Stampado Ransomware campaign decrypted before it Started

bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started

By
Lawrence Abrams

- July 22, 2016
- 06:54 PM
- 10

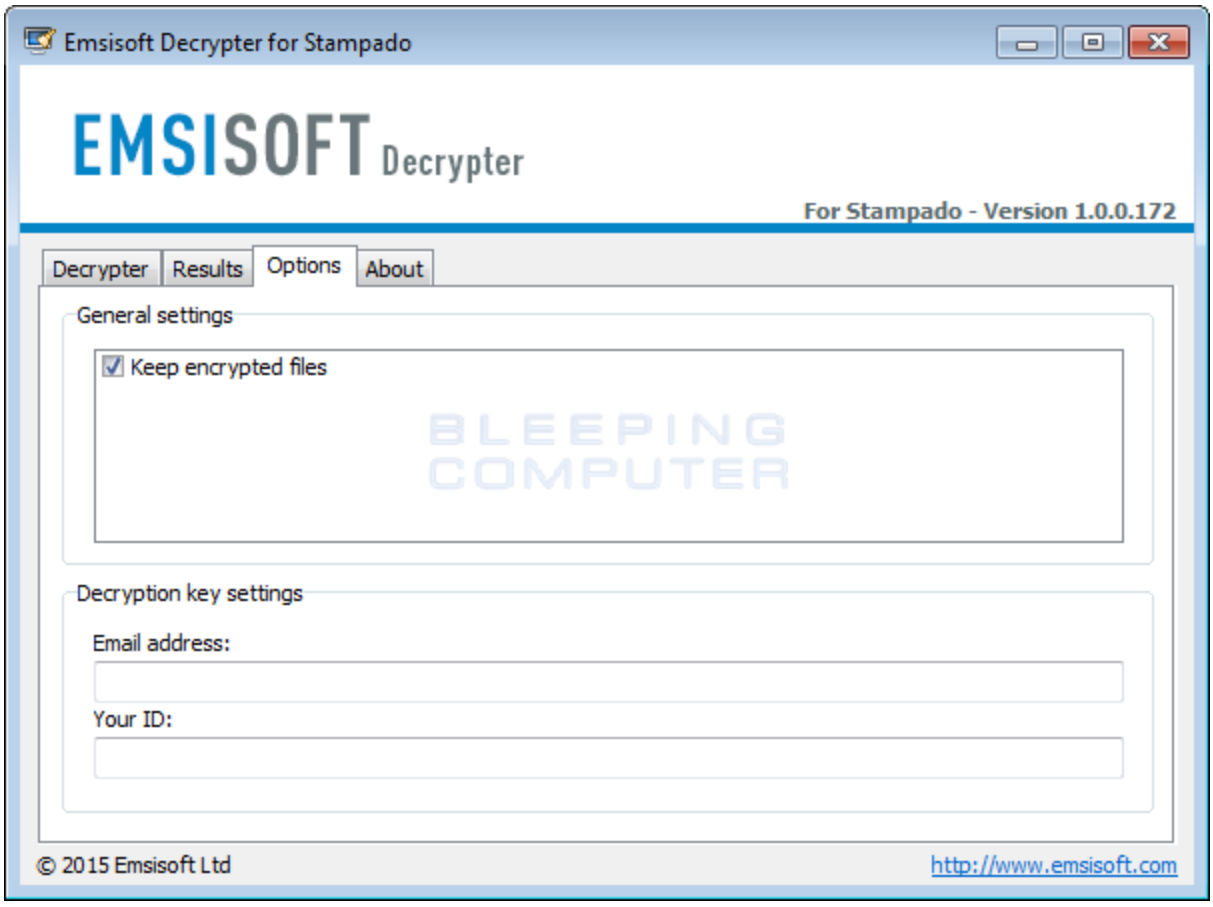
Since Stampado was discovered being sold on the darkweb for the cheap price of $39 USD, no samples were available. That changed today when I discovered two samples of Stampado on VirusTotal. It is currently unknown if these samples are from a live distribution campaign or were submitted by the distributor/developer to test how well they are detected by security programs. The best part is that it really doesn't matter as from these samples a decryptor has already been made by Fabian Wosar.

Stampado Lock Screen

What we do know, though, is that Stampado is fully functional and written in the AutoIT scripting language. When installed, it will encrypt a victim's files using AES encryption and then demand a ransom in order to get your files back. The two samples I have discovered have the names **kek.exe** and **WifiHack.exe.** At this time the ransom amount is currently unknown and you need to email the specified email address in order to get payment instructions.

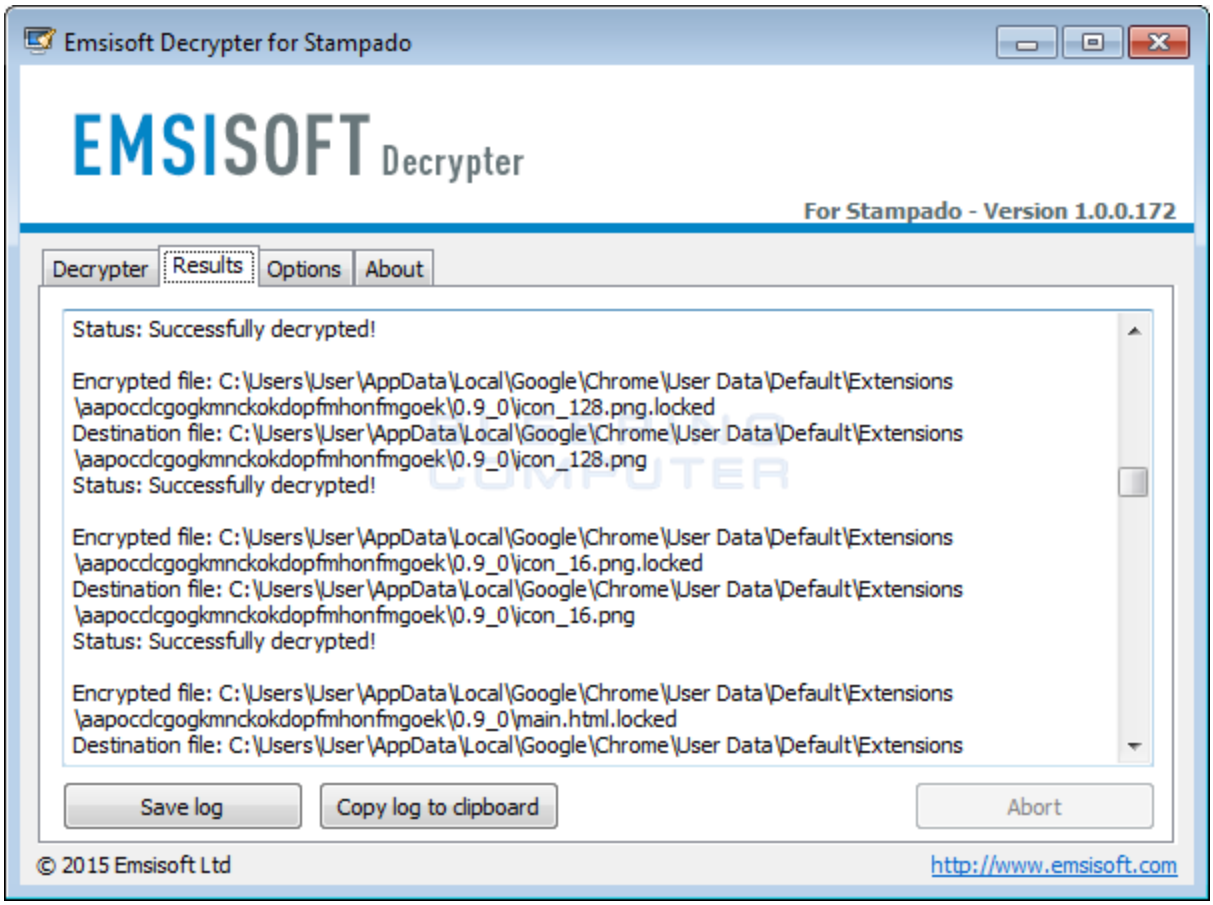
How to Decrypt files encrypted by Stampado

Fabian Wosar, of Emsisoft, was able to analyze the Stampado samples and create a decryptor for the infection. To use Fabian's decryptor, simply download it from the following URL: https://decrypter.emsisoft.com/stampado. Once downloaded, execute it and go into the options screen, where you will need to enter your ID and the email address found on the lock screen.



Decryptor Options

Once you enter in the required information, you can go back to the Decryptor tab and begin decrypting your files.



Decrypting Files

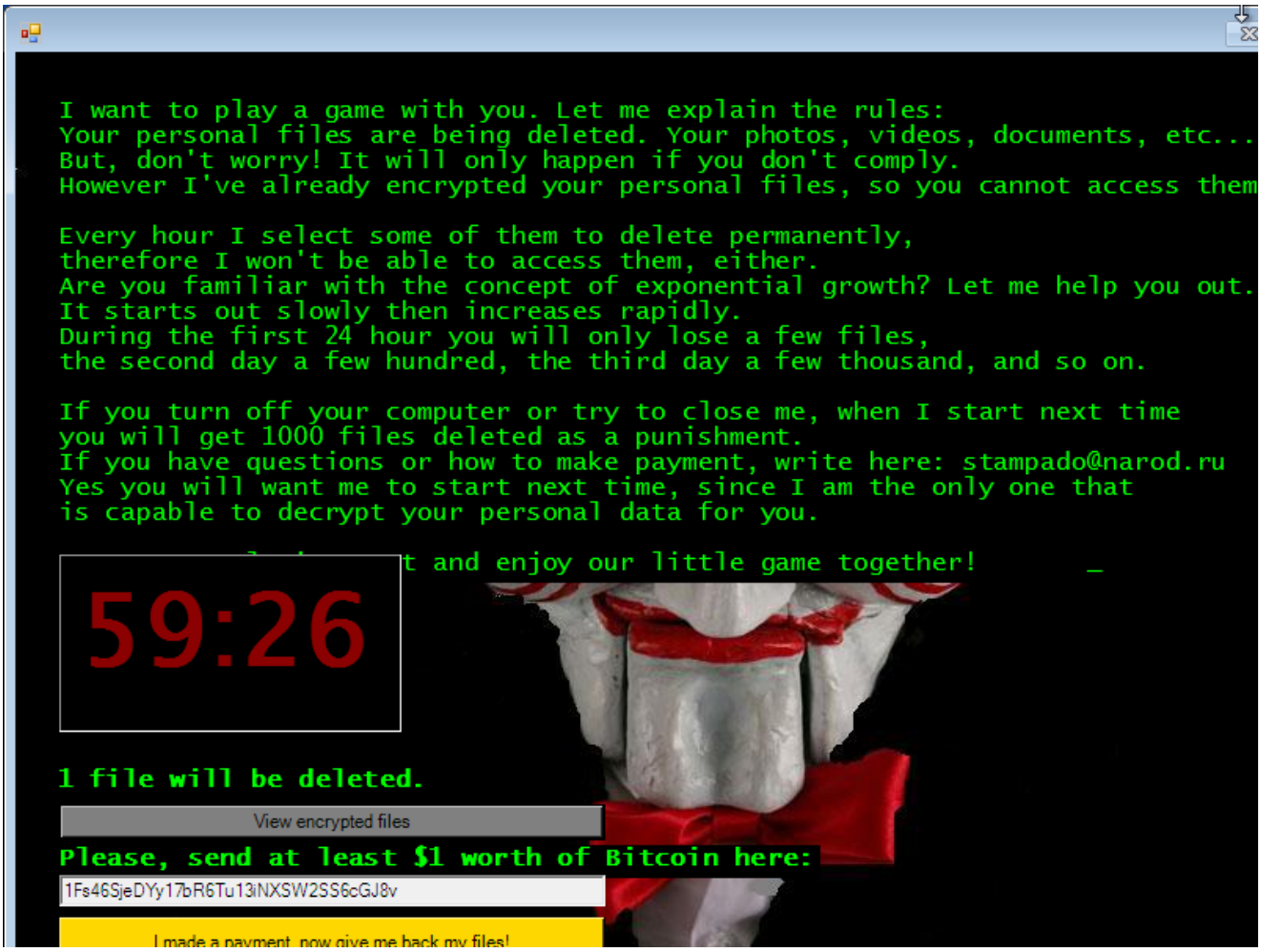
When the decryptor finished decrypting the files, you can close the program.

Possible link between Stampado and Jigsaw?

There are some interesting correlations, though possibly weak, between the Jigsaw ransomware and Stampado.

One of the nastier "features" of Stampado is its Russian Roulette, which will randomly delete an encrypted file every 6 hours. Each time this roulette countdown reaches 0, the amount of files are doubled. This is the same incrementing file deletion behavior is also exhibited by Jigsaw during its countdown. As file deletion in ransomware is very rare, it is interesting to see a similar behavior between the two ransomware infections.

Coincidentally, Michael Gillespie found a variant of Jigsaw yesterday that included the email address **stampado@narod.ru.** Coincidence or not?



Jigsaw background containing a email with Stampado

Last, but not least, Stampado is being sold on the same darkweb site as Jigsaw. Granted, these connections are weak at best, yet I felt it was worth mentioning.

How Stampado encrypts a victim's Files

When Stampado is installed it will copy itself to **%AppData%\scvhost.exe** and encrypt specific file types found under the victim's %UserProfile% folder using AES encryption. When it encrypts a file, it will append the **.locked** extension to it. This means that a file called test.jpg, will be named test.jpg.locked. The files currently targeted by Stampado are:

```
.jpg, .jpeg, .gif, .bmp, .c, .doc, .docx, .ppt, .pptx, .xls, .xlsx, .mov, .mp3, .cpp,
.au3, .pas, .php, .wav, .wma, .wmv, .mp4, .rar, .zip, .7z, .001, .html, .pdf, .txt,
.ai, .dmg, .dwg, .ps, .flv, .xml, .skp, .aiml, .sql, .cdr, .svg, .png, .ico, .ani,
.m4a, .avi, .csv, .d3dbsp, .sc2save, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb,
.tax, .pkpass, .bc6, .bc7, .bkp, .bak, .qic, .bkf, .sidn, .sidd, .mddata, .itl,
.itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbackup, .syncdb, .gho, .cas, .map, .wmo, .itm,
.sb, .fos, .mcgame, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm,
.001, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl,
.arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb,
.db0, .DayZProfile, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge,
.ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, .unity3d,
.wotreplay, .xxx, .desc, .py, .m3u, .js, .css, .rb, .p7c, .p7b, .p12, .pfx, .pem,
.crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw,
.mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng,
.cdr, .indd, .eps, .pdd, .psd, .dbfv, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .pst,
.accdb, .mdb, .pptm, .ppsx, .pps, .xlk, .xlsb, .xlsm, .wps, .docm, .odb, .odc, .odm,
.odp, .ods, .odt
```

During the encryption process, Stampado will also create two files in the %AppData% folder that have 32 character hexadecimal names. One file will be used to store a list of the encrypted files and the other file will contain status information used by the ransomware.

When the encryption is finished, Stampado will display a lock screen that contains a unique ID that is associated with the victim and an email address that is needed to get payment information. The current emails used by the ransomware are **ransom64@sigaint.com** and **paytodecrypt@sigaint.org**. Victim's are told to email the associated email address for payment instructions and once payment is made, they will receive a key to enter into the lock screen to decrypt the files.

Stampado Lock Screen

On the lock screen there will also be a timer called **Next Russian Roulette file deletion** and **Time until total loss**. When the Russian Roulette countdown reaches 0, a randomly selected encrypted file will be deleted. Each time the Russian Roulette countdown reaches 0, the amount of encrypted files deleted will be doubled. When the Time until total loss timer reaches zero, all of the encrypted data on the computer will be deleted.

As already stated, there is no need to pay a ransom to Stampado as a decryptor has already been made.

Files associated with the Stampado Ransomware:

```
%UserProfile%\AppData\Roaming\[random]
%UserProfile%\AppData\Roaming\[random]
%UserProfile%\AppData\Roaming\scvhost.exe
```

Registry entries associated with the Stampado Ransomware:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Windows Update
%UserProfile%\AppData\Roaming\scvhost.exe
```

IOCs:

```
SHA-256 Hash: 342933cb4cbb31a2c30ac1733afc318a6e5cd0226160a59197686d635ec71b20
SHA-256 Hash: 78db508226ccacd363fc0f02b3ae326a2bdd0baed3ae51ddf59c3fc0fcf60669
```

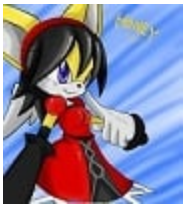
- Decrypted
- Ransomware
- Stampado

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments



BinaryHedgehog - 5 years ago

The behavior of the ransomware author is odd. I think he's keeping an eye on the security community and might patch the program soon.

ScathEnfys - 5 years ago

It's possible, but kits don't typically receive the same attention as a private/restricted sale ransomware.

- 

ScathEnfys - 5 years ago

Out of curiosity, is the flaw that allows decryption similar at all to the flaw in Jigsaw? I'm assuming not due to the requirement of the ID by this decryptor but am still curious :)

- 

Lawrence Abrams - 5 years ago

Jigsaw uses AES as well, but this is a different method used to decrypt it.

- 

Amigo-A - 5 years ago

Grinler, Starting ransom 1 BTC.

- 

  Lawrence Abrams - 5 years ago

  May I ask where you got that info?

- 

  Pakokkie - 5 years ago

  Hi,
  I am trying to decrypt the files from the Stampado ransomware, but i do not have the email and ID from the ransomware pop up page. Please, can somebody help me out?

- 

Lawrence Abrams - 5 years ago

Is the screen not showing? Unfortunately, no way to decrypt without that info.

- 

Motor - 5 years ago

Why you delete my message?

- 

Lawrence Abrams - 5 years ago

You posted the same comment in multiple accounts. I left it in the previous location. If oyu want to post it here, I can remove it from the other article.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: