

## Stampado Ransomware campaign decrypted before it Started

By Lawrence Abrams

Published: 2016-07-22 · Archived: 2026-04-05 12:47:08 UTC

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](#).

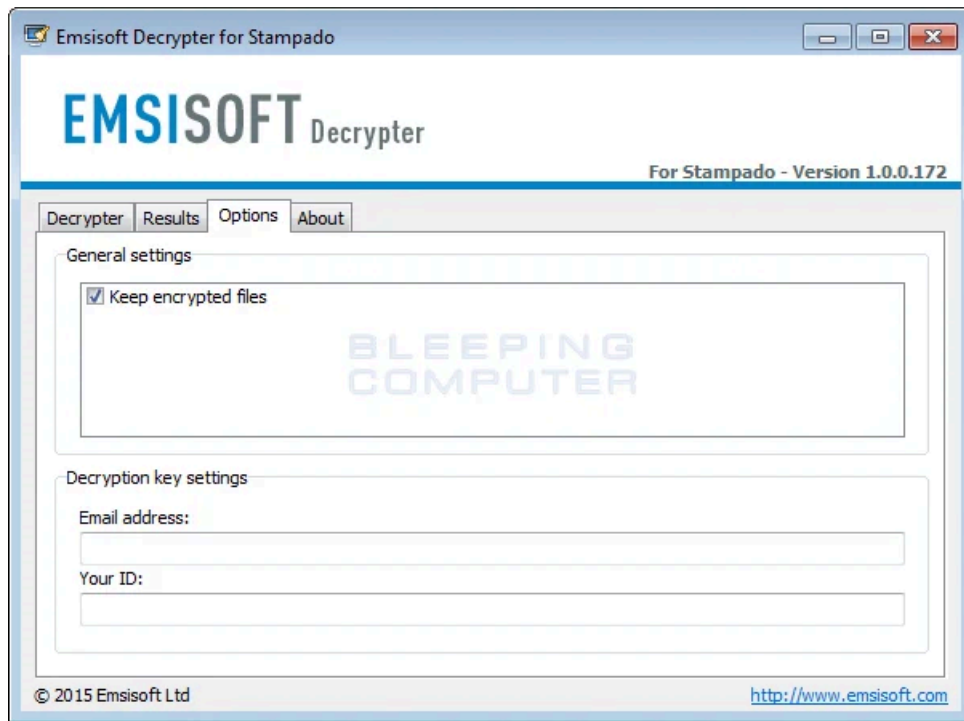


Stampado Lock Screen

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.

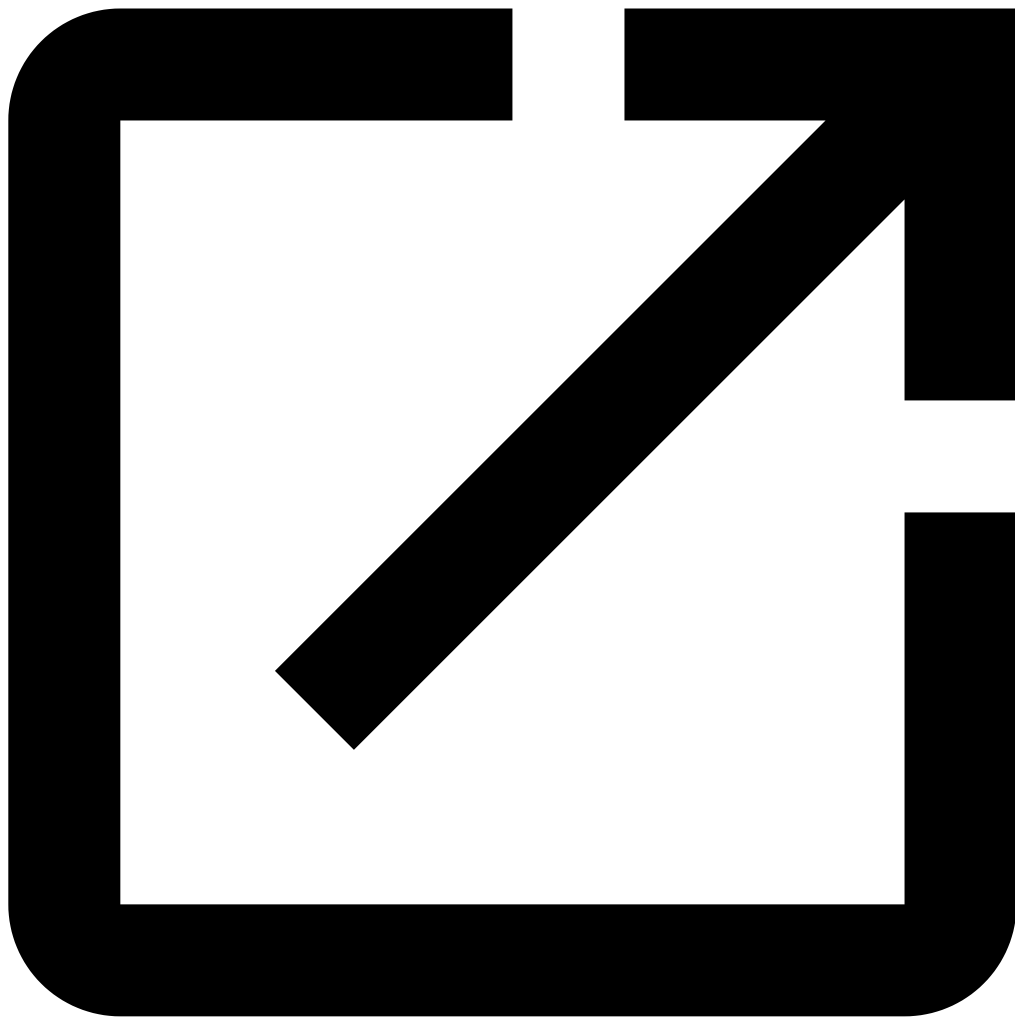
### How to Decrypt files encrypted by Stampado

[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.

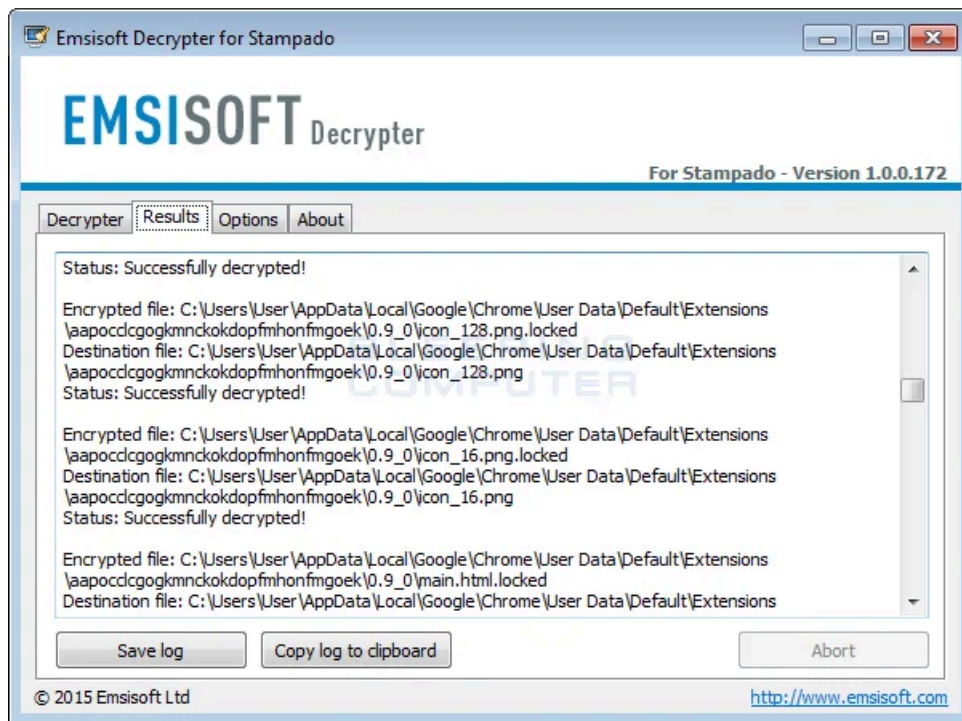


### Decryptor Options

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



Visit Advertiser website [GO TO PAGE](#)



### Decrypting Files

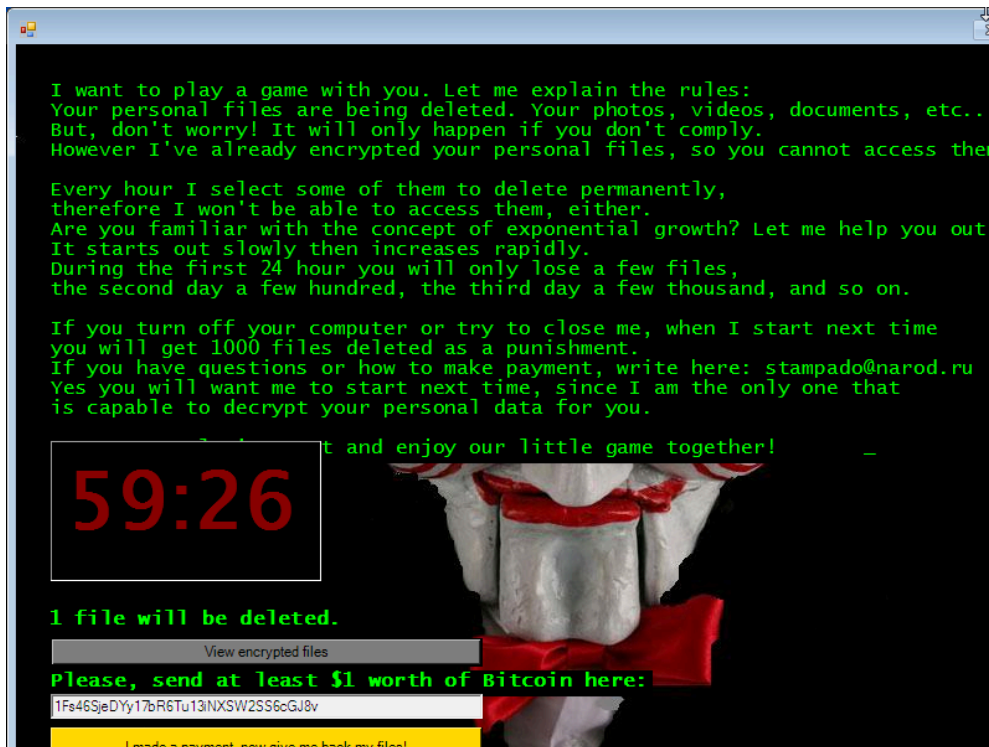
When the decryptor finished decrypting the files, you can close the program.

### 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,
```

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:

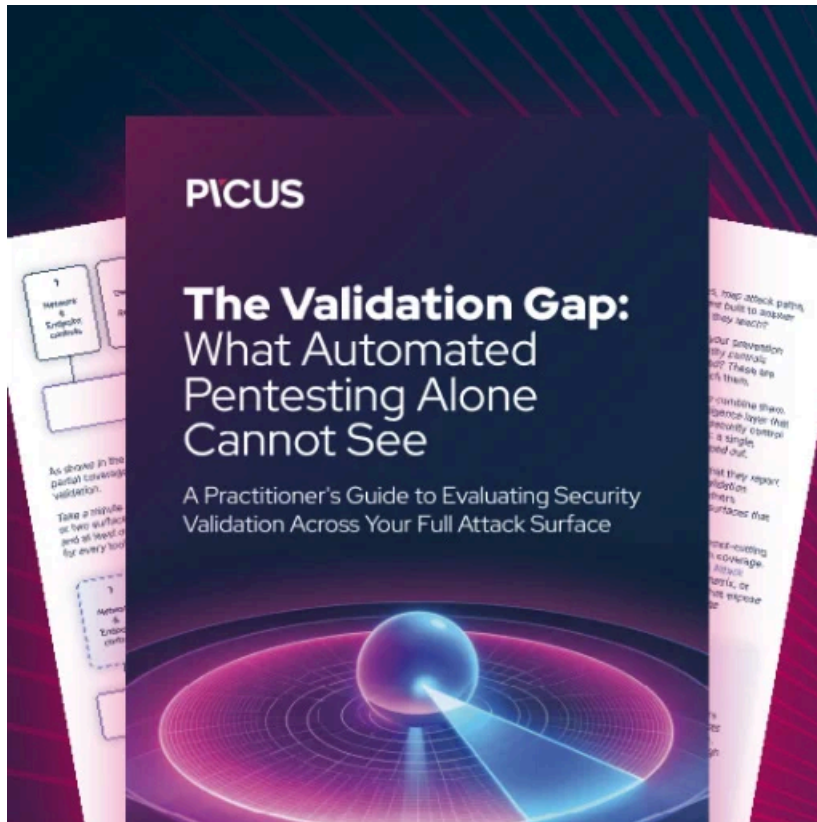
```
%UserProfile%\AppData\Roaming\[random]
%UserProfile%\AppData\Roaming\[random]
%UserProfile%\AppData\Roaming\scvhost.exe
```

### 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
```



### [Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/stampado-ransomware-campaign-decrypted-before-it-started/>