RANSOMEWARE : A HIGH PROFILE ATTACK

Abhay pratap singh

---***---

ABSTRACT

Ransomware is combination of ransom and software which basically means that encrypt your all data files in computer and it's impossible to access these files, until you pay some ransom to attacker. A ransom is the money that has to be paid to victim via untraceable currency like (e.g.- bit-coin). Ransomware is more complex and stealthy kind of nature, so it's always been daunting task to traditional based detection system to detect that kind of popular threat as well. Now a days, Ransomware is more growing threat in business areas that costs millions of dollars each year, attackers are also use some complex encrypting algorithm to make harmful code so that they could easily bypass antivirus also. In this paper our main focus to provide full information regarding Ransomware like what are the various ways to prevent and detect that kind of popular threat in computer security.

Keywords – Ransomware, Malware, Encrypting algorithm, Bitcoin, Phishing

1 **Introduction**

The growing threat of Ransomware is become big concern for cyber security experts, figure[1] shows the rise in Ransomware attacks below here.

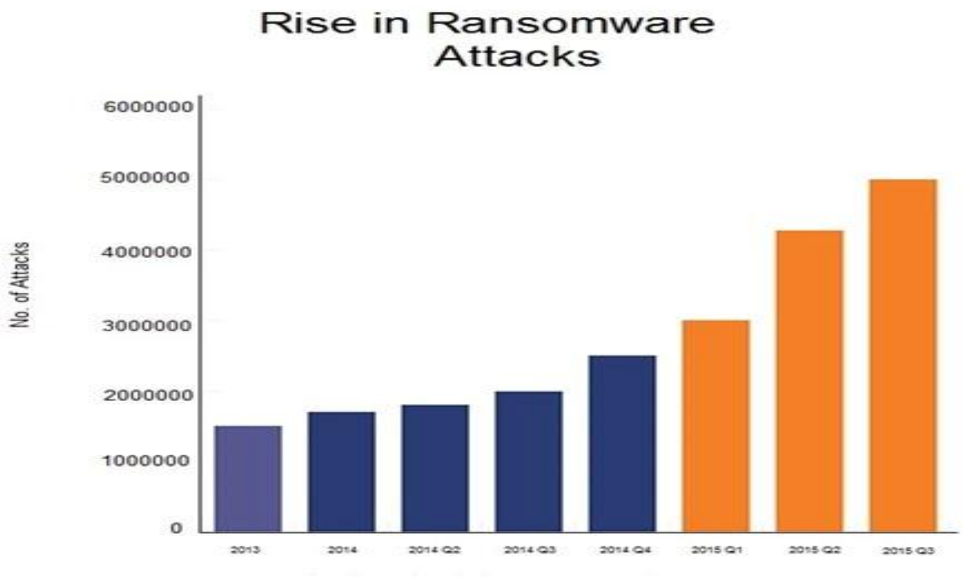


Figure 1 Increased Volume Of Ransomware From 2013 To 2015

Encrypting Ransomware deals with some complex kinds of algorithm, its basically designed to block system files and want ransom to provide the victim with the decryption key so that he can access the blocked content. This kind of Ransomware is also known as crpto Ransomware. Examples include **crptolocker**,**locky**,**crptowall** and many more.

Locker Ransomware is different kind of Ransomware, if we compare to other types of Ransomware, eventhough functionalities are same,but it doesnot encrypt your data files,instead it's used in scareware fashion,the locker displays a message in computer and trying to convinced to user, that he has done something wrong in his system like viewing of child pornography and later demands ransom to victim.
The popular examples include **winlocker**.

Another important type of Ransomware is MBR Ransomware that stands for master boot record Ransomware, The MBR is the section of a computer hard drive which enables the operating system to boot up. when MBR Ransomware hits, the boot process can't complete as usual, and shows a ransom note to be displayed in screen [1], the popular examples include Petya Ransomware.

2. Related work –

The first Ransomware was developed by Dr.joseph Popp, a biologist with a Phd from harvard in 1989, The original Ransomware was manually distributed via a 5.25-inch floopy disk[2].

Ransomware not only hit the private organization or individual but it could also hit electric authority or water supply, in recent news Ransomware malware deployed Israel's electric authority[3].

Ransomware can be major security threat to cloud computing [4] as it becomes the basic infrastructure of information system, Simple locker[5] also targets smart phone users of the Android environment.

"The effective Ransomware prevention technique using process monitoring on android platform", in this paper [6] author proposed technique specifies and intensively monitors processes and specific file directories using statistical methods based on processor usage, memory usage, and I/O rates so that the process with abnormal behaviors can be detected.

Ransomware is designed for direct revenue generation. The four most prevalent direct revenue generating risks include misleading apps, fake antivirus scams,locky Ransomware and crpto Ransomware[7].

According to Bitsight insights report ,researchers analyzed the growing trend of Ransomware across nearly 20,000 companies to identify common forms of Ransomware and identify which industries are most susceptible to these types of attacks[8].

Bitcoin Ransomware is very difficult to trace it out, eventhough [9] proposed three approaches to revealing the identity of criminals involved in bitcoin Ransomware schemes, but it doesn't guarantee the complete identification of such criminals.

3. Ransomware attack channels –

3.1 Phishing Email – Phishing is one of the most popular and common method to deliver malware on victims machine. Attackers cleverly designed a legitimate email, send it to the victim, now a days attackers choose one of the best way to deliver malware via spear phishing attack, in this kind of attack, attackers gathered all kind of information about particular person or companies, the probability of getting successful chances is more rather than compare to other types of phishing attack.

3.2 Drive By Download – A drive by download is a malicious program that automatically download the virus without user knowledge, it will usually find some vulnerabilities in outdated application, once the weakness has been found virus enters into system and take control of it, so it"s always better to update your all application and software to prevent that kind of threat as well.

3.3 Click Jacking – Click jacking is malicious technique that used by attacker, when a user visited a web page, attacker force them to click random things, when they click it, it will redirect the page in other page and gains whole system access, this type of attack is known as click jacking.

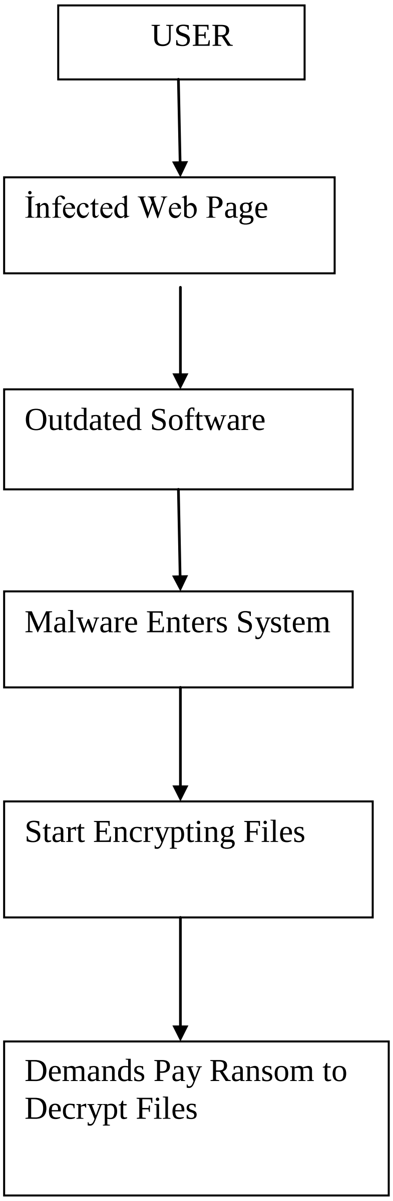
3.4 Malwaretising Campaign- Malwaretising is new technique to spread malware with the help of online advertising . Online advertising provide a good platform for spreading malware because it's easy to attract users to sell or watch new products online

3.5 Botnets- Botnet is kind of computer network, that is interconnected each other and controlled by attacker, without user knowledge. They are typically used for DDOS attack and Spam.

3.6 Vulnerable Software – Cyber criminals are always looking for vulnerability in software or network, they never attack on router, firewall, intrusion detection system(ids). Attacker always want to find some weakness in software,once they found it
They can easily exploit it and access to whole network.

3.7 Exploit Kit – Exploit kit is infection kit that are used to execute malicious code onto
Your machine. One popular way to spread malware via exploit kit to users are if a user
Visit website which is already hosted on exploit kit, then malware could be download automatically without user knowledge.

4. How Do Ransomware Spread Via Web –



5. Prevention Of Ransomware Attacks –

5.1 Backup and Data Recovery- Before you infected via Ransomware, first thing you have to do,back up your data in regular intervals, there are two important ways which you can store multiple copies of data , first cloud based storage example- Google drive,
Drop box, and second external hard drive.

5.2 Apply Whitelisting Software- Traditional security is become inefficient to combat new kind of virus and malware, so whitelisting new approach that it allows only trusted program, if anything doesn't match his own database then it will completely discard other things.

5.3 Keep Your Operating System And Software Update- This is the most general tip to all those novice users, who don't have much knowledge about cyber security, if a user continuously running all application without update, attacker may be exploit these loop holes and easily access to computer,so always update O.S and software in regular intervals.

5.4 Recover The Data Using Forensic Technique- On windows, deleting a file means deleting the pointer to the file (not the contents) in NTFS/FAT/EFS file system.this space is then marked as free and available for overwriting. With the help of forensic techniques, its possible to clear the free space on the disk for useful information [10].

5.5 Disabale Macros In Microsoft Office Suite – Macros are bit of code embedded in Microsoft office documents. They are very dangerous and make you vulnerable to virus infections. İn new version of microsoft office contain some security features that will safe you from macros, if you disable macros then it would be better for security point of view as well.

5.6 Use Ad-blocker Software – Malwaretising is new technique to spread malware with the help of advertisement known as malwaretising, in this paper we already discussed malwaretising , using ad blocker software we can easily disable ads in our web page so it gives freedom to user surface web page easily in internet.

5.7 Disable Windows Power Shell If You Don't Use It- Power shell is tool that's much more powerful than the command prompt. İts based on .NET framework and it includes command line shell and a scripting language. İn a way its also intended to replace the command prompt, as it delivers more power and control over the windows operating system[1]. So if you don't use power shell then disable it.

6. CONCLUSION -

Ransomware is massively effective and lucrative for cyber criminals,in this digital world
Cyber criminal uses various obfuscation techniques and mix of social engineering techniques as well so, it's always been difficult task to Non IT-user and IT user to fight against that kind of complex threat , because what happen sometimes our antivirus couldn't detect threat so that if you follow some vital prevention tips regarding Ransomware or Malware,which we have already discussed in this paper then you should be able to mitigate Ransomware attack altogether.

7. REFRENCES –

[1] https://heimdalsecurity.com/blog/

[2] Deloitte threat intelligence and analytics,threat study issued date: August 12,2016.

[3] https://thehackernews.com/2017/02/android-malware-israeli-military.html

[4] Y. Liu, Y. L. Sun, J. Ryoo, S. Rizvi, and A. V. Vasilakos, "A survey of security and privacy challenges in cloud computing: solutions and future directions," Journal of Computing Science and Engineering, vol. 9, no. 3, pp. 119–133, 2015.

[5] T. M.Marengereke and K. Sornalakshmi, "Cloud based security solution for android smartphones," in Proceedings of the IEEEInternational Conference on Circuit, Power and Computing Technologies (ICCPCT '15), pp. 1–6, Nagercoil, India, March 2015.

[6] The Effective Ransomware Prevention Technique Using Process Monitoring on Android PlatformSchool of Computing, Soongsil University, Sangdo-ro, Dongjak-gu, Seoul 06978, Republic of Korea.

[7] The evolution of Ransomware http://www.symantec.com

[8] https://www.bitsighttech.com

[9] Ransomware Hostage Rescue Manual, www.knowbe4.com

[10]https://www.**sans**.org/readingroom/whitepapers/riskmanagement/**ransomware** -37317