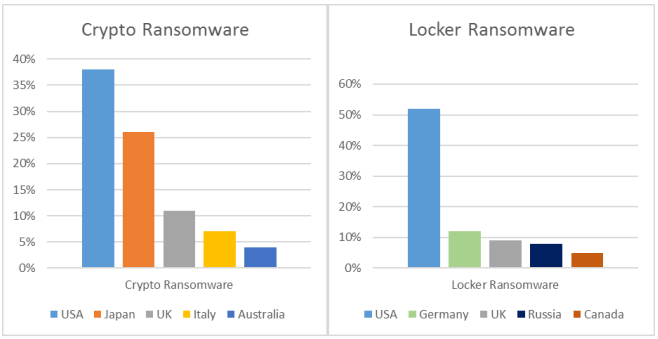

Figure 1: Symantec's report on Top countries with Crypto Ransomware and Locker Ransomware appeared [4].

Reference [5] argues that ransomware has becoming the most popular malicious software being dropped by exploit kits in the form of payload. Exploit kit as a toolkit that automates the exploits on client-side vulnerabilities by delivering payload to victims system [6]. Figure 2 shows the statistics of exploit payload summary.

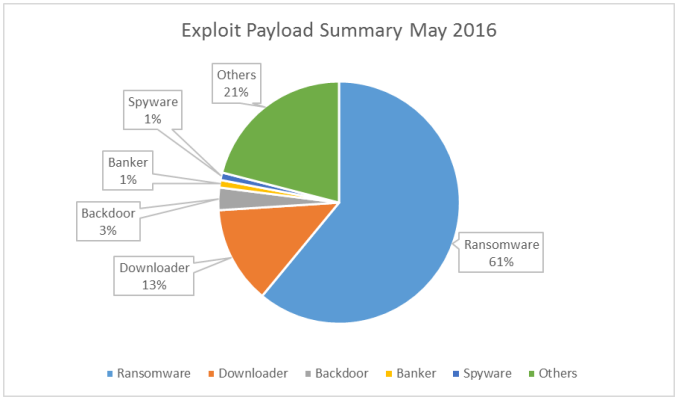

Figure 2: Types of payload summary May 2016 [5].

On the other hand, ransomware has started to invade the mobile devices as well [7]. The attacks of ransomware on mobile devices quadrupled at April 2015 to March 2016 compared to previous 12 months [8]. Kan's statement is supported by Kaspersky's statistics where the users who encountered ransomware spears from 35,413 to 136,532 throughout the observation period. Figure 3 shows the statistics of mobile ransomware that runs on Android [9], [10].

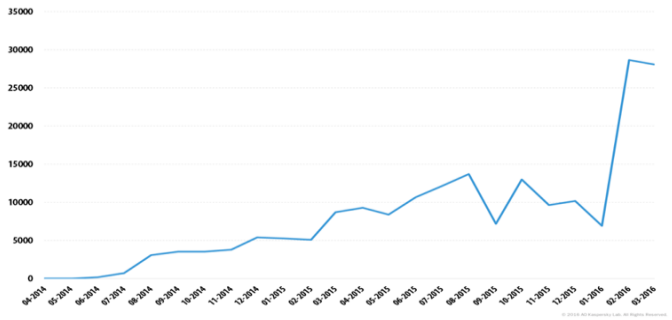

Figure 3: Amount of Android users that have encountered mobile ransomware in the period of April 2014 to March 2016 [9]

EVOLUTION OF RANSOMWARE

Ransomware has evolved since the first ransomware in 1989 and it is distinctively different today [4]. The ransomware back in 1989 which involves AIDS Trojan was deemed unsuccessful due to low amount of personal computer users except by the experts in science field and the transaction of payment internationally is difficult to process. Ransomware has affected users in various countries especially the well-developed countries such as USA and UK. As shown in figure 4, the evolution of crypto ransomware is fast-tracked in recent years as plenty of cybercriminals copied the concept of crypto ransomware to emulate the success of others.

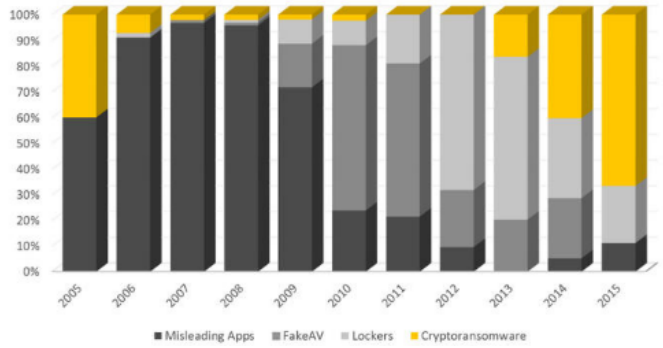

Figure 4: Evolution of Ransomware [4]

The first wave of crypto ransomware which is popular today occurred in 2005. For example, the symmetric encryption algorithm based ransomware is easy to decrypt and the authors continues with the concept. Archiveus was released in 2006 where it requests the victim to purchase pharmacy products online in order to obtain the password to decrypt the files [4].

The occurrence of crypto ransomware was minimized from 2007 to 2012 as the misleading advertisement dominates the malware attacks. During the period of 2011 and 2012, locker ransomware was emerging and charges around USD 180 to unlock the computer. The access of the computer can be regain through the use of security software.

The awareness has been increased among the public on the locker ransomware among the reason for the cybercriminal to move back to crypto ransomware. The crypto ransomware found in the PC today has high maturity with strong encryption procedures and demands for around USD 350 per computer. The use of disposable asymmetric key make the victim almost impossible to get back the information without paying the attacker.

HOW RANSOMWARE INFECTS THE COMPUTER

Ransomware attack consists of 5 phrases [11], [12] which are:

i) Exploitation

For a successful ransomware attack, the files that contains ransomware have to be executed on the computer. The exploitation is habitually complete through exploit kit and phishing email.

ii) Delivery and Execution

This phase is where the ransomware executable files have arrived to the system of the victim. This phase takes within a minute after the exploitation is completed.

iii) Damaging Backup Files

The ransomware will seek for the folders where the backup files is stored which includes the hidden path of the folder and damage it in order to prevent the computer users to perform backup restoration.

iv) Encrypting Files

After the backup files is inaccessible, the ransomware will perform secure key exchange with command and control server and generating the keys that will be implemented on the local system.

v) Notify users and demand for money

After deleted the backup files and encrypt the current files on the victim's system. The demand of payment will be prompted with the payment instructions to clear the ransomware as shown in figure 5. The price to unlock the infected device increases usually after a few days.

Figure 5: Image of WannaCry Ransomware which notifies the user [13].

On the other hand, ransomware can infects through 2 primary channels which are Emails and compromised websites [10].

A. Emails

Internet users utilize emails as one of the primary way to send and receive information. Cyber criminals seize the opportunity to launch the attack through the vulnerable center of victims' network with social engineering [10]. Phishing is a form of social engineering where the attackers send spoofed emails by masking as a trustworthy individual to the end users and tricking them to execute a suggested act that profits the attackers [14]. Reference [10] describes phishing as an effective ways to exploit the victims' machine backed by the statistics of 30% phishing emails will be open by the recipient. Apart from that, in March 2016, 90% of the phishing emails have ransomware included inside [15]. Figure 6 shows the phishing emails with ransomware inside from October 2015 to March 2016.

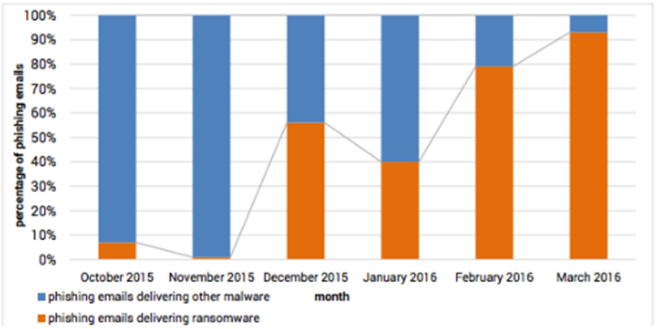

Figure 6: Phishing emails that contains ransomware and other malware [10].

The ransomware in the emails can either be in the form of infected attachments or links to the infected website.

Portable Document Format (PDF), Microsoft Office documents, PowerPoint slides and excel spreadsheet are among the common attachments that ransomware embedded in. To illustrate, Locky ransomware family utilize macros in Word document to execute the ransomware payload to victims' computer [16]. The recipient of the emails will be tricked to enable the macro as the documents will usually mentioned that it will not be displayed correctly unless macro is enabled. The macro with custom scripts will download the executable files of Locky and scans the drives on the victim's pc then encrypts the files and requests payment from the victim to unlock the files.

B. Compromised website

This ransomware invades method does not even require the interaction of the users to infect users' computer [17]. Rather than sending phishing emails, the attacker can put up malicious advertisement on a compromised website and redirects to the exploit kit website. To illustrate, when the visitor is using an outdated version of Adobe Flash Player the exploit kit can influence the vulnerability in the outdated software to download the ransomware. Reference [17] discusses on the Angler malware kit which infects established websites like BBC, New York Times with video advertisement where it does not even require the users to click on it. The ransomware will be installed when the video ads started to play. The discussion from Harbison has shown us that the internet users can become the victims of ransomware attacks even when browsing in reputable sites provided that the plugin such as Flash Player and Sliverlight is not up-to-date. Figure 7 shows the targeted websites in the video ransomware campaign.

Publisher	Traffic (monthly)*
msn.com	1.3B
nytimes.com	313.1M
bbc.com	290.6M
aol.com	218.6M
my.xfinity.com	102.8M
nfl.com	60.7M
realtor.com	51.1M
theweathernetwork.com	43M
thehill.com	31.4M
newsweek.com	9.9M

Figure 7: Targeted website for the ransomware video ads attack campaign. [17]

HOW THE MANAGERS OR OWNER OF THE BUSINESS TO PROTECT THEMSELVES

Business computers contains sensitive data which includes business plans, reports and customers database which is essential to the operation of the company's business [4]. Therefore, the managers and business owner should have the initiatives to protect themselves from ransomware as discuss below.

A. Develop the company staffs to have adequate awareness and knowledge on malware attacks

User security training is essential to secure the company's data and information to achieve data integrity [18]. Human, often being referred as the weakest link in the cybersecurity, is the main catalyst and the biggest vulnerability to malware attacks [19]. The attackers exploit the lack of knowledge and awareness of average internet users and launching the ransomware attacks on the organizations through the employee. Therefore, the manager of the organization should plan a comprehensive cyber security training to the employees in the organization to protect themselves from ransomware attacks.

The employees of different user group ranging from end users to senior manager should made compulsory to attend the

training on the cyber security which covers internet security threats and the ways to avoid falling into the traps set by the attackers. To illustrate, educate the employees to identify the phishing emails and not to response and click any link on that email, at best not opening any email for from unknown sources. On the other hand, include other logical analysis during the explanation during the training will leave the employees have a stronger impression in the mind. For example, it is not logical to receive an email from a third party to download the software from the link in the email to operate the computer smoothly. As the computer is managed by the organization and any updates will have a proper announcement from the management of the company rather than the third party email. Also, the IT managers should establish email security protocols and avoid peer to peer file sharing among the organization's network.

By increasing the awareness of the employees in the company with periodic training, the staffs in the company will have the updated knowledge on the latest malware attacks and be able to alert on the ever changing attack vectors. Hence, the company can keep themselves a further distance from ransomware attacks.

B. Backup the information periodically in various location

Most of the company do backup the data, but in an ambiguous way. The company could have stored a copy of backup data in the cloud storage without extra backup. Today's ransomware attack is sophisticated whereby the attackers locate the backup server systems through the network and encrypt it all together. Consequently, the backup cannot be retrieved when ransomware attacked into the computer of the organization's computer system. Therefore, the organization is require to draft the assets that need to backup which includes workstations and servers

A robust backup, especially off-site storage is necessary in order to keep the company's data retrievable when the attack happens. Reference [20] echoes the statement with the backup rules of 3-2-1, 3 backup copies by 2 different formats with 1 offsite backup.

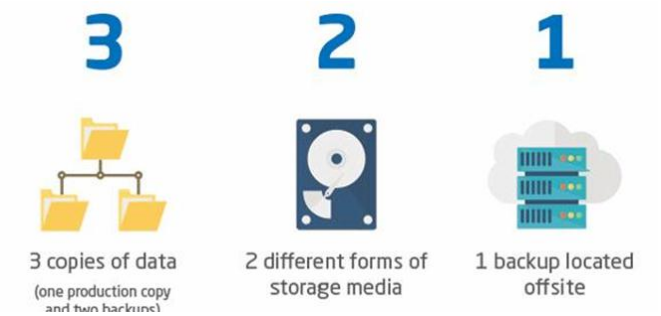

Figure 8: 3-2-1 backup rule [21].

To illustrate, the organization should have 3 copies of data for backup apart from the primary data. Also, the backups should be stored in different types of media such as hard disk and DVD. This will provide the extra protection when one form of backup fails due to the hardware problems. Then, 1 offsite backup is essential as if natural disasters happened onsite, there is still backup copy that can be retrieved. The company should store one of the backup files its branch company which is not connected to internet as well.

After backing up the data, periodically checking the files is essential as well to ensure that it is functionally. Reference [22] emphasizes that lack of consistency in backup testing will put the organization at risk as the backup files might be incomplete and having errors which will cause impact on the data recovery. The statement is supported by reference [23] where police department in Cockrell Hill, Texas lost 8 years of evidence after being infected by ransomware due to data could not be recovered from the backups. The incident have shown the importance of the validating the data from time to time.

With comprehensive backup of the company's information and regular testing on it, there will be sufficient resources to recover when it has been attacked by ransomware. Therefore, the company will not require to pay the attackers to unlock the files which can saves up a lot of money and uncertainty that might affects the operation of company.

Recommended Tool for Company to perform data backup

AOMEI Backupper is a recommended data backup and restore software due to the practical features that allows the users to backup and restore the files easily [24]. Also, the standard version is free for commercial use as well. This make the AOMEI Backupper a good tools for small organization with limited budget to have a backup system. There are various types of backup offered by the systems from system backups to file backups.

Figure 9: Interface of AOMEI Backupper

The staffs in the organization can schedule the backup by themselves especially on the files where the files that are not included in the organization backup with few clicks.

Below are the illustration to setup an automated file backup.

Step 1 Select the folder to backup

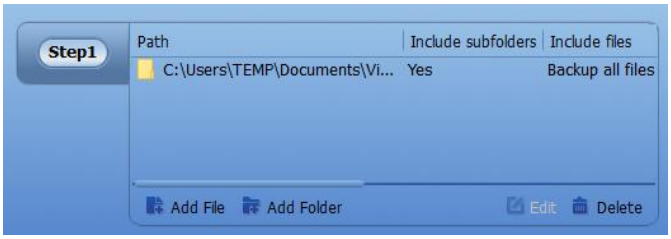

Figure 10: Folder selection tab of AOMEI Backupper

Step 2 Select the location to store the backup files.

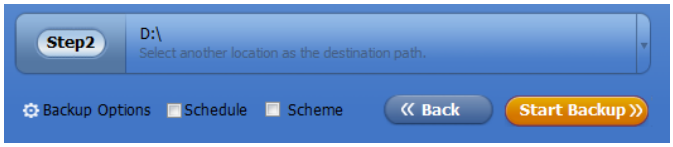

Figure 11: Location selection tab of AOMEI Backupper

Step 3 Click on the schedule options to customize the backup schedule

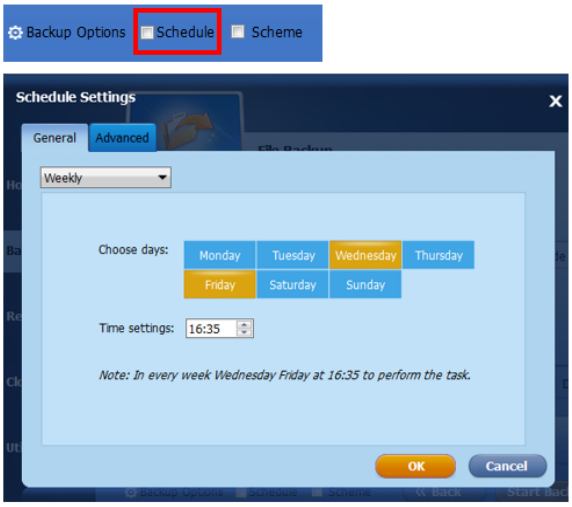

Figure 12: Schedule setting tab of AOMEI Backupper

After selected the backup location and the schedule, click on start backup will complete the backup process.

C. Network segmentation

Most of the ransomware will spread to the server from the endpoint. If the network of the organization does not have segmentation, the whole organization network will be affected. With network segmentation, the resources that the attackers can access will be limited. The ransomware cannot infects the other segment of the network which have no linkage.

Company should practice network segmentations based on the departments or based on the necessity [25], [26]. For instance, the communication to the network outside the company will be regulated as well as communication between the segments such as HR department and Project team. If the computer of the HR department is infected by ransomware, the network of the Project team will not the affected immediately. The limited access of the network will slow down the pace of the ransomware infection and let other departments to have sufficient time to make countermeasures on it hence limiting the damage to the whole company.

Therefore, network segmentation is essential to keep the critical devices and applications on the divided network to reduce the area of ransomware infects.

ADVICE TO VICTIM WHEN HIT BY RANSOMWARE

Ransomware can sneaks through email attachments and compromised network to infect the computer system without the user notice it until it is too late [27]. The statement made by Siciliano has been proven precise in the recent WannaCrypt ransomware outbreak. Reference [28] reports a ransomware named WannaCrypt outbreak in May 2017 which affected more than 200,000 machines globally with various field of organization such as healthcare and telecommunications companies affected.

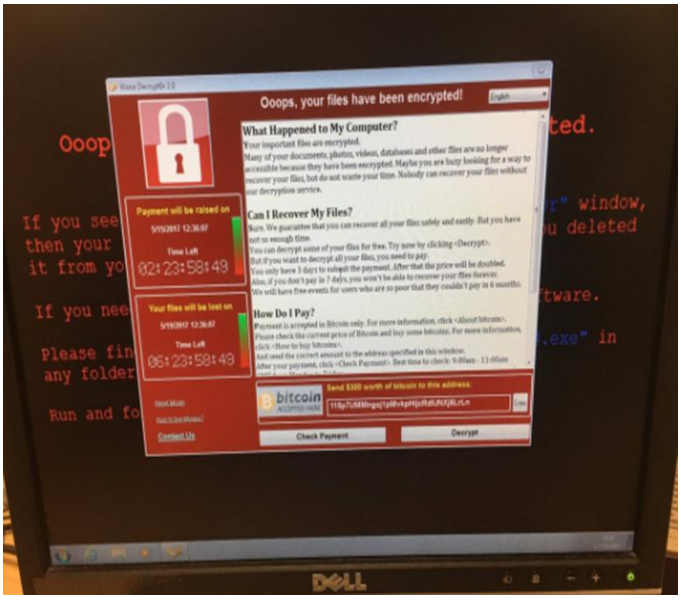

Figure 13: WannaCrypt infected PC in National Health Service England [29]

Paying to the ransomware attacker is not the first option an organization should perform as there is a chance of the files will not be back in the original state even after paying. The organization should do the following steps when the computer systems is infected by ransomware.

A. ***Stage 1*** *Isolate the infected computer from network*

The first thing to do is to disconnect the computer from the internet when it is infected by ransomware. Disconnecting the infected computer from the internet connection can minimize the propagation of the ransomware. Apart from that, the shared network drives must be taken care as well. Temporary disable the network share drive is sensible since the ransomware is capable of spreading through network share drive. Ransomware such as Locky and CryptoFortress will extend the infection from the compromised computer to the network shared drives which it is connected to [18].

B. ***Stage 2*** *Investigate on the ransomware*

The type of ransomware

After isolating the infected computer systems, it is to figure out what type of ransomware that the organization have been infected. The type of ransomware that infected the computer system usually can be determined by the file extension of the encrypted files. For instance, the file affected by ransomware with the extensions of Cerber ransomware will have an extension of .cerber while .locky belongs to Locky ransomware. Some of the ransomware is in a form of scareware where the files are not being encrypted properly therefore it is essential to determine the type of ransomware. With the file extension, the organization can check online there is decryptor available.

Tools that can be used to identify the types of ransomware

Ransomware Identifier

There are plenty of online tools available online to identify the types of ransomware which infected the computer belongs to. To illustrate, the Ransomware Identifier which is develop by Varonis. The tool search for the ransomware information from the raw data as illustrated below

BarRax	.BarRax			Based on HiddenTear		
Bart	.bart.zip .bart .perl		recover.txt recover.bmp	Possible affiliations with RockLoader, Locky and Dridex		BaCrypt
BitCryptor	.clf			Has a GUI. CryptoGraphic Locker family. Newer CoinVault variant.		
BitStak	.bitstak				Base64 + String Replacement	
BlackShades Crypter	.Silent		Hacked_Read_me_to_decrypt_files.html YourID.txt		AES (256)	SilentShade
Blocatto	.blocatto			Based on HiddenTear	AES (256)	
Booyah				EXE was replaced to neutralize threat		Salam!
Brazilian	.lock		MENSAGEM.txt	Based on EDA2	AES(256)	
Brazilian Globe		.id-%ID%_garryweber@protonm	HOW_OPEN_FILES.html			
BrLock					AES	
Browlock				no local encryption, browser only		
BTCWare	.btcware		#_HOW_TO_FIX_!.hta	Related to / new version of CryptXXX		

Figure 14: Sample of Raw data which utilized by Ransomware Identifier [30]

How to use Ransomware Identifier to search for ransomware type

Step 1 Visit the Ransomware Identifier website

https://www.varonis.com/ransomware-identifier

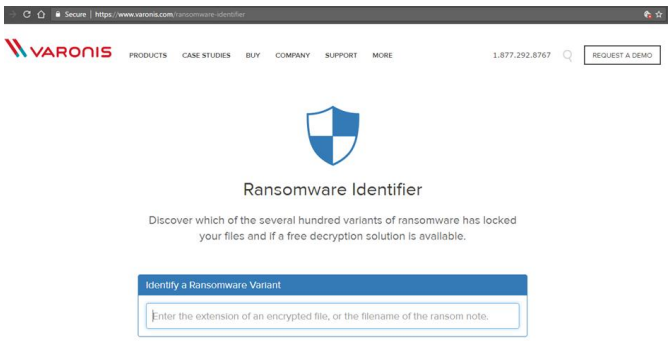

Figure 15: Webpage of Ransomware Identifier

Step 2 Type the file details (eg. filename, file extension) that have been infected by the ransomware in the search field.

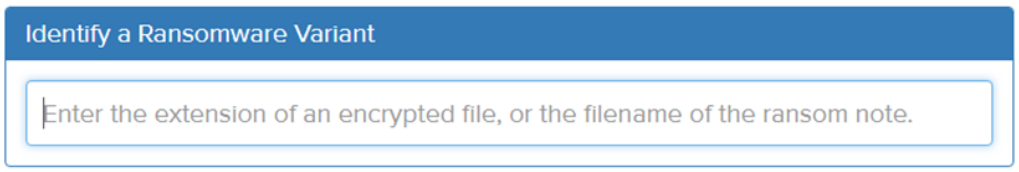

Figure 16: Text field to enter ransomware details

Step 3 Check the ransomware details

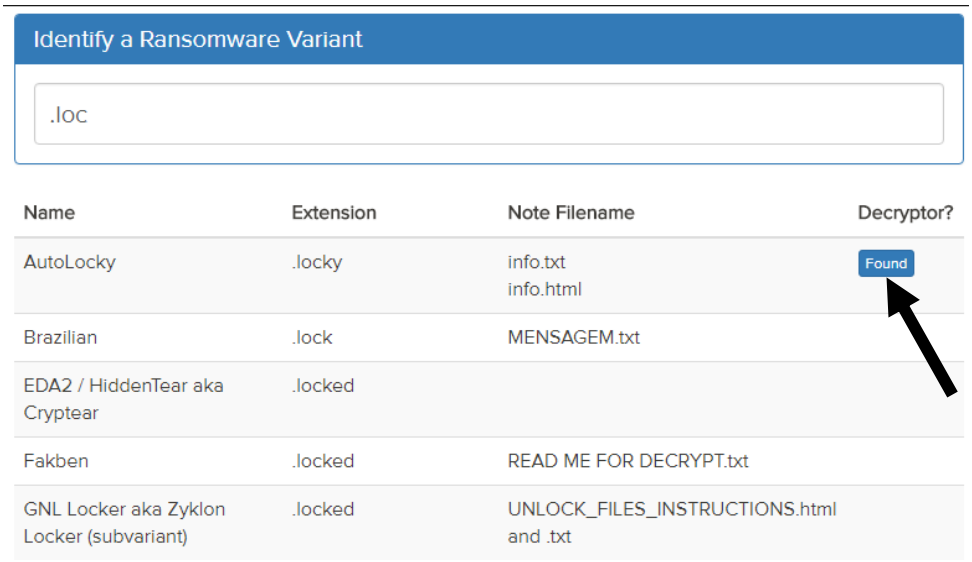

Figure 17: List of related Ransomware

The results which is related to the input given will be displayed and some ransomware type even have a decryptor available which is displayed with the arrow. If the decryptor is available, the victim can follow the link to download the decryptor.

Source of infection and the damage extent

It is essential to figure out the source of the ransomware attack in order to trace it down to determine the area which the ransomware has spread to. Viewing the file properties of the encrypted files to know the last user that appended the files is a good way to find out the first person in the organization infected by ransomware. Hence, the organization should discuss with the first person in the organization who have been infected with the ransomware. Through the discussion, recall the network and computer activities of the first infected user and share it to the colleagues to be cautious on the malware.

When the activities that have been done in step 2 is still unable to retrieve the information and remove the ransomware, performing restoration of the data to the computers are required.

C. ***Stage 3*** *Perform restoration of data*

If the files cannot be decrypted with the decryption tools, restore the files from backup is the activity should be done. The organization should perform a full format on the affected computers and revert it to factory settings in order to remove the malware completely and restore the information from the backup. Also, it is essential that not to include the ransomware during the restoration. One of the strategy can be done is performing roll back to the status where the ransomware has not infect the computer systems.

As discussed in the previous section, it is crucial to have a proper backup strategy from the organization. The proper backup will ensure that the files and information are able to restore properly when the incident like ransomware attacks happened.

If the company are not able to backup the files due to malfunction or outdated backup, the organization will have to

decide if the encrypted data is worth to retrieve by paying the attackers.

D. ***Stage 4*** *Strengthen the security policies*

After solving the incident, it is essential to review the ransomware attack process and evaluate the security policies in the organization. To illustrate, if the ransomware sneaked through email to infect the computer systems, identify the gaps in the security policies such as email filtering that allows the phishing mail to deliver to the system.

On the other hand, invest on comprehensive security training to educate the employees on the various malware attacks will help to strengthen the weakest link of the cybersecurity. Below are some of the suggested checklist to reduce the chances of getting infected by ransomware and easier to recover from the infection [31].

i) Constant patching of the software and security applications or automated patching

ii) Disable Microsoft Office macros

iii) Limit user access privileges to the job requirement only

iv) Restrict the usage of elevated privileges

v) Regular testing of the backup data

vi) Review Retention policy for different categories of data

In a nutshell, it is advisable for the companies that have been affected by the ransomware not to pay the attackers. The companies should seek for the alternatives which have been discussed above rather than paying ransomware as reference [16] emphasizes that the attacker will focus on attacking the companies that pays to unlock the ransomware again to gain more profit. In brief, once the organization paid the attackers to remove the ransomware, the higher chances that the organization will be hit by ransomware once again. Therefore, the organization should perform effective backup from time to time as a strategy to defend against ransomware.

CONCLUSION

Ransomware has emerged as the biggest threat to computer system in recent years. The increase of awareness among the internet users and organizations has made the attacker evolve the ransomware to a mature state where the architecture of the ransomware is sophisticated and harder to be detected and removed using common security tools. As the ransomware in today's world is not only a scareware where the files of the users is actually not affected, the internet users has low chance of retrieve their data back without paying the attacker. In the meantime where the complete solution to eliminate the ransomware infection, the organization and internet users should increase the awareness of various malware attacks and avoid the internet browsing behaviour which ransomware might attack from. Apart from that, keeping the systems software up to date with decent preventive measures are also good strategies to reduce the chances of the attack of the ransomware. Also, when the computer systems have been infected, do not pay to unlock the ransomware, by not paying to the ransomware attacker, they will not gain profit from transmitting ransomware to the victim and when everyone doing this, the attacker cannot sustain time loss without profit and stop developing more ransomware attack.

ACKNOWLEDGMENT

The author appreciates the guidance and constructive feedback provided by the supervisor, Nor Azlina Binti Abdul Rahman which essentially enhancing the quality of the research paper. Apart from that, the author would like to express gratitude to Asia Pacific University of Technology and Innovation for providing comprehensive resources which is beneficial for the author to conduct the research.

REFERENCES

[1] Zaharia, A., 2016. *What is Ransomware and 15 Easy Steps To Keep Your System Protected [Updated].*[Online] Available at: https://heimdalsecurity.com/blog/what-is-ransomware-protection/# ranso mwaredefinitionc [Accessed 1st April 2017].

[2] TrendMicro, 2016. *Ransomware.* [Online] Available at: https://www.trendmicro.com/vinfo/us/ security/definition/ ransomware [Accessed 4th April 2017].

[3] Sjouwerman, S., 2016. *What Is Ransomware?.* [Online] Available at: https://www.knowbe4.com/ransomware [Accessed 11th April 2017].

[4] Savage, K., Coogan, P. & Lau, H., 2015. *The evolution of ransomware,* s.l.: Symantec.

[5] Malwarebytes, 2016. *Ransomware dominates the threat landscape.* [Online] Available at: https://blog.malwarebytes.com/ cybercrime/2016/06/ransomware-dominates-the-threat-landscape/ [Accessed 12th April 2017].

[6] Zeltser, L., 2015. *What Are Exploit Kits?.* [Online] Available at: https://zeltser.com/what-are-exploit-kits/ [Accessed 12th April 2017].

[7] Symantec, 2016. *Internet Security Report,* Mountain View, California: Symantec.

[8] Kan, M., 2016. *Mobile ransomware use jumps, blocking access to phones.* [Online] Available at: http://www.pcworld.com/article/3090049/

security/mobile-ransomware-use-jumps-blocking-access-to-phones.html [Accessed 10th April 2017].

[9] Kaspersky Lab, 2016. *KSN Report: Mobile ransomware in 2014-2016.* [Online] Available at: https://securelist.com/analysis/publications /75183/ksn-report-mobile-ransomware-in-2014-2016/ [Accessed 10th April 2017].

[10] Crowe, J., 2016. *Ransomware by the Numbers: Must-Know Ransomware Statistics 2016.* [Online] Available at: https://blog.barkly.com/ransomware-statistics-2016 [Accessed 10th April 2017].

[11] Klein, T., 2017. *5 Phases of Ransomware Attack.* [Online]
Available at: http://www.edci.com/2017/03/5-phases-of-ransomware-attacks/ [Accessed 29th April 2017].

[12] DeNisco, A., 2016. *Infographic: The 5 phases of a ransomware attack.* [Online] Available at: http://www.techrepublic.com/article/infographic-the-5-phases-of-a-ransomware-attack/ [Accessed 13th April 2017].

[13] Epstein, Z., 2017. *WannaCry: Everything you need to know about the global ransomware attack.* [Online]
Available at: http://bgr.com/2017/05/15/wanna-cry-ransomware-virus-windows-wannacry-explainer/[Accessed 21st May 2017].

[14] Flores, W. R. & Ekstedt, M., 2013. *Countermeasures for Social Engineering-based Malware Installation Attacks,* s.l.: AIS Electronic Library (AISeL).

[15] Higbee, A., 2016. *Phishing and Ransomware Threats Soared in Q1 2016.* [Online] Available at: https://phishme.com/phishing-ransomware-threats-soared-q1-2016/ [Accessed 13th April 2017].

[16] Gallagher, S., 2016. *"Locky" crypto-ransomware rides in on malicious Word document macro.* [Online]
Available at:
https://arstechnica.com/security/2016/02/locky-crypto-ransomware-rides-in-on-malicious-word-document-macro/[Accessed 13th April 2017].

[17] Harbison, C., 2016. *New Ransomware Installers Can Infect Computers Without Users Clicking Anything, Say Researchers.* [Online]
Available at: http://www.idigitaltimes.com/new-ransomware-installers-can-infect-computers-without-users-clicking-anything-say-522756[Accessed 13th April 2017].

[18] Sjouwerman, S., 2017. *Ransomware Protection & Removal: How Businesses Can Best Defend Against Ransomware Attacks.* [Online]
Available at:
https://digitalguardian.com/blog/ransomware-protection-attacks [Accessed 14th April 2017].

[19] Vishwanath, A., 2016. *Cybersecurity's weakest link: humans.* [Online]
Available at: http://theconversation.com/cybersecuritys-weakest-link-humans-57455 [Accessed 14th April 2017].

[20] Hedge, M., 2016. *Disaster Recovery and the 3-2-1 Backup Rule.* [Online] Available at: https://www.contegix.com/disaster-recovery-and-the-3-2-1-backup-rule/ [Accessed 15th April 2017].

[21] Woodward, S., 2016. *How DRaaS Helps VARs And MSPs Grow Their Business.* [Online] Available at: https://www.bsminfo.com/doc/how-draas-helps-vars-and-msps-grow-their-business-0001 [Accessed 4th May 2017].

[22] Mook, D., 2013. *The Importance of Double-Checking Your Computer Backup Procedure.* [Online] Available at: http://www.thewanderinglensman.com/2013/05/the-importance-of-double-checking-your.html [Accessed 28th April 2017].

[23] Cimpanu, C., 2017. *Police Department Loses Years Worth of Evidence in Ransomware Incidents.* [Online]
Available at: https://www.bleepingcomputer.com/news /security/police-department-loses-years-worth-of-evidence-in-ransomware-incident/[Accessed 10th May 2017].

[24] Ellis, C., 2017. *AOMEI Backupper review.* [Online]
Available at: http://www.techradar.com/reviews/aomei-backupper
[Accessed 22nd May 2017].

[25] Gasca, P., 2016. *How Network Segmentation Can Help Entrepreneurs Manage Ransomware Risks.* [Online]
Available at:
https://www.entrepreneur.com/article/274379
[Accessed 15th April 2017].

[26] Thweatt, M., 2016. *3 Tips for Preventing A Ransomware Attack.* [Online] Available at: http://blog.wei.com/3-tips-for-preventing-a-ransomware-attack [Accessed 15th April 2017].

[27] Siciliano, R., 2017. *Ransomware: What You Should Know About This Dangerous Attack.* [Online] Available at: https://www.americanexpress.com/us/small-business/openforum/ articles/protecting-your-business-from-ransomware/[Accessed 10th January 2017].

[28] Jones, S., 2017. *Timeline: How the WannaCry cyber attack spread.* [Online] Available at: https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23 [Accessed 20th May 2017].

[29] Longfield, M., 2017. *Shocking that our @NHS is under attack and being held to ransom.* [Online] Available at: https://twitter.com/myleslongfield

/status/863046176899293191/photo/1 [Accessed 20th May 2017].

[30] Roth, F., Gillespie, M., Rivero, M. & Gallaghe, D., 2016. *Ransomware Overview.* [Online] Available at: https://docs.google.com/ spreadsheets/d/1TWS238xacAto fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml# [Accessed 1st May 2017].

[31] Mehmood, S., 2016. *Enterprise Survival Guide for Ransomware Attacks.* [Online] Available at: https://www.sans.org/reading-room/whitepapers/incident /enterprise-survival-guide-ransomware-attacks-36962[Accessed 16th April 2017].