EMSISOFT Blog

Remove Cry128 ransomware with Emsisoft's free decrypter

In Emsisoft Lab by Sarah on May 1, 2017 | English

Today, Emsisoft CTO and Malware researcher Fabian Wosar released a free decrypter for the most recent strain from the CryptON ransomware family, 'Cry128'. Victims can now decrypt files for free!

Variants of the Russian-originated CryptON ransomware, such as X3M and Nemesis, started to appear on the Bleeping Computer forums from December 2016. All of them seem to be put together using the same "builder", a term that describes a software application which automates the process of customizing a malware executable.

The Cry128 strain began to appear on the 22nd April 2017.

How the Cry128 ransomware works

So far, it appears that all variants of the CryptON ransomware (such as Cry9 ransomware) are infecting systems via RDP (remote desktop services) brute force attacks, which allows them to log into the victim's server and execute the ransomware.

Once the criminals have access, the malware will delete the system's recovery points so shadow copies cannot be used to recover the files once encrypted.

Since Cry128 does not contain an extension list, it will encrypt all file types on the machine. It does, however, exclude *C:\Windows*, *C:\Program Files* and the user profile folder from the encryption operation, so that boot operation and other critical processes are not impacted.

Cry128 relies on a modified AES version that works on 128 byte blocks and with 1024 bit keys in ECB mode.

Once the files are locked, the malware will append one of the following extensions that are known to the Emsisoft team at the time of writing:

```
.fgb45ft3pqamyji7.onion.to._
.id_<id>_gebdp3k7bolalnd4.onion._'
.id_<id>_2irbar3mjvbap6gt.onion.to._
.id-<id>_[qg6m5wo7h3id55ym.onion.to].63vc4
```

Based on the team's analysis, all files appear to be 132 bytes larger than the original file once the encryption process is completed.

How Cry128 ransomware victims are supposed to pay

Contrary to the previous versions of this ransomware, Cry128 uses a payment portal hosted on tor and tor2web links to make it more accessible for the average user.

How to decrypt Cry128 encrypted files using the Emsisoft decrypter

As explained in our thorough ransomware removal guide, it's critical to follow the right steps when dealing with and removing ransomware. We suggest to read it before attempting any hasty removal attempts.

For infected users that have verified the ransomware type and are just looking for the decrypter, you can download it for free on Emsisoft's decrypter site.

Have a great (ransomware-free) day!

www.emsisoft.com