# CryptoHost Decrypted: Locks files in a password protected RAR File

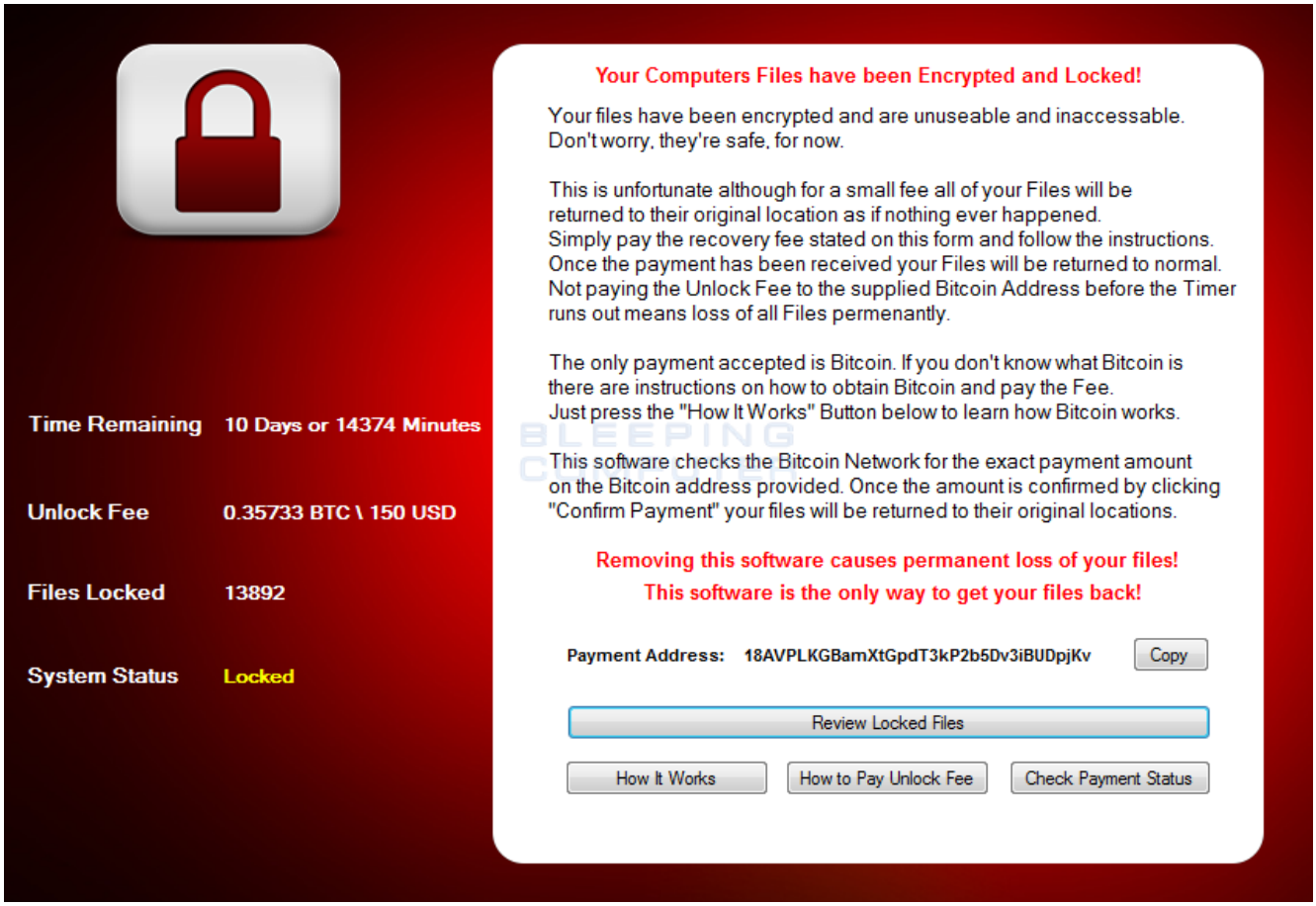
bleepingcomputer.com/news/security/cryptohost-decrypted-locks-files-in-a-password-protected-rar-file

By
Lawrence Abrams

- April 8, 2016
- 01:52 PM
- 13

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**

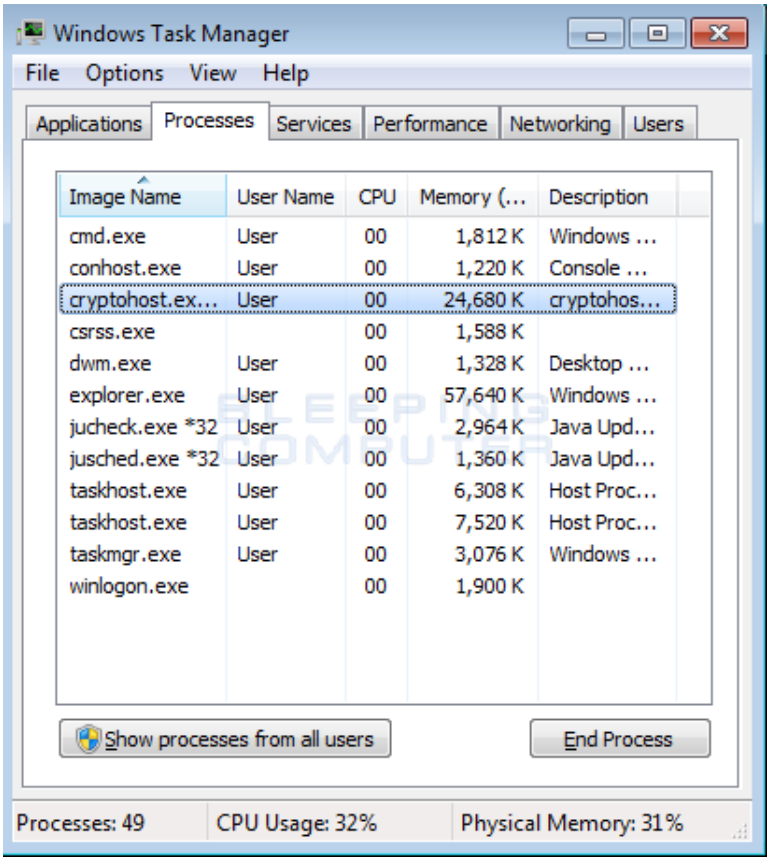
## How to Decrypt or get your data back from the CryptoHost Ransomware

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.**

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

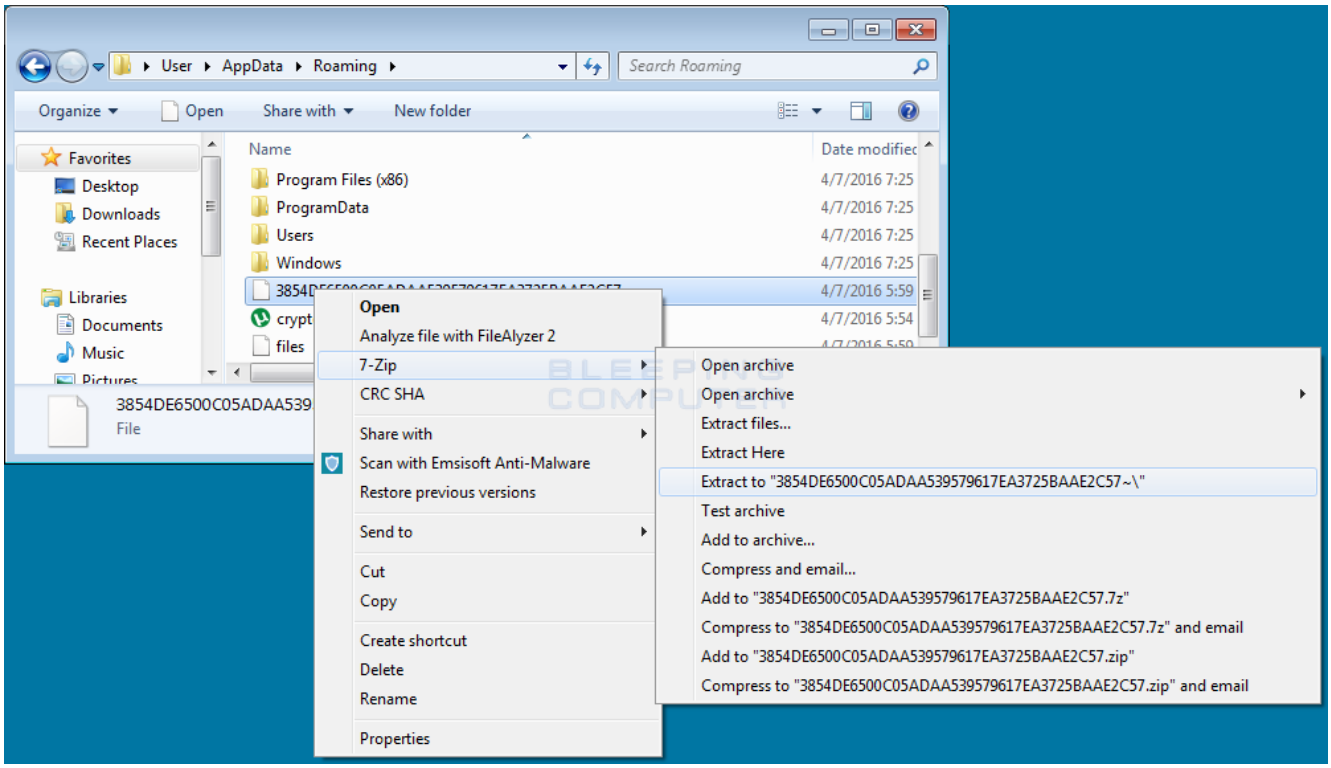
Before we begin, we want to first terminate the **cryptohost.exe** process. To do this, open the **Start Menu** and type **Task Manager**. When the Task Manager search results appears, click on it to start the program. Now click on the **Processes** tab and select the **cryptohost.exe** process as shown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




**End the Cryptohost.exe Process**

Now to 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. You 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 alsocreate 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.

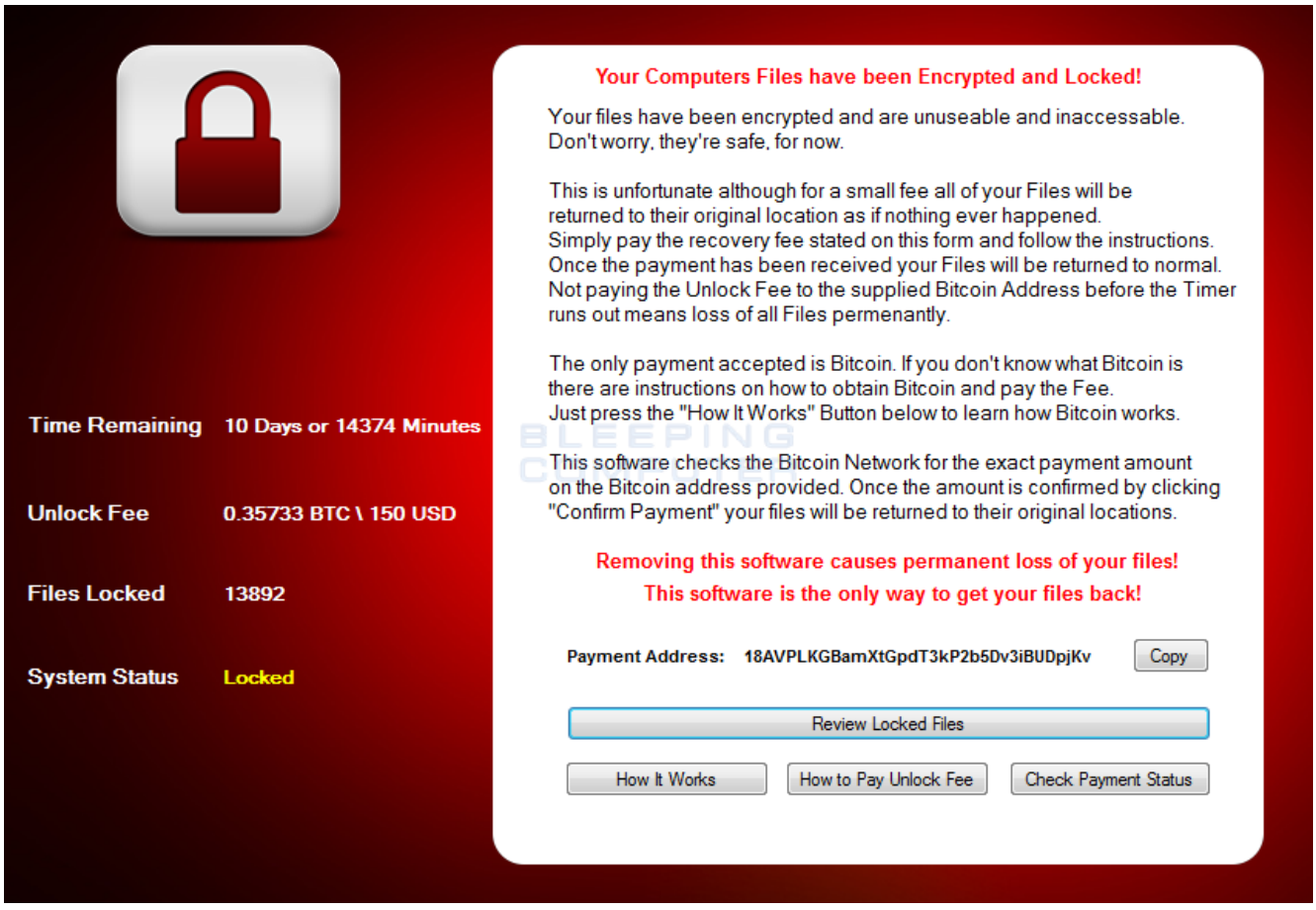
```
processorId + volume_serial_number_of_c: + motherboard_serial_number
```

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:

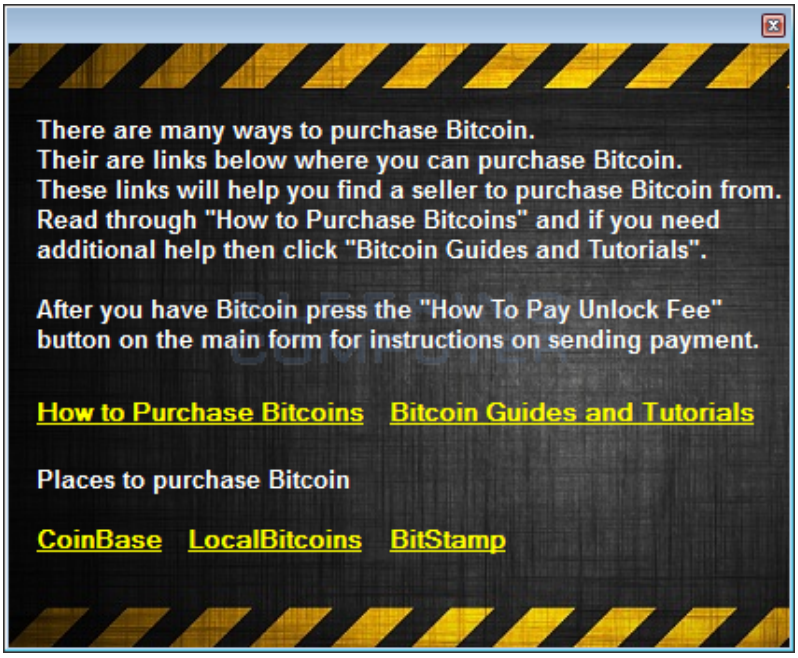
```
jpg, jpeg, png, gif, psd, ppd, tiff, flv, avi, mov, qt, wmv, rm, asf, mp4, mpg, mpeg, m4v,
3gp, 3g2, pdf, docx, pptx, doc, 7z, zip, txt, ppt, pps, wpd, wps, xlr, xls, xlsl
```

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.

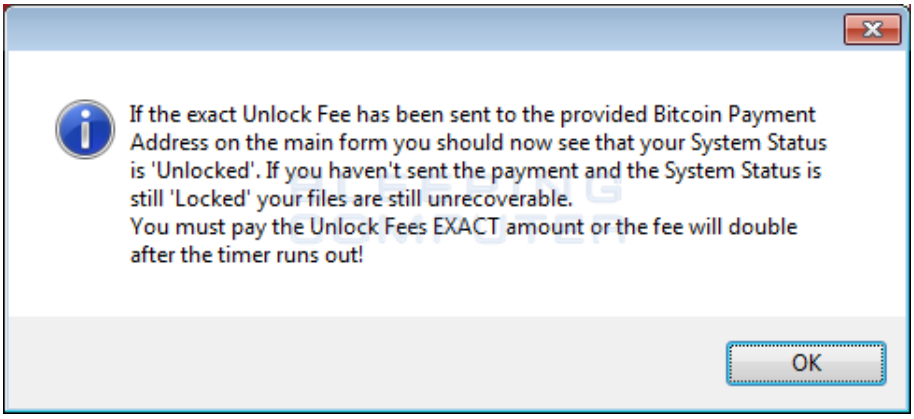



**CryptoHost Ransomware Screen**

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, debugger, monitor, registry, system restore, kaspersky,
norton, ad-aware, sophos, comodo, avira, bullguard, trend micro, eset, vipre, task manager,
system configuration, registry editor, game, steam, lol, rune, facebook, instagram, youtube,
vimeo, twitter, pinterest, tumblr, meetme, netflix, amazon, ebay, shop, origin
```

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%\cryptohost.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%\cryptohost.exe
```

### Related Articles:

Indian airline SpiceJet's flights impacted by ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

The Week in Ransomware - May 20th 2022 - Another one bites the dust

- CryptoHost
- Decrypted
- Manamecrypt
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

### Comments

- 


Demonslay335 - 6 years ago

Also as a note to potential victims, do NOT CLOSE the program by trying to simply "X" it out. It will prompt you if you really wish to lose your data, and if you continue, it will try to delete the entire RAR file. This is why it is recommended to kill it from Task Manager. If this does occur, however, you may be able to use "undelete" software such as Recuva to recover the archive, as it does not do a secure wipe of the file.

- 

Lawrence Abrams - 6 years ago

I left that out as I do not think its active in the build. There is no close button.

- 


Demonslay335 - 6 years ago

Ah, gotcha. I see it now when I double-checked the source. There is indeed a button with the text "Remove This Software and Delete All Locked Files" that triggers the delete. It is not visible and is disabled. Supposed to show with the other buttons I believe.

- 

ScathEnfys - 6 years ago

"CryptoHost is currently being bundled with a uTorrent installer..."
Yet another reason not to use µTorrent or other p2p software

- 

Lawrence Abrams - 6 years ago

Its not a legit utorrent installer from the company themselves.

- 

ScathEnfys - 6 years ago

I understand that. But the people who use p2p programs are also more likely to use alternative download sites.

- 
  ScathEnfys - 6 years ago

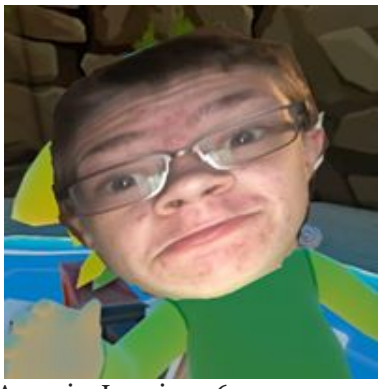
  This RW screams "skiddie" all over... the cheesy password protected RARFile rather than a real encryption method, the easy to find password, and the "meh" graphics.

- Curie - 6 years ago

  Ah, I had hoped to tell you something new, but you got lots of people helping out already. :)

- 
  peterracine - 6 years ago

  These scripts are sold to script kiddies and that is why they sometimes are easily decripted or sometimes do not make any sense. Its the authors that we should somehow go after. we will eventually win so, don't worry.

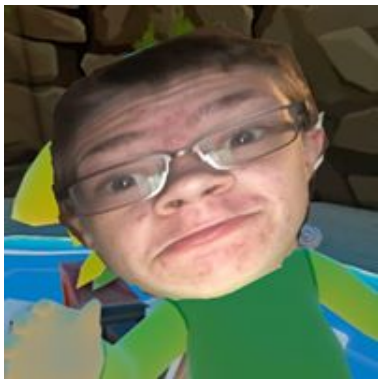
- 
  AaroniusLeonius - 6 years ago

  Script Kiddies. "Oh no! my files have been archived in a RAR file that is protected with an easy to find password. What am I going to do?" Also, why aren't they actually encrypting files? Archiving them isn't encrypting them but the creator clearly doesn't know that.

- 


Demonslay335 - 6 years ago

WinRAR actually technically uses AES encryption on the final compressed stream when you use a password. The password is stored as a protected hash (I think it's SHA1) in the file. If the password is securely generated, it is actually a fairly secure "encryption" since the RAR format implements it properly (WinZIP formats are a bit easier to crack).

- 

AaroniusLeonius - 6 years ago

Wow. I did not know that. You learn new things every day. Thanks.

- 

sometri - 2 years ago

help me how to recover my files with extension ".format". thanks.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

## You may also like: