

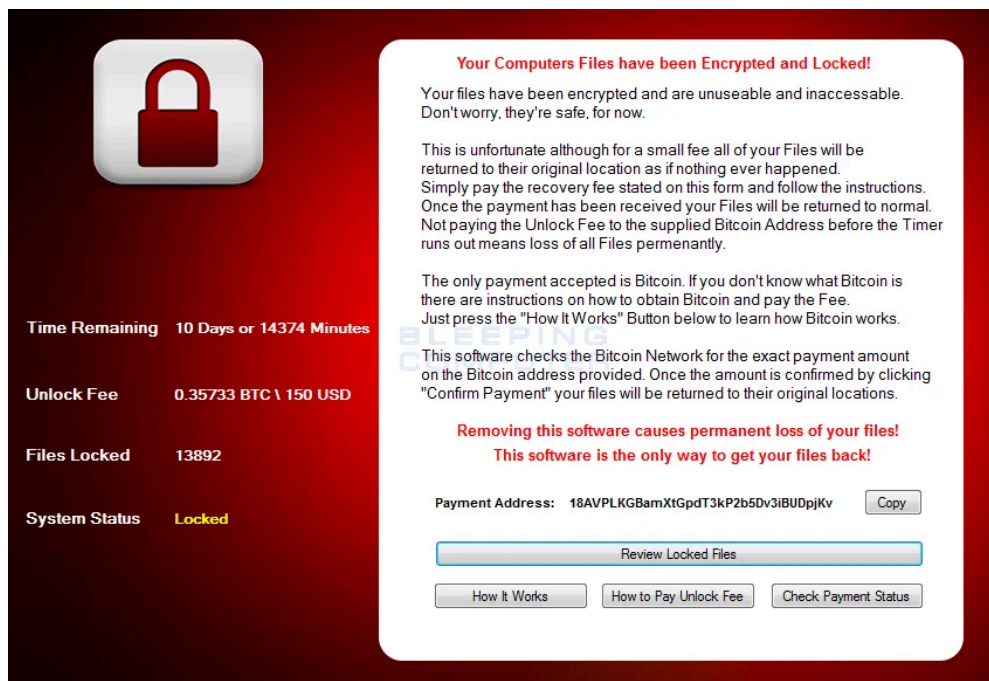
CryptoHost Decrypted: Locks files in a password protected RAR File

By Lawrence Abrams

Published: 2016-04-08 · Archived: 2026-04-05 18:24:01 UTC

A new ransomware called CryptoHost was discovered by security researcher [Jack](#) that states that it encrypts your data and then demands a ransom of .33 bitcoins or approximately 140 USD to get your files back. In reality, though, your data is not encrypted, but rather copied into a password protected RAR archive . Thankfully, the password created by this infection is easily discovered so infected users can get their files back. This infection is currently being detected as Ransom:MSIL/Manamecrypt.A and Ransom_CRYPTOHOST.A.

I would also like to thank [Michael Gillespie](#) and [MalwareHunterTeam](#) for their additional analysis.

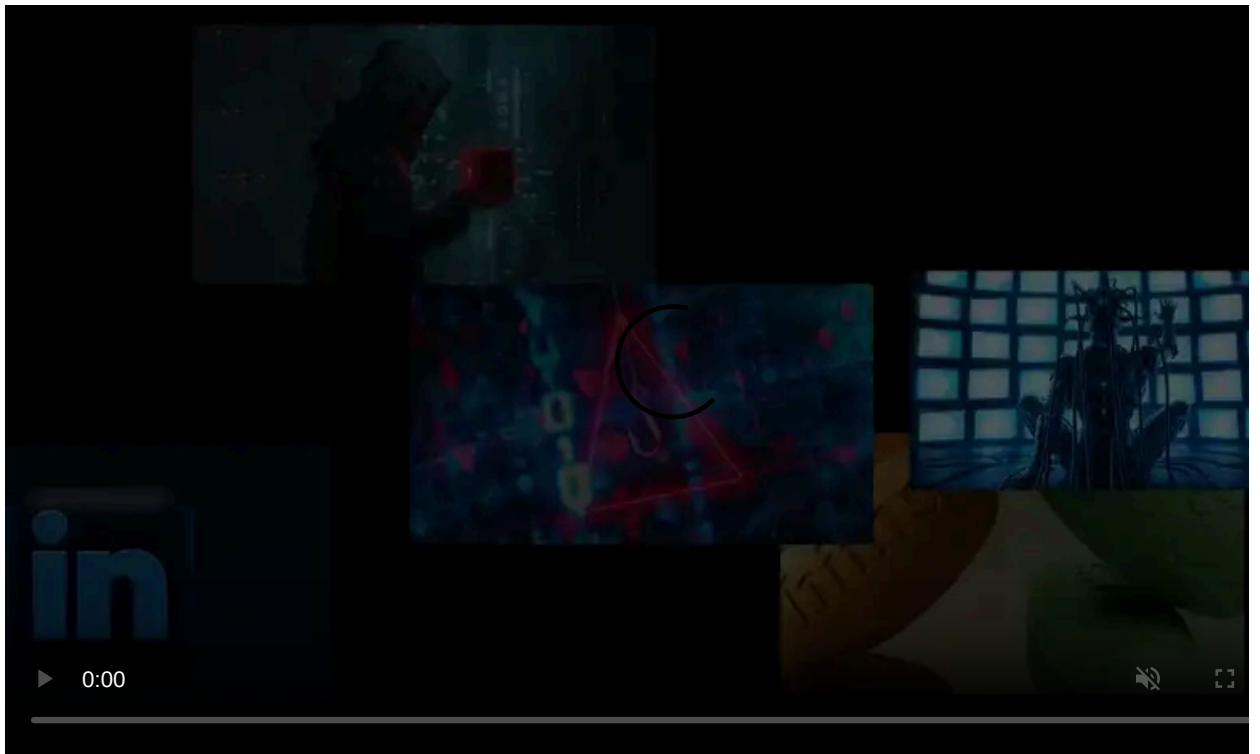


The CryptoHost Ransomware

How to Decrypt or get your data back from the CryptoHost Ransomware

Normally I would not disclose a vulnerability in a ransomware as it will just lead to the developer fixing it in a future version. Unfortunately, a certain site who will not be named, irresponsibly revealed the method that can be used to decrypt these files, so the secret is already out.

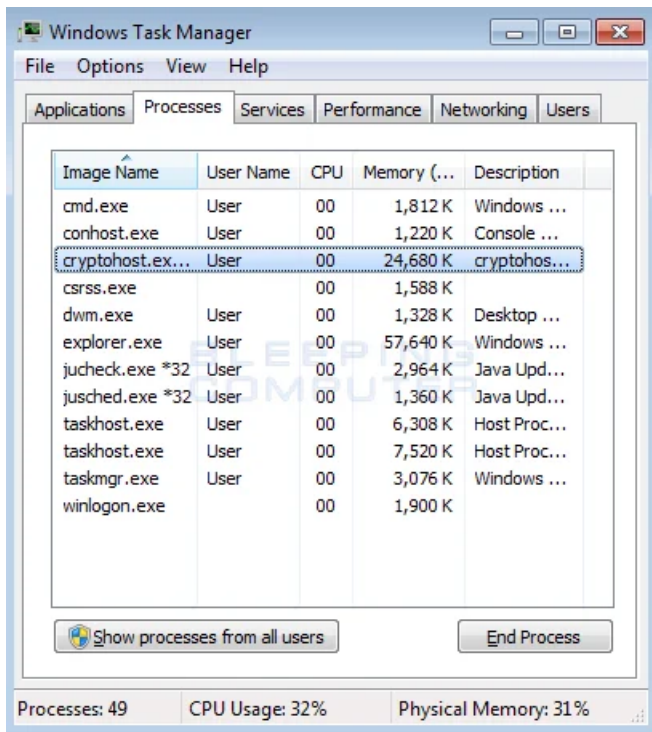
When CryptoHost infects your computer it will move certain data files, which is detailed in the technical analysis below, into a password protected RAR archive located in the C:\Users\[username]\AppData\Roaming folder. This file will have a 41 character name and no extension. An example file is **3854DE6500C05ADAA539579617EA3725BAAE2C57**. The password for this archive is the name of the archive combined with the logged in user name. So for example, if the name of the user is **Test** and the RAR archive is located at **C:\Users\Test\AppData\Roaming\3854DE6500C05ADAA539579617EA3725BAAE2C57**, the password would be **3854DE6500C05ADAA539579617EA3725BAAE2C57Test**.



Visit Advertiser website [GO TO PAGE](#)

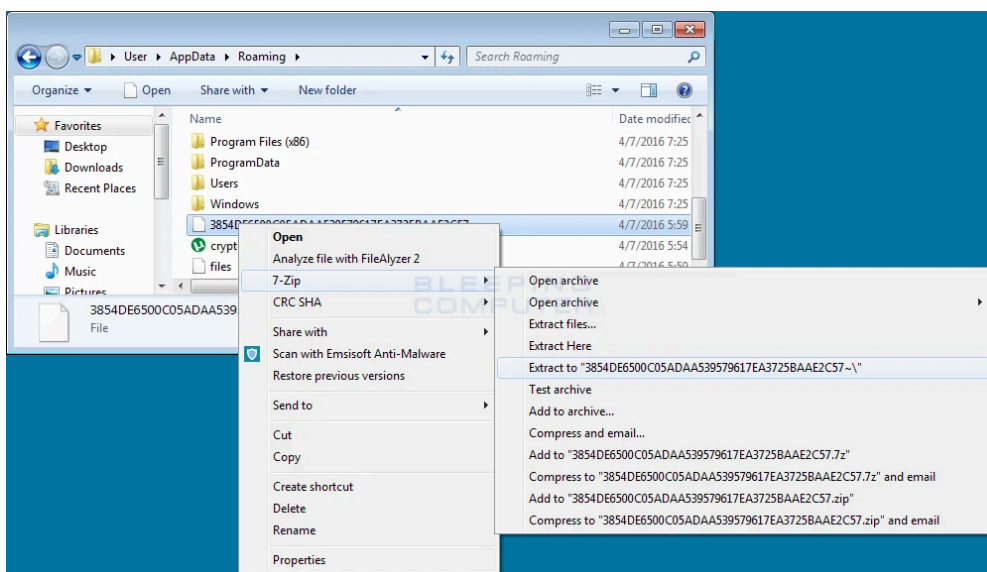
For those who do not want to deal with figuring out the password, you can use [this password generator](#) created by [Michael Gillespie](#).

Before we begin, we want to first terminate the **cryptohost.exe** process. To do this, open the **Start Menu** and type **Task Manager**. When the Task Manager search results appears, click on it to start the program. Now click on the **Processes** tab and select the **cryptohost.exe** process as shown below. Then click on the **End Process** button to terminate it.



End the Cryptohost.exe Process

Now to extract the password protected RAR archive with your files in it, we first need to install the [7-Zip application](#). Once it is installed, open up the **C:\Users\[username]\AppData\Roaming** folder and locate the archive file using the info described above. Now right-click on it and then select the **Extract to "foldername"** option as shown in the image below.



Extraction Wizard

When the 7-Zip prompts you for the password, enter the password as described above and press enter. Your data will now be extracted into a folder name that is the same name as the RAR archive. When done, open that folder and copy all of the folders in it to the root of your C: drive. Your data files should now be restored.

How to remove the CryptoHost Ransomware

When CryptoHost is installed it will create a file called `cryptohost.exe` and store it in the `C:\Users\[username]\AppData\Roaming` folder. It will also create an autorun called **software** that executes the ransomware on login. To remove this infection, simply end the `cryptohost.exe` process using Task Manager and then delete the `cryptohost.exe` file. To remove the autorun you can delete this registry key:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\software %AppData%\cryptohost.exe
```

Most security products should detect this infection at this point and remove it automatically if you do not wish to remove CryptoHost manually.

CryptoHost Ransomware Technical Analysis

CryptoHost is currently being bundled with a uTorrent installer that when installed extracts the **cryptohost.exe** to the `%AppData%` folder and executes it. Once executed, CryptoHost will move all files that match certain extensions into a password protected RAR archive located in the `%AppData%` folder. The name of the archive will be a SHA1 hash of the following information with any dashes removed.

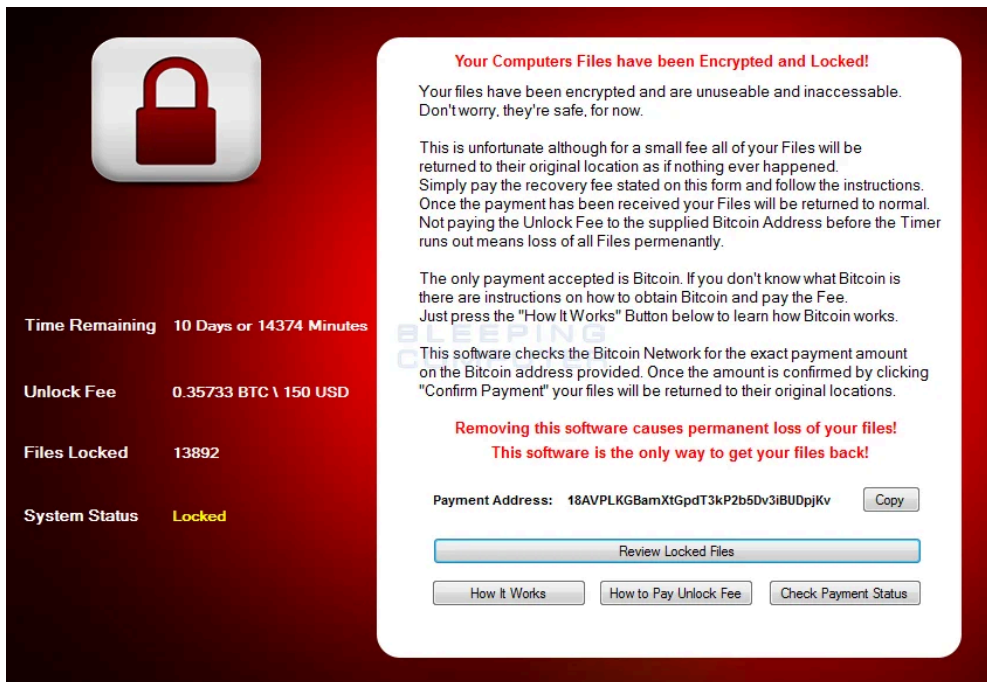
```
processorId + volume_serial_number_of_c: + motherboard_serial_number
```

The password for this archive will be in the form of the **SHA1 hash+username**. So if the SHA1 hash is **3854DE6500C05ADAA539579617EA3725BAAE2C57** and the user is **Test** the password would be **3854DE6500C05ADAA539579617EA3725BAAE2C57Test**.

The file extensions that will be moved into the password protected archive by CryptoHost are:

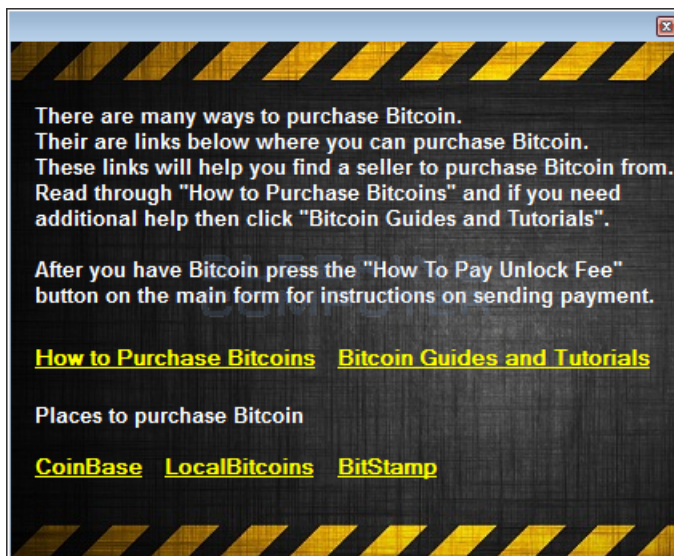
```
.jpg, .jpeg, .png, .gif, .psd, .ppd, .tiff, .flv, .avi, .mov, .qt, .wmv, .rm, .asf, .mp4, .mpg, .mpeg, .m4v, .3gp, .3g2, .pdf, .docx, .pptx, .doc
```

When the archive is finished being created, the ransomware will then perform a listing of the files in the archive and save that list to the `%AppData%\Files` file. CryptoHost will now display the ransomware screen as shown below.

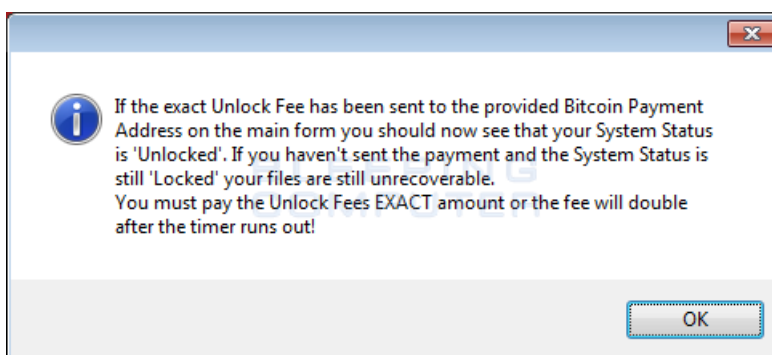


CryptoHost Ransomware Screen

This screen is broken up into four subscreens that allow you to get various information about the infection and to list the affected data files. Below are two of these screens.



How it Works Screen



Check Payment Screen

When a victim wants to decrypt their files, they need to click the Check Payment Status button, which simply checks blockchain.info for any payments to the assigned bitcoin address. If the text returned by the blockchain query contains the **exact** numbers listed in the Fee label of the CryptoHost interface, then the ransomware will extract your files. This means that a victim has to pay the exact amount and if more is paid, the ransomware will still not decrypt the files.

When first started CryptoHost will also try to delete the HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot key in order to make it impossible to boot into safe mode. Thankfully, this process does not run under the required privileges that are necessary to remove this key.

CryptoHost will also monitor process names and Window titles for certain strings. If these strings are detected the associated process will be terminated. In my tests this method only worked on process names and not Window titles. The list of strings that it searches for are:

```
anti virus, anti-virus, antivirus, avg, bitdefender, eset, mcafee, dr.web, f-secure, internet security, obfuscator, debug
```

It is interesting to note that the dev not only targets security products, but also common sites and processes that a victim may want to visit or use for games. This is done to further aggravate the victim into paying the ransom.

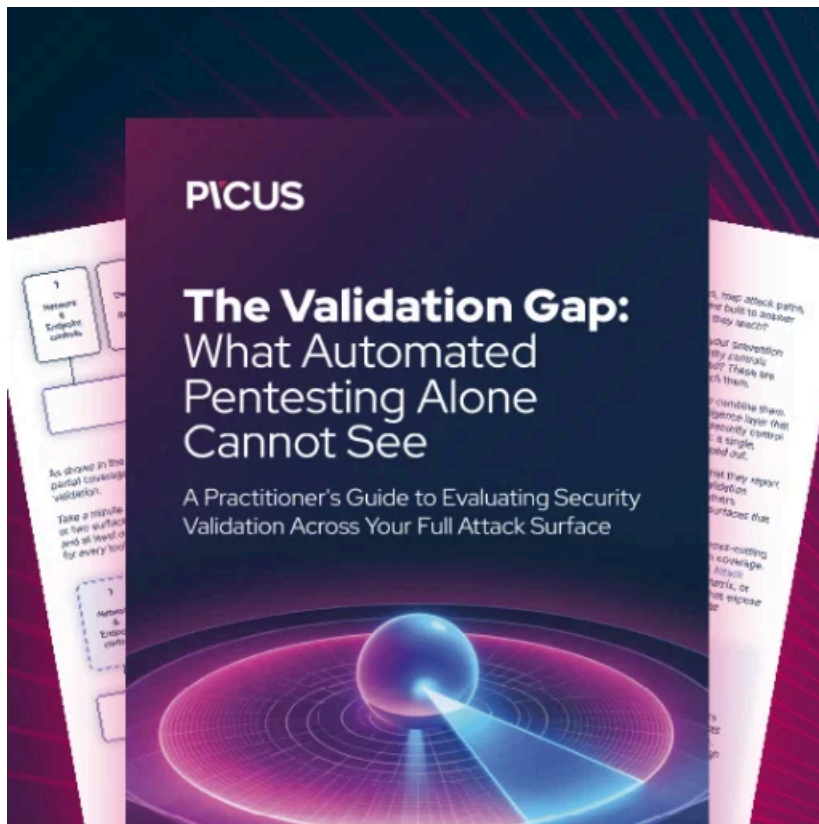
Last, but not least, this ransomware does not communicate with the malware developer in any way and the only network communications is when it checks the blockchain.info site for payment.

Files associated with the CryptoHost Ransomware:

```
%Temp%\uTorrent.exeuTorrent.exe  
%AppData%\crypghost.exe  
%AppData%\files  
%AppData%\processor.exe
```

Registry entries associated with the CryptoHost Ransomware:

```
HKCU\Software\Classes\FalconBetaAccount  
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\software %AppData%\crypghost.exe
```



[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/crypghost-decrypte-locks-files-in-a-password-protected-rar-file/>