IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 6, PP 22-26

Ransomware:Past, Present, And Future

Shilpa Jaiswal Ritu Sharma Kunal Shriwas Jyoti Gurav
EXTC Department EXTC Department EXTC Department EXTC Department
ACE (Malad) ACE (Malad)) ACE (Malad) ACE (Malad)

Abstract: *On 12 May 2017, a massive ransomware attack occurred across a wide range of sectors, including health care, government, telecommunications and gas. To date, WannaCry has spread to over 300,000 systems in over 150 countries. The countries that appear to be the most affected are Russia and China, probably because of the high percentage of legacy software, with significant impacts elsewhere, notably to the UK National Health Service. The spread of the ransomware reportedly slowed in the two days following the launch of the attack, in part due to the discovery of a "kill switch" in its code. However, there are reports of new variants of the malware (such as Uiwix) which do not have this kill switch. Data on new variants is unconfirmed and limited at the moment,and EY wil publish updates as more information becomes available*
Keywords: *kill switch, ransomware and legacy software.*

I. Overview Of Wannacry

WannaCry is a type of ransomware, or extortive malware, that encrypts files, disks and locks computers. The malware demands a ransom of ~$300-600 to be compensated to one of three bitcoin accounts within three days in return for decrypting the files.WannaCry spreads via SMB, the Server Message Block protocol operating over ports 445 and 139, typically used by Windows machines to communicate with file systems over a network. Once successfully installed, this ransomware scans for and propogates to other at-risk devices. WannaCry checks to see if backdoors (like DoublePulsar) are already on previously infected machines. Both DoublePulsar and the EternalBlue exploit the SMB vulnerability that was made public by the Shadows Brokers hacking set in April

Fig 1. How it attacks

1. Attacker uses a yet-to-be-confirmed intial attack vector
2. WannaCry encrypts files in the victim's machine using AES-128 cypher, deletes shadow copies. It then displays a ransom note requesting $300 or $600 in bitcoin
3. Tor.exe is used by wannadecryptor.exe, initiating connections to tor nodes in order to connect back to the attacker (therefore making this extremely difficult, if not impossible, to track)
4. IP address of the tainted machine is checked; then IP addresses of the same subnet are scanned for additional vulnerable machines and connected to via port 445 TCP
5. When a machine is successfully connected, data containing the exploit payload is transferred Global impact of WannaCry

There are approximately 30–40 publicly named companies among the likely thousands that were impacted by this ransomware.

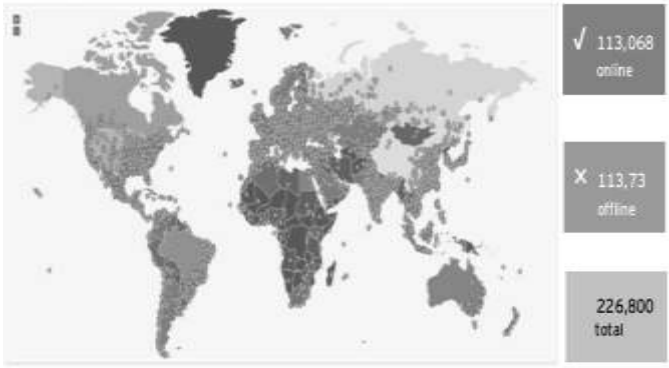

Fig2 . Global impact of WannaCry

As shown in above diagram total affected data was 226,800. There are reports that in China over 40,000 organizations have been exaggerated, including over 60 university institutions

II. How Wannacry Works

The initial vector of delivery for this malware was originally widely reported to be phishing emails, however data to validate this has not been confirmed and other reports suggest other vectors, such as the use of public-accessible vulnerable SMB (Server Message Block) to spread the malware in a worm-life fashion. Once an infection takes place, WannaCry beacons out to the kill switch URL in order to determine if the malware is in a sandbox environment. If the URL does not respond, then the malware starts to encrypt the victim's files using an AES-128 cipher. Files encrypted by WannaCry are appended with a file extension of .wanaacry as well as others. Unlike other ransomware families, WannaCry continues to encrypt victim files following any name changes and any new files created following infection. A ransom note is then displayed on the victim's machine, which is completed using text from a library of rich text format (RTF) files, in multiple languages and chosen based on machine location. Observed ransom demands require victims to pay either US$300 or US$600 worth of bitcoin (BTC) for a decryption key. Once infected, the user will see a screen (see Figure 2) with instructions on how to pay the ransomware.

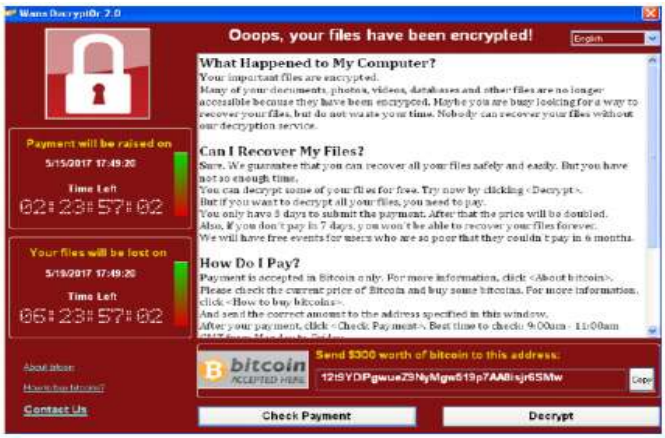

Fig 3. Ransomware screen

WannaCry utilizes the exploit Eternal Blue, created by NSA and released by Shadow Brokers (full details in Appendix IV) on 14 April 2017. Of note, the malware also checks fo existing backdoors via Double Pulsar, also out by Shadow Bro-kers, in order to help propogate through client networks. It should also be stated that the kill switch will not pause the attack if an organization is routing through a proxy for internet access.

A. Propagation

One of the first questions many victims ask is "how did I get infected with ransomware?" While it is not always immediately clear, the infection method for ransomware follows the same modus operandi used by cybercriminals to infect victims with any malware. As seen in Figure 4, there are many paths that can lead to a ransomware virus. However, the skillset and resources required to overcome modern defenses for the distribution of malware is outside of the scale of many amateur cybercriminals.

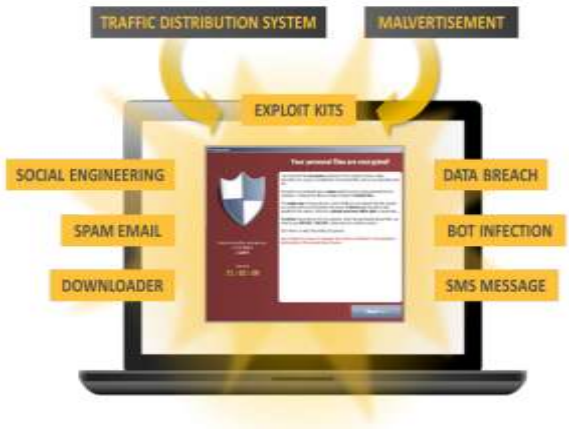

Fig4. Routes for ransomware to arrive on a computer

This has led to an secretive cybercrime ecosystem where different groups specialize in distinct areas of cybercrime, such as malware allocation, for a price. In many ways, these malware distribution services are run like any other business service. In some cases, they have even adopted common software industry reward methods for malware installs, such as the pay-per-install (PPI) model. Ransomware attackers have been seen to use different techniques or services to get their malware onto a victim's computer.

III. Systems impacted by ransomware

Modern ransomware can impact many different types of systems. With the increasing computerization of everyday activities, we are finding that computers are becoming ubiquitous and can be found almost everywhere. Trends such as iot will widen the horizon further for computerization. There are already lightweight linux-based systems in many types of small gadgets and household appliances, such as portable media players, routers, refrigerators, tvs, mobile phones, tablets, set top boxes, network-attached storage (nas) devices, and surveillance cameras. Most of these can potentially be targeted with ransomware attacks. However, at this time, the most frequently targeted computing environments for ransomware are personal computers, mobile devices, and servers.

Personal computers:

Personal computers the vast mass of ransomware threats today are designed to target personal computers running the windows operating system. This is unsurprising, as windows-based computers make up around 89 percent the os market share for desktop computers, with mac os x and linux making up the rest. Given that ransomware is a commercial activity for cybercriminals, it makes sense for them to maximize potential returns on their investments. Ransomware has to be tailored specifically for a given operating system because it often has to leverage system api hooks to block or limit access to controls such as the mouse or keyboard. In addition, many crypto ransomware threats now make use of inbuilt encryption libraries or apis supplied with the operating system to perform the encryption and decryption process itself. This saves the attackers from inventing their own protected encryption method (a very difficult task) and propagating additional files and libraries with their ransomware distribution. The downside of using os-specific apis is that the ransomware is tied to a particular operating system, but given the massive market share of the windows operating systems, this minor drawback may not be a major factor for cybercriminals however, in recognition of the small but significant pool of non-windows users, some enterprising cybercriminals have created the browlock trojan (detected by symantec as trojan.ransomlock.ag). The threat is implemented in javascript and is designed to work on a wide range of web browsers, making it operating system agnostic. While this browser-locking technique is less efficient from a technical point of view, this tactic is designed to hoover up the lasting potential victims who may not otherwise be targeted.

Moble Phones:

The next most targeted types of devices are tablets and mobile phones. These devices have become ubiquitous worldwide, with studies showing that users are spending more time on mobile devices than ever before. Ever since the advent of the iPhone back in 2007 and Android in 2008, smartphone and tablet device ownership has been on a steep upward trajectory. Today, there are basically just two main players in the mobile OS market: Android and iOS. Android has a massive global footprint, with a share of over 80 percent of the mobile market, representing billions of smartphone and tablets worldwide. In terms of the malware landscape,

there is a world of difference between the Android and iOS world. Page 15 The evolution of ransomware iOS users who have not jail-broken their phones have been quite well protected by Apple's tightly controlled ecosystem.

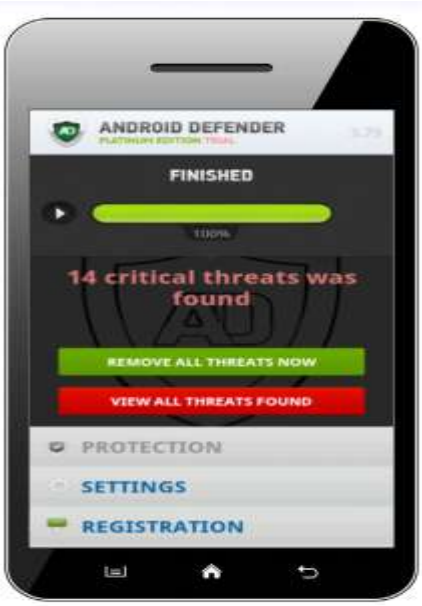

Fig 5. False threats found by Android.Fake defender

For a non-jail-broken iOS user, the ability to install apps outside of the official App Store is extremely limited with some exceptions such as apps developed with enterprise-provisioning certificates. A ransomware developer who wishes to explore this route would first have to obtain an enterprise developer certificate from Apple, build their app, sign it with the enterprise certificate, distribute it to potential victims, and convince them to install it. The problem for the cybercriminals in this scenario is that their room to maneuver could be highly restricted and Apple could easily shut down their operation simply by revoking the certificate. This makes ransomware development activity for iOS very risky with tiny prospect of payback. Android is a much more open and permissive platform. This sincerity has reward and disadvantages. Many users like the freedom and flexibility to wish to install whatever type of app they wish from any source they like. The downside is that this same flexibility can make it easier for malware creators to operate and spread their creations. This is one key reason why we see many more Android-based threats compared with threats for iOS. To tap into this growing and potentially lucrative user base, ransomware targeting Android devices has already been created. Android. Fakedefender, discovered in June 2013, marked the crossover from the standard fake antivirus scam to locker ransomware on the Android platform. Android. Fakedefender purported to be a security scanner but when it inevitably found "critical threats," the device interface was locked down to prevent victims from launching other apps or change settings in the operating system. The malware also tried to prevent victims from uninstalling it. These tactics were all designed to coerce victims into paying for a license for the fake software, which the ransomware promised would resolve the issues reported. Later entrants began to focus purely on being a locker ransomware rather than pretending to be a security tool. Android.Lockdroid.E, seen in 2014, was one of the earliest examples of this class of ransomware hitting Android devices. It borrowed heavily from the techniques and tactics used by desktop-locker ransomware, which had reached a high level of maturity by this time. Lockdroid.E was packaged up as a mobile app for a popular adult video website to entice potential victims into installing it. Once installed, the Trojan displayed a fake FBI warning that demanded payment of a US$500 fine for accessing "forbidden pornographic sites" and then locked the device while displaying the notice. In 2014, we also saw the emergence of crypto ransomware for Android devices in the shape of Android. Simplocker. Simplocker was heavily inspired by desktop crypto ransomware at the time, but its execution of the scam was somewhat curtailed by the security model of the Android operating system. Security restriction prevents apps from accessing file and data belonging to other apps. However, in previous versions of Android, files such as images, documents, and media files stored on external SD memory cards were often not protected by this mechanism in older versions of the OS, so they could be accessed by other apps. This means Simplocker could access and encrypt files stored in the memory card. Many Android devices are designed with meagre amounts of internal storage, so an SD card is a common upgrade that users implement to boost the internal storage of the device. Some AndroidFigure 8. False threats found by Android.Fakedefender Figure 9. FBI-themed lock screen from Android.Lockdroid.E, one of the first pure locker ransomware for mobile devices. The growth of

ransomware based ransomware even tried to set a device PIN code if there was none implemented, making it impractical for the user to access content on their phone. Studies have shown that mobile devices tend to be used more for messaging and leisure-related activities such as web browsing or media consumption rather than output. This makes it less likely that highly valuable files will be present on the mobile device compared to a desktop computer. Based on these usage trends along with the technical boundaries previously mentioned, the chances of securing payment using crypto ransomware on mobile devices are likely to be considerably smaller. At this time, we would still consider mobile ransomware to be at the experimental stage of development, where cybercriminals are releasing their ransomware into the countryside and observing the results before making decisions on future iterations. We have not yet seen an explosion of ransomware for mobile devices as we had for desktop computers. This may change in the future as mobile technology and usage patterns such as mobile payments continue to evolve, blurring the line between mobile and desktop computing.

Servers:

Servers represent a different type of plan for cybercriminals aiming to extract ransom payments. Servers are much more likely to contain data that is critical to the operations or even survival of an organization. They act as central repositories for documents, source code, financial records and transactions, user databases, and trade secrets, making them high-value potential targets. Given the critical role that servers play, many organizations have disaster recovery and business continuity plans (BCP) built around maintaining operations and ensuring the backup of data. Despite this, taking out a critical server even for a short time could be incredibly disturbing and damaging. Because of these contingency plans, cybercriminals have been forced to adopt a different approach to extracting ransoms when attacking organizations and their servers. 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. As a result of this, many organizations who are susceptible to DDoS attacks have enlisted the help of DDoS mitigation services to reduce the impact of these attacks. This in turn has encouraged cybercriminals to look for alternative ways to hold organizations to ransom by targeting one of their most critical infrastructural assets–the servers and the data held in them. Some groups do this by sensitive the target server and patching the software so that the stored data is in an encrypted format where only the cybercriminals have the key to decrypt the data. The premise of this attack is to silently encrypt data held on a critical server, along with all of the backups of the data. This process may take some time, depending on the organization, so it requires patience for the cybercriminals to carry it out successfully. Once a suitable number of backups are encrypted, the cybercriminals remove the decryption key and then make their ransom demands known, which could be in the order of tens of thousands of dollars.

IV. Conclusion

Ransomware is not cheap; the average ransom demand hitting individual users now stands at a hefty US$300. In the past 12 months, we saw ransom demands range from US$21 to US$700. The exact amounts may vary depending on the ransomware family and the location of the victim. Striking a balance between volume and pricing is a continuing challenge for cybercriminals and some even offered to return data for free after a set period.

References

[1] en.wikipedia.org/wiki/Cryptolocker
[2] http://www.darkreading.com/attacks-breaches/new-zeus-banking-trojantargets-64-bit-s/240164713
[3] http://blog.fortinet.com/Ransomware/
[4] http://www.symantec.com/connect/blogs/grappling- zeroaccess-botnet
[5] http://threatpost.com/zeus-source-code- leaked-051011
[6] http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-inlaundered-bitcoin-7000024579/
[7] http://threatpost.com/virut-and-waledac-botnets-spamming-sharedmachines-011513/
[8] http://www.fortinet.com/resource_center/whitepapers/quarterly-threatlandscape-report-q213.html
[9] https://www.decryptcryptolocker.com/
[10] http://www.fbi.gov/news/pressrel/press-releases/u.s.-leads-multi-nationalaction-against-gameover-zeus-botnet-and-cryptolocker-ransomware-chargesbotnet-administrator
[11] http://www.kyrus