EMSISOFT Blog

Decrypt Amnesia ransomware with Emsisoft's free decrypter

In Emsisoft Lab by Sarah on May 6, 2017 | English

Update *(June 1st, 2017): Our Lab team has updated the Amnesia decrypter to support the newer variants. If you had issues previously, head to decrypter.emsisoft.com/amnesia2 and download the latest version (1.0.0.41).*

Today, Emsisoft CTO and Malware researcher Fabian Wosar released a free decrypter for a new Delphi-based ransomware called "Amnesia", which began to appear on 26th April 2017.

How the Amnesia ransomware works

The main infection vector of Amnesia appears to be via RDP (remote desktop services) brute force attacks, which allow the malware author 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. It will also copy itself into the %APPDATA% directory using the file name "guide.exe" and register itself within the "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce" key to start automatically during the next boot.

Since Amnesia ransomware 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 various other folders from the encryption operation, so that boot operation and other critical processes are not impacted.

Amnesia encrypts up to the first 1 MB of files using AES-256 encryption in ECB mode. Once the files are locked this way, the malware will append the ".amnesia" extension to them.

How Amnesia ransomware victims are supposed to pay

Amnesia victims are asked to contact the malware author via email to "s1an1er111@protonmail.com".

How to remove Amnesia ransomware encryption 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:

- Amnesia (1.0.0.33): covers the initial variants prior to June 1st, 2017
- Amnesia2 (*1.0.0.41): covers all the latest variants*

Have a great (ransomware-free) day!

www.emsisoft.com