CautelaLabs

Volume 2016-182-1

Ransomware – TeslaCrypt

Summary

TeslaCrypt is an encryption ransomware Trojan. Encryption ransomware changes your files so you can't open them. It does this by encrypting the files. TeslaCrypt, which often targets gamers infects systems through malicious downloads, web domains which loads exploit kits and phishing campaigns. As ransomware, TeslaCrypt will infect systems and encrypts user files forcing a landing page and removing access to the PC until the ransom is paid, usually by Bitcoin.

Detailed Information

TeslaCrypt perform the following:

- Delete all system Volume Shadow Copies by executing "vssadmin.exe delete shadows /all /quiet" command
- Open the "key.dat" file and recover encryption keys. If "key.dat" file doesn't exist, create the keys and store them in an encrypted form in the "key.dat" file.
- Send the new master encryption key to the C&C server through POST request (the latest sample that we have analyzed contains the following C&C server URLs:

    - 7tno4hib47vlep5o.63ghdye17.com
    - 7tno4hib47vlep5o.79fhdm16.com
    - 7tno4hib47vlep5o.tor2web.blutmagie.de
    - 7tno4hib47vlep5o.tor2web.fi

- Implement anti-tampering protection: every 200 milliseconds, TeslaCrypt enumerates all running processes and if a process with a filename that contains any of the words below is found, that process is terminated using the Terminate Process Windows API function

    - taskmgr
    - procexp
    - regedit
    - msconfig
    - cmd.exe

Preventive Actions

- Don't click on a link on a webpage, in an email, or in a chat message unless you absolutely trust the page or sender.
- If you're ever unsure – don't click it!
- Often fake emails and webpages have bad spelling, or just look unusual. Look out for strange spellings of company names (like "PayPol" instead of "PayPal") or unusual spaces, symbols, or punctuation (like "iTunes Custamer Service" instead of "iTunes Customer Service").

Corrective Actions

Security developers have provided a universal decryption key. Please follow the below steps to decrypt your files.

- Download the ESETTeslaCryptDecryptor.exe tool and save the file to your Desktop.

  http://download.eset.com/special/ESETTeslaCryptDecryptor.exe

- Click **Start** → **All Programs** → **Accessories,** right-click **Command prompt** and then select **Run as administrator** from the context menu.
- Windows 8 / 8.1 / 10 users: press the Windows key + **Q** to search for applications, type **Command prompt** into the **Search** field, right-click **Command prompt** and then select **Run as administrator** from the context menu.
- Type the command cd %userprofile%\Desktop (do not replace "userprofile" with your username–type the command exactly as shown) and then press **Enter**.
- Type the command ESETTeslaCryptDecryptor.exe and press **Enter**.
- Read and agree to the end-user license agreement.
- Type ESETTeslaCryptDecryptor.exe C: and press **Enter** to scan the C drive. Files encrypted by TeslaCrypt V.3 and V.4 will automatically be decrypted. To scan a different drive, replace C: with the appropriate drive letter.
- The TeslaCrypt cleaner tool will run and the message "Looking for infected files…" will be displayed. IfSSS an infection is discovered, follow the prompts from the TeslaCrypt cleaner to clean your system.

Additional References

http://support.eset.com/kb6051/

http://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key/

https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Ransom:HTML/Tescrypt.D