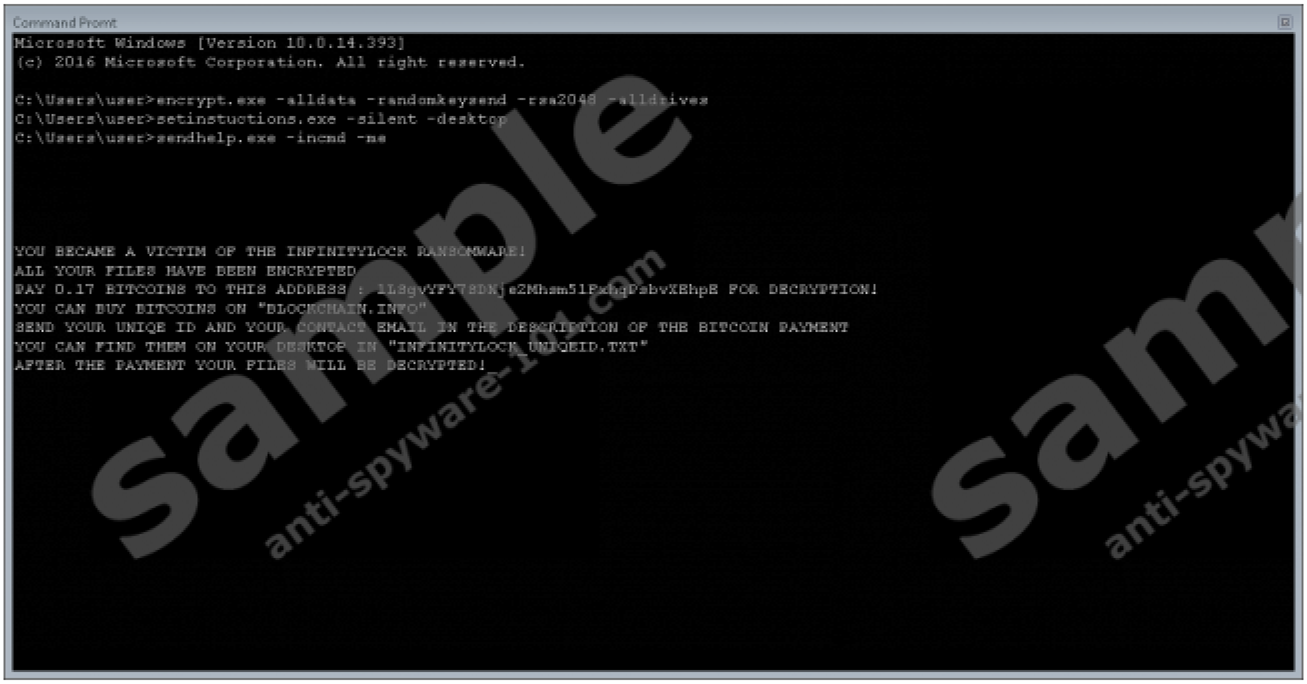
InfinityLock Ransomware

anti-spyware-101.com/remove-infinitylock-ransomware

What is InfinityLock Ransomware?

We want to inform you about a newly found ransomware-type computer malware called **InfinityLock Ransomware**. This program is dangerous because it masquerades as a crack for Adobe Premier, so it can infect your PC secretly and then encrypt many of your files. Its creators want you to pay for a decryption key that is not cheap. However, do not recommend you just to jump right in and pay the ransom because it is possible that the cybercriminals behind this ransomware will not decrypt your files. If you want to find out more about this highly dangerous, we suggest you read this short description.



```
Microsoft Windows [Version 10.0.14.393]
(c) 2016 Microsoft Corporation. All right reserved.

C:\Users\user>encrypt.exe -alldata -randomkeysend -rsa2048 -alldrives
C:\Users\user>setinstuctions.exe -silent -desktop
C:\Users\user>sendhelp.exe -incmd -me



YOU BECAME A VICTIM OF THE INFINITYLOCK RANSOMWARE!
ALL YOUR FILES HAVE BEEN ENCRYPTED
PAY 0.17 BITCOINS TO THIS ADDRESS : 1L8gvYFY78DNje2Mhsm51PxhqPsbvXEhpE FOR DECRYPTION!
YOU CAN BUY BITCOINS ON "BLOCKCHAIN.INFO"
SEND YOUR UNIQE ID AND YOUR CONTACT EMAIL IN THE DESCRIPTION OF THE BITCOIN PAYMENT
YOU CAN FIND THEM ON YOUR DESKTOP IN "INFINITYLOCK UNIQEID.TXT"
AFTER THE PAYMENT YOUR FILES WILL BE DECRYPTED!
```

What does InfinityLock Ransomware do?

As a ransomware-type program, InfinityLock Ransomware is dedicated to encrypting your files which it does with a combination of the RSA an AES encryption methods. As a result, the files are subject to a strong encryption and decrypting them using a third-party tool is unlikely but then again, there is no free decryptor tailored for this particular ransomware.

This ransomware was configured to encrypt files only in predetermined locations, so many of your files can avoid encryption. According to our malware analysts, this ransomware can encrypt files located in the following locations.

- %PUBLIC%
- %USERPROFILE%\Documents

- %USERPROFILE%\Pictures
- %USERPROFILE%\Videos
- %USERPROFILE%\OneDrive
- %USERPROFILE%\Music
- %USERPROFILE%\Downloads
- %USERPROFILE%\Desktop
- %PROGRAMFILES%
- %PROGRAMFILES(X86)%
- %COMMONPROGRAMFILES%
- %COMMONPROGRAMFILES(X86)%

InfinityLock Ransomware encrypts a wide variety of file types that include pictures, videos, audios, documents, databases, file archives, executable files, and so on. It appends all encrypted files with a ".HWID" file extension that acts as a file marker. Basically, the cybercriminals behind this ransomware want to encrypt as many of your files as possible to compel you to pay a 0.17 BTC (Bitcoins) ransom that translates to almost 650 USD.

After it has encrypted your files, InfinityLock Ransomware drops a ransom note named nfinityLock_Recover_Instructions.txt on the desktop. The note says how much you have to pay and how to buy Bitcoins to do that. Furthermore, it drops a text file named InfinityLock_UniqeID.txt that features a unique ID that you can send together with the ransom. However, we urge you to refrain from paying the ransom because there is no telling whether the cybercriminals will pay the ransom.

Where does InfinityLock Ransomware come from?

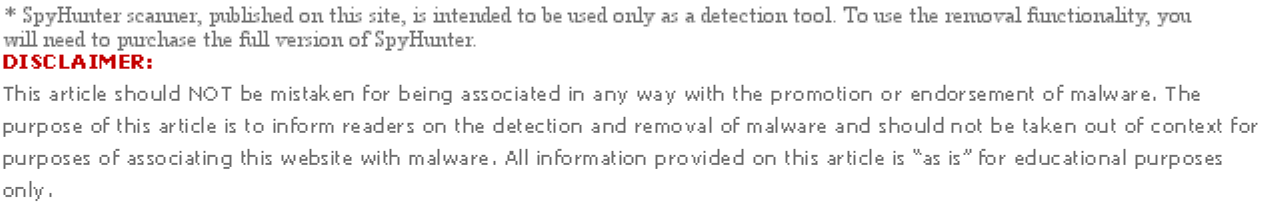
While most ransomware is distributed using email spam and security exploits, InfinityLock Ransomware is different. Our cyber security experts have received information that this new ransomware is distributed disguised as a crack for Adobe Premier. If you launch this file, it will start encrypting your files immediately. This crack is probably featured on some website that distributes cracks. Nevertheless, this crack might also be included along with the software itself and distributed via torrent websites. Unfortunately, no concrete information has surfaced on what websites host this fake crack.

How do I remove InfinityLock Ransomware?

Since there is no guarantee that your files will be decrypted and the fact that your files might not be worth the money, we recommend that you remove InfinityLock Ransomware program from your PC as soon as the opportunity arises. We suggest using our manual removal guide that includes the most likely places this ransomware might reside. Nevertheless, you can also get an antimalware program such as SpyHunter to do the finding and the deleting for you.

Removal Guide

1. Press **Windows+E** keys to open File Explorer.
2. In the address box, enter the following locations and locate the malicious executable.
   - %WINDIR%\Syswow64
   - %WINDIR%\System32
   - %ALLUSERSPROFILE%\Start Menu\Programs\Startup
   - %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup
   - %USERPROFILE%\Microsoft\Windows\Start Menu\Programs\Startup
   - %ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Startup
   - %ALLUSERSPROFILE%\Application Data\Microsoft\Windows\Start Menu\Programs\Startup
   - %USERPROFILE%\Desktop
   - %USERPROFILE%\Downloads
   - %TEMP%
3. **Find** and **right-click** the executable and click **Delete**.
4. Then, go to the desktop and **delete** InfinityLock_UniqeID.txt and InfinityLock_Recover_Instructions.txt
5. **Right-click** the Recycle Bin and click **Empty Recycle Bin**. Download Removal Tool100% FREE spyware scan and tested removal of InfinityLock Ransomware*



* SpyHunter scanner, published on this site, is intended to be used only as a detection tool. To use the removal functionality, you will need to purchase the full version of SpyHunter.

DISCLAIMER:

This article should NOT be mistaken for being associated in any way with the promotion or endorsement of malware. The purpose of this article is to inform readers on the detection and removal of malware and should not be taken out of context for purposes of associating this website with malware. All information provided on this article is "as is" for educational purposes only.

- Terms of Service
- Archive

↑ Top