DecryptorMax Ransomware Decrypted, No Need to Pay the Ransom

Emsisoft researchers creates decryption tool

By Catalin Cimpanu 28 Nov 2015, 10:31 GMT

Fabian Wosar of Emisoft has created a tool capable of decoding files encrypted by the DecryptorMax ransomware, also known as CryptInfinite.

The ransomware gets its name from the fact that the "DecryptorMax" string is found in multiple places inside its source code. Additionally, the CryptInfinite moniker is also used by some researchers because the ransomware adds the CryptInfinite key to the Windows registry, using it to store a list of all encrypted files and their location on disk.

According to Bleeping Computer's Lawrence Abrams, the ransomware is spread via Word documents attached to spam email. These files pose as resumes.

Users get infected via weaponized Word documents

Infection occurs when users open the document and enable Word Macros so that they can view the "proper" file. Word Macros are a known security vulnerability used by many malware developers to spread Web-hosted malware to Windows computers.

If this happens, from here on out, the ransomware is installed and immediately starts encrypting data files, adding the .crinf extension to all altered files.

Ransom notes are left in each folder that contains encrypted files, telling the user they have 24 hours to send a PayPal MyCash voucher code to one of three email addresses (silasw9pa@yahoo.co.uk, decryptor171@mail2tor.com, decryptor171@scramble.io).

Additionally, the ransomware also changes the user's desktop wallpaper with a version of the ransom note, then deletes all Shadow Volume copies, and also disables Windows Startup Repair so that the user won't be able to load previous backups.

The decryption process, with Emsisoft's DecryptInfinite

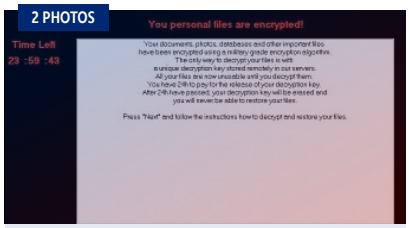
Mr. Wosar's tool, called DecryptInfinite, is quite easy to use and will allow DecryptorMax victims to unlock their files without paying the ransom. Using it is quite straightforward, and users need to go through some simple steps before decrypting files.

After they start the tool, users are required to drag and drop two files over the tool's main window. These have to be an encrypted file along with a version of the same file but in unencrypted form.

If users don't have at least one file in its unencrypted form, they should take a random PNG from the Web and drag it together with an encrypted PNG image from their computer. This will have the same results.

From here on out, the tool will compute the decryption key needed to decode files. This is a lengthy process, so have patience when using DecryptInfinite.

More details on how to use DecryptInfinite and how the tool works can be found in a forum thread on Bleeping Computer.



Ransom message left behind by DecryptorMax

MORE ON THIS TOPIC

Linux.Encoder.1 Ransomware Has an Older Brother, Just as Dumb

CryptoWall 4.0 Ransomware Already Part of Exploit Kits

Linux.Encoder.1 Ransomware Spreads to 3,000 Websites

Browser Ransomware

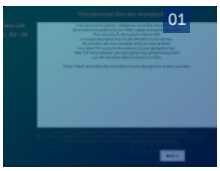
MORE +

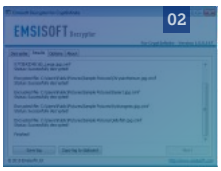
DecryptInfinite tool from Emsisoft

CHECK OUT THE GALLERY (2 Images)

#ransomware, #DecryptorMax, #CryptInfinite, #decryption tool, #decryption key

Photo Gallery (2 Images)





Hot right now · Latest news

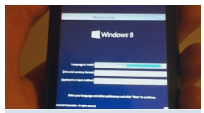
Verizon Says Microsoft Never Wanted Them to Sell the Lumia 950 and Lumia 950 XL

Warn... Crim... Heat... GPUs, Users Report - Update

Browser Ransomware Passes As Microsoft Support, Plays Audio to Scare Users

MORE ON: BROWSER RANSOMWARE

Websites in Iceland to Protest Whale Hunting



Windows Phone Device Hacked to Run Windows RT

5 Comments

Share your thoughts on this story!

SUBMIT

fart knocker
29 Nov 2015, 04:58 GMT

why no link to emsi web page, only download link? plebs

1 REPLY

catalin.cimpanu
29 Nov 2015, 10:04 GMT

They don't have one. Not even a blog post. Weird that they didn't promote the tool at all. It's their decision.

– REPLY

HSone
28 Nov 2015, 19:14 GMT

Just reinstall damned OS :) That's not a case of corse for not experienced users who keepin all the stuff on 1 partition C

– REPLY

LOAD NEXT 2 COMMENTS

LOAD ALL