Discussion On Ransomware,Wannacry Ransomware and Cloud Storage Services Against Ransom Malware Attacks

Anjana TK

Assistant Professor
Department of Computer Science & Engineering,
AWH Engineering College, Calicut, India

***Abstract*— Today cybercrimes are focused over returns, especially in the form of monetary returns. A commonly seen problem is extortion in the form of an infection named Ransomware that encrypts the files of the target and demands ransom to recover the locked data. This paper discusses on ransomware, wannacry ransomware and also how cloud storage serves as a strategy against such attacks.**

***IndexTerms*— cybercrime, extortion, ransomware, encryption, wannacry ransomware, cloud storage**

I. INTRODUCTION

Today, most of the important tasks of general day to day life can be performed in more or less digital form.Tthe concentration of personal and important data in devices with weak security configurations has made the digital platforms the main targets for attackers and different forms of blackmailing.Ransomware is a type of malware that prevents or limits users from accessing their system, by locking the system's screen or by locking the users' files and demand a ransom . More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.[1]

Bitcoins[2]-[6] are used by ransom operators for payments.Aalternative payment options such as iTunes and Amazon gift cards have also been liste.Paying the ransom does not guarantee that users will get the decryption key or unlock tool required to regain access to the infected system or hostaged files.Through a variety of means users may encounter this threat. It can arrive as a payload either dropped or downloaded by other malware. Certain ransomware are known to be delivered as attachments from spammed email, downloaded from malicious pages through malvertisements, or dropped by exploit kits onto systems that are vulnerable.

Ransomware that is executed in the system can either lock the computer screen, or, encrypt predetermined files. In the first case, a full-screen image or notification is displayed on the infected system's screen, which prevents victims from using their device. It shows the instructions on how users can pay for the ransom. In the second case of ransomware it prevents access to files to potentially critical or valuable files like documents and spreadsheets.

There are two main forms of ransomware[7] in circulation today: Locker ransomware (computer locker): Denies access to the computer or device .Crypto ransomware (data locker): Prevents access to files or data. Crypto ransomware doesn't necessarily have to use encryption to stop users from accessing their data, but the vast majority of it does. Both types of ransomware are aimed squarely at our digital lifestyle. They are designed to deny us access to something we want or need and offer to return what is rightfully ours on payment of a ransom. Despite having similar objectives, the approaches taken by each type of ransomware are quite different.

The Wanna Cry ransomware attack[8],a cryptoransomware – was one of the largest ever cyber attacks – appeared on May 2017,affected over 200,000 systems around the world . Czech Republic-based anti-virus provider Avast, however, gave a more conservative estimate of around 126,000 systems being affected. As data shared by Kaspersky, a Russian anti-virus company India was among the countries worst affected by the Wanna Cry attack .

Securing our digital assets has become increasingly challenging[9] as our reliance on rapidly evolving technologies continues to grow. The security perimeter in computing has changed from a well-defined boundary that was relatively easy to identify and defend, to an elastic boundary that helps the threats to evolve constantly.Cloud computing provides virtual resources to its consumers through internet. General example of cloud services is Google apps, provided by Google and Microsoft SharePoint. Security[10][11] in cloud computing is still a hurdle.Securing data, examining the utilization of cloud by the cloud computing vendors etc are the security issues surrounded by cloud computing. The wide acceptance of www has raised security risks along with the uncountable benefits, so is the case with cloud computing.

The purpose of attacks on cloud won't change, but the delivery methods certainly will. Because cloud environments offer scalable and flexible resources, they allow enterprises to reliably keep up with changes in the threat landscape.Sensitive industries like healthcare, retail, and finance can leverage the cloud by partnering with security providers who offer strong security.Also simply adopting cloud-based security and storage is not an adequate response against ransomware attack.

II.UNDERSTANDING RANSOMWARE

History of Ransomware

Ransomware has been around for quite a long time. The first asymmetric ransomware[12][13] prototypes were developed in the mid-1990s. The idea of using public-key cryptography for computer attacks was introduced in 1996 by Adam L. Young and

Moti Yung in the 1996 Proceedings of the IEEE Symposium on Security and Privacy. In the abstract, Young and Yung said their prototype was meant to show how cryptography could be "used to mount extortion-based attacks that cause loss of access to information, loss of confidentiality, and information leakage, tasks which cryptography typically prevents." The defining characteristic of public key cryptography is the use of an encryption key by one party to perform either encryption or decryption and the use of another key in the counterpart operation. In symmetric-key algorithms, there is a single key used and shared between receiver and sender, thus the key used by the receiver and sender is "symmetric" because it is the same.In asymmetric public key cryptography where multiple keys are used that allows ransomware to encrypt items on a system with a public key while never exposing the private key, thus keeping it secret.

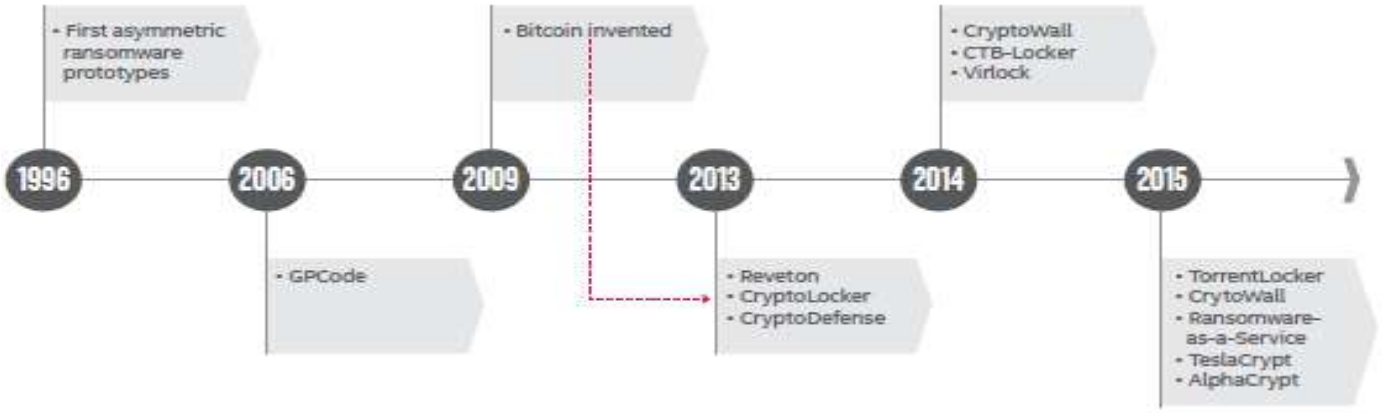


Fig.1:Timeline of Some Noteworthy Ransomware Familes

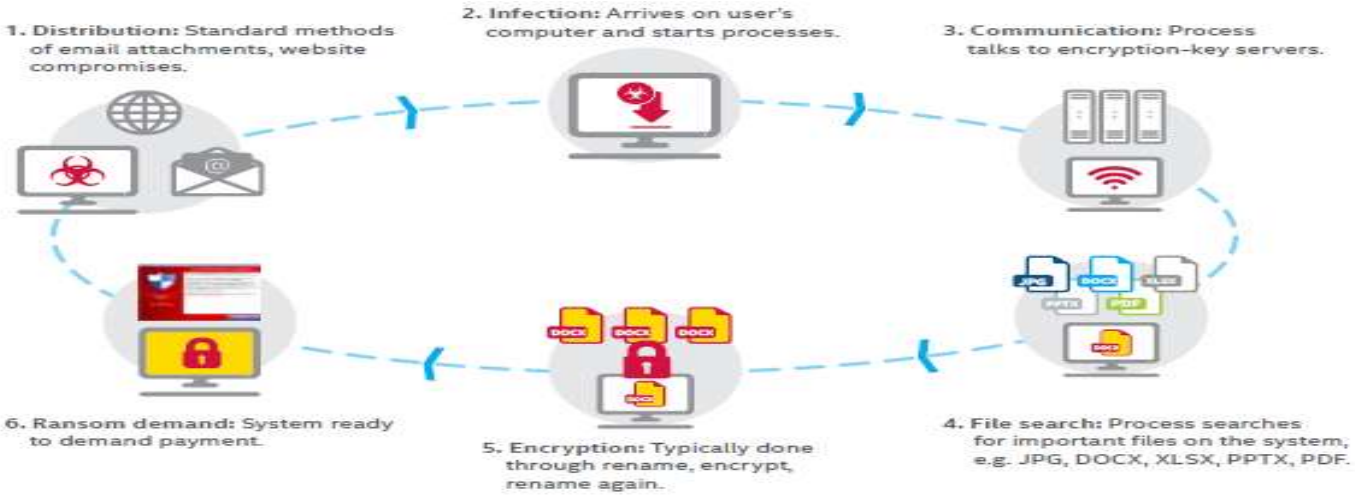
There was a logistical problem for the first asymmetric ransomware prototype that is how could the ransom be paid without exposing the malware author to risk. As a result, things were pretty quiet until 2005, when GPCode, also called PGPCoder, a relatively simple Trojan encrypting common user files that matched the extensions matching those in its code. (These extensions included .doc, .html, .jpg, .xls, .zip, and .rar.) The Trojan would drop a text file that demanded payment in each directory with affected files. Back then, the payment was typically between $100–$200 in e-gold or a Liberty Reserve account. The security industry was able to come up with a variety of solutions to this Trojan (such as virus detection and utilities to combat GPCode). PGP coder was considered modestly successful in that the malware author(s) behind GPCode and its variants were able to collect some money, but many variants had flaws (using symmetric encryption, deleting the unencrypted files in a way that allowed disk scanners to recover the files, etc.) that helped users to recover data without paying the ransom amount.

Bitcoin

Ransomware started to really take off by combining capabilities such as more powerful asymmetric encryption methods and using the new cyber currency of Bitcoin[14][15] as payment. (In Figure 1, we see a dotted line leading from Bitcoin to CryptoLocker, which was the first of a new generation of ransomware using Bitcoin for payments.) CryptoLocker was estimated to have earned its author $27 million in Bitcoin before it was shut down.

Satoshi Nakamoto [16][17] invented the digital asset and payment system,bitcoin and released as opensource software in 2009. Bitcoin is the first decentralized digital currency. It is unique in that it solves a number of problems that plagued earlier attempts to produce this kind of currency. Bitcoin owners can prove they have funds without risk to the owner.There is no central bank or authority for the currency, which eliminates the ability of the currency's value to be manipulated by that authority.Transactions on the Bitcoin network are pseudonymous, meaning that although a currency transaction is announced on the network, there is no easy way to link Bitcoin account addresses to real-world identities, so the people conducting the transaction have a significant amount of privacy. Transactions are not location-specific, so currency can be seamlessly sent across borders. Basic transactions are irreversible. Once a transfer is made, there is no way for a third party to force a chargeback (as with a credit card). Here's the really clever part: There are no hard assets (such as gold) backing Bitcoin. Rather than relying on hard assets, Bitcoin miners use Bitcoin mining software to solve Bitcoin algorithms [17]and earn Bitcoins. The algorithms are extremely hard to solve and require a lot of computation.

How Ransomware Works



.

Fig 2: Ransomware Follows A Number Of Typical Steps To Success

Ransomware generally uses six steps to accomplish its task

Distribution: Ransomware uses standard methods of distribution. Generally it is spread through phishing schemes involving email attachments or downloads and installs on an endpoint through website compromises.

Infection: The binary arrives on the user's computer and starts the processes it needs to complete its malicious activities. These may include quite a bit of new, sophisticated behaviors

Communications.:The process will communicate to encryption-key servers to retrieve the public key needed to encrypt data.

File search: The ransomware process searches for files on the system in a systematic fashion. It typically looks for files that are important to the user and cannot be easily replicated, such as files with extensions of jpg, docx, xlsx, pptx, and pdf

Encryption: by moving and renaming the targeted files, then encrypting and renaming the files after a successful encryption.

Ransom demand:by taking over the screen of the infected endpoint and demanding payment.

III.WANNACRY RANSOMWARE

WannaCry[18] ransomware cryptoworm attacked worldwide, that targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin.Cyber attack was initiated on Friday, 12 May 2017, and within a day was reported to have infected more than 230,000 computers in over 150 countries. As data shared by Kaspersky India was among the countries worst affected by the Wanna Cry attack.

It was the biggest ransomware outbreak in history and estimated that 130,000 systems in more than 100 countries had been affected as per Mikko Hypponen, chief research officer at a Helsinki-based cyber security company called F-Secure. Hypponen added that Russia and India were hit particularly hard, largely because Microsoft's Windows XP - one of the operating systems most at risk - was still widely used in the countries.Police computers across 18 units in Andhra Pradesh's Chittoor, Krishna, Guntur, Visakhatpatnam and Srikakulam districts were affected. There was also a news that the U.S. National Security Agency (NSA) had discovered the vulnerability in the past, but instead of informing Microsoft, had built the EternalBlue exploit for their own offensive work.

Fig 3:Message Displayed By The Wannacry Ransomware

To attack any systems, WannaCry spreads across local networks and the Internet to systems that have not been updated with recent security updates. A "critical" patch had been issued by Microsoft [19]on 14 March 2017 to remove the underlying vulnerability for supported systems, nearly two months before the attack, but many organizations had not yet applied it.Exposed older, unsupported operating systems such as Windows XP and Windows Server 2003, were initially at particular risk but the day after the outbreak Microsoft took the unusual step of releasing updates for these operating systems.There are still millions of computers using Windows XP, and without custom support, they're all vulnerable, systems are still widely used in Africa and Asia — not just to this latest ransomware.Also software upgrades outrunning their hardware,is a problem and that's much bigger than Microsoft. A computer sold in 2007 likely isn't equipped to run Windows 10 and millions of those old machines are still in use, which is why XP has remained neck and neck with Windows 8.1.

IV.CLOUD STORAGE SERVICES AGAINST RANSOM MALWARE ATTACKS

The Cloud can also be used to spread malware[10] to other users through the sharing of infected files and automatic syncing. For example, Virlock ransomware specifically targets cloud storage and collaboration platforms, allowing it to replicate rapidly through the whole network from a single infected user. Office 365 users were targeted by a ransomware called cerber via malicious macros in Office documents that are attached to spam emails.Cerber uses social engineering to trick the user into bypassing the security feature. Cloud services are not safe from ransomware,as they offer the option to recover the previous version of files.File-sharing, collaboration and social networks are becoming one of the most common ways of spreading malware and 1 out of every 10 companies has malware in their cloud .Therefore it is vital that any company using the cloud for storage or collaboration invests in automated daily backup and daily cloud apps auditing in order to detect and recover from malware.Most small to medium businesses do not have the resources to ensure state-of-the-art security for their data and in this case, relying on the more sophisticated security measures of enterprise cloud providers is both economical and provides enhanced data security[11].

How to Reduce the Risk and Impact of Ransomware Attacks in The Cloud

Hackers gain access to systems through software vulnerabilities, allowing ransomware to be installed. The best way to protect yourself from vulnerabilities is to ensure that software is always kept up to date and patched for urgent security updates. Patches must be upto date and installed on every machine within the organization, so a system for deploying updates in a timely fashion is essential for securing the integrity .Mobile code such as Java and Flash can also be used to make calls to a website to download malicious software. Avoiding them from your browser will increase the security and make ransomware attacks less likely. It is also important to provide thorough security training for staff and educate them on the ways in which malware can infect files. Each organization should develop their IT security policies carefully, making sure to account for working in the cloud[20].Cloud-based antivirus software, network monitoring and threat detection including the ability to block suspicious activity is another very effective way to create a more secure computing environment when there are a lot of users on the network.Backups with efficient recovery capability are the best way to recover from a ransomware attack.Almost all cloud service providers have secure backups[21], if they do not have an efficient recovery procedure , its tedious to restore files to their original unencrypted state, which can cost affected organizations greatly in terms of lost business hours.

V.CONCLUSION

Ransomware is a type of malware that prevents or limits users from accessing their system, by locking the system's screen or by locking the users' files and demand a ransom. Bitcoins are used by ransom operators for payments. The Wanna Cry ransomware attack,a cryptoransomware – was one of the largest ever cyber attacks – appeared on May 2017,affected over 200,000 systems around the world. Exposed older, unsupported operating systems such as Windows XP and Windows Server 2003, were initially at particular risk but the day after the outbreak Microsoft took the unusual step of releasing updates for these operating systems. Cloud computing provides virtual resources to its consumers through internet. Security in cloud computing is still a hurdle. Sensitive industries like healthcare, retail, and finance can leverage the cloud by partnering with security providers who offer strong security.Also simply adopting cloud-based security and storage is not an adequate response against ransomware attack.

.

REFERENCES

[1] L. Kelion, "Cryptolocker ransomware has 'infected about 250,000 PCs'," BBC News techology, 2013. [Online].Available:http://www.bbc.com/news/technology-25506020. [Accessed 2016].
[2] V. Weafer, "McAfee Labs Threats RepOlt," *McAffe*, March 2016
[3] A. Simmone, "Ransomware' s stranger-than-fiction origin story,"*UNIHACKABLE - Medium,* March 2015.
[4] G. O'Gorman and G. McDonald, "Ransomware: A growing Menace," *Symantec,2012*
[5] M. Zapotosky and E. Nakashima, 'These hackers can hold a town hostage. And they want ransom- paid in bitcoin," *The Washington Post*, March 2016
[6] L. Wagner, " LA Hospital Pays Hackers Nearly $17,000 To Restore Computer Network," *NPR*, Februrary 2016
[7] *Ransomware*, Microsoft Malware Protection Center, Februrary 2015
[8] http://spectrum.ieee.org/tech-talk/computing/it/wannacry-updates-microsoft-touts-digital-geneva-convention-to-thwart-future-cyberattacks

[9] Bishop, M. and Gates, C. 2008. Defining the insider threat. In Proceedings of the 4th Annual Workshop on Cyber Security and information intelligence Research: Developing Strategies To Meet the Cyber Security and information intelligence Challenges Ahead (Oak Ridge, Tennessee, May 12 - 14, 2008). F. Sheldon, A. Krings, R. Abercrombie, and A. Mili, Eds. CSIIRW '08, vol. 288. ACM, New York, NY, 1-3. DOI= http://doi.acm.org/10.1145/1413140.1413158
[10] R. La'Quata Sumter, ―Cloud Computing: Security Risk Classification‖, ACMSE 2010, Oxford, USA
[11] Mladen A. Vouch, ―Cloud Computing Issues, Research and Implementations‖, Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246
[12] G. O'Gorman and G. McDonald, "Ransomware: a growing menace," Symantec Corporation, 2012.
[13] B. N. Giri, N. Jyoti and M. AVERT, "The Emergence of Ransomware,"AVAR, Auckland, 2006
[14] L. O'Brien and J. Morparia, "Trojan.Cryptowall," *Symantec*, March 2015
[15] B. Fraga. Swansea police pay $750 "ransom" after computer virus strikes. *The Herald News*, 2013.
[16] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998
[17] Satoshi Nakamoto,Bitcoin: A Peer-to-Peer Electronic Cash System
[18] Brenner, Bill. "WannaCry: the ransomware worm that didn't arrive on a phishing hook". 18 May 2017
[19] "Microsoft Security Bulletin MS17-010 – Critical". *TechNet*. Microsoft. Retrieved 13 May 2017
[20] R. La'Quata Sumter, ―Cloud Computing: Security Risk Classification‖, ACMSE 2010, Oxford, USA
[21] Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. 2009. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In Proceedings of the 16th ACM Conference on Computer and Communications