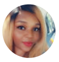
Ransomware Attacks: Critical Analysis, Threats, and Prevention methods



Asibi Imaji
Fort Hays State University

Ransomware Attacks: Critical Analysis, Threats, and Prevention methods

Asibi O. Imaji

Fort Hays State University

March 5, 2019

Table of Contents

Abstract

Ransomware has rapidly become one of the biggest threats on the internet, with new variations being deployed periodically. It is a growing threat to the data of businesses and as a result of the large amounts of money to be made, new variants appear frequently. Ransomware attacks have become a worldwide incidence, with the primary objective of making monetary gains through illegal means. It can result in loss of sensitive information, regular operations' disruption and harm to an organization's reputation. It encrypts targets' files and displays notifications, requesting for payment before the data can be unlocked. This malware is responsible for hundreds of millions of dollars of losses annually. The ransom demand is usually in the form of virtual currency, bitcoin because it is hard to track. This paper gives a brief overview of the history of ransomware, best practices in the bid to finding preventive measures, and lasting solutions to the menace of ransomware that challenge computer, network security, and data privacy.

Keywords: Ransomware, Ransomware families, data privacy, preventive measures, threat

Introduction

Ransomware is a form of malevolent software, or “malware,” that typically encrypts or deletes data stored on computer networks, trapping the data and making it unavailable and unusable (Cadwlader & Taft, 2017). The use of computer and the internet has skyrocketed, with more than 360 million people coming online for the first time during 2018, at an average rate of about 1 million new users each day (Kemp, 2019). Cybercriminals have emerged to feed off this growing market, aiming at unsuspecting users with an extensive array of threats such as worms, spyware, phishing, and other malware. Most of these threats are intended to make money from the victims. In 2015, a large portion of 140 million new malware was discovered, and ransomware made up a large portion of the malware. (Sgandurra, Muñoz-González, Mohsen, & Lupu, 2016).

Ransomware attacks have become more prevalent, brutal and recurrent. Factors such as anonymous payment processing and new sophisticated encryption methods have contributed to the rapid growth of ransomware nowadays (Balogun, 2018). In 2017, the FBI’s Internet Crime Complaint Center (IC3) received 1,783 ransomware complaints that cost victims over $2.3 million (De Groot, 2019).

According to Luo & Liao (2017), 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.). Knowing these files are of possible crucial importance to the victims, the attacker encrypts these files, making them impossible for the victim or owner to access. (Luo & Liao, 2017). Anyone with important data stored on their computer or network is at risk, including government or law enforcement agencies and healthcare systems or other critical infrastructure entities (Us-cert, n.d.).

Ransomware

Ransomware is a class of self-propagating malware that uses encryption to hold the victims' data ransom (Chen & Bridges, 2017). It is identified as a major threat to computer and network security across the globe and has emerged in recent years as one of the most dangerous cyber threats, with widespread damage. Payment does not guarantee that encrypted files will be released, and similarly decrypted file doesn’t mean that malware is removed from the system (Scaife, Carter, Traynor, & Butler, 2016).

Ransomware is one of the most expensive threats that can affect an organization. During 2016, the average ransom demand seen in new ransomware families increased dramatically, rising more than threefold from US$294 to $1,077 (O’Brien, 2017). Ransomware families occupy a vital place in malware families. Many users and organizations have been exposed to ransomware threat, resulting in major financial and reputation loss. The analysis, discussions, investigations, and measures to prevent cyber threats have been published by many researchers, automated approaches are also being introduced. Nath & Mehtre (2014) went so far as to compare various machine-learning techniques used for malware, focusing on statistical analysis. Again in 2016, Pathak covered the essential discussion of malware, malvertising and the attack methods used to distribute malicious advertisements and enlists several measures to combat the problem.

Types of Ransomware

Ransomware is pre-dominantly classified into two major types:

Crypto Ransomware

Crypto Ransomware finds and encrypts valuable data stored on the computer, making the data useless unless the user obtains the decryption key (Narain, 2018). It searches silently in the background until it targets a file, while the operating system and applications work normally so that no suspicion is raised at the end of the oblivious receiver (Thakkar, 2017). Crypto ransomware targets weaknesses in the typical user's security posture for extortion purposes (Lau, Coogan, & Savage, 2015).

Crypto ransomware has proven to cybercriminals to be a lucrative venture as evident from the number and variety of families of ransomware that has emerged (kalaimannan, John, DuBose, & Pinto, 2017). Crypto ransomware is designed to search for end-user files and data with extensions as FLV, PDF, RTF, MP3, MP4, PPT, CPP, ASM, CHM, TXT, DOC, XLS, JPG, CGI, KEY, MDB and PGP (Bhardwaj, Avasthi, Sastry, & Subrahmanyam, 2016).

Locker Ransomware

The locker ransomware typically takes the form of locking the computer's or device's user interface and then asking the user to pay a fee in order to restore access to it (Lau, Coogan, & Savage, 2015). It does not tamper with its victims' data but only locks their devices and leaves it with limited capabilities, such as only allowing the user to interact with the ransomware and pay the ransom. It also prevents the computer's Operating system and applications from running and likewise the computer from performing normal procedures. Since it is possible to remove most locker ransomware cleanly, cybercriminals tend to go to great lengths to incorporate social-engineering techniques to pressure victims into paying (Narain, 2018).

Evolution of Ransomware

The following examines the history of ransomware over twenty-six years, with approximate dates based on what is known about the ransomware. The ransomware has kept certain elements constant across its fast-paced evolution (Narain, 2018). While ransomware has been around for decades, ransomware variations have grown increasingly advanced in their capabilities for spreading, evading detection, encrypting files, and coercing users into paying ransoms (De Groot, 2019).

1989

The first ransomware virus to be discovered was called the AIDS Trojan, also known as the PC Cyborg. It was created by Joseph L. Popp, who was a Harvard-trained evolutionary biologist. The AIDS Trojan was released into the unsuspecting world through snail mail using 5¼" floppy disks (Lau, Coogan, & Savage, 2015). It was distributed at the World Health Organization's International Aids conference. It used simple symmetric cryptography to encrypt file names and tools were soon available to decrypt them (Sjouwerman, 2015). The AIDS crypto ransomware demanded payment by way of a check sent to a post office box in Panama.

2005

The first wave of modern crypto ransomware was Trojan.Gpcoder, it was released in May 2005 and initially used a weak and unsophisticated custom symmetric encryption technique that was easy to overcome. It generated a four-byte long encryption key (32-bit) which was then stored in the registry of the compromised computer; hence it was possible for people to find the key on the computer (Lau, Coogan, & Savage, 2015). It was spread through spam email attachment in disguise of job applications. Most of the early ransomware was created in Russia by Russian organized criminals. It was mostly aimed at Russian victims and those in neighboring countries, like Belarus, Ukraine, and Kazakhstan (Hughes, 2016).

2006

In early 2006, ransomware was starting to gain momentum, and more attackers started to be unraveled. Trojan.Cryzip appeared on March 2006 and copied data files to password-protected archive files and deleted the originals. It basically affected machines running Windows 98, ME, NT, 2000, XP, and Server 2003 (Hughes, 2016). It encrypts compress document files, database files, and multimedia files into a password-protected ZIP file. The decryption key used for the ZIP file is stored in file Cryzip (Qinyu, 2008).

The code for the malware included the password, so recovering it was straightforward. Trojan.Archiveus also came on the scene in 2006, it operated much like Trojan.Cryzip, the only difference was in the method of demanding for a ransom, it required victims to buy medication from specific online pharmacies and submit the order ID to get the password (Lau, Coogan, & Savage, 2015). Criminal organizations began using more effective asymmetric RSA encryption (Harshada & Ravindra, 2016).

2007

The Locker ransomware emerged in 2007, it did not involve encryption but basically locked out the user's devices (Sjouwerman, 2015). Early versions struck Russia and exhibited a pornographic image on the machine and required payment to remove it, either by text message or calling a premium-rate phone number that would generate revenue for the attacker (Zetter, 2017).

2008

A variant of Trojan.Gpcoder called GPcode.AK first appeared. It encrypts all files using a 1024-bit RSA algorithm key. It demands a payment of $100 to $200 in e-gold or Liberty Reserve (Tromer, 2008). The emergence of Gpcode ransom virus featured a 660-bit key, which could take security professionals about 30 years to break using a 2.2 GHz computer (Luo & Liao, 2017). Gpcode’s infection vector generates a thread to scan the directories and files for encryption, to locate archive and document file formats (Richa & Anuj, 2018).

2011

A ransomware worm named Trojan.Winlock emerged, it imitated the Windows Product Activation notice, making it more difficult for users to tell the difference between genuine notifications and threats (De Groot, 2019). The first large-scale outbreak of ransomware, mainly due to emerging anonymous payment services occurred during this period. The Trojan.Winlock blocked access to the keyboard and mouse and displayed an image using law enforcement imagery (Symantec, 2017). The image claimed a crime had been committed, and the victim must pay a fine to get access to a computer. There were about 30,000 new ransomware samples in the first quarter and 30,000 in the second quarter, by the third quarter there were 60,000 new samples (Sjouwerman, 2015).

2012

A toolkit called Citadel malware was used to produce and distribute a ransomware named Reveton. The ransomware lures the victim to a drive-by download website, and then it’s installed into the victims ‘computer (Foxworth, 2012). Cybercriminals bought another toolkit in 2012, called Lyposit. It is a malware that pretends to come from a local law enforcement agency based on the computer’s regional settings and instructs victims to use payment services in a specific country (Sjouwerman, 2016).

2013

This year witnessed a major change in the ideology and working patterns of ransomware with the discovery of crypto-ransomware and its elaborated family (Indu & Sharma, 2018). The first version of the CryptoLocker was posted on September 2013, it usually targets companies and individuals by sending emails and phishing attacks. If a user clicks on the executable files, it immediately starts to scan network drives, renames and encrypts all the files and folders (Harshada & Ravindra, 2016). This ransomware was released by a hacker named Slavik. It encrypts users’ files using asymmetric encryption, which requires public and private cryptographic keys to lock and unlock a victim's file (Zetter, 2017). It was distributed through the Gameover ZeuS botnet, which had been capturing online banking information since 2011 (Sjouwerman, 2016).

2014

On February 2014, a ransomware named CryptoDefense was released. It uses Tor and bitcoin for anonymity. It uses Windows’ built-in encryption APIs, which stores the private key in plain text on the infected computer (Sjouwerman, 2016). It is estimated that more than 500,000 victims were infected with CryptoLocker from September 2013 to May 2014, with an estimate of 1.3 percent of victims paid the ransom (Cannell, 2018). On May 2014, a coalition of law enforcement agencies and security vendors intercepted a worldwide network of hijacked home computers that was used to spread CryptoLocker (Titan HQ, 2018). The cybercriminals were intercepted while transmitting their key database for backup. Two vendors FireEye and Fox-IT released a service which allows victims to retrieve private decryption key and decrypt their files for free. CryptoDefense was released in February and earned $34,000 within its first month. An improved version called CryptoWall was released in April, it used Java vulnerability and was delivered via malicious advertising. (Sjouwerman, 2016).

2015

On January 2015, CryptoWall 2.0 was released into the market. This version uses a unique bitcoin address for each user and safely deletes unencrypted files (BleepingComputer, 2016). Towards the end of 2015, the FBI estimated that victims had paid $27 million in ransoms to the attackers behind CryptoLocker (Cannell, 2018). Hence, surpassing CryptoWall as the leading version of ransomware. The third and fourth version of CryptoWall was released in June and November of 2015 respectively. A study by Kaspersky found that for 2014-2015, ransomware attacks increased by 17.7 percent, but crypto ransomware attacks increased by 448 percent (Townsend, 2016). In May, ransomware-as-a-service was introduced, attackers used a TOR website to create ransomware for free. The site handles payment and takes a 20 percent cut of the ransom (Sjouwerman, 2016). Several strains of Ransomware-as-a-Service (RaaS) like TOX, Fakben, and Radamant appeared in 2015 (Sjouwerman, 2019).

2016

In January, a JavaScript-only ransomware-as-a-service (Raas) called Ransom32 was discovered. Ransom32 RaaS is a simple, but efficient, service where anyone can download and distribute their very own copy of the ransomware executable as long as they have a bitcoin address (Abrams, 2016). On April 2016, Petya ransomware was discovered. Petya makes the whole hard disk inaccessible, by overwriting the master boot record (MBR) of the infected computer until the ransom is paid (Fitzpatrick & Griffin, 2016). Research shows that Petya is the first significant ransomware to possess an entire offline cryptosystem design, which is placed at low-level (Narain, 2018). According to the Federal Bureau of Investigation (FBI), estimated losses of about one billion US dollars ($1 billion) was incurred to ransomware attacks in the year 2016 (Popoola, et al., 2017). In February, a malware called Xbot was found to be targeting Android devices in Australia and Russia. It encrypts files and steals online banking information (Kirk, 2016).

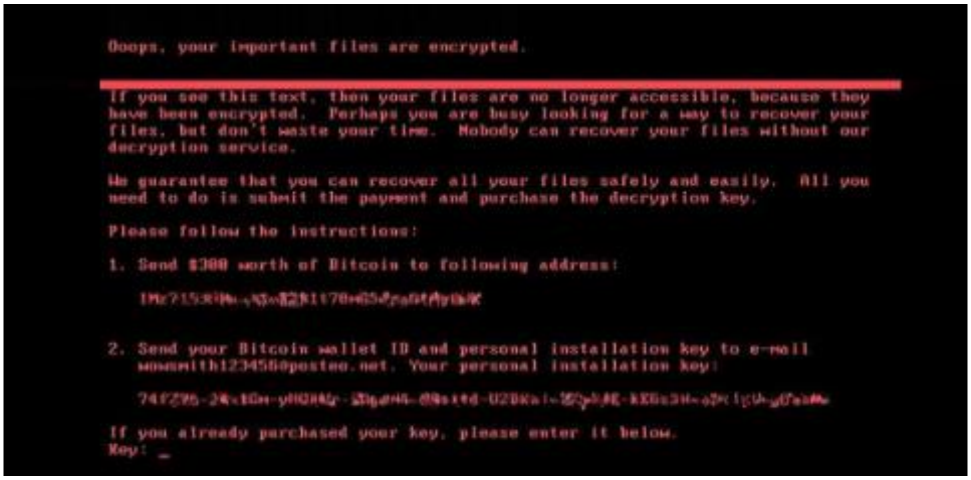
Ransomware Families

Ransomware families occupy a very important place in malware families. Many users, institutions, and organizations have been exposed to ransomware threat, resulting in major financial and reputation loss (Celiktas, 2018). The features of the most commonly known ransomware will be discussed below:

Petya Ransomware

Petya ransomware family was discovered on May 2016, its trademark includes infecting the Master Boot Record to execute the payload and encrypt the data available locally (Narain, 2018). It is a form of malware that infects a target computer, encrypts some of the data on it, and gives the victim a message explaining how they can pay in Bitcoin to get their data back (Fruhlinger, 2017). Petya can self-propagate like a worm, it does this by targeting computers and propagates using the Eternal Blue exploit. It also uses classic SMB network spreading techniques, and as a result of that, it can spread within organizations, even if they are patched against Eternal Blue (Symantec Security Response, 2017).

The following ransom note is displayed on infected computers, demanding payment to recover files:



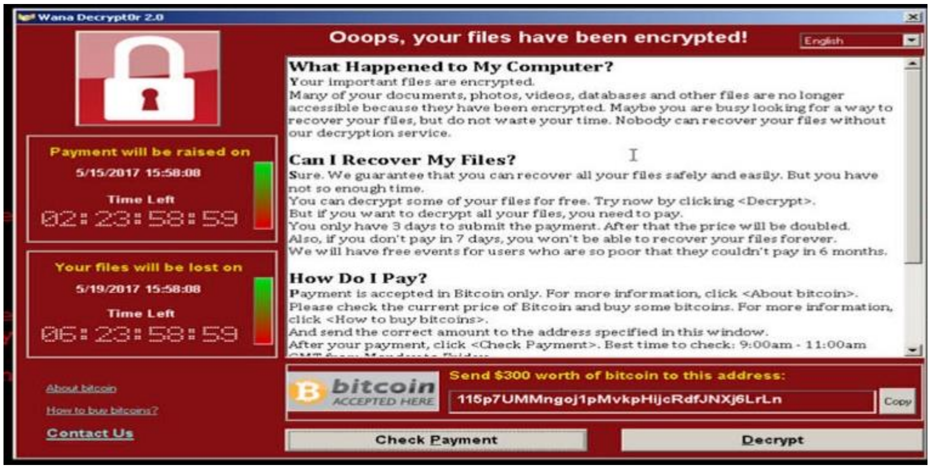
```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   74f296-[illegible]

If you already purchased your key, please enter it below.
Key: _
```

Figure1. Petya Ransom note (Verge Staff, 2017). The massive attack swept across systems worldwide and affecting a variety of companies. “Petya ransom note” by Verge Staff, 2017, *Petya ransomware: everything we know about massive cyber-attack.*

WannaCry Ransomware

On May 12th, 2017 the WannaCry ransomware disrupted hundreds of organizations in at least 150 countries (Lakhani, 2017). WannaCry ransomware attack was one of the largest attacks that were ever carried out, it grabbed the world by storm (Mohrule & Patil, 2017). The WannaCry ransomware targets Microsoft's widely used Windows Operating System, and it encrypts personal data, critical documents, and files. It demands at least $300 USD in bitcoin currency for the victim to unlock their file, which doubles after 3 days and the files are permanently deleted after 7 days. WannaCry Bitcoin addresses indicate that the attackers had received at least $100,000 after the first week. WannaCry ransomware attacked universities, transport sector, health sector, and telecommunication sector, implying that the ICT industry can’t bury its head in the sand but rather address the emerged new challenge (Zimba, Simukonda, & Chishimba, 2017). WannaCry ransomware preyed on unsuspecting users by capitalizing on imperfection in the structure of Microsoft Windows operating systems referred to as Server Message Block (SMB) protocol (Vigliarolo, 2017). It also demands for ransom in 28 languages.

The following ransom note is displayed on infected computers, demanding payment to recover files:



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

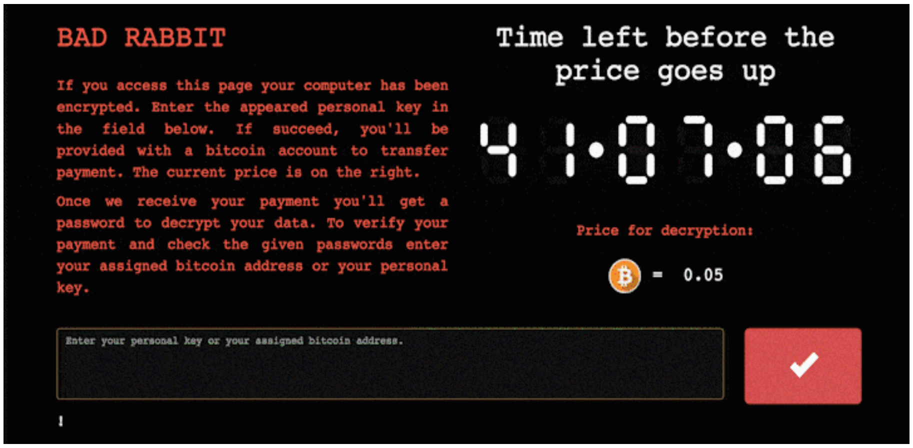
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Figure 2. WannaCry ransom note (Palmer, 2018). The attackers demanded $300 of bitcoin to be sent to a specific address and threatened to double the ransom if it wasn't paid within three days. "WannaCry ransom note" by Palmer, D., 2018, *WannaCry ransomware crisis, one year on: Are we ready for the next global cyber-attack*?

Bad Rabbit Ransomware

In September 2017, Bad Rabbit infected computers worldwide by showing itself as an Adobe Flash Player update patch (Celiktas, 2018). Bad Rabbit spreads through drive-by downloads on infected websites. In most cases of Bad Rabbit infections, visitors are tricked into clicking the malware by falsely alerting them that their Adobe Flash player requires an important update (Immanuel, 2019). Bad Rabbit infects the computer by attempting to spread across the network using a list of usernames and passwords buried inside the malware (Brenner, 2017). Bad Rabbit encrypts the contents of a computer and asks for a payment of $280.

The following ransom note is displayed on infected computers, demanding payment to recover files:



BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

41:07:06

Price for decryption:

₿ = 0.05

Enter your personal key or your assigned bitcoin address.

✓

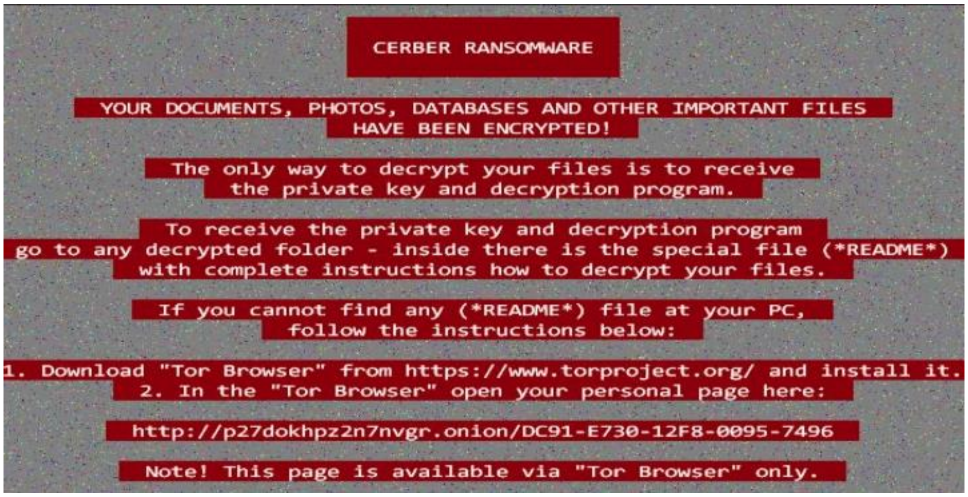
!

Figure 3. Bad Rabbit ransom note (Brook, 2017). Bad Rabbit Ransomware Hits Russia, Ukraine. Once infected Bad Rabbit requires victims to navigate to a Tor Hidden Service and pay attackers a fraction of a Bitcoin (0.05 BTC), roughly $280. "Bad Rabbit ransom note" by Brook, C., 2017, *Bad Rabbit Ransomware Hits Russia, Ukraine.*

Cerber Ransomware

The Cerber ransomware emerged in 2016, it was propagated by large spam operations, involving the distribution of emails with an attachment of a malicious Microsoft Word document. If a recipient were to open the document, a malicious macro would contact an attacker-controlled website to download and install the Cerber family of ransomware (Anubhav & Ellur, 2016). Cerber makes use of a ransomware-as-a-service (RaaS) model where affiliates acquire and then distribute the malware (Raymond, 2019). Once Cerber targets a system, it encrypts email, word documents, and gaming related files by attaching the encrypted files with the '.cerber' file extension (Spring, 2016). It is the first ransomware to interact with the victims, it leaves an audio record along with the ransom note (Liska & Gallo, 2017). It presents its information in 12 different languages, indicating it was a global attack. The Cerber ransomware demand $512 from its victims and the ransom will be doubled if the victim does not pay within seven days.

The following ransom note is displayed on infected computers, demanding payment to recover files:



CERBER RANSOMWARE

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES
HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive
the private key and decryption program.

To receive the private key and decryption program
go to any decrypted folder - inside there is the special file (*README*)
with complete instructions how to decrypt your files.

If you cannot find any (*README*) file at your PC,
follow the instructions below:

1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

http://p27dokhpz2n7nvgr.onion/DC91-E730-12F8-0095-7496

Note! This page is available via "Tor Browser" only.

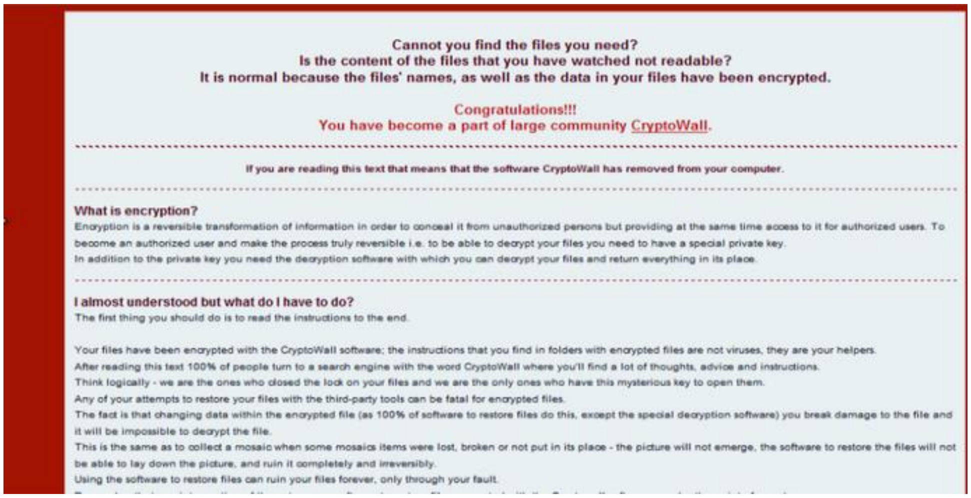
Figure 4. Cerber ransom note (Palmer, 2017). Bad Rabbit Ransomware Hits Russia, Ukraine. The ransomware uses very strong encryption and the ever-evolving nature of Cerber means there aren't any decryption tools available for the latest versions. "Cerber ransom note" by Palmer, D., 2017, *Now Cerber ransomware wants to steal your Bitcoin wallets and passwords too.*

CryptoWall Ransomware

Crptowall emerged on April 2014, it is a file-encrypting ransomware program that targets all versions of Windows including Windows XP, Windows Vista, Windows 7, and Windows 8 (BleepingComputer, 2016). Cryptowall infected more than 600,000 machines and encrypted about 5.25 billion files within 6 months (Celiktas, 2018). On June 2015, the FBI's Internet Crime Complaint Center identified CryptoWall as the most significant ransomware threat targeting US individuals and businesses (kalaimannan, John, DuBose, & Pinto, 2017). The Crypto Wall encrypts data by checking its command-and-control server and reporting the IP address of the infected computer (Richardson & North, 2017). The command-and-control server checks a database and returns a price for the country associated with that IP address (Lau, Coogan, &

Savage, 2015). CryptoWall initially demands about $500 ransom and after seven days about $1,000 (Celiktas, 2018).

The following ransom note is displayed on infected computers, demanding payment to recover files:



Cannot you find the files you need?
Is the content of the files that you have watched not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.

Congratulations!!!
You have become a part of large community CryptoWall.

If you are reading this text that means that the software CryptoWall has removed from your computer.

What is encryption?

Encryption is a reversible transformation of information in order to conceal it from unauthorized persons but providing at the same time access to it for authorized users. To become an authorized user and make the process truly reversible i.e. to be able to decrypt your files you need to have a special private key.
In addition to the private key you need the decryption software with which you can decrypt your files and return everything in its place.

I almost understood but what do I have to do?

The first thing you should do is to read the instructions to the end.

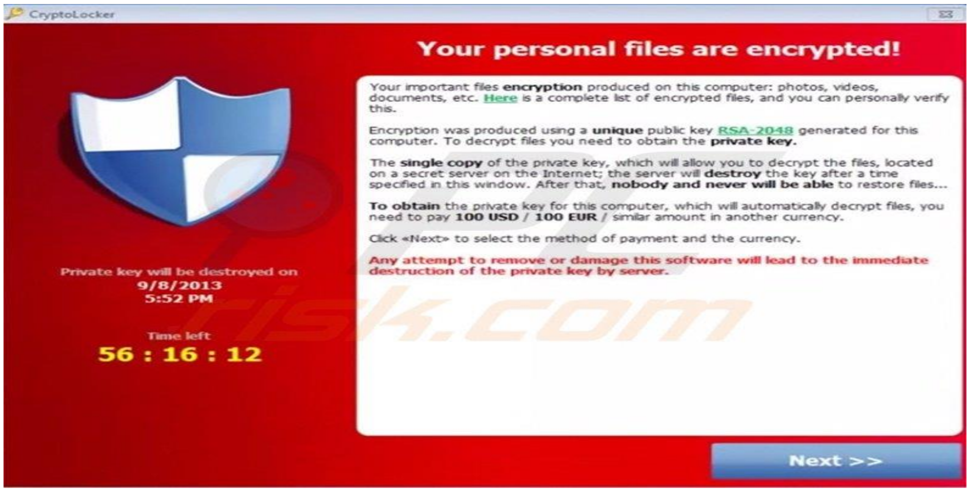
Your files have been encrypted with the CryptoWall software; the instructions that you find in folders with encrypted files are not viruses, they are your helpers.
After reading this text 100% of people turn to a search engine with the word CryptoWall where you'll find a lot of thoughts, advice and instructions.
Think logically - we are the ones who closed the lock on your files and we are the only ones who have this mysterious key to open them.
Any of your attempts to restore your files with the third-party tools can be fatal for encrypted files.
The fact is that changing data within the encrypted file (as 100% of software to restore files do this, except the special decryption software) you break damage to the file and it will be impossible to decrypt the file.
This is the same as to collect a mosaic when some mosaics items were lost, broken or not put in its place - the picture will not emerge, the software to restore the files will not be able to lay down the picture, and ruin it completely and irreversibly.
Using the software to restore files can ruin your files forever, only through your fault.

Figure 5. CryptoWall ransom note (Tsapakidis & Passidomo, 2017). CryptoWall has emerged as a breakthrough development in ransomware due to the strength of its cryptographic capabilities. “CryptoWall ransom note” by Tsapakidis, D., & Passidomo, 2017, *Detecting CryptoWall 3.0 Using Real-Time Event Correlation.*

CryptoLocker Ransomware

The CryptoLocker ransomware encrypts files using AES with a random key which is then encrypted with a 2048-bits RSA public key (Narain, 2018). CryptoLocker emerged in September 2013 with a widespread attack, and in just one month the attack generated over $34,000 in revenue (Symantec, 2014). CryptoLocker can enter a protected network through several vectors, such as email, file sharing sites, and downloads (Petters, 2018). After successful infection, crypto locker ransomware covertly searches for and encrypts the files that it deems most valuable (Cabaj & Mazurczyk, 2016). CryptoLocker is generally processed using recovery tools (Song, Kim, & Lee, 2016).

The following ransom note is displayed on infected computers, demanding payment recover files:



Your personal files are encrypted!

Private key will be destroyed on
9/8/2013
5:52 PM

Time left
56 : 16 : 12

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Figure 6. CryptoLocker ransom note (Meskauskas, 2017). CryptoLocker encrypts files on an infected machine and demands payment of a $300 in order to unblock the computer and decrypt the files. “CryptoLocker ransom note” by Meskauskas, T., 2017, *CryptoLocker.*

Emerging Trends in Ransomware

Law enforcement agencies are starting to pay attention to ransomware. This has forced criminals to change the way they operate. Ransomware attackers are using Tor to hide their tracks. The attackers make use of cryptocurrency like Bitcoin as a method of payment to hide their identity. As the pressure on ransomware increases, the criminals will likely look for more ways to block and obfuscate attempts to track and understand their activities (Lau, Coogan, & Savage, 2015). At first, ransomware was mainly a problem for the Windows platform. However, as discussed earlier, it has begun to move to Apple and Android systems. That trend is likely to continue. Researchers have written ransomware that can attack a smart thermostat (Fitzpatrick & Griffin, 2016). Already, locker ransomware that attacks smartwatches has been seen in the wild. As the world moves to the Internet of Things (IoT), there is no doubt that ransomware will move to the IoT. While that might seem farfetched at first, researchers have already been able to take over the computer systems of a moving Jeep Cherokee. If researchers can do it, so can ransomware (Lau, Coogan, & Savage, 2015).

How widespread is the problem of ransomware?

Most widespread ransomware makes intensive use of file encryption as an extortion mean. Basically, they encrypt various files on a victim's hard drives before asking for a ransom to get the files decrypted (Gazet, 2010). Ransomware has become a worldwide threat, causing individuals and organizations to lose a large sum of money. Even though it is a global problem, certain countries tend to be affected more than others. According to research surveyed by Symantec's telemetry has shown that some countries are most affected by ransomware, it was discovered that certain types of binary-based ransomware are more often targeted at particular countries like USA, Uk, Japan, Canada, Germany e.t.c. (Lau, Coogan, & Savage, 2015). The rise of ransomware as a cybersecurity threat is nothing short of spectacular, from its dormant introduction nearly three decades ago, to present day, where ransomware is widespread and has become a serious threat (Nieuwenhuizen, 2017). This telemetry shows that the cybercriminals behind ransomware are for the most part targeting more affluent or populous countries in the hope of finding rich pickings. As a result, 11 of the top 12 countries impacted by ransomware are members of the G20 organization, representing industrialized and developing economies that make up roughly 85 percent of the world's global domestic product (GDP).

Ransomware-as-a-Service

Cybercriminals have now started to provide services to those who wish to carry out ransomware attacks, by effectively providing ransomware-as-a-service (RaaS) (Ravindra & Harshada, 2016). Ransomware has already proven to be a lucrative activity for cybercriminal actors. A study in 2007, found that ransomware victims had paid more than $25 million in ransoms over the past two years, which is a significant amount of money that is likely to entice many other would-be criminals to want to get a piece of the earnings (Hahad, 2018). The success of crypto malware vector has not only led to the development of more and better ransomware, but also to the development of ransomware -as -a -service (Tuttle, 2016). Ransomware is now provided as a service via the Tor network (Dark Web). RaaS creators are able to host their code and systems on the dark web, where affiliates can subscribe to the service (Conner, 2018).

Ransomware-as-a-Service becomes a new trend because it allows nontechnical criminals to make attacks at a very low cost (Feng, Liu, & Liu, 2017). The growing ransomware-as-a-Service trend operates differently from ransomware threat. The malware developer recruits partners who spread the malware in return for a percentage of the profits. This tactic allows the malware to achieve a wider reach and generate greater revenue (Cerber, 2017). This enables non-technical attackers who may lack the necessary skills to develop malware to engage in highly profitable business and run independent campaigns. RaaS developers make an easy-to-use ransomware development kit available, which clients can buy and use to create ransomware that pays out to their own crypto-currency address (Nieuwenhuizen, 2017).

Ransomware-as-a-Service provided the cybercriminal with the ability to purchase ransomware creation kits and source code and distribute ransomware with very little technical knowledge (Alhawi, Baldwin, & Dehghantanha, 2018). RaaS creates a viable criminal business model that is easily available and deployed. A unique feature of RaaS service panel is that it is extremely user-friendly, this encourages more users to use the service which guarantees paybacks (Ganorkar & Kandasamy, 2017).

A case of widespread and cost-effective instances of RaaS occurred in 2016. The criminals released a ransomware variant called Stampado on the Dark Web for a cheap cost of $39. This price tag not only let non-technical hackers purchase the ransomware at an exceedingly low cost, but it also provided a lifetime license, essentially enabling anyone with $39 to instantly become a lifelong hacker as they wished (Hahad, 2018).

Ransomware operations continue to get more creative in monetizing their efforts, with Petya and Cerber ransomware pioneering ransomware-as-a-service schemes (De Groot, 2019). The effects of Ransomware-as-a-Service are negative and unlimited. This might lead to the creation of new ransomware versions much more aggressive than their originals (Ojeda, 2017).

Targets of ransomware

The cybercriminals behind ransomware do not particularly care who their victims are, as long as they are willing to pay the ransom. The following are the targets of ransomware:

Home users

Ransomware can prevent a user from accessing a device and its files until a ransom is paid to the attacker, most frequently in Bitcoin (Paquet-Clouston, Haslhofer, & Dupont, 2018). Home users should have knowledge of ransomware, and the reaction methods to take when hit with this malware. Even advanced computer users can be hit and suffer from ransomware attacks (Ali, 2017). Hence, awareness is very essential. The installation of the ransomware is often accompanied by a ransom note. The ransom note contains the details of the amount to be paid and the time frame for payment. When the user clicks on the executable ransomware file, it immediately starts to scan network drives, renames all the files & folders and encrypts them (Harshada & Ravindra, 2016). The goal of ransomware is to stay unnoticed until it can find and encrypt all the files that could be important and valuable to the user (Narain, 2018).

Organizations

Today's organizations confront not only keen peer competition in business society but also increasingly sophisticated information security threats in the cyber world, an online presence and business transaction are considered as a possible profit-driven avenue, and a necessary means for global competence (Luo & Liao, 2017). Notably, at first individual users were the main target of ransomware, but recently a shift towards attacking companies and institutions is observable (Cabaj & Mazurczyk, 2016). Symantec has previously observed that attackers traditionally blackmail businesses by unleashing an unexpected distributed denial-of-service (DDoS) attack against an organization's servers and then following up with an extortion demand (Lau, Coogan, & Savage, 2015).

Servers

The server performs a lookup of the IP address and determines the country that the infected computer is located in. Then, based on various factors, the price returned to the infected computer is adjusted to suit the location (Lau, Coogan, & Savage, 2015). Company desktops and servers are more likely to contain sensitive or critical data, e.g., customer databases, business plans, source code, tax compliance documents, or even webpages. (Cabaj & Mazurczyk, 2016). The ransomware must communicate with a server to get an encryption key and report its results. This requires a server hosted by a company that will ignore the illegal activity and guarantees the attackers' anonymity (Richardson & North, 2017). Ransomware applications collect information like IMEI number, call logs, contacts, profile, history bookmarks, SMS, the list of accounts in account service, phone state, GPS location of the phone, and IP address. Some of the ransomware even check the tasks running on the device. Ransomware Simplocker family contacts Command and control server and sends the information found on the mobile device to the attacker (Zavarsky, 2016). German organizations reported the highest level of ransomware infection via desktop computers among the nations we surveyed, as well as the highest level of infection through servers (Malwarebytes, 2016).

Mobile Phones

Ransomware has evolved to attacking mobile phones, by changing the PIN number of the phone and demanding for payment to have access to the phone. In 2015 new Android ransom-lockers known as Android/Lockerpin.A was unleashed by Cyber criminals. Once it infects the system, users cannot regain access to their device without root privileges or without some other security management solution installed, apart from a factory reset which would also delete all their data (Stefanko, 2016). Ransomware families continue to increase as variants are now being introduced for mobile devices apart from just home systems or portable devices like laptops (Narain, 2018).

Preventing strategies of Ransomware

Experts have recommended the following ways for individuals and businesses trying to prevent a ransomware infection and for dealing with the infection if it happens:

Educate and inform

The computer, banking, and retail industries need to develop and implement a major initiative to educate current and potential customers on how to be safe and secure online. The key is to promote the awareness and education of corporate employees, management as well as individuals' users and small business owners (Luo & Liao, 2017). Education is essential to protect your business from ransomware. It's critical that your staff understands what ransomware is, and the threats that it poses. Provide your team with specific examples of suspicious emails with clear instructions on what to do if they encounter a potential ransomware lure (Brunau, 2018).

Make backups plan

If the data is backed up, there is no need to pay a ransom to get the data back. Instead, it can be recovered from the backups (Zetter, 2017). Of course, the backups need to be up to date. It is essential to maintain backups of critical data that are maintained separately from the organization’s internal computer network and regularly testing the backups to ensure they work correctly (Cadwlader & Taft, 2017). A survey carried out by Osterman research on those that chose not to pay the ransom that was demanded from them showed that availability of recent backups was cited frequently as the reason that the organization could opt for the decision not to pay the ransom (Osterman, 2016). Backups can be used to restore data and systems to a known good state prior to ransomware infection (Thomas & Galligher, 2018).

Understand the Risks

Organizations cannot make good decisions regarding prevention without understanding the full extent of the threat that ransomware makes to the organization (Richardson & North, 2017). Recognizing the risk involved as regards to ransomware ensures that necessary protections are in place. Threat intelligence helps you take steps to make changes to protect your organization and make better decisions not only on attacks that are happening but attacks that are coming in the very near future (Todros, 2018).

Develop Adequate Policies

It is important to understand how to use technology along with policy and practices. Most ransomwares are propagated by spear phishing. This is most of the times facilitated by information gathered through social media. Hence, it is essential to set up a social media policy in place that limits work-related information, such as job titles from being posted on social media (Lord, 2018). A policy that limits what a user can access, minimizes the areas ransomware can attack.

Institute Best Practices for Users

These would include avoiding malicious links or attachments from a seemingly suspicious, organizing information security practices and security awareness for employees, invoking advanced security threat intelligence in an organization and collecting threat indicators from across the organization (Lord, 2018). The U.S. Government (USG) also recommends the following: Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users, configure firewalls to block access to known malicious IP addresses, set anti-virus and anti-malware programs to conduct regular scans automatically, execute operating system environments or specific programs in a virtualized environment, and consider disabling Remote Desktop Protocol (RDP) if it is not being used (FBI, 2016).

Avoid Email Links and Attachments

These would include issuing a notice to all employees not to open unknown attachments and emails, recommending blocking executable and zip file attachments, and instructing all employees not to check their personal email on the company's computer, as most free email services will not have advanced security scanning of attachments (Correa, 2017). The most common channel of delivery of ransomware is by masquerading the malware like a Trojan horse via an email attachment (Shashidhar, 2017). Attackers use different social engineering techniques to implore the victim to open attachments or to follow a link which consequently results into the installation of the ransomware and subsequent infection (Zimba, Simukonda, & Chishimba, 2017).

Reaction Strategies of Ransomware

Patching software

One of the response plan to ransomware is to patch any security holes (Brunau, 2018). When WannaCry ransomware came into the scene in 2017 and the vulnerability was discovered, Microsoft issued a critical patch for all Windows versions that were currently supported at that time, these included Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, and Windows Server 2016, in addition to Windows Vista (Vijayalakshmi, Natarajan, Manimegalai, & Babu, 2017). WannaCry outbreak is a significant security incident that spurs everyone to consider the fundamentals of patching computers to current status (Da-Yu, Shou-Ching, & Raylin, 2018). Organizations should be more diligent about patching software vulnerabilities. Long delays in upgrading or applying critical software patches in organizations offer great opportunities for attackers (Morato, Berrueta, Magaña, & Izal, 2018).

Drop-and-Roll

At the first sign of an infection, the infected system should be disconnected from the network, turn off all Wi-Fi and Bluetooth, and remove any external drives, USBs or devices (Shaw, 2016). Lastly, restore your data from your latest backup.

Use a ransomware decryption tool

This tool is essential for removing ransomware viruses from the computer and decrypting any file that has been encrypted during the attack.

Reaction Strategy for Android Devices

According to Avast (2016), the following are general steps to remove ransomware by entering Safe Mode and uninstalling suspicious apps (These steps can vary depending on the device):

Boot Android into Safe Mode

Find the power button and then press it for a few seconds until you see a menu.

Click Power off.

Once you receive a dialog window that suggests you reboot your Android to Safe Mode, select this option and press OK.

If this does not work for you, just turn off your device and then turn it on.

Once it becomes active, try pressing and holding Menu, Volume Down, Volume Up or both these buttons together to see the option for Safe Mode.

Uninstall ransomware and/or any suspicious and unknown apps

When in Safe Mode, go to Settings. Then, click on Apps or Application manager (this may differ depending on your device).

Look for the previously-mentioned suspicious app(s) and uninstall them all.

What does the future hold for ransomware?

Ransomware is still a major threat to users worldwide, and large-scale attacks, such as WannaCry and Petya are still causing havoc to organizations outside of ransom demands (Grant & Parkinson, 2018). Ransomware could grow larger as a result of the online supply available to anyone who is willing to use it.

Ransomware has a reputation for targeting many users as quickly as possible. It uses mass phishing campaigns to encrypt important files and documents. Recently, random ransomware campaigns deliberately targeting enterprise networks, have come to light. However, this is an indication of what's to come; a portent for the future of ransomware (Largent, 2016).

The emergence of RaaS implementations is another possible indicator that the crypto ransomware idea is close to maturity and market saturation (Lau, Coogan, & Savage, 2015). Some of the most advanced cybercriminals are monetizing ransomware by offering ransomware-as-a-service programs, which has led to the rise in prominence of well-known ransomware like CryptoLocker, CryptoWall, Locky, and TeslaCrypt. CryptoWall (De Groot, 2019). The main and ultimate purpose of Ransomware as a Service (RaaS) is earning money, hence this is a growing market.

Ransomware will probably get to the point where there would be no reverse to encryption, as the length of ransomware encryption keys is pushing the boundaries of modern cryptography. For example, if add a rootkit to hide the installer of the ransomware so that if we break its password it then randomly encrypts the files again, or after say five failed logins, it scrambles everything. In this way, it can hold us to total ransom. But so far, no fancy rootkits like this has been reported. Overall, Trojans which archive data tend to present a threat to Western users; Russian virus writers are more likely to use data encryption for blackmail purposes (Qinyu, 2008).

Focus on effective security

Ransomware payment methods, such as Bitcoin, often does not require the use of cash-out services due to the increased privacy afforded by the cryptocurrency. Cybercriminals are aware that law enforcement investigators are on their trail, so Bitcoin laundering services have sprung up to meet the demands of cybercriminals who don’t want to be identified. These shady businesses mix up bitcoins from legitimate sources as well those from ill-gotten gains (Lau, Coogan, & Savage, 2015).

The risks to corporate data can be mitigated through active security management, documented security policies, controlled access environments, skilled security personnel, and enterprise firewalls and backup solutions (Hampton & Baig, 2015). Insurance is a critical element of preparing for ransomware attacks. The forensic and information security experts available through cyber insurance policies are an important resource in examining the extent of damage and attempting to minimize downtime, for example, and some of the costs of paying a ransom and losses from business interruption may well be recoverable (Tuttle, 2016).

Increasing localization

Many of the G20 nations are affected by ransomware but is predominantly prevalent in the more affluent member countries (Lau, Coogan, & Savage, 2015). Ransomware initially emerged in Europe and then spread all over the world. Its primary focus was on affluent and English-speaking regions of the world. But increasingly we have seen cybercriminals turn their attention to countries in the Far East (Hamada, 2015). The message displayed by the ransomware threat can be localized depending on the user's location, with text written in the appropriate language (Power, 2015). The ransomware may only display a message in the language spoken by its authors. A variant that was specifically localized for Japanese targets, had the user interface's language translated to Japanese, and the image used was also changed to a cartoon character that has cultural relevance to the local population. This suggests that the cybercriminals, in this case, are aware of the popular culture of Japan and are likely to be Japanese nationals or are a foreign-based group with Japanese partners who provide the localization services (Lau, Coogan, & Savage, 2015).

The use of bitcoin as a method of payment serves as leverage for potential threats to become active attacks with unique attack vectors and zero-day vulnerabilities making it harder to trace the malicious attacker (Liska & Gallo, 2017). Cryptocurrency doesn't fall under the category of a national currency and it is quite easy to purchase from any of the existing bitcoin exchanges online (Lau, Coogan, & Savage, 2015).

Concise Conclusion

This paper presents a broad outline of ransomware in terms of its origin, evolution, malicious effects and prevention practices. Ransomware has become one of the most critical problems in the digital world. It is emerging as a serious threat and challenge to home users, companies, healthcare systems, and information security professionals. Given the feasible monetary gains, ransomware has become the focus of many cyber-criminals leading to its rapid growth. Majority of the countries have been hit by ransomware. Preventative measures should be taken regularly to back up important data and files. The purpose of this paper is to highlight the need to gain knowledge about the ransomware threat and accordingly take precautions and measures to prepare for and minimize hazard from ransomware attacks.

References

Abrams, L. (2016, January 4). *Ransom32 is the first Ransomware written in Javascript*. Retrieved from https://www.bleepingcomputer.com/news/security/ransom32-is-the-first-ransomware-written-in-javascript/

Alhawi, O. M., Baldwin, J., & Dehghantanha, A. (2018). Leveraging machine learning techniques for windows ransomware network traffic detection. *Cyber Threat Intelligence,* 93-106.

Ali, A. (2017). Ransomware: A research and a personal case study of dealing with this nasty malware. *Issues in Informing Science and Information Technology, 14*, 87-99. doi:10.28945/3661

Anubhav, A., & Ellur, R. (2016, July 18). *Cerber: Analyzing a Ransomware Attack Methodology To Enable Protection « Cerber: Analyzing a Ransomware Attack Methodology To Enable Protection*. Retrieved from FireEye: https://www.fireeye.com/blog/threat-research/2016/07/cerber-ransomware-attack.html

Avast. (2016). *What is Ransomware and how to Protect Yourself*. Retrieved from https://blog.avast.com/what-is-ransomware#how-to-remove-ransomware

Balogun, P. (2018, May 18). *Solution to2017 WannaCry Ransomware Attack By Cyber Criminals*. Retrieved from Academia: https://www.academia.edu/36712074/SOLUTION_TO_2017_WANNACRY_RANSOMWARE_ATTACKED_BY_CYBER_CRIMINALS

Bhardwaj, A., Avasthi, V., Sastry, H., & Subrahmanyam, G. V. (2016). Ransomware Digital Extortion: A Rising New Age Threat. *Indian Journal of Science and Technology, 9*(14), 17-19. doi:10.17485/ijst/2016/v9i14/82936

BleepingComputer. (2016, December 2). *CryptoWall and Help_Decrypt Ransomware Information Guide and FAQ*. Retrieved from Bleeping computer: https://www.bleepingcomputer.com/virus-removal/cryptowall-ransomware-information

Brenner, B. (2017, October 25). *Bad Rabbit ransomware outbreak*. Retrieved from Naked security: https://nakedsecurity.sophos.com/2017/10/24/bad-rabbit-ransomware-outbreak/

Brunau, C. (2018, July 26). Retrieved from https://www.datto.com/au/blog/how-to-protect-against-ransomware: https://www.datto.com/au/blog/how-to-protect-against-ransomware

Cabaj, K., & Mazurczyk, W. (2016). Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall. *IEEE Network, 30*(6), 14-20. doi:10.1109/mnet.2016.1600110nm

Cadwlader, W., & Taft, L. (2017). Wannacry Ransomware Attacks Should Be A Wake-Up Call for. *Clients & Friends Memo*, 1.

Cannell, J. (2018, February 21). *Cryptolocker ransomware: What you need to know*. Retrieved from Malwarebytes Labs: https://blog.malwarebytes.com/101/2013/10/cryptolocker-ransomware-what-you-need-to-know/

Celiktas, B. (2018). The Ransomware Detection and Prevention Tool Design by Using SIgnature and Anomaly-Based Detection Methods. *Istanbul Technical University*, 1-101. doi:10.13140/RG.2.2.16758.29765

Cerber. (2017, March 29). *CerberRing: An In-Depth Exposé on Cerber Ransomware-as-a-Service*. Retrieved from https://blog.checkpoint.com/2016/08/16/cerberring/

Chen, Q., & Bridges, R. A. (2017). Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware. *16th IEEE International Conference on Machine Learning and Applications (ICMLA)*. doi: doi:10.1109/icmla.2017.0-119

Conner, B. (2018, February 21). *Ransomware-As-A-Service: The Next Great Cyber Threat?* Retrieved from https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/

Constantin, L. (2016, April 14). *Ransomware authors use the bitcoin blockchain to deliver encryption keys*. Retrieved from CIO: https://www.cio.com/article/3056604/ransomware-authors-use-the-bitcoin-blockchain-to-deliver-encryption-keys.html

Correa, F. (2017). "WannaCry" Ransomware Attack. *Technical intelligence analysis*, 17-20.

Da-Yu, k., Shou-Ching, H., & Raylin, T. (2018). Analyzing WannaCry Ransomware Considering The Weapon And Exploit. *ICACT Transactions on Advanced Communications Technology (TACT), 7*(2), 1098-1107.

De Groot, J. (2019, January 3). *A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time*. Retrieved from Digital Guardian: https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

De Groot, J. (2019, January 9). *A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time*. Retrieved from Digital Guardian: https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

Ezhil, K., & Anthony, P. (2017). Influences on ransomware’s evolution and predictions for future challenges. *Journal of Cyber Security Technology, 1*(1), 23-31. doi:10.1080/23742917.2016.1252191

FBI. (2016, April 6). *How To Protect Your Networks From Ransomware: Technical Guidance Document.* Retrieved from FBI: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

Feng, Y., Liu, C., & Liu, B. (2017). Poster：A New Approach to Detecting Ransomware. *the 38th IEEE Symposium on Security and Privacy.* Retrieved from https://www.ieee-security.org/TC/SP2017/poster-abstracts/IEEE-SP17_Posters_paper_26.pdf

Fitzpatrick, D., & Griffin, D. (2016, April 15). *Cyber-extortion losses skyrocket*. Retrieved from CNN: https://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/index.html

Foxworth, D. (2012, August 17). *Citadel Malware Continues to Deliver Reveton Ransomware in Attempts to Extort Money*. Retrieved from The FBI Federal Bureau of Investigation: https://archives.fbi.gov/archives/sandiego/press-releases/2012/citadel-malware-continues-to-deliver-reveton-ransomware-in-attempts-to-extort-money

Fruhlinger, J. (2017, October 17). *Petya ransomware and NotPetya malware: What you need to know now.* Retrieved from csoonline: https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

Ganorkar, S. S., & Kandasamy, K. (2017). Understanding and defending crypto-ransomware. *ARPN Journal of Engineering and Applied Sciences, 12*(12), 3920-3925.

Gazet, A. (2010). Comparative analysis of various ransomware virii. *Journal in computer virology, 6*(1), 77-90.

Grant, L., & Parkinson, S. (2018). Identifying File Interaction Patterns in Ransomware Behaviour. *Computer Communications and Networks Guide to Vulnerability Analysis for Computer Networks and Systems*, 317-335. doi:10.1007/978-3-319-92624-7_14

Hahad, M. (2018, March 1). *Ransomware-as-a-Service: Hackers' Big Business*. Retrieved from https://www.securitymagazine.com/articles/88786-ransomware-as-a-service-hackers-big-business

Hamada, J. (2015, April 22). *Ransomware increasingly turning to the Far East*. Retrieved from Symantec: www.symantec.com/connect/blogs/ransomware-increasingly-turning-far-east

Hampton, N., & Baig, Z. A. (2015). Ransomware: Emergence of the cyber-extortion menace. *The Proceedings of the 13th Australian Information Security Management Conference*, (pp. 47-56). Edith Cowan University Joondalup Campus, Perth, Western Australia. doi:10.4225/75/57b69aa9d938b

Harshada, U. S., & Ravindra, V. k. (2016). Ransomware: A Cyber Extortion. *Asian Journal of Convergence in Technology, 2*(3). doi:10.1212/ajct.v2i2.55

Hughes, M. (2016, August 30). *A History of Ransomware: Where It Started & Where It's Going*. Retrieved from http://www.makeuseof.com/tag/history-ransomware-russia-reveton/

Immanuel. (2019, February 14). *Bad Rabbit | How to Prevent Bad Rabbit Ransomware Attacks*. Retrieved from Comodo Security Solutions: https://antivirus.comodo.com/blog/comodo-news/bad-rabbit-ransomware/

Indu, R., & Sharma, A. (2018). Ransomware: A New Era of Digital Terrorism. *Computer Reviews Journal, 1*(2), 168-226.

kalaimannan, E., John, S. K., DuBose, T., & Pinto, A. (2017). Influences on ransomware's evolution and predictions for future challenges. *Journal of Cyber Security Technology, 1*(1), 23-31. doi:10.1080/23742917.2016.1252191

Kemp, S. (2019, January 30). *Digital 2019: Global Digital Overview.* Retrieved from https://datareportal.com/reports/digital-2019-global-digital-overview?rq=Digital 2019: Global digital overview

Kirk, J. (2016, February 19). *A new Android trojan steals your banking info and holds your files ransom*. Retrieved from https://www.pcworld.com/article/3035106/a-new-android-banking-trojan-is-also-ransomware.html

Largent, W. (2016, April 11). *Ransomware: Past, Present, and Future.* Retrieved from https://blog.talosintelligence.com/2016/04/ransomware.html

Lau, H., Coogan, P., & Savage, K. (2015). Evolution of Ransomware. *Symantec*, 5-8. Retrieved February 2, 2019, from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

Liska, A., & Gallo, T. (2017). *Ransomware: Defending against digital extortion.* Sebastopol: OReilly Media.

Lord, N. (2018, December 14). *Ransomware Protection & Removal: How Businesses Can Best Defend Against Ransomware Attacks*. Retrieved from https://digitalguardian.com/blog/ransomware-protection-attacks

Luo, X., & Liao, Q. (2017). Awareness Education as the Key to Ransomware Prevention. *Information Systems Security, 16*(4), 195-202. doi:10.1080/10658980701576412

Malwarebytes. (2016). *Understanding the Depth of the Global Ransom Problem.* Black Diamond, Washington: Osterman Research.

Mohrule, S., & Patil, M. (2017). A Brief Study of WannaCry Ransomware Threat: Ransomware Attack. *International Journal of Advanced of Research in Computer Science*, 8(5), 1938 - 1940.

Morato, D., Berrueta, E., Magaña, E., & Izal, M. (2018). Ransomware early detection by the analysis of file-sharing traffic. *Journal of Network and Computer Applications, 124*, 14-32. doi:10.1016/j.jnca.2018.09.013

Narain, P. (2018). Ransomware - Rising Menace to an Unsuspecting Cyber Audience. The *University of Houston, Department of Information and Logistics Technology*. Retrieved February 28, 2019, from http://hdl.handle.net/10657/3145

Nath, H. V., & Mehtre, B. M. (2014). Static Malware Analysis Using Machine Learning Methods. *Communications in Computer and Information Science Recent Trends in Computer Networks and Distributed Systems Security*, 440-450. doi:10.1007/978-3-642-54525-2_39

Nieuwenhuizen, D. (2017). *A behavioral-based approach to ransomware detection.*

O'Brien, D. (2017). Internet Security Report: Ransomware 2017. *Symantec,* 17-19.

Ojeda, M. (2017, December 14). *Ransomware as a Service (RaaS): The new growing trend to face*. Retrieved from https://www.gb-advisors.com/raas-ransomware-as-a-service/

Osterman. (2016). *Understanding the Depth of the global ransom problem.* Black Diamond, Washington: Osterman Research.

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2018). Ransomware payments in the bitcoin ecosystem.

Pathak, P. B. (2016). Malware a Growing Cybercrime Threat: Understanding and Combating Malvertising Attacks. *International Journal of Advanced Research in Computer Science, 7*(2), 1-4.

Petters, J. (2018, October 22). *CryptoLocker: Everything You Need to Know*. Retrieved from Varonis: https://www.varonis.com/blog/cryptolocker/

Pope, J. (2016). Ransomware: Minimizing the Risks. *Innovations in Clinical Neuroscience, 13*(11), 37-40. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5300711/

Popoola, I. S., Iyekekpolo, U., Ojewande, S., Sweetwilliams, F., John, S., & Atayero, A. (2017). Ransomware: Current Trend, Challenges, and Research Directions. *In Proceedings of the World Congress on Engineering and Computer Science, 1*, 169-174.

Power, J. (2015, August 6). *Trojan.Ransomlock*. Retrieved from Symantec: https://www.symantec.com/security-center/writeup/2009-041513-1400-99

Qinyu, L. (2008). Ransomware: A Growing Threat To SMEs. *Southwest Decision Science Institutes,* (pp. 1-7). Brownsville.

Ravindra, K. V., & Harshada, S. U. (2016). Ransomware: A Cyber Extortion. *Asian Journal of Convergence in Technology, 2*(3), 1-6. doi: https://doi.org/10.1212/ajct.v2i2.55

Raymond, J. (2019, March 14). *Cerber Ransomware | What is Cerber Virus and how to remove them?* Retrieved from COMODO: https://antivirus.comodo.com/blog/how-to/cerber-ransomware/

Richa, I., & Anuj, S. (2018). Ransomware: A New Era of Digital Terrorism. *Computer Reviews Journal, 1*(2), 168-226.

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation, and prevention. *International Management Review, 13*(1), 10-21.

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. *IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*. doi:10.1109/icdcs.2016.46

Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. C. (2016, September 10). *Automated Dynamic Analysis of Ransomware: Benefits, Limitations, and use for Detection*. Retrieved from Cornell University: https://arxiv.org/pdf/1609.03020.pdf

Shashidhar, N. K. (2017). Ransomware Analysis and Defense-WannaCry and the Win32 environment. *International Journal of Information Security Science, 6*(4), 57-69.

Shaw, V. (2016, November 7). *Ransomware Virus Prevention: CryptoLocker, TeslaCrypt, Cryptowall & Locky*. Retrieved from https://www.smartfile.com/blog/ransomware-virus-prevention/

Sjouwerman, S. (2015). *A Short History and Evolution of Ransomware*. Retrieved from knowbe4: https://www.knowbe4.com/ransomware#ransomwaretimeline

Sjouwerman, S. (2016, January 22). *Ransomware on the rise: The evolution of a cyber attack*. Retrieved from TechBeacon: https://techbeacon.com/security/ransomware-rise-evolution-cyberattack

Sjouwerman, S. (2019, January 5). *First Javascript-only Ransomware-as-a-Service Discovered*. Retrieved from https://blog.knowbe4.com/first-javascript-only-ransomware-as-a-service-discovered

Song, S., Kim, B., & Lee, S. (2016). The Effective Ransomware Prevention Technique Using Process Monitoring on Android Platform. *Mobile Information Systems*, 1-9. doi:10.1155/2016/2946735

Spring, T. (2016, May 13). *Cerber Ransomware On The Rise, Fueled By Dridex Botnets*. Retrieved from Threatpost: https://threatpost.com/cerber-ransomware-on-the-rise-fueled-by-dridex-botnets/118090/

Stefanko, L. (2016). *Aggressive Android ransomware spreading in the USA*. Retrieved from http://www.welivesecurity.com/2015/09/10/aggressive-androidransomware-

Symantec. (2014, March 14). *CryptoDefense, the CryptoLocker Imitator, Makes Over $34,000 in One Month*. Retrieved from Symantec: https://www.symantec.com/connect/blogs/cryptodefense-cryptolocker-imitator-makes-over-34000-one-month

Symantec. (2017, March 16). *A short history of ransomware*. Retrieved from https://medium.com/threat-intel/ransomware-history-3165f10ab5a5

Symantec Security Response. (2017, October 24). *Petya ransomware outbreak: Here’s what you need to know*. Retrieved April 9, 2019, from Symantec Blogs: https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper

Thakkar, D. (2017). Preventing digital extortion: Mitigate ransomware, DDoS, and other cyber-extortion attacks. Birmingham, UK: Packt Publishing.

Thomas, J. E., & Galligher, G. C. (2018). Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware. *Computer and Information Science, 11*(1), 14-18. doi:10.5539/cis.v11n1p14

Titan HQ. (2018). *Investigating the increasing menace of ransomware!* Retrieved from https://www.titanhq.com/the-nuts-bolts-of-ransomware-in-2016

Todros, M. (2018, February 18). *Ransomware: Latest Developments and How to Defend Against Them*. Retrieved from https://www.recordedfuture.com/latest-ransomware-attacks/

Townsend, K. (2016, June 24). *History and Statistics of Ransomware*. Retrieved from https://www.securityweek.com/history-and-statistics-ransomware

Tromer, E. (2008). *Cryptanalysis of the Gpcode.ak*. Retrieved from http://rump2008.cr.yp.to/6b53f0dad2c752ac2fd7cb80e8714a90.pdf

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

Us-cert. (n.d.). *Ransomware*. Retrieved from Department of Homeland Security: https://www.us-cert.gov/Ransomware

Vigliarolo, B. (2017). *WannaCry: The Smart Person's Guide – TechRepublic.* Retrieved from http://www.techrepublic.com/article/wannacry-the-smart-persons-guide/

Vijayalakshmi, Y., Natarajan, N., Manimegalai, P., & Babu, S. (2017). Study on Emerging Trends in Malware Variants. *International Journal of Pure and Applied Mathematics, 116*(22), 479-489.

Zavarsky, P. &. (2016). Experimental analysis of ransomware on windows and Android platforms: Evolution and characterization. *Procedia Computer Science, 465-472*, 465-472.

Zetter, K. (2017, May 14). *What Is Ransomware? A Guide To The Global Cyberattack's Scary Method*. Retrieved from https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/

Zimba, A., Simukonda, L., & Chishimba, M. (2017). Demystifying Ransomware Attacks: Reverse Engineering and Dynamic Malware Analysis of WannaCry for Network and Information Security. *Zambia ICT Journal*, 1, 35-40.