WWJMRD 2017; 3(10): 215-217
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Ankur Gupta
Assistant Professor in Computer Science
RSD College, Ferozepur City, India

Correspondence:
Ankur Gupta
Assistant Professor in Computer Science
RSD College, Ferozepur City, India

A brief study of Most Advance Data Threat: Ransomware Virus

Ankur Gupta

Abstract
Ransomware — Malware designed to prevent access to a system until a sum of money is paid. As cybersecurity threats continue to evolve, ransomware is fast becoming the number one menace. Financial gain is the primary motivation for computer intrusions. Unlike malware that allows criminals to steal valuable data and use it across the digital marketplace, ransomware directly targets the owners of data, holding their computer files hostage until a ransom is paid. They always demand digital currency like Bitcoin to decrypt the data.

Keywords: Ransomware, Menace, Malware,Security, Financial, Bitcoin

Introduction
Ransomware is a category of malicious software which, when run, disables the functionality of a computer insome way. The ransomware program displays a message that demands payment to restore functionality. Themalware, in effect, holds the computer ransom. In other words, ransomware is an extortion racket

Fig.1:. Example of First screen to show after Ransomware virus Pic.

From virus and the countdown begins. The whole computer files are encrypted using public and private keys. Users have to give some money in form of digital currency like bitcoin have to pay to get the decrypt key. These threats are not limited to any particular geography or operating system, and can take action on any number of devices. Everything from your Android devices, iOS systems, or Windows systems all are at risk of this type of exploitation via ransomware. Depending on the target, the method of compromise of the device may be different, and the final actions taken would be limited by the device capability itself, but there are also recognizable patterns that many extortionists follow.

Background

The first ransomware was developed by Dr. Joseph Popp, a biologist with a PhD from Harvard, in 1989 and was dubbed the PC Cyborg Trojan, otherwise known as the AIDS Info Disk Trojan. But Ransomware which locked a screen and demanded payment was first seen in Russia/Russian speaking countriesin 2009. Prior to that, ransomware was encrypting files and demanding payment for the decryption key.

Fig. 2: is an example of the message displayed how they demand for ransome.

Ransomware is frequently divided into two different categories: Locker and Crypto.

Locker Ransomware — Locker ransomware does not encrypt victims' files or data; instead, it is used in a scareware fashion to generate payment. Upon infection, the locker displays a message stating the computer has been commandeered by law enforcement in relation to some sort of crime committed by the user (e.g., viewing of child pornography or pirating of copyrighted materials), and demands the victim pay a fine (ransom) or face criminal charges, additional fines, and/or imprisonment. In many cases, the user's public IP address, Internet service provider, and geographic location are displayed in the threat and accompanying ransom demand, increasing the credibility of the message to trick the user into paying the ransom.

Crypto Ransomware — Crypto ransomware encrypts victims' files or data using a variety of different cryptography methods, then notifies the victims that their files have been encrypted and demands a ransom to decrypt them (see Figure 1). Recent crypto ransomware variants, such as Locky, TeslaCrypt, and Cerber, encrypt the files, the contents within the files, as well as the file names, all without notification. Encryption makes it very difficult for victims to access their data, short of complying with the ransom demands.

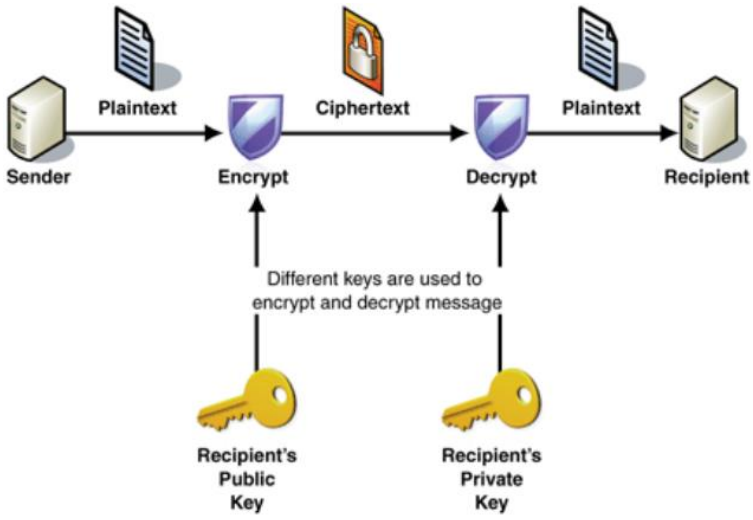

Fig. 3: shows how crypto Ransomware works.

Preventive Measures:

Prevention is essential in keeping computer safe. It's a recommendation for users to keep their operating system and software updated. Make use of multilayers protection security solutions that is reliable. Back up all important and valuable data offline regularly.

Ransomware can be sent through various sources like Emails, Advertisement, by creating websites and many

more things that can share the ransomware to the computer users. Ransomware restricts the use of the system in various ways after intruding the system. It is mainly classified into the following three types: Scareware, Lock-Screen, and Encrypting [8] [9]. WannaCryransomware virus attacked the whole world and no one knows how to decrypt these files. Ransomware is a type of malicious software designed to block access to computer system until some of money is paid. Following are some of the preventive measure to avoid ransomware:

- Antivirus should always have a last update.
- Spam messages should not be opened or replied.
- Back up the data. To defeat, regularly updated backup
- Personalize the anti-spam settings the right way.
- Apply patches and keep the operating system, antivirus, browsers, Adobe Flash Player, Java, and other software up-to-date.
- Keep the Windows Firewall turned on and properly configured at all times.
- Enhance the security of your Microsoft Office components (Word, Excel, PowerPoint, Access, etc.).
- Think of disabling remote services.
- Filter EXEs in email.
- Use a reputable security suite.
- Use System Restore to get back to a known-clean state.
- Use System Restore to get back to a known-clean state.
- Sure to disable file sharing.
- Switch off unused wireless connections, such as Bluetooth or infrared ports.
- Exercise caution before using Wi-Fi network.
- Do not click on harmful links in your email.
- Do not visit unsafe and unreliable websites.
- Rather than clicking any web links, type out web address on address bar.

A novel practise to protect against ransomware attack is to back all files completely on another system frequently to avoid loss of data.

Conclusion

There is a constant growth in the security risks among Windows users, be itworms, Trojans or ransomware. In case of systems infected with ransomware, if anattack is suspected or detected in its early stages, it takes some time for encryption totake place, then immediate removal of the malware before it has completed encryptionwould limit its damage to the data. One of the best way to protect the system fromransomware is to protect the system by hardening and updating OS and antivirusregularly.

References

1. SavitaMohurle***et al,*** International Journal of Advanced Research in Computer Science, 8 (5), May-June 2017,1938-1940
2. en.wikipedia.org/wiki/Cryptolocker
3. http://www.excitingip.com/5130/ransomware-an-introduction/
4. https://www.symantec.com/content/dam/...papers/istr-ransomware-2017-en.pdf
5. Deloitte Threat Intelligence and AnalyticsIssue Date: August 12, 2016 | TLP: WHITE1 | Serial: W-TS-EN-16-00734 | Industry: