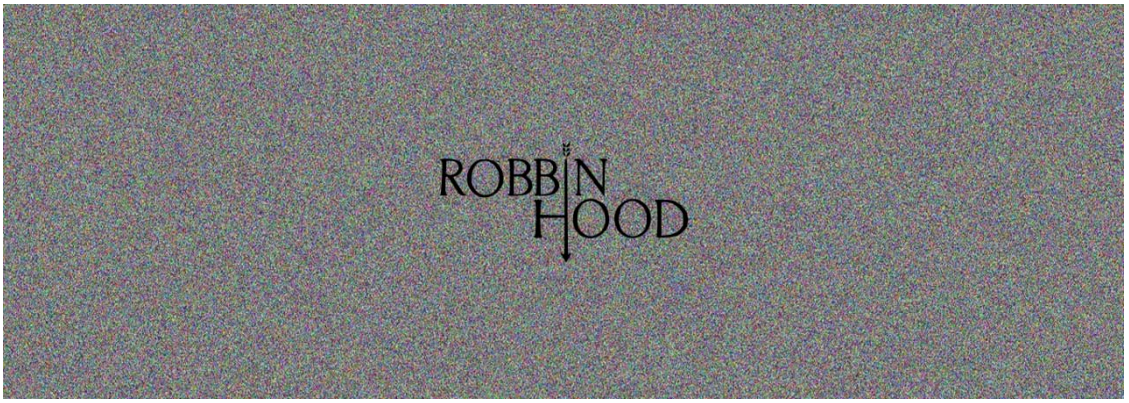
A Closer Look at the RobbinHood Ransomware

By Lawrence Abrams

Published: 2019-04-26 · Archived: 2026-04-05 14:54:28 UTC



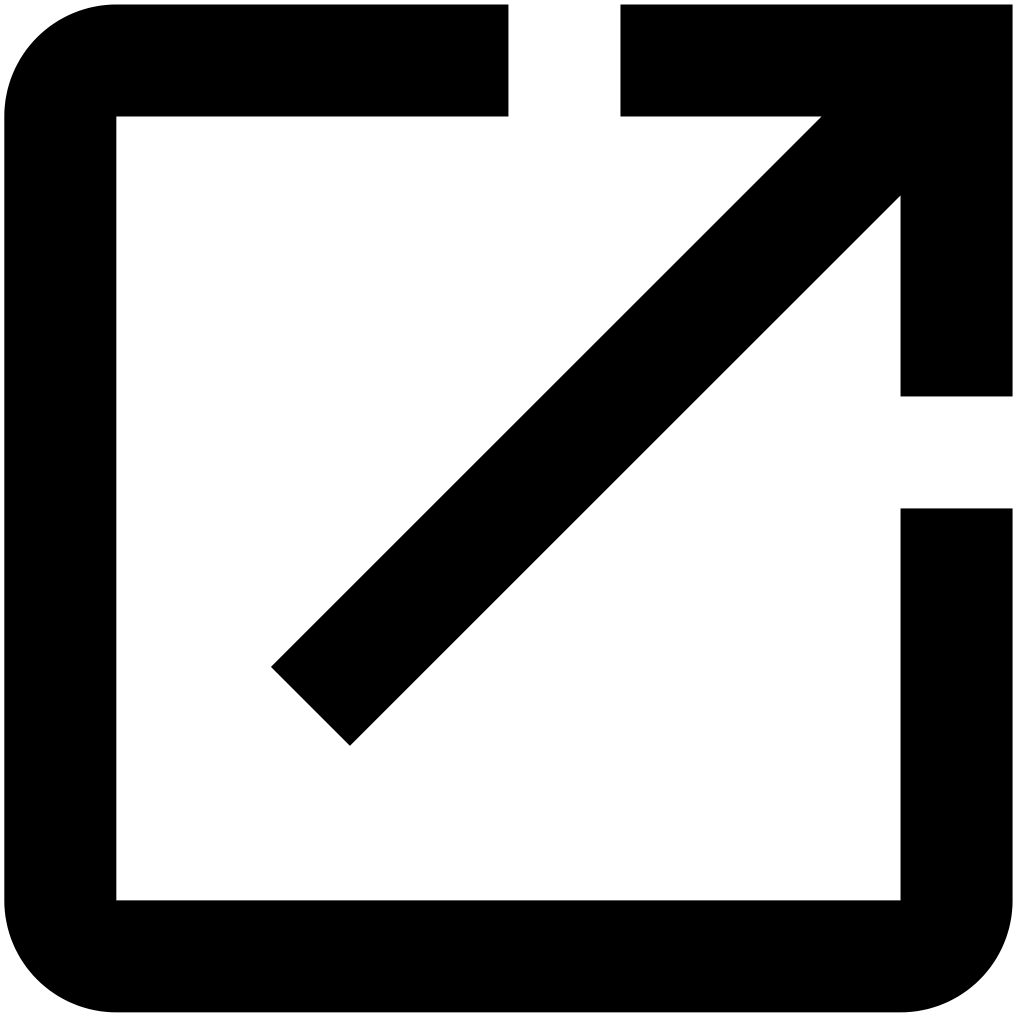
The RobbinHood Ransomware is the latest player in the ransomware scene that is targeting companies and the computers on their network. This ransomware is not being distributed through spam but rather through other methods, which could include hacked remote desktop services or other Trojans that provide access to the attackers.

Since it first came out, samples of the RobbinHood ransomware have not been easy to come by. Yesterday, though, MalwareHunterTeam was able to find a sample so that it could be reverse engineered and tested to learn more about it.

Taking a look at RobbinHood

As we previously stated, it has not been confirmed how the ransomware gains access to a network and the computer's on it.


DIE LINKE.
0:00



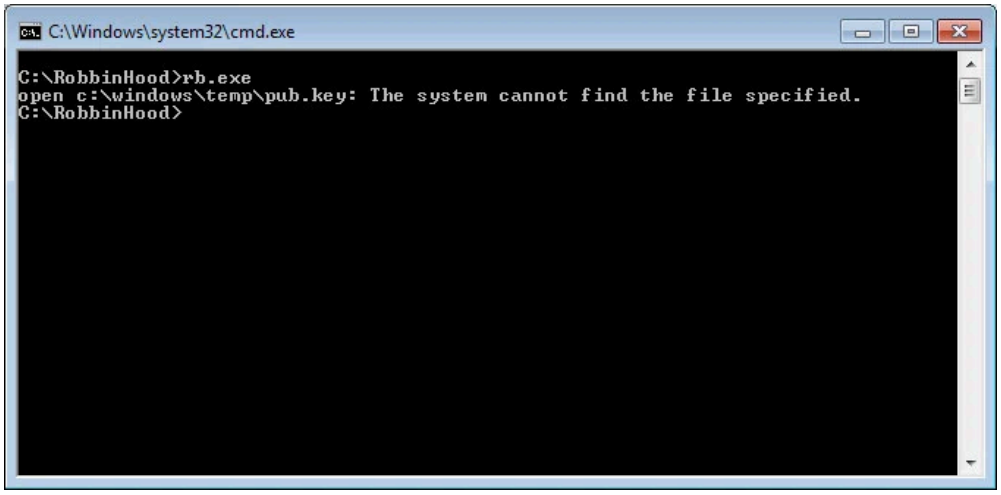
Security researcher Vitali Kremez, who reverse engineered the sample, told BleepingComputer that on execution, RobbinHood disconnects all network shares from the computer using the following command:

```
cmd.exe /c net use * /DELETE /Y
```

This means that each computer is targeted individually and that other computers are not encrypted via connected shares. Kremez told us that this could indicate that the payload is being pushed to each individual machine via a domain controller or through a framework like Empire PowerShell and PSExec.

"One of the most notable ones is "cmd.exe /c net use * /DELETE /Y" since the malware does not encrypt or crawl any shares and actually disconnects from network, which indicates each variant is likely pushed into each machine via the domain controller or some other automated means (maybe via psexec)"

Before continuing, the ransomware will now attempt to read a public RSA encryption key from C:\Windows\Temp\pub.key. If this key is not present, it will display the following message and the ransomware will exit.



Can't find pub.key error

If a key is present, it will continue preparing the victim's computer for encryption. To test the ransomware, BleepingComputer generated a test public key and saved it to C:\Windows\Temp.

Next it will stop 181 Windows services associated with antivirus, database, mail server, and other software that could keep files open and prevent their encryption. It does this by issuing the "sc.exe stop" command as shown below.

```
cmd.exe /c sc.exe stop AVP /y
```

A full list of services stopped by RobbinHood are found at the end of the article.

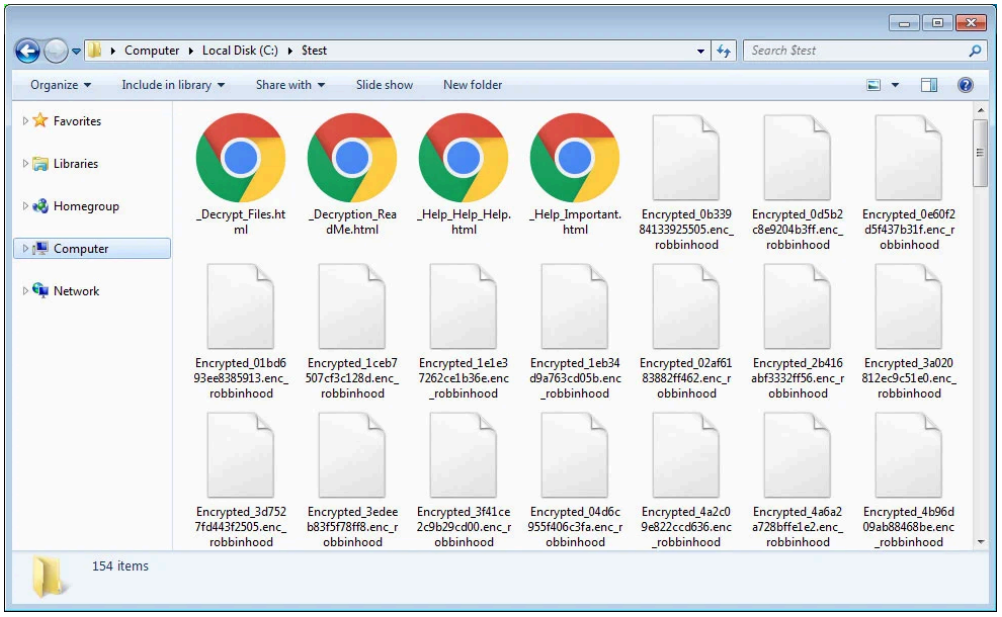
During this preparation stage, RobbinHood will also clear Shadow Volume Copies, clear event logs, and disable the Windows automatic repair by executing the following commands:

```
 vssadmin.exe delete shadows /all /quiet
WMIC shadowcopy delete
wevtutil.exe cl Application
wevtutil.exe cl Security
wevtutil.exe cl System
Bcdedit.exe /set {default} recoveryenabled no
Bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
```

Now that the computer is prepped, it begins to encrypt the victim's targeted files.

Kremez told BleepingComputer that when encrypting files an AES key is created for each file. The ransomware will then encrypt the AES key and the original filename with the public RSA encryption key and append it to the encrypted file.

Each encrypted file will then be renamed using the format **Encrypted_[randomstring].enc_robbinhood** as shown below.



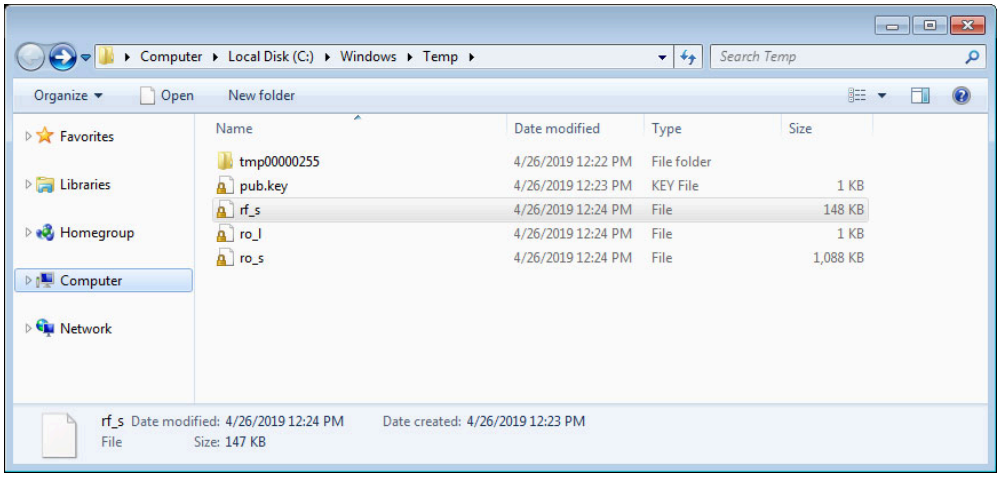
Encrypted RobbinHood Files

When encrypting files, RobbinHood will skip any files found in or under the following directories:

```
 ProgramData
Windows
bootmgr
Boot
$WINDOWS.~BT
Windows.old
Temp
tmp
Program Files
Program Files (x86)
AppData
$Recycle.bin
System Volume Information
```

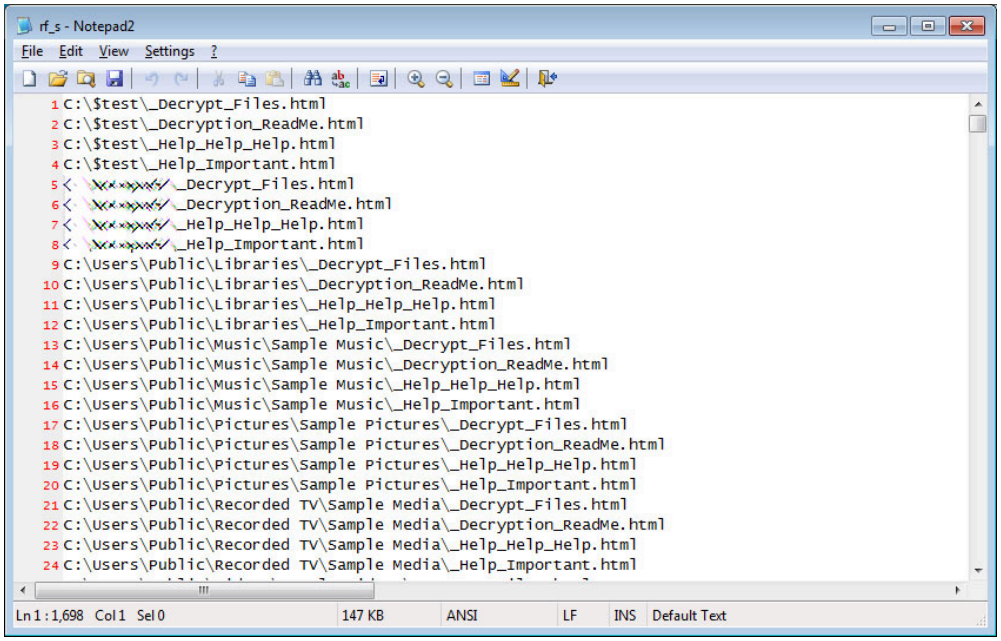
While running, RobbinHood has the ability to send debug output to the console. This feature is currently disabled in distributed versions of the ransomware and does not have a runtime value to enable it.

The ransomware will, though, create numerous log files under the C:\Windows\Temp folder. These files are called **rf_, ro_l**, and **ro_s**.



Log Files

It is not currently known what each log file is for other than the rf_s file, which is used to log the creation of ransom notes in each folder.



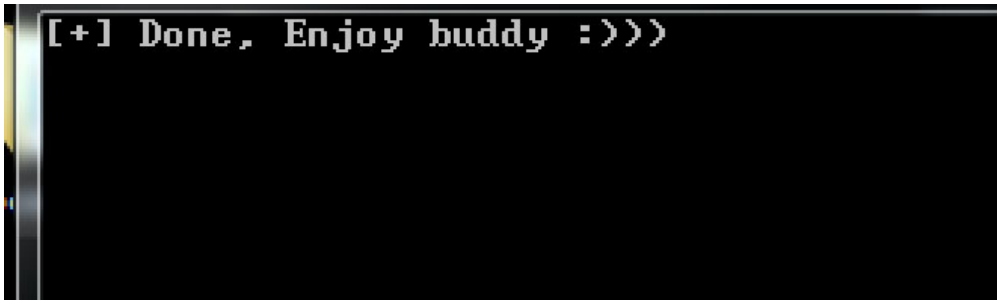
Example logfile for RobbinHood ransom note creation

After encryption has been completed, these log files will be deleted. Below is an example of some of the debug messages that would be displayed during this cleanup stage if console output was enabled.

```
2314869  (~) Try encrypting: C:\Users\___\Downloads\xxxx-2018.1.1.exe
2314870  (-) public key error
2314871  [ERR] Error on filename encryption
2314872  Error: public key error
2314873  File:C:\Users\__\Downloads
2314874  Removed file: C:\windows\temp\rf_s
2314875  Removed file: C:\windows\temp\rf_l
2314876  Removed file: C:\windows\temp\ro_s
2314877  Removed file: C:\windows\temp\ro_l
2314878  [+] Done, Enjoy buddy :)))
```

Cleaning up Logs

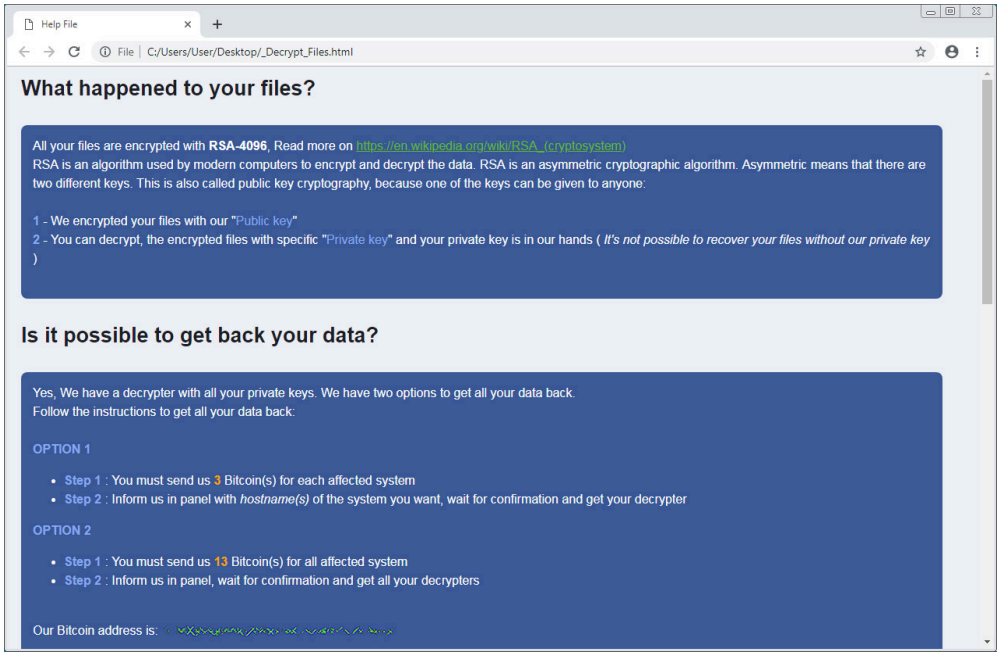
Furthermore, if console output is enabled in the ransomware, when done encrypting a computer it will display a final message stating "Enjoy buddy :)))" as shown below.



Final message when RobbinHood is done encrypting

While encrypting the computer it will also create four different ransom note named **_Decrypt_Files.html**, **_Decryption_ReadMe.html**, **_Help_Help_Help.html**, and **_Help_Important.html.**

These ransom notes contains information as to what has happened to the victims files and a bitcoin address that they can use to make a ransom payment. The ransom payments are currently set at 3 bitcoins per affected system or 13 bitcoins for the entire network.



RobbinHood Ransom Note

Unfortunately, at this time no weakness has been found in the ransomware and there is no way to decrypt files for free.

Protecting yourself from the RobbinHood Ransomware

As ransomware is only damaging if you have no way of recovering your data, the most important thing is to always have a reliable backup of your files. These backups should be stored offline and not made accessible to ransomware, which have been known to target backups in the past.

While this ransomware is not being spread via spam, it is possible that it is being installed by Trojans that are. Therefore, it is important that all users be trained on how to properly identify malicious spam and to not open any attachments without first confirming who and why they were sent.

Finally, it also important to make sure that your network does not make Remote Desktop Services publicly accessible via the Internet. Instead, you should put it behind a firewall and make it only accessible through a VPN.

Update 4/27/19: Added further info about debug logs

IOCs:

Hashes:

```
3bc78141ff3f742c5e942993adfbef39c2127f9682a303b5e786ed7f9a8d184b
```

Associated File Names:

```
 _Decrypt_Files.html
_Decryption_ReadMe.html
_Help_Help_Help.html
_Help_Important.html
C:\Windows\Temp\pub.key
C:\Windows\Temp\rf_s
C:\Windows\Temp\ro_l
C:\Windows\Temp\ro_s
```

List of Stopped Services:

```
 AVP, MMS, ARSM, SNAC, ekrn, KAVFS, RESvc, SamSs, W3Svc, WRSVC, bedbg, masvc, SDRSVC, TmCCSF, mfemms, mfevtp, sacsvr, DCAg
```

Ransom Note Text:

```
 What happened to your files?
All your files are encrypted with RSA-4096, Read more on https://en.wikipedia.org/wiki/RSA_(cryptosystem)
RSA is an algorithm used by modern computers to encrypt and decrypt the data. RSA is an asymmetric cryptographic algorithm

1 - We encrypted your files with our "Public key"
2 - You can decrypt, the encrypted files with specific "Private key" and your private key is in our hands ( It's not possi

Is it possible to get back your data?
Yes, We have a decrypter with all your private keys. We have two options to get all your data back.
Follow the instructions to get all your data back:

OPTION 1
Step 1 : You must send us 3 Bitcoin(s) for each affected system
Step 2 : Inform us in panel with hostname(s) of the system you want, wait for confirmation and get your decrypter
OPTION 2
Step 1 : You must send us 13 Bitcoin(s) for all affected system
Step 2 : Inform us in panel, wait for confirmation and get all your decrypters

Our Bitcoin address is: xxx

BE CAREFUL, THE COST OF YOUR PAYMENT INCREASES $10,000 EACH DAY AFTER THE FOURTH DAY

Access to the panel ( Contact us )
The panel address: http://xbt4titax4pzza6w.onion/xx/

Alternative addresses
https://xbt4titax4pzza6w.onion.pet/xx/
https://xbt4titax4pzza6w.onion.to/xx/
Access to the panel using Tor Browser
If non of our links are accessible you can try tor browser to get in touch with us:
Step 1: Download Tor Browser from here: https://www.torproject.org/download/download.html.en
Step 2: Run Tor Browser and wait to connect
Step 3: Visit our website at: panel address
```

```
If you're having a problem with using Tor Browser, Ask Google: how to use tor browser
Wants to make sure we have your decrypter?
To make sure we have your decrypter you can upload at most 3 files (maximum size allowance is 10 MB in total) and get your
Where to buy Bitcoin?
The easiest way is LocalBitcoins, but you can find more websites to buy bitcoin using Google Search: buy bitcoin online
```

Interesting Strings:

```
 C:/Users/valery/go/src/oldboy/config.go
C:/Users/valery/go/src/oldboy/functions.go
C:/Users/valery/go/src/oldboy/main.go
```

Source: https://www.bleepingcomputer.com/news/security/a-closer-look-at-the-robbinhood-ransomware/