A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat: Proceedings of ICDMAI 2018, Volume 2

Chapter *in* Advances in Intelligent Systems and Computing · January 2019

DOI: 10.1007/978-981-13-1274-8_31

2 authors:

Aditya Tandon
Krishna Engineering College

Anand Nayyar
Duy Tan University

A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat

Aditya Tandon and Anand Nayyar

Abstract Never in the history of humanity, people all over the world are subject to exaction on a huge scale as they are today. In the recent years, the usage of PCs and the Internet has exploded and, along with this huge increase, cybercrooks have come to feed this souk, aiming acquitted consumers with a wide range of per-ware. Most of these threats are meant unswervingly or meanderingly in receiving currency from victims. Today, the ransomware appears to be one of the most unpleasant per-ware categories of the time. Several works have been published in the field of information and Internet security, various pernicious attacks, and cryptography. The objective of this research paper is to present everything with regard to latest crypto-virus trend known as ransomware. The paper explains the history, the modus operandi as well as the architecture of ransomware attack.

Keywords Ransomware · Payoff · Cryptography · Trojan · Cybercrime Malicious code · Cybersecurity · Bitcoin

1 Introduction

Since the 50s, the world has seen the merits and the wonders of the Internet and World Wide Web (WWW). Every user today is now being connected to it at an immensely quick pace. The amount of data is now exceeding zettabytes (2^{70} bytes) since last year, and the concerns for its safety are now taking the shape of a major problem. Pernicious content and corrupt programs have been attacking and infecting various devices around the world, and the efforts for their prevention and eradication have also gained pace simultaneously. The software code written

A. Tandon (✉)
Ch. Brahm Prakash Government Engineering College, New Delhi, India
e-mail: adityat1988@outlook.com

A. Nayyar
Graduate School, Duy Tan University, Da Nang, Vietnam

V. E. Balas et al. (eds.), *Data Management, Analytics and Innovation*,
Advances in Intelligent Systems and Computing 839,
https://doi.org/10.1007/978-981-13-1274-8_31

especially toward causing damage or stealing information becomes what is known as per-ware (pernicious software) or per-ware in short.

Organization of Paper
Section 2 outlines the concept of ransomware as well as elaborates the types of ransomware and provides an insight of how the ransomware attack is commenced. Section 3 goes further into the concept of the basic framework of the ransomware outbreak by explaining the detailed steps involved and stating real life and recent examples. Section 4 highlights some of the tried-and-tested preventive measures and some detection (or symptoms) before any ransomware attack. Section 5 gives detailed explanation of WannaCry—the latest ransomware scare. Section 6 concludes the paper with future scope.

1.1 History

Since the advent of the digital era, worldwide aggressors have tested the security of various companies and institutions through e-mail, phishing sites, fake antivirus, etc. The encipherment method has been implemented to ensure the exchange of information around the world. However, the concept of poly-alphabet encipherment was proposed in AD 1467 by Leon Battista Alberti, often known as the "Father of Cryptology". The need for secure and selective communication has given rise to the art of encoding messages so that only recipients may have access to the information, while unauthorized denial of information extraction, although balderdash messages fell into his hand. Art and science to hide messages to enter secret information is called cryptography. An encipherment system has been designed to implement numerous cryptographic techniques and accompanying infrastructures to ensure the security of information. A typical model of a cryptosystem (also known as cipher system) is depicted in Fig. 1.

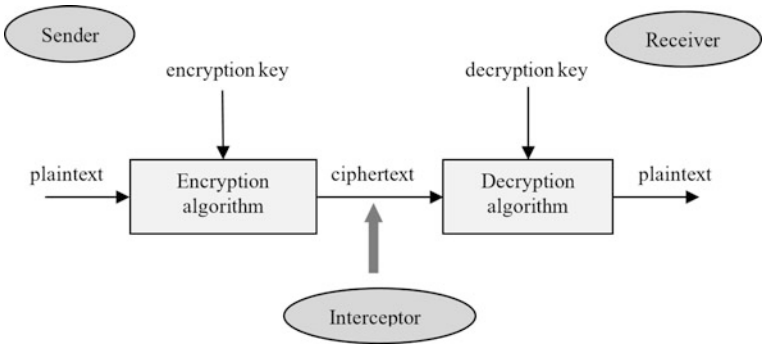

Fig. 1 A typical cipher system

This concept of applying the cipher system was a benediction to data dispensation and communications as atomic fission is to energy production. In both ways, these systems are vulnerable to attacks and, therefore, can be misused.

1.2 Concept of Ransomware

The concept of public-key cryptography (also known as symmetric-key cryptography) can also be used offensively as stated in [1]. Clearly, the authors predicted the methods used for our systems' security can be misused, also known as cryptovirology (amalgamation of public-key cryptography and Trojans or viruses). The first asymmetric ransomware prototypes were developed in the 1989 with the name Acquired Immune Deficiency Syndrome (AIDS) Trojan which was distributed through a less suspicious 5¼ floppy disk (since World Wide Web (WWW) was not famous enough) and given to the dignitaries who were attending a conference on an international level which happened to be about the AIDS disease [2]. The software enciphered file names (not the files themselves), displayed a demand for payment to a location in Panama. Ransomware is the kind of strategy that uses extortionary pernicious software to keep the computer system hostage user until a redemption is paid. Ransomware strikers often request bitcoin currency redemption due to the perceived anonymity of encipherment transactions. The per-ware blocks a user for a limited time after which the refunds or user data are destroyed [3].

Since 1990, how drastic the scare of ransomware spread throughout the globe is illustrated in Fig. 2 [4]. A typical AIDS (PC Cyborg) threat message is shown in Fig. 3.

2 Outlining Ransomware

Ransomware is a per-ware that employs asymmetric encipherment to hold a prey's information at payoff. Asymmetric (public–private) encipherment, also known as cryptography, uses a couple of keys to encode as well as decode a file. This public–private couple of keys are uniquely created by the invader for the prey, with the private key to decipher the files stored on the invader's server. The invader ensures that the private key becomes obtainable to the prey only after the payoff is paid, although that does not happen often—as observed in recent payoff software operations. Without the access to the private key, it is nearly impossible to decode the files that are being held for payoff.

It is commonly divided into two main forms—Locker ransomware and crypto-ransomware. Locker ransomware or PC locker refutes access to the PC or device. Crypto-ransomware or data locker foils access to files or data. It does not necessarily need to use encipherment to prevent users from retrieving their data, but most of the people do so. Both types of these payoff software are targeted directly at

Year	Ransomware
1989-90	- AIDS Trojan (PC Cyborg) becomes the first known ransomware.
2005-06	- Gpcode, TROJ.RANSOM.A, Archiveus, Krotten, Cryzip, and MayArchive. First to utilize encryption algorithms
2008	- Gpcode.AK. Utilized 1024-bit RSA keys
2010	- WinLock. Originated in Russia, flashed porn content on the computer screen until the user would make a $10 phone call to a premium-rate telephone number.
2011	- Unnamed ransomware Trojan. Locked the user's computer and directed the visitor to a fake list of phone numbers which they could call to reactivate their operating system.
2012	- Reveton ransomware would let the user know their machine has been utilized to download either copyright material or child pornography and would demand the user to pay a fine. A form of Scareware.
2013	- CryptoLocker, the most notorious ransomware. Had increased encryption, and was extremely difficult to prevent. - Locker is discovered and would demand a ransom payment of $150 in which the user had 72 hours to pay. - CryptoLocker 2.0 was released and utilized Tor to increase anonymity for payment. - Cryptorbit, another ransomware that utilized Tor and would encode the first 1024 bits of every file it encoded. Cryptorbit would also install a Bitcoin miner on the victim's machine to create more profit.
2014	- CTB-Locker (Curve, Tor, Bitcoin), would leverage elliptical curve cryptography. Tor for anonymity, and Bitcoin for payment. - CryptoWall, another infamous CryptoLocker clone that was responsible for infecting billions of files worldwide utilizing infected emails. - Cryptoblocker didn't encrypt Windows files that were over 100MB in size. Utilized AES for encryption. - SynoLocker targeted Synology NAS devices, and would encrypt all files.
2015	- CryptoWall 2.0 used for Tor for anonymity and was delivered through multiple attack vectors. - TeslaCrypt and VaultCrypt originally targeted computers that had certain games installed. Newer variants targeted non-gaming machines. - CryptoWall 3.0 shared some of the same features as its predecessor but added additional features such as Anti-VM check and was delivered via exploit kits. - CryptoWall 4.0 would not only encrypt the data in the files but the file names as well. It also would disable any system restore functionality and shadow volume copies. - Chimera was more of a scareware ransomware that not only encrypt files but also threatened the user that it would publish them online when ransoms are not paid. Also known as doxing.
2016	- Locky is ransomware that would not only encrypt the user's files, but would first scramble the files and then rename your file extensions to .locky. - SamSam targets servers instead of end-users. The ransomware exploits vulnerabilities in JBoss application servers and compromises the server to gain shell access. SamSam then proceeds to spread to Windows machines and encrypts their files.

Fig. 2 A chronology of notable ransomware development

Fig. 3 PC Cyborg threat message on PC screen

our digital routine. They are created to refute us the access to something we desire and to offer to return what belongs to us in paying for a payoff. While having similar aims, the approaches adopted by any type of payoff software are very distinguishable [4].

2.1 Locker Ransomware (PC Locker)

It was created to refute access to computing reserves. This characteristically requires the method of blocking the PC or device user interface (UI) and then prompts the user to pay a fee to restore access to it. Blocked PCs are often released with restricted functionality, such as allowing only the user to interact with the per-ware and recompense the payoff [5].

Locker ransomware is specially designed to prevent access to the PC's UI, leaving largely intact the basic system and files. This means that the per-ware could possibly be removed to restore a PC to something near its default state, thus making locker ransomware less active in extracting payoffs as shown in Fig. 4. Some victims of advanced users (or superusers) can often be accessed using various tools and techniques offered by security vendors. Since this type of ransomware can be easily cleaned, it tends to use social engineering methods to pressure victims to pay or perhaps disguise themselves from a police authority by sustaining fines for alleged online users or criminal activity rumors. Those devices which have restricted choices for the users to interact with, for example, Internet of Things (IoT) devices, are at potentially greater risk than other PC systems or mobile phones.

2.2 Crypto-Per-Ware (Data Locker)

This variety of per-ware aims to find and encipher important data stored on user's PC, making the data useless, unless the user gets the decipher key. As the world

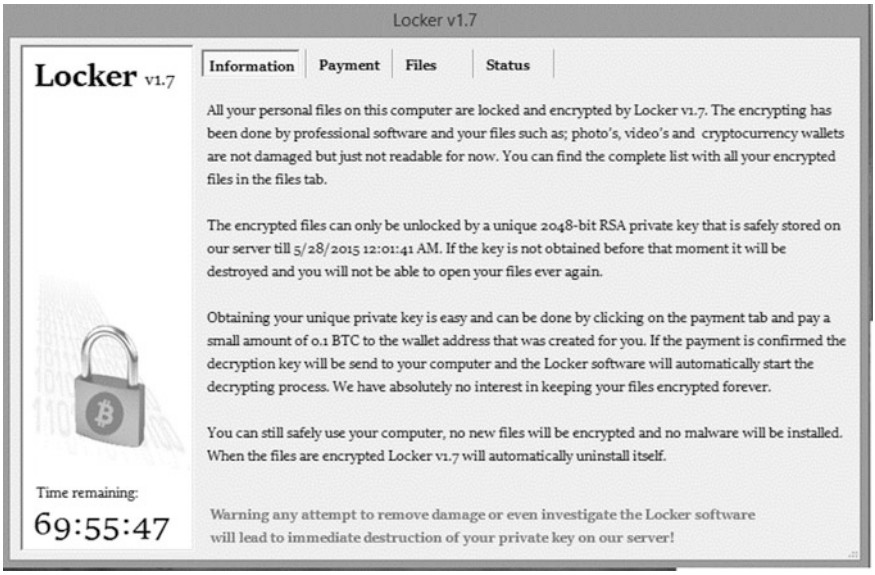

Fig. 4 A locker ransomware dialog box

becomes more and more digital, people are storing the most significant data on their PCs and devices [6].

Many users are unaware of the need to back up backups of hard drive failures or lost or stolen PCs, let alone a possible ransomware crypto attack. This may be because they have the know-how or do not realize the value of the data until it is lost. Dialog data points for these shortcomings and designers are aware of how these data are important to users, for example, memories of their loved ones, university project due to presentation, financial report for work, etc. After installation, a typical crypto-ransomware threatens and enciphers the files in silence. The goal of hacker is to remain unnoticed until it finds and enciphers all the files that might be valuable to the user. By the time the prey is presented with the threat message (the data is enciphered), the damage is already done. With data most of the cabinet infections, the infected PC continues to work normally because per-ware is not directed to critical system files and denied access to PC functionality.

2.3 Overview of a Coordinated Ransomware Attack

Ransomware is an absolute deadline for a category of per-ware that is used to digitally extradite victims in paying a precise payment. Assailants distribute these ransomwares from paid service called ransomware-as-a-service (RaaS) through numerous web servers [7]. RaaS means that the member does not need any special programming knowledge, only the will to spread ransomware (usually via botnet e-mail). The affiliate can register as an affiliate and simply download a custom binary ransomware. These customizations come from Ransom32, the world's first ransomware written in JavaScript. With the advent of the onion router (TOR) and a robust underground economy (sometimes referred to as the Dark Web), it has become significantly easier for skilled hackers to offer their services to other upcoming novice hackers who apparently do not have the skills, or the infrastructure, to deliver ransomware widely to take advantage of existing capabilities to launch a ransomware campaign. Long before the idea of RaaS came along, attackers who had amassed many prey hosts using a botnet would rent it out to anyone who wanted to launch a spam campaign or launch a DDoS attack against a target. Many varieties of the RaaS models with different offering are mention in [8].

However, these attackers pass through defined steps to perform a successful and effective attack on prey(s). Their methods under normal circumstances have been understood to follow certain series of definitive steps which are illustrated in Fig. 5.

3 Framework of a Ransomware Attack

The execution of a ransomware attack is not as sophisticated as it seems. Through a series of carefully grafted simple steps, one can easily deploy a ransomware to any such prey network or an individual. Figure 6 demonstrates how actually in the real world the ransomware attack is being executed.

Fig. 5 Modus operandi usually followed by most attackers

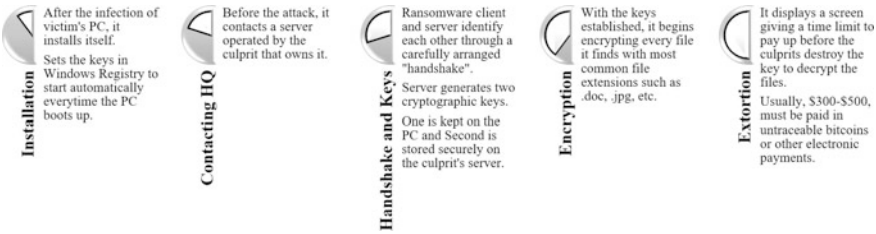

Fig. 6 Framework of a ransomware outbreak

3.1 Installation

The first step involves the installation of the infected Trojan containing the ransomware that is to be achieved first. To do that, careful *e-stalking* is executed in deploying the *infected* original files necessary for the prey's OS to download. This can be achieved either by a drive-by download, i.e., the OS implicitly downloads a portion of the per-ware or a spyware without letting the user or prey to have prior knowledge in the background. The prey is often selected based on his/her network accessibility, the web links clicked, the web searches, and dealt with popups (a novice user would click any popup showing a blinking "Your PC is infected. Run this scan now.").

Thus, the prey becomes a relatively easy catch, and the attacker can now fool the prey and easily penetrate and infect his/her PC or network. If the prey proves to be a

little-experienced one, phishing emails or websites are then used to lure him/her. These luring strategies are rather extensive, untargeted spam, or specially crafted to any organization or industry [2].

This concept is like the concept of shooting the American way—fire as many bullets as you can, hoping to hit mostly on target. These emails may include attachments which might be familiar to the prey's current organization or previously worked for. These may redirect to some pernicious websites [9].

In Windows OS, the Trojan sets the keys in the Registry so that it can start automatically on every PC reboot. In case of mobile devices (especially Android devices), the unprotected phishing app stores do the job of the attacker. Some may use stolen rather valid application development certificates for iOS. The need to jailbreak or root the mobile devices has made them highly vulnerable to the ransomware attack. The necessity for side-by-side download pernicious applications substantially upsurges the danger as these devices are no longer under the protection of the fortified protocols, pre-installed by most of the smartphone manufacturers [10].

The installation of the ransomware marks the cybercrook starts to take the control over the prey's device and the parts are again divided into a flurry of processes, batch files, scripts, and other tools to avoid scanning from signature-based antivirus scanners. In another direct attack, installation techniques, obfuscation, packaging, and code operation may be more damaging to maximize rescue. Ransomware uses this initiative to spread slowly through the infected network and install it into various common opening files and systems which are obviously enciphered simultaneously when the next step instructions are sent. Most crypto-ransomware variants would first take some advantage in the form of macro-virus or an infected PDF to get onto the system or use Java or Adobe Flash. Once downloaded, the per-ware will execute its embedded code which will analyze whether the machine is real or virtual [11].

After confirming that the system is worth infecting, the per-ware disguises itself as one of the Windows processes such as *svchost.exe*. To make it more unique, the computer name's MD5 hash or any identifier like MAC address is used to ensure the culprit to know which device has been contaminated. After the phase-one dropper's achievement, the phase-two runs a flurry of scripts to certify that any inherent protections by the Windows OS are disabled (the user might observe that after a certain installation and a reboot, the Windows Security Service gets disabled automatically at system log on, and the homepage or tab pages change to rather different or weird-looking search pages). By doing this, a utility by the Windows OS environment collects and makes copies of the steady system images for backing up the currently running systems, especially the servers, without inadvertently limiting the performance and the steadiness of the services it provides, and the system recovery characteristics of this platform are turned off and any anti-per-ware processes are killed. This utility is known as the volume shadow copy service (VSS).

3.2 Contacting Headquarters (HQ)

The second stage includes contacting the source, i.e., C&C (Command and Control) or headquarters (HQ) server before the commencement of attack. This all happens in the background; the operating system (OS) keeps working fine, and there is no way that prey knows what is going on. This concept can be understood in this way—without receiving orders, it is probable that a portion of ransomware can be found lying dormant on the prey's machine right now waiting for orders. Once the pernicious code is positioned and installed, it would commence reaching out to the headquarters, searching for orders which can be numerous requests of specific types. These requests comprise mostly finding out the file types to target for encipherment, estimating the time to wait for the process to begin, and whether to continue the spread before starting the process. Some of the variants report back an important summed-up information about the prey's device, including which anti-per-ware products are installed, operating system, installed browsers, domain name, and the IP address. The information thus gathered helps the culprits to determine whether they have managed to attack a high-value target or not and ultimately defining the amount of the payoff according to the importance of target.

The communication channels can vary with different variants and categories of per-ware. In some cases, these can be as unpretentious as web-based communications (unenciphered hypertext transfer protocol (HTTP)) to complex systems involving embedded TOR services [12] to connect. More complex systems use this very concept to conceal their whereabouts and motives. Even on android platform, the embedded TOR services can still be used over TCP channels [13, 14].

3.3 Exchanging the Keys and the Concept of Handshake

Almost all the scenarios of per-ware comprised of the malevolent code being positioned on the prey's system is a client, and the control-and-command (C&C) server functioned by the pernicious foe is specifically a server. After the placement of the client, it will make sure that it is collaborating with the main culprit's server with the help of a preset handshake procedure. This handshake procedure is distinguishable from each ransomware fraternity. The CryLocker ransomware applies an exceptional method; it sends everything wrapped as an album's PNG (Portable Network Graphics) file on genuine web pages like Imgur.com and Pastee.org. Once the agreement between the client and server is done, the next step is the generation and exchange of a key. As per the complexity of the ransomware, this can range from a simple symmetric-key cipher to a rather more sophisticated RSA 4096-bit encipherment algorithm. The key exchange executes, and the private key is kept at the culprit servers while the public key is carried to the enciphering constituent of the pernicious code installed on the prey machine. However, in some cases, the use

of a simple encipherment system or generation of a not-so-unique key every now and then can be easily be thwarted out using public decipherment modules and could recover the files.

3.4 Encipherment

Then, at this juncture, the key that is supposed to be applied to damage the files on the machine enciphered is now active and ready for use by the pernicious code on the prey machine. All the HQ identified files will commence the encipherment procedures by the pernicious code. This can include any file or any type of file extension ranging from all forms of MS Office applications to GIFs, JPGs, or PNGs. Some crypto-lockers not only encipher the files but also the filenames. The CryLocker ransomware enciphers the target files and changes their extension to *.cry*; the OSIRIS, a new variant of Locky ransomware, enciphers the stored data using asymmetric cryptography after infiltration using the "[8 arbitrary typescripts]-[4 arbitrary typescripts]-[4 arbitrary typescripts]-[8 arbitrary typescripts]-[12 arbitrary typescripts].osiris" pattern. It would rename a file, say, "sample.jpg" to "HL56PP89-H6B3-4T30-ER2R4O3Y-S9QT5NC0NA31.osiris".

3.5 Extortion

Following encipherment, these pernicious codes create their own unique HTML files, placing on the desktop and changing the desktop wallpaper letting the victims know that their machines have been compromised. Both the HTML file and desktop wallpaper contain the identical message stating that the files are enciphered using asymmetric encipherment algorithms and in case of OSIRIS crypto-locker, these files can only be restored using a private key only accessible when paying a payoff of 2.5 Bitcoin (currently 1 Bitcoin = $2804.23). Some ransomware variants will allow the victims to decipher only a single file for free to prove that there is key to their system. Some would delete files to scare the prey, thus enforcing them into more paying the payoff more rapidly. Upon payment, there is no assurance that the provided key by the culprits will decipher their files and moreover, there is no assurance that the per-ware would be aloof by itself.

Some ransomware lockers display a window (probably full screen) that spans the handler's entire desktop or limit the handler to just this single window by supervising the system's desktop through a background thread. The contents of these windows are generally localized (in local language) to certify that they aid, confined (local language support) content of the prey. Once the machine has been locked, the per-ware will do anything to confirm it and preserve perseverance on the machine, constituting sending signals for shutdown to the other processes, dispensing instructions to kill processes that would ultimately be used to end the per-ware

executable, and generating a virtualized desktop to again ensure that the end user is incapable to get out of the simulated desktops formed by the per-ware. Some variants would lock the browser, a cross-platform mechanism by the culprits, popping-up the pernicious web pages every time the victims try to shut the browser or redirect from the affected web page [13].

4 Prevention Strategies

As more cybercrooks are looking forward to the usage of ransomware as a malicious income source, there is no surprise that the attacks are mushrooming, specifically targeting the fruitful businesses; therefore, it is the need of the hour that certain steps must be taken place to dodge these payoff bullets and put several operational systems out of the harm's way likewise in [15]. Over cloud network, the authors in [16] have proposed an enhanced ransomware prevention system CloudRPS. Authors in [14] have highlighted the formal methodologies to rescue stolen data from our smartphones over insecure networks. Thus, every business running on Windows platform, despite their Original Equipment Manufacturer (OEM) certificates, is still taken as hostages [17]. More prevention and detection strategies are mentioned in [18]. For this, we need to look at some of the measures that can be taken on diverse levels to prevent or reduce the impact of crypto-ware.

4.1 Awareness Among the Users

The first and foremost prevention measure must be taken is keeping the end users informed and aware since an infection always starts with a human fault. The risks of opening attachments, suspicious software, or the links are some of the first attacks prevalent on the basic systems. Some highly trained people may be even more prone to these attacks. It is must for the users to learn about how the ransomware works, how are they spread (like a disease), and what are they made of (actually). Moreover, the techniques that the per-ware uses needs an understanding up to a quite-a-good level, for example, the spam emails which involve the social engineering tricks. In the end, the aforementioned methods will surely benefit the Internet community to recognize and dodge further attacks.

4.2 Backing Up on a Regular Basis

Performing systematic backups of all crucial information to limit the impact of data or system loss will surely help the end users and the administrators to expedite the recovery progression. If possible, this data should be kept on an isolated device,

and backups should be stored disconnected. Disabling macros which are suspiciously infected (pernicious) is a relatively good approach first since the ransomware attacks the system and mostly enciphers Microsoft Office documents. With Office 2007 and Office 2010 being the most vulnerable versions, it is highly probable that most computer workstations in the public and private sector offices and homes have this version and most of them are pirated. Thus, the effects are more far-reaching that one can imagine.

4.3 Disabling Windows Services

A service known as volume shadow copy service (VSS) is a set of Windows management instrumentation (WMI), component object model (COM), and application programming interfaces (APIs) that implement a framework (sort of a layered structure indicating what kind of programs can or should be built and how they would interrelate) to allow drive backups to be done while the programs on the operational system linger on writing into these drives. VSS provides a persistent UI that allows the proper cooperation between the user applications which alter the data on the disk by using I/O applications known as writers and those that back up these applications by using applications known as requesters which manage shadow copies to support some other functionalities such as backup and restore procedures and disk mirroring. Since Windows Vista, Microsoft has been bundling a utility called vssadmin.exe in Windows that allows an administrator to manage the shadow volume copies that are on the computer. Unfortunately, with the rise of crypto-ransomware, this tool has become more of a problem than a benefit and everyone should disable it. The developers of these per-wares are aware of shadow volume copies and designate their attacks such that they delete all these copies when the per-ware infects the computer system. This is done purely to restrict the prey from recovering any enciphered files. Ransomware injects themselves into the processes that run as administrator (to avoid any user account control prompt) so that the CMD command *vssadmin.exe Delete Shadows/All/Quiet* which will execute this utility to quietly delete all the shadow volume copies on the computer system. One must rename this file since it is rarely used in order to prevent the per-ware to utilize it to delete the shadow volume snapshots and ultimately save the files on the system. Most of the per-ware attacks can be foiled by using this method.

Another Microsoft utility which provides scripting abilities to the computing system is Windows Script Host (WSH). These code scripts can be executed directly from the desktop environment by double-clicking the code script file, or from MS-DOS. They can also be executed from either the protected-mode wscript.exe (Windows-based host) or the real-mode cscript.exe (command shell-based host). Some per-ware may use WSH to execute certain pernicious JavaScript codes when they are opened under this environment. It is then advised to disable WSH if the end user has no intention to run VB scripts in future.

4.4 File and Mail Servers

The file sharing mechanisms must be less sophisticated for the end user and more to the culprit. To do that, the shares must be fragmented as some rights on different shares must be reduced so that they (per-ware) cannot encipher; ultimately, they cannot edit these shares. Also checking up the creation of specific extensions which are used by them must be done regularly, the attachments on the gateway must be filtered by blocking those emails which contain executables (like Trojans) and those file types which should not be emailed around, for example, .chm, .lnk, and .js.

4.5 Securing the Network

Every institution or a corporation or even a lonesome Internet user, all require the connection to the Internet through basic networking devices. The end user must employ the following techniques so that the invader may not make use of the possible vulnerabilities. The first method would be using a proxy with web filtering: Some proxies allow us to filter the traffic from the blacklisted domains. It is must to ensure that the end user has the knowledge of these bad websites. This could largely reduce the chances of infection, if the list is updated thoroughly. Second, the magnitude of network sharing can become the target of certain per-ware. If the information being shared is of the highest significance, then it is highly advisable that these networks must be fragmented and thus the number of shares being available will be sufficiently reduced.

5 Latest Ransomware—WannaCry

Year 2017, month of May, the CTU scientists inspected a prevalent and cunning per-ware operation known by the names WCry, WannaCrypt, WanaDecryptor, and WannaCry that wedged numerous machines across the globe, most of them having national as well as international significance. These scientists correlate the quick infection of the per-ware to the use of a single, lone maggot or a virus component that subjugated susceptibilities in the Windows server message block (SMB) v1 protocol. It was then addressed by Microsoft in the month of March in the same year with a security bulletin MS17-010 [19]. Apparently, it is seen that WannaCry uses the MS17-010 exploit (phishing websites for the patch download) to spread to other machines through network basic input–output system (NetBIOS) as explained under common vulnerabilities and exposures (CVE).

5.1 How Are They Delivered?

The operation uses a maggot which is known as a server message block (SMB) maggot which is again used to dispense WCry donating to the per-ware's embitterment. It then tries a hypertext transfer protocol (HTTP) linkage to www [dot] asndasnqwkhekqjnskcjnkjwnekqjw [dot] com. Upon the successful linkage, the maggot halts execution and exits. Then, the maggot leverages an SMBv1 exploit (goes by the name EternalBlue) which explicitly searches for the presence of a backdoor application named as DoublePulsar [20] on infected machines. It is a backdoor implant tool developed by the NSA equation group (part of USA Security Agency) that was oozed by a hacker group known by the name "The Shadow Brokers" in early 2017. In case this backdoor is not available, the maggot tries to infect the pawn using the SMB version 1 EternalBlue [21] malcode (as mentioned earlier). Proliferation of this maggot banks on two threads (of processes), where the primary one ordains the LAN sub-nets, the SMB scans local addresses starting of the range of IP addresses that a specific ISP or datacenter owns or assigns at will and then incrementing 1-by-1 to its very end. The second thread scans arbitrarily chosen external IP addresses.

The maggot distributes itself to the infected machine as a dynamic link library (DLL) file cargo. After the DLL execution using PlayGame (a lone-exported application), it creates (or literally writes) a copy of the actual SMB maggot to the Microsoft Security Service (*mssecsvc.exe*). The SMB maggot then drops a tributary cargo from its with reserve section to the task scheduler (*tasksche.exe*) with both the files that reside in the default core directory of MS Windows operating systems are executed one after another. According to the research, this subordinate cargo is the WCry per-ware.

5.2 How They Infect Our Systems?

After the successful encipherment of the file system (whether File Allocation Table 32-bit (FAT32) or New-Technology File System (NTFS)), WannaCry displays the payoff demand dialog box as illustrated in Fig. 7. The per-ware then continuously supervises this window to make sure it remains above all windows (when the prey tries to switch over other applications), re-running if it is closed (it is like a popup on the desktop under Windows environment). Additionally, the per-ware changes the desktop wallpaper (just as Locky does).

It is then dispersed as a *.exe* file that comprises ZIP record (password-protected) in its reserves area. This record gets unwrapped when executed in the current directory and the files are the content which is shown in Fig. 8.

During the infection, some supplementary files are also created (shown in Fig. 9).

Fig. 7 WCry payoff demand interface

- b.wnry – Bitmap image used as desktop wallpaper
- c.wnry – Configuration containing TOR command (similar modus operandi of CryptoWall 2.0) and C2 addresses (HQ or the base of operations), Bitcoin addresses and other data.
- r.wnry – Ransom demand text
- s.wnry – ZIP archive containing TOR software to be installed on the prey's system; saved in TaskData directory.
- t.wnry – Encrypted DLL containing file-encryption functionality.
- u.wnry – Main module of the WCry ransomware "decryptor"
- taskdl.exe – WNCRYT temporary file cleanup program (delete any tasks native to OS)
- taskse.exe – Program that displays decryptor window to RDP sessions.
- msg – Directory containing Rich Text Format (RTF) ransom demands in multiple language (localized attack)

Fig. 8 Content of the reserve section

- 00000000.pky – Microsoft PUBLICKEYBLOB (public key binary large object) containing the RSA-2048 public key (the culprits are presumed to hold the private key).
- 00000000.res – Reserve section which holds the Data for HQ communication.
- 00000000.eky – Prey-unique RSA private key encrypted with embedded RSA public key.
- 00000000.dky – Decrypted RSA private key transmitted to prey after payoff expense.
- f.wnry – List of randomly chosen files encrypted with an embedded RSA private key that allows WCry to demonstrate decryption to the preys.
- @WannaDecryptor@.exe – Main module of the ransomware (decryptor), identical to u.wnry.
- @Please_Read_Me@.txt – Payoff demand test, identical to r.wnry.

Fig. 9 Supplementary files for the per-ware operations

The per-ware begins executing two commands when started—one is the *attrib +h* command which hides all the files as quickly as the handler moseys through every file or folder by means of the *Windows Explorer* and the second one is the *icacls ./grant Everyone:F /T/C/Q* which is used to change the file system permissions (generally NTFS file system) across various server and client operating systems. After this, WCry executes "Run As" or "runas" command to delete all shadow copies of the volume using elevated privileges; terminates several services using taskkill.exe so that their data stores can be encoded; and generates a file (particularly a batch file) using any arbitrarily generated large integer that creates a shortcut to the per-ware executable. It is then saved under "wd" registry value under HKLM registry store; otherwise, in the HKCU store.

5.3 How They Encrypt Our Files?

RSA and AES algorithms are used by this per-ware to encipher the file system. Windows crypto API for RSA encipherment and arbitrary key generation is the preferred usage choice of per-ware's method. Prior to this, WCry tallies all the accessible disks in the system. This inventory includes hard disk or local disk drives, removable drives (USB thumb drives), and network drives. However, this per-ware does not contain functionality to search the local network. WCry targets files with extensions of multimedia formats, compressed records, databases, and their add-ons likewise Locky ransomware. Most of these methods have directly been "inherited" from the other versions of CryptoWall or Locky crypto-ransomware. The file extensions targeted are .wma, .zip, .rar, .txt, .docx, .mov, .mp4, etc., perhaps almost all the extensions. Using the EKY extension (as shown in Fig. 9), a private key couple (RSA-2048) is generated and detailed to each contagion and is then stored on the local storage media and then it is used encipher the arbitrary AES-128 key produced for each enciphered file. These files are renamed using the filename format <*arbitrary_number*>.WNCRY and are replaced with the original ones. However, it is not done entirely and thus there is a hope of a forensic retrieval of file inside conditional to the milieu.

5.4 Payment Prompts and Communication with Headquarters (HQ)

WCry shows a meter that countdowns to the date and time when the payoff amount increments (see Fig. 7), probably 4 days or maybe 5 and when these files will become irrevocable (probably after seven days). Different variants of WCry set the payoff either in bitcoins or dollars ($300–$600). How much the culprits claim, they do not have the capability or intent to decipher the files after the prey pays them the

payoff. It is very likely for them to increase the payoff demand and thus the prey falling into their trap. The TOR framework run by WCry is run as a task host service (*taskhsvc.exe*) which then creates a SOCKS5 proxy server which is again used on the loopback address, i.e., 127.0.0.1 and afterward receives the signals on port 9050 (TCP). Ultimately, it tries to access some HQ services like transmit encipherment keys, communicate with the culprits, or check payment status as elaborated in [4].

6 Conclusion

This study is more comprehensive in nature than it looks, in writing which represents a thorough analysis of the idea of a ransomware, that how cryptovirology and extortion-based cryptographic techniques gave birth to a new kind of threat in the twenty-first century, evolution of these attacks since 2005, their modes of operation, and how can we protect our computing systems and datacenters from becoming the next prey. It is clear that the ransomware will continue to grow more sophisticated and will surely become more widespread like a pneumonic plague which engulfed the Europe in the twentieth century. We believe that this cyber-plague will cripple most of the cyber-superpowers which control the Internet flow in the world today. The security agencies, anti-per-ware enterprises, antivirus multi-national corporations (MNCs), and research centers will have to be on-the-toes in tackling these novel threats to the very existence and a pillar of our digital progress. Opportunistic ransomwares like WCry use their propagation methods which powers them to spread quickly. Before the end user even knows it, the per-ware gets the hold of the prey's precious data and information and then runs phishing and trapping other victims in the network that the current machine is connected. As discussed in Sect. 4, several prevention techniques are in place now, and that the Federal Cyber Emergency Team, India (CERT.in) has communicated guidelines and strategies to protect their home machines or office machines and obviously Microsoft's MS17-010 update/patch helped most of the machines to make themselves immune to these attacks.

Future Scope

The learning, awareness, and knowing-your-foe stratagems have enabled the digital infrastructure to be able to withstand the constant evolving threats from the cyber-culprits. How threatening this evolution may seem, there is always a persistent idea of hope that the good will prevail and a fightback will always be there in counter the spread and effect of pernicious elements. Our such efforts in this paper will make the reader feel the very concept of ransomware rather than building them the sole understanding. We hope that in near future, these frequencies of these attacks will plummet and our data on the Internet can be shared in full confidence and in utmost relief. However, it would take away the motivation and may allow the systems to become a little complacent (that can do more harm than being vulnerable).

References

1. Young, A. L., & Yung, M. (2017). Cryptovirology: The birth, neglect, and explosion of ransomware. *Communications of the ACM, 60*(7), 24–26.
2. Mercaldo, F., Nardone, V., & Santone, A. (2016, August). Ransomware inside out. In *2016 11th International Conference on Availability, Reliability and Security (ARES)* (pp. 628–637). IEEE.
3. Unit 42 Palo Alto Networks Threat Report—Ransomware: Unlocking the Lucrative Criminal Business Model (2016, May). Retrieved June 21, 2017. https://www.paloaltonetworks.com/resources/research/ransomware-report.
4. Deloitte Threat Intelligence and Analytics Report (2016). Retrieved June 21, 2017. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-ransomware.pdf.
5. Symantec Security Response Whitepaper. The evolution of ransomware (2015, August). Retrieved June 19, 2017. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf.
6. Orman, H. (2016). Evil offspring-ransomware and crypto technology. *IEEE Internet Computing, 20*(5), 89–94.
7. McAfee Whitepaper—Understanding Ransomware and Strategies to Defeat it (2016). Retrieved June 21, 2017. https://www.mcafee.com/in/resources/white-papers/wp-understanding-ransomware-strategies-defeat.pdf.
8. Liska, A., & Gallo, T. (2017). *Ransomware: Defending against digital extortion*. Beijing; Boston; Farnham; Sebastopol; Tokyo: OReilly.
9. CERT.be (Cyber Emergency Team, Belgium) Ransomware Whitepaper (2016). Retrieved June 21, 2017. https://www.cert.be/files/ransomware_whitepaper.pdf.
10. Moore, C. (2016, August). Detecting ransomware with honeypot techniques. In *Cybersecurity and Cyberforensics Conference (CCC)*, 2016 (pp. 77–81). IEEE.
11. Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016, June). Cryptolock (and drop it): Stopping ransomware attacks on user data. In *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)* (pp. 303–312). IEEE.
12. The TOR Project. Retrieved June 21, 2017. https://www.torproject.org/.
13. Yang, T., Yang, Y., Qian, K., Lo, D. C. T., Qian, Y., & Tao, L. (2015, August). Automated detection and analysis for android ransomware. In *2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conference on Embedded Software and Systems (ICESS)* (pp. 1338–1343). IEEE.
14. Mercaldo, F., Nardone, V., Santone, A., & Visaggio, C. A. (2016, June). Ransomware steals your phone, formal methods rescue it. In *International Conference on Formal Techniques for Distributed Objects, Components, and Systems* (pp. 212–221). Cham: Springer.
15. Luo, X., & Liao, Q. (2007). Awareness education as the key to ransomware prevention. *Information Systems Security, 16*(4), 195–202.
16. Lee, J. K., Moon, S. Y., & Park, J. H. (2017). CloudRPS: A cloud analysis based enhanced ransomware prevention system. *The Journal of Supercomputing, 73*(7), 3065–3084.
17. Mansfield-Devine, S. (2016). Ransomware: Taking businesses hostage. *Network Security, 2016*(10), 8–17.
18. Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. *Network Security, 2016*(9), 5–9.
19. Microsoft Security Bulletin MS17–010—Critical (2017, March). Retrieved June 21, 2017. https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.
20. Double Pulsar NSA leaked hacks in the wild (2017, April). Retrieved June 21, 2017. https://www.wired.com/beyond-the-beyond/2017/04/double-pulsar-nsa-leaked-hacks-wild/.
21. NSA-leaking Shadow Brokers (2017, April). Retrieved June 20, 2017. https://arstechnica.com/security/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/.