Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 5, May 2017, pg.29 – 33

AN OVERVIEW ON TESLACRYPT VIRUS: VIRUS VARIANT, VERSIONS, TOOLS AND REMOVAL APPROACH

Parvathy.K
PG Scholar, Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore, India
parvathykrishna1808@gmail.com

Abstract – The Teslacrypt is a malicious program that makes users to encrypt the files using the algorithm called AES encryption. In Teslacrypt virus it is impossible to decrypt the files which makes the system to be in the infection system. In order to perform the decryption process two tools are introduced called Talos and ESET decryption tool. In this paper deals about variants of teslacrypt virus and its extensions and the removal of teslacrypt virus.
Index Terms –Teslacrypt

INTRODUCTION

The [1]teslacrypt is a suspicious program that helps the user files to encrypt them by using AES encryption. When the files are encrypted, it is decrypted by the files using private key. During the decryption the files are not in secure. It mainly effects to window operating system.[4][5] The early version of teslacrypt mainly effects to computer games.

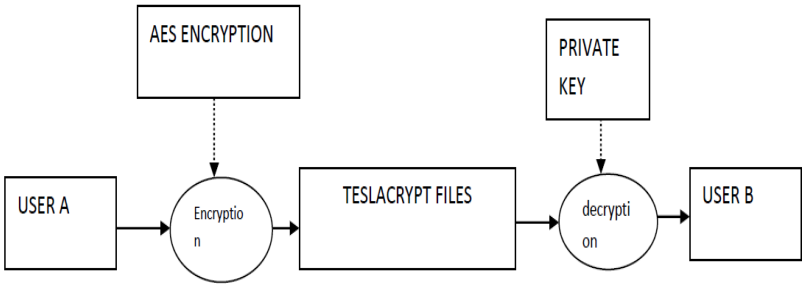

Fig.1.1.Teslacrypt

In the early days, [2][7]Teslacrypt was mainly focussed on game play data for computer games. It mainly include the call of duty, World of Wildcraft, manucraft and world of tanks.

The[3] teslacraft now encrypt not only games, it include all files like word, pdf, jpeg. For the decryption key, the user need to pay for the ransomware.
Teslacrypt uses[5][7] asymmetric encryption for developing the decryption tool. There are various versions currently found out in the teslacrypt virus[10].
At the current year, Teslacrypt releases the master decryption key for decryption of files.

How the teslacrypt is created?

The teslacrypt is[7][14] created by changing the desktop background by creating a new file called "HELP_TO_DECRYPT_ YOUR _FILES.Txt" like NOW_RECOVER_HTML,NOW_RECOVER_.TXT to the desktop. The Teslacrypt which occurs in the different file extensions that encrypt the files by creating the ransom ware.

A.TESLACRYPT MASTERKEY

The master key[11][15] which decrypt the files and unlock all the encrypted files.so the decrypted tool is created and downloaded to decrypt the files by using with the master key. It is simple to use. The mitigation or to closing down the teslacrypt the master key is introduced to decrypt the files.[8] The master key, that helps the decryption key to update the key versions like version 1.0, version 2.0 version 3.0 and version 4.0 of the teslacrypt encrypted files. The teslacrypt encrypted files that has the file extension called .xxx, .ttt,.micro,.mp3.

TeslaDecoder -Decryption of Teslacrypt Encrypted Files

The Encrypted[12][14] files that need to be decrypted by downloading the tesladecoder to decrypt the encrypted files, after the successful execution of the files, set the key for the encrypted files while the decrypted files are set with the key for the decryption.
The Decryption process will scan all the files for finding the threat. The tesladecoder which will overwrite all the unencrypted version of files[9][10].

TESLACRYPT DECRYPTION TOOL (TALOS)

The talos is the tool that will perform the user to encrypt their files by using the ransomware.[5][7] The tool called talos decryption tool which is an open source tool command that decrypt files that decrypt the encrypted files that change to its normal state from the ransomware.[10] It encrypt mainly the user files such as photos, video, documents, saved game files etc. The user downloads the decryption key to restore the files from formatting them.[12][13] For this purpose the user need to pay the ransom to download the key. The tool which removes the ransomware by decrypting files. The versions for teslacrypt to decrypt the files.

- *Teslacrypt 0.x* – the version encrypt the files by using AES-256 CBC Algorithm.
- *Alphacrypt 0.x*- The version encrypt the files using AES 256 and encrypt the key using EC.
- *Teslacrypt 2.x*-This version which EC to create a weak recovery key .so that it helps to recover the user's global private key.
- *Teslacrypt 3&4*- The latest version of encrypting the files and decrypting without any circumstances.

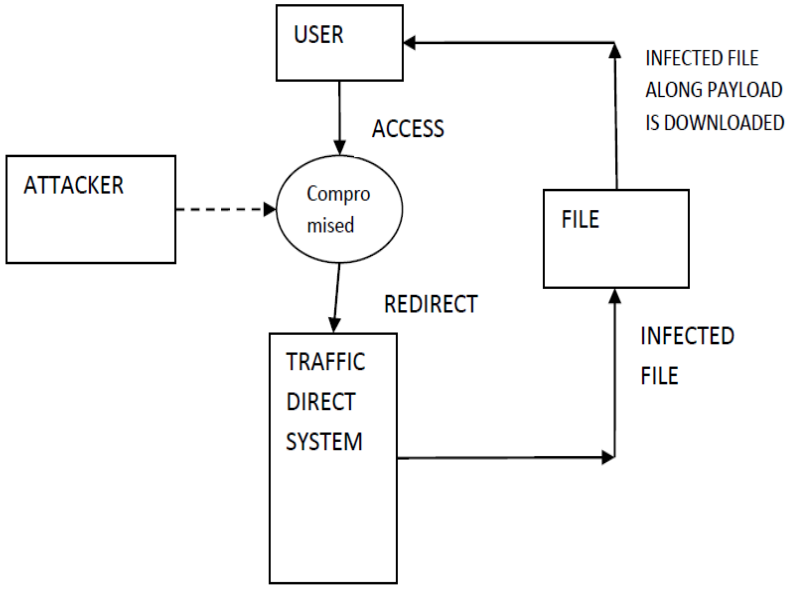

Fig.1.2.System with TESLACRYPT Ransomware

TESLA DECRYPTION TOOL (ESET)

The decryption tool to create the decryption of key for encrypting of files called ESET.[6][8] This tool which also use for the locky virus. The ESET tool which makes a free decrypting tool to unlock the files between 3.0.0 and 4.2.

TYPES OF TESLACRYPT VIRUS
There are[7][10] different types of virus along with there extensions they are as:

TESLACRYPT 2.0

It encrypt the files in the infected system. The algorithm called ECHD algorithm which makes master key to each and every infected system. The extension for this type of virus is ".vvv".
.vvv File Extension virus:

When the system is infected and got encrypted it change the file extension to .vvv and creates a file document to the desktop as HOW_RECOVER.HTML,HELP_RESTORE.HTML,HOW_RECOVER.TXT.

TESLACRYPT 3.0

When the system which get infected, it encrypt the files and the decryption key is deleted from the system. As a result it is difficult to recover the lost data.

- *.ccc File Extension virus:*

The most serious virus which block the user to open the files. It encrypt the files by using advanced encryption technology. thus the extension of the files changes to .ccc these types of virus is to be removed, it may cause to loss of files.

- *.xxx File Extension virus:*

The threat which makes the user to block of accessing the files and attach with .xxx files.

- *.ttt file Extension virus:*

The extension called .ttt files appears on the computer without any knowledge of the user.

- *.micro File Extension virus:*

It is a paid virus extension. When the file is encrypted it changed to .micro file extension.

Teslacrypt 4.0

The virus is an advance alternative virus where, it does not add additional file extension. It uses to complex encryption Algorithm –RSA-4096.

Teslacrypt 4.1 b

It is latest version of virus. The virus mainly uses to WMIC (Window, Management Instrumentation Command Line) for deletion of the show copies in files. This makes impossible for restoring the files in the system backup.

REMOVAL OF TESLACRYPT VIRUS

To remove the teslacrypt virus,[10] the following task is to be done. If the threat is infected in the system with the data is to be encrypted.

- The Computer should be disabled from the internet.
- Use Reimage tool to scan the entire system and check the system to remove the virus from the system.
- Use Teslacrypt decryption tool to use system backup.

For the permanent removal of teslacrypt virus there are two methods they are.

- Safe Mode with Network
- System Restore

REMOVAL OF TESLACRYPT VIRUS USING SAFEMODE WITH NETWORKING

To remove the virus,[10][11][15] if the system can't able to detect using Anti-Spyware, Reboot the system using Safe Mode with Networking.

STEP 1: The System which need to be Reboot using Safe Mode with networking

- Select start->Shutdown->Restart->OK.
- Select F8 by pressing and select advanced boot options.
- Enable Safe Mode with Networking.

STEP 2: To remove the Teslacrypt open the Browser and download the Reimage or anti-spyware program. Update all the function to scan the entire system.

REMOVAL OF TESLACRYPT USING SYSTEM RESTORE

The other method for[10][12][15] removing the teslacrypt the following steps to remove the malware software.

STEP 1: System is to be rebooting with safe mode in the command prompt.

- Select start->Shutdown->Restart->OK.
- Select F8 by pressing and select advanced boot options.

STEP 2: The system should be restore their files and the settings. Open the command prompt and type cd restore. Then after restoring type rstrui.exe.

STEP 3: After successful Restoring of file, install the reimage to scan the system and remove the teslacrypt

CONCLUSION

In this paper, an overview of teslacrypt virus is been discussed. For the decryption process, types of decryption tools and the virus extensions are been discussed. The removal approach for the teslacrypt virus which helps for removing the infection from the system as well as remove the threat from the system.

REFERENCES

[1] Abrams, Lawrence (27 February 2015). "New TeslaCrypt Ransomware sets its scope on video gamers". Bleeping Computer.

[2] "Gamers targeted by ransomware virus". BBC News. 13 March 2015. Retrieved 14 March 2015.

[3] Sean Gallagher (Mar 12, 2015). "CryptoLocker look-alike searches for and encrypts PC game files". Ars Technica. Retrieved 14 March 2015.

[4] "New CryptoLocker ransomware targets gamers". ZDNet. March 13, 2015. Retrieved 14 March 2015.

[5] "TeslaCrypt Ransomware Encrypts Video Game Files". Security Week. March 13, 2015. Retrieved 14 March 2015.

[6] "Achievement Locked: New Crypto-Ransomware Pwns Video Gamers". Bromium Labs. March 12, 2015. Retrieved 14 March 2015.

[7] "Decryption tool available for TeslaCrypt ransomware that targets games". PC World. 2015. Retrieved 17 May 2015.

[8] Sinitsin, Fedor. "TeslaCrypt 2.0 disguised as CryptoWall". securelist. AO Kaspersky Lab. Retrieved 5 November 2015.

[9] Abrams, Lawrence. "TeslaCrypt Decrypted: Flaw in TeslaCrypt allows Victim's to Recover their Files". Bleeping Computer. 2015 Bleeping Computer LLC. Retrieved 21 January 2016.

[10] Abrams, Lawrence. "TeslaCrypt 3.0 Released with Modified Algorithm and .XXX, .TTT, and .MICRO File Extensions". BleepingComputer. 2015 Bleeping Computer LLC. Retrieved 21 January 2016.

[11] "BehaviorReport Ransomware Teslacrypt". securelist. Joe Security. Retrieved 29 Dec 2015.

[12] "TeslaCrypt shuts down and Releases Master Decryption Key". BleepingComputer. Retrieved 2016-05-19.

[13] Stub icon "Disk encrypting Cryptolocker malware demands $300 to decrypt your files". Geek.com. Retrieved 12 September 2013.

[14] "ESET Tops Worldwide Growth List for Consumer Security in Leading Industry Analyst Firm's Security Software Market Share Report". BusinessWire. SAN DIEGO. 2012-04-26.

[15] Vincentas (11 July 2013). "Trojan Horse in SpyWareLoop.com". Spyware Loop. Retrieved 28 July 2013.

