Ransomware Analysis: Prevention and Damage Control

[1]Parul
Mtech,
Mahrishi Dayanand University, Rohtak

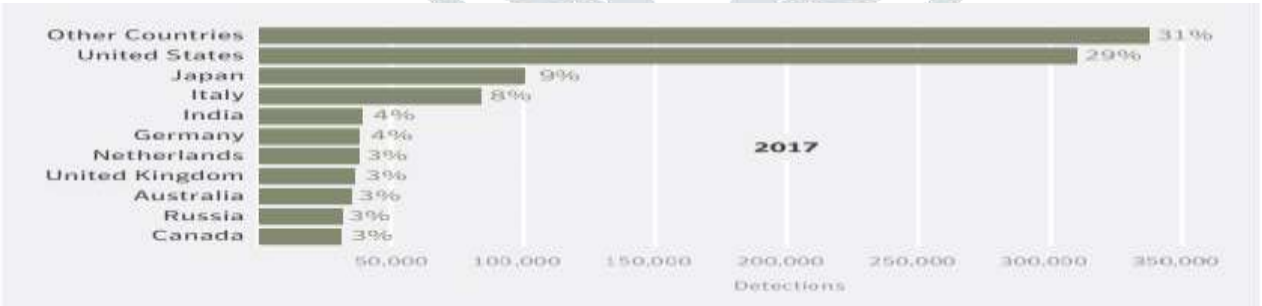
***Abstract*— Now these days technology becoming worldwide lifeline of government and businesses across it is important to build a safe network. There is also a need to build a secure and rule based framework with across the board stakeholder consultation. In today's society malware and virus's are an increasingly growing threat to users and businesses that range from independent owners to corporate giants globally. Recently a new type of virus has made its threatful presence across the world because of its destructive nature. Scholars and IT giants termed it as Ransomware. The purpose of this paper is to highlight the threat originated by Ransomware and prevention from it as well as the damage control.**

***Keywords*— Malware, Damage control and Prevention e**tc.

Introduction: Ransomware is basically a type of malware that prevents or limit the users from accessing their system, either by blocking the system or by blocking the file system unless a desired amount of ransom is not being paid. Despite the rigorous efforts of the IT giants and cyber experts, problems have been faced by these type of malwares. The modern age of malwares like Ransomware started with Cryptolocker in 2013. In the following years attackers have become increasingly sophisticated and business minded, Ransomware is a form of malicious software that, once taken over the computer, threatens with harm and usually by denying access to your data. The very first known Ransomware attack was recognized as AIDS Trojan and was unleashed via floppy disks during 1989, but it is bitterly known until 2017 global panic caused by WannaCry. There were also an earlier history of Ransomware seen in Russia in between 2005 and 2006 [1]. In the threat's early stages, .DOC, .XLS, .JPG, .ZIP, .PDF, and other commonly used files were held hostage. Later on, variants that could infect mobile phones [2] and even computers' Master Boot Record (MBR),[3] preventing the OS from loading, emerged. The United States has continued to the region that was most affected by the Ransomware during 2017 to date, approximate 30% of all attacks. Japan with 9% and Italy 8% stands next to US. India accounted for 4% of the total infections.

The top 10 regions most affected by Ransomware in the first half of 2017 were identical to the top 10 in 2016. The only major difference is that the U.S. share of Ransomware infections fell from 34 percent in 2016 to 29 percent in the first half of 2017. Aside from this decline, there were no other major changes and no other region moved more than one percent. [4]

Table 1: Ransomware infection across the globe.



Understanding the Ransomware:

Ransomware comes in two types basically, the first encrypts the files on a computer or a network and the second locks the user's screen. There is a different case with the WannaCry- it behaves like a worm, once inside a network it will spread laterally to the other systems without interaction by the attacker or the infected user. Usually malware is presented as Ransomware but after the ransom is being paid the malicious files are not decrypted, this is known as 'Wiper' malware. The tracking of ransom is almost impossible because the attacker uses the Cryptocurrency as a medium of exchange such as Bitcoin or gift vouchers. In many cases the ransom is modest, a strategy designed to make paying the fastest and easiest way to resume use. There are also a number of vectors Ransomware can take to access a system. One of the most common is Phising spam i.e. attachments that comes to the victim in an email, impersonating as a file they should trust. Once's the user downloaded and opened the file, they can take over the victim's computer, especially if they have built-in social engineering tools that trick users into allowing administrative access. Some other, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users. [5]

There are several things the malware might do once it's taken over the victim's computer, but by far the most common action is to encrypt some or all of the user's files. If you want the technical details, the Infosec Institute has a great in-depth look at how several flavors of ransomware encrypt files. But the most important thing to know is that at the end of the process, the files cannot be decrypted without a mathematical key known only by the attacker. The user is presented with a message explaining that their files are now are now inaccessible and will only be decrypted if the victim sends an untraceable Bitcoin payment to the attacker. The following image has shown that how the attackers gain access to network sector wise [6].

Table 2: Sector wise representation of the attacks made by Ransomware.

Sources of attack	Business and Professional Service	Energy and Gas Sector	Financial Services	IT and Telecom	Construction and Property	Manufacturing and Production	Public Sector	Retail Sector	Other commercial sectors	Total
Email/ Social Media	55%	82%	86%	69%	55%	52%	79%	71%	72%	64%
Drive by download click	55%	45%	31%	50%	36%	40%	29%	44%	44%	44%
Infection via Botnet	45%	73%	34%	71%	45%	36%	17%	38%	28%	42%
Infection via worm	20%	27%	24%	35%	27%	16%	33%	32%	21%	27%
Others	0	0	0	0	0	0	0	0	0	0

Table 2: Sectorwise representation of the attacks made by Ransomware.

Spread of WannaCry and Petya:

WannaCry incorporated with EternalBlue first appeared on 12 May 2017 at around 6 a.m. UTC and began spreading immediately. Once it installed itself on a computer, it attempted to use the EternalBlue exploit to spread to the other computer systems on the local network. In addition to this, it would attempt to spread itself across the internet by scanning random Internet Protocol address in an attempt to find out the further vulnerable computers. The propagation mechanism explains how WannaCry heavily affected organizations and how it managed itself to jump from one organization to another. Symantec products proactively blocked any attempt to exploit the vulnerabilities used by WannaCry, meaning users were completely protected before WannaCry outbreak. After observation, the number of exploit attempts blocked per hour gave some indication of the immediate impact. At the midday the number of blocked jumped to almost a rate of around 80,000 per hour. WannaCry was so infectious because it used an exploit developed by US NSA and then leaked by the Shadow Brokers and dumped on the web but there was a patch available for vulnerability months before it was used to such destructive effect in WannaCry. Patching system is difficult and very time consuming and often those patches have to be tested to make sure they don't break. When executed, WannaCry malware first checks the kill switch domain name, if it is found then the Ransomware encrypts the computer data, then it attempts to exploit the SMB vulnerability to spread out to random computers on the internet. It's also discovered that windows encryption APIs used by WannaCry may not completely clear the prime numbers used to generate the payload's private key from the computer memory, making it possible to potentially retrieve the required key if they had not yet been overwritten from the system memory. In the response, French researcher develop a tool known as WannaKey, which automates this process on Windows XP computer systems, resulting a second tool was iterated known as Wanakiwi, which was tested on Windows 7 and SQL server 2008R2. Microsoft has already released patches previously to close the exploit. Emergency security patches for Windows 7 and Windows .1 as well as for Windows XP, Windows 8 and Windows server 2003 were released. Microsoft created these patches in February 2017 after getting a tip in the January. Connected organizations were advised to patch windows and plug the vulnerability in order to protect from the cyber attacks. Researchers from Boston University and University College London reported that their PayBreak system could defeat WannaCry and related Ransomware threats. According to the Kespersky Lab, four most affected countries were Russia, Ukraine, India and Taiwan. There were speculations that Petya is going to be the last Ransomware crisis the world is likely to see. Petya is also an encrypting Ransomware that was initially reported in 2016 [7]. Petya targeted Microsoft Windows base platform thus infecting the master boot record to execute a payload that encrypts the hard disk file system and prevent windows from booting.

Is there further protection from Ransomwares?

Major antivirus software companies proclaimed that their software has updated to actively detect and provide protection against Petya and WannaCry infections. For examples: Semantic products using definitions version 20170627.009, kespersky security

updated software etc. Moreover keeping windows upto date i.e. installing necessary patches at least from the March 2017 critical patches defending against EternalBlue vulnerability. For this malware outbreak an another line of defence has been created i.e. Petya checks for read only file C:\Windows\perfc.dat, if it is find it will not run the encryption side of the software system. It is being considered that Petya was a deliberate, malicious, destructive attack and another Ransomware virus as like WannaCry and also there were some speculations that original petya was not designated to make money.

Recent Developments:

There were some major Ransomware, who made havoc in the world Cerber, Jaff, Sage, Globalmposter, Locky, mamba etc. Past security solutions installed on computer systems and other devices has always been a challenge for Ransomware. The latest is TorrentLocker i.e. Trojan- Ransom.Win32.Rack is a type of cryptographic Ransomware. [8]. Unfortunately, starting from version four, the malware authors have identified and fixed this flaw, Trojan-Ransom.Win32.Rack uses a symmetric block cipher AES to encrypt the victim's files and an asymmetric cipher RSA to encrypt the AES key. Versions 1-3 contain a flaw which makes it possible to decrypt the victim's files, and this has been implemented in our Rannoh Decryptor utility.rendering this decryption method impossible. Current versions of this malware demand ransom payments through the Bitcoin system and host its payment web pages in the Tor network.

Ransomware Mitigation and Prevention:

Ransomware is becoming havoc and a growing threat to many businesses and organizations across the world. If Ransomware were to effectively penetrate a business's infrastructure and infect the workstations, then daily business functions would come to an immeasurable halt. The ability for a business to remain functional and have a near constant uptime is crucial for the business continuity of many businesses today; thus, many industries are implementing Ransomware in their risk analyses as real threats that need to be mitigated and prevented. There are four steps an individual or a workplace should take to prevent Ransomware: back up data, avoid email links and attachments, patch and block, and drop-and-roll.

1. ***Back Up data***: Backing up is an excellent way to mitigate the malware attacks. Instead of paying money to attackers to unlock data, who might not even give the data back, or trying to decrypt the data, having backups may recover the data if a good system is in place and there are many ways to back up the data but every unique way has fluctuating cost factor.
2. ***Review System Permissions***: It is always an absolute idea to remove any unwanted local administrative rights. This step can override the malware spreading process. Local administrative rights matter much in this case because they serves as a major components in the process of Ransomware attacks. When you remove the local admin rights, you are effectively blocking access to all the important system files and resources that the Ransomware might choose to encrypt.
3. ***Email Security***: Email filtering is one of the best thing to prevent these kind of attacks because the common method to attack the systems are email or social media platforms. Email.cloud technology includes Real Time Link Following (RTLF) which processes URLs present in attachments, not just in the body of emails. In addition to this, Email.cloud has advanced capabilities to detect and block malicious JavaScript contained within emails through code analysis and emulation. The most prevalent formats include MS Office files that feature .zip files and macros that are either executable themselves or hold executable files. Thus, you should have a policy in your organization whereby such attachments cannot be sent via email. Even if an employee does so, the email security feature will automatically remove it.
4. **Network Security***:* Securing the entire network can prove very tedious task. Start by implementing robust blacklisting within the organization, and it will successfully prevent any web-based download of malware. Moreover, it will not give Ransomware any opportunity to connect to your command-and-control server. A firewall is useful for restricting or entirely blocking the remote desktop protocol (RDP) along with other management services at the network level. You should even initiate spam detection features, like spam lists, so that compromised emails do not reach the inbox of users. Another option is to limit the kinds of file extensions that you can deliver as an email attachment.
5. ***Best Practices***: System users are strictly advised to immediately delete any such suspicious email they receive, especially those containing links and attachments. Microsoft has already disabled macros from loading office documents by default. Attackers can use social engineering techniques to convince the end users to enable the macros.

Future and Conclusion:

It will not be surprising if Ransomware change in a few years. In terms of potential, they can evolve into malware that disable entire infrastructure (critical not only to a business's operation but also a city's or even a nation's) until the ransom is paid. Cybercriminals may soon look into approaches like hitting industrial control systems (ICS) and other critical infrastructure to paralyze not just networks but ecosystems. A key area that could become a bigger target for cybercriminals are payment systems, as seen with the Bay Area Transit attack in 2016 where the service provider's payment kiosks were targeted with Ransomware. We have seen Ransomware operators hit hospitals and transportation service providers. [10] What would stop attackers from hitting even bigger targets like the industrial robots that are widely used in the manufacturing sector or the infrastructure that connect and run today's smart cities? Online extortion

is bound to make its way from taking computers and servers hostage to any type of insufficiently protected connected device, including smart devices, or critical infrastructure. The return on investment (ROI) and ease with which cybercriminals can create, launch, and profit from this threat will ensure it continues in the future.

References:

[1] TrendLabs. (2017). Threat Encyclopedia. "Ransomware." Last accessed on 20 March 2017, https://www.trendmicro.com/vinfo/ us/security/definition/Ransomware.

[2] Nart Villeneuve. (12 January 2011). TrendLabs Security Intelligence Blog. "SMS Ransomware Tricks Russian Users." Last accessed on 20 March 2017, http://blog.trendmicro.com/trendlabs-security-intelligence/sms-ransomware-tricks-russian-users/.

[3] Cris Pantanilla. (12 April 2012). TrendLabs Security Intelligence Blog. "Ransomware Takes MBR Hostage." Last accessed on 20 March 2017, http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-takes-mbr-hostage/.

[4] O'Brien Dick, International Security Threat Report "Ransomware 2017": An ISTR Special Report.

[5] Fruhlinger Josh: What is Ransomware? How it works and how to remove it, article 3236183, Csoonline.

[6] SentinelOne: Global Ransomware Study 2018.

[7] Greenberg, Andy (2018-08-22). "The Untold Story of NotPetya, the Most Devastating Cyberattack in History". *Wired*. Retrieved 2018-08-27.

[8] https://www.kaspersky.co.in/resource-center/threats/torrentlocker-malware

[9] Ransomware: Past, Present and Future, TrendLabs Ransomware Roundup

[10] TrendLabs. (7 September 2016). Trend Micro Security News. "Ransomware as a Service Offered in the Deep Web: What This Means for Enterprises." Last accessed on 21 March 2017, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-anddigital-threats/ransomware-as-a-service-what-this-means-for-enterprises.