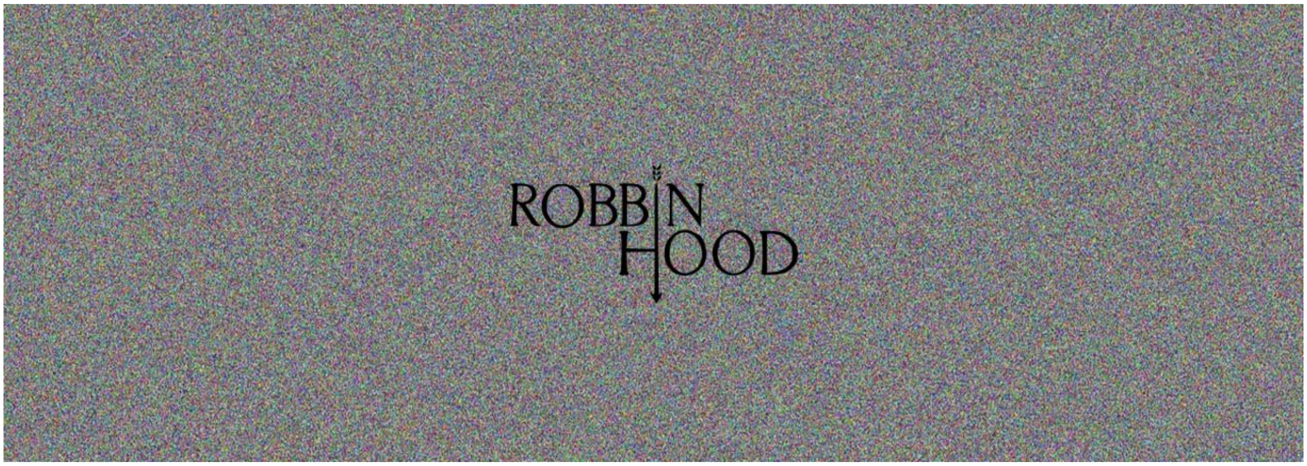
A Closer Look at the RobbinHood Ransomware

bleepingcomputer.com/news/security/a-closer-look-at-the-robbinhood-ransomware/

Lawrence Abrams

By
Lawrence Abrams

- April 26, 2019
- 01:45 PM
- 5



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.

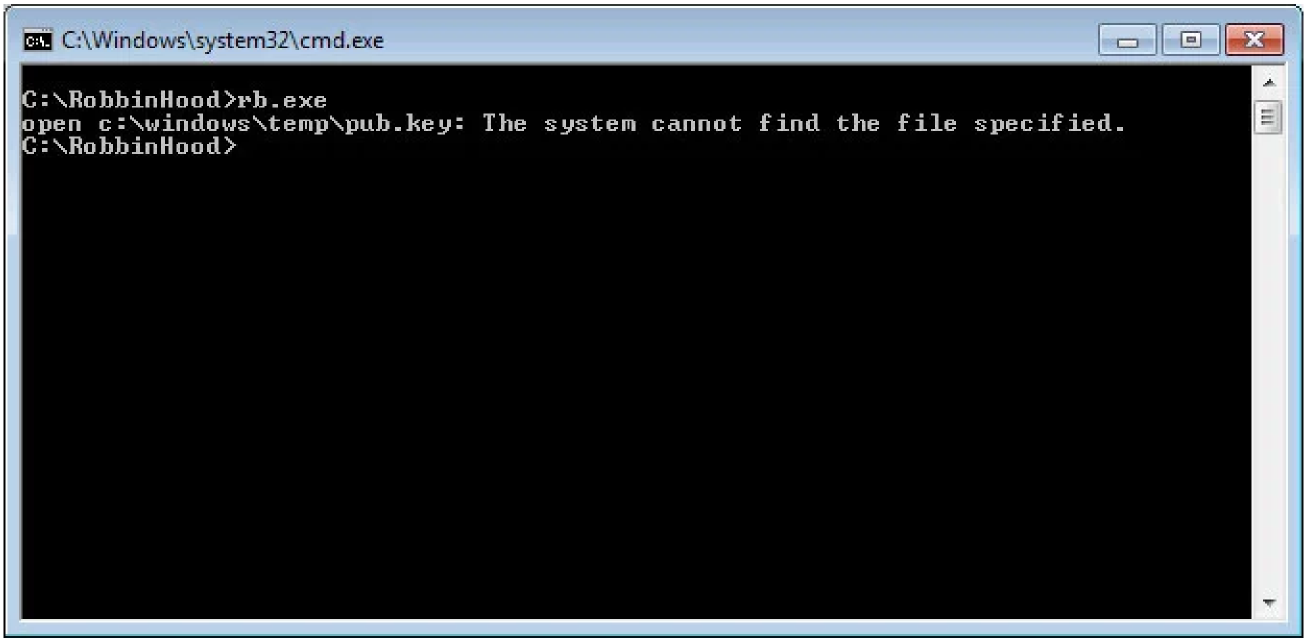
Security researcher Vitali Kremez, who reverse engineered the sample, told BleepingComputer that on execution, RobbinHood disconnects all network shares from the computer using the following command:

```
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.



```
C:\RobbinHood>rb.exe
open c:\windows\temp\pub.key: The system cannot find the file specified.
C:\RobbinHood>
```

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.

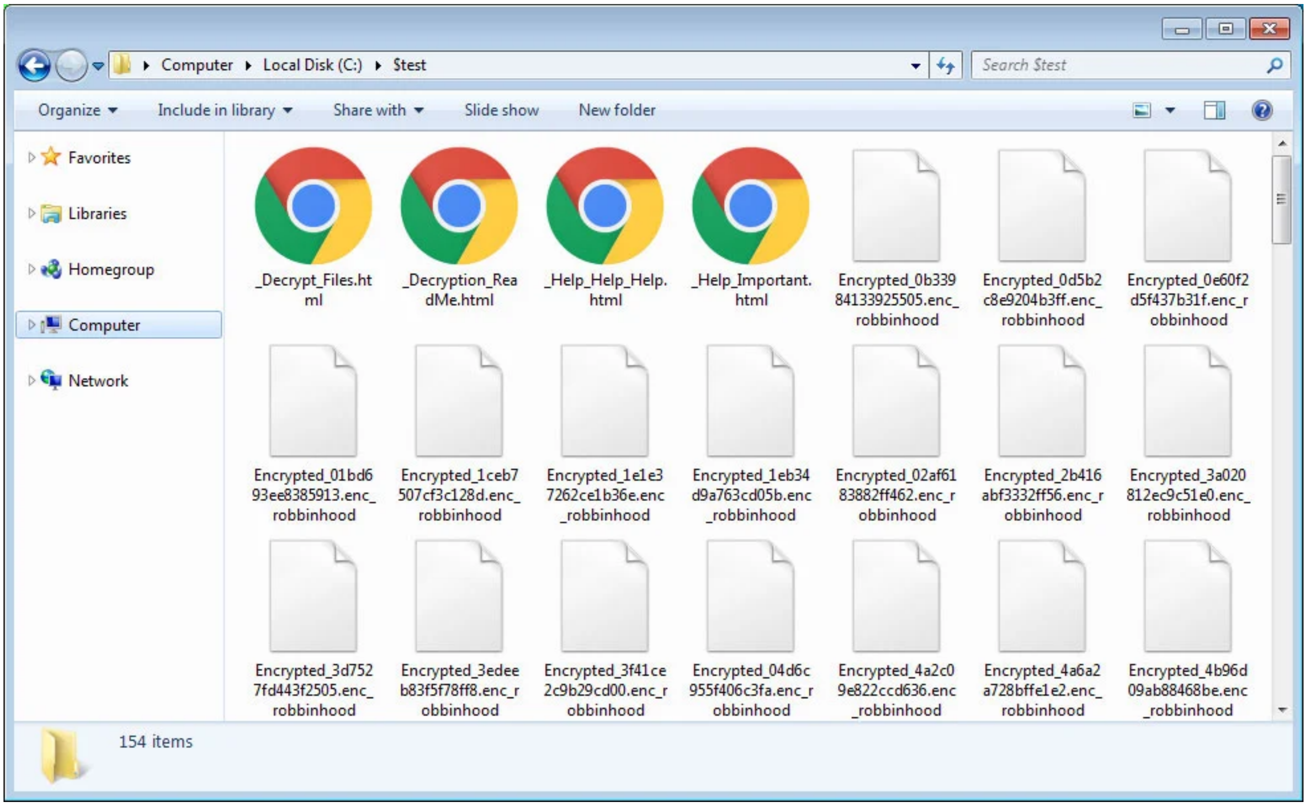
During this preparation stage, RobbinHood will also clear Shadow Volume Copies, clear event logs, and disable the Windows automatic repair by executing the following commands:

```
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.


Computer ▸ Local Disk (C:) ▸ $test
Search $test
Organize
Include in library
Share with
Slide show
New folder
Favorites
Libraries
Homegroup
Computer
Network
_Decrypt_Files.html
_Decryption_ReadMe.html
_Help_Help_Help.html
_Help_Important.html
Encrypted_0b33984133925505.enc_robbinhood
Encrypted_0d5b2c8e9204b3ff.enc_robbinhood
Encrypted_0e60f2d5f437b31f.enc_robbinhood
Encrypted_01bd693ee8385913.enc_robbinhood
Encrypted_1ceb7507cf3c128d.enc_robbinhood
Encrypted_1e1e37262ce1b36e.enc_robbinhood
Encrypted_1eb34d9a763cd05b.enc_robbinhood
Encrypted_02af6183882ff462.enc_robbinhood
Encrypted_2b416abf3332ff56.enc_robbinhood
Encrypted_3a020812ec9c51e0.enc_robbinhood
Encrypted_3d7527fd443f2505.enc_robbinhood
Encrypted_3edeeb83f5f78ff8.enc_robbinhood
Encrypted_3f41ce2c9b29cd00.enc_robbinhood
Encrypted_04d6c955f406c3fa.enc_robbinhood
Encrypted_4a2c09e822ccd636.enc_robbinhood
Encrypted_4a6a2a728bffe1e2.enc_robbinhood
Encrypted_4b96d09ab88468be.enc_robbinhood
154 items

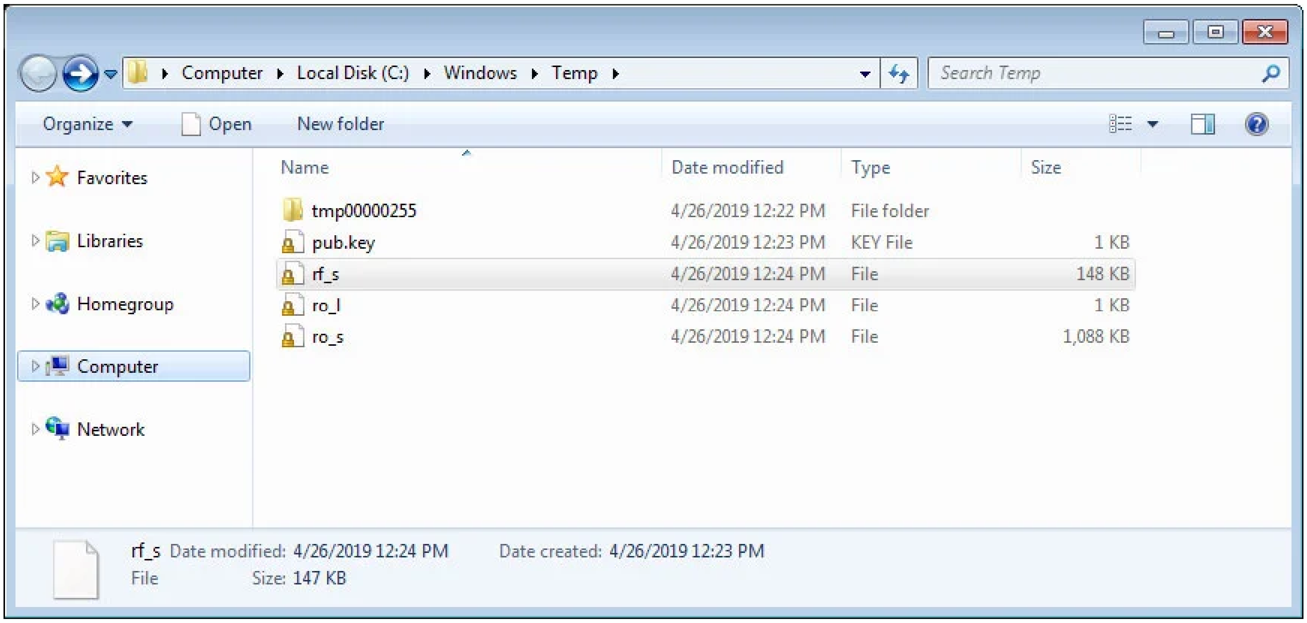
Encrypted RobbinHood Files

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**.

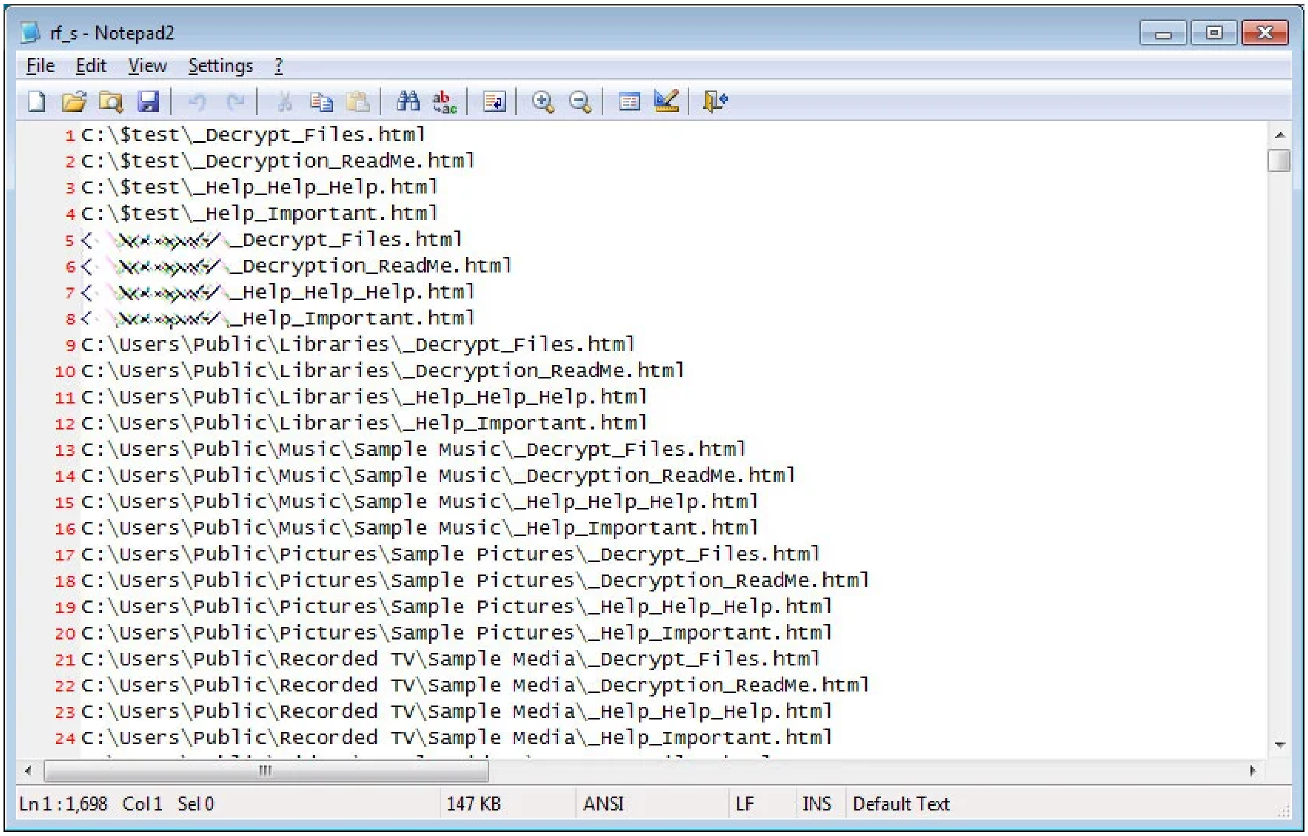


Name	Date modified	Type	Size
tmp00000255	4/26/2019 12:22 PM	File folder	
pub.key	4/26/2019 12:23 PM	KEY File	1 KB
rf_s	4/26/2019 12:24 PM	File	148 KB
ro_l	4/26/2019 12:24 PM	File	1 KB
ro_s	4/26/2019 12:24 PM	File	1,088 KB

rf_s Date modified: 4/26/2019 12:24 PM Date created: 4/26/2019 12:23 PM
File Size: 147 KB

Log Files

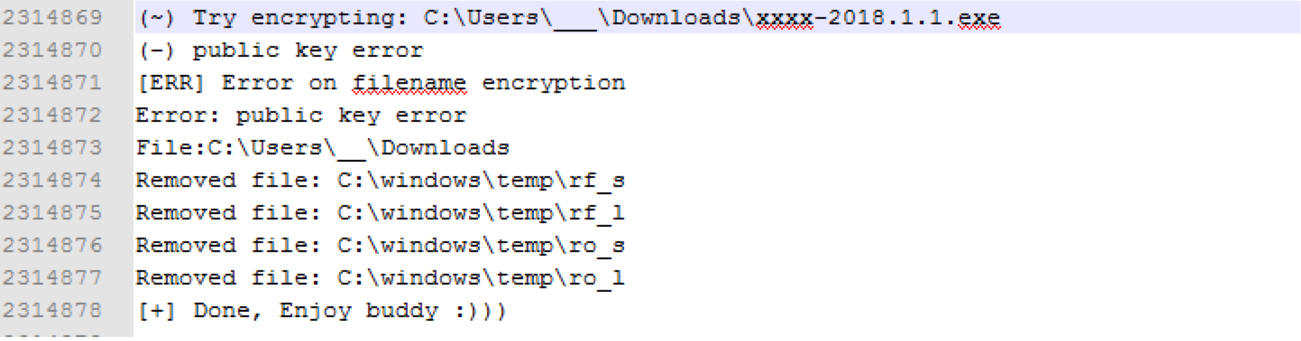
It is not currently known what each log file is for other than the rf_s file, which is used to log the creation of ransom notes in each folder.



```
C:\$test\_Decrypt_Files.html
C:\$test\_Decryption_ReadMe.html
C:\$test\_Help_Help_Help.html
C:\$test\_Help_Important.html
[redacted]_Decrypt_Files.html
[redacted]_Decryption_ReadMe.html
[redacted]_Help_Help_Help.html
[redacted]_Help_Important.html
C:\Users\Public\Libraries\_Decrypt_Files.html
C:\Users\Public\Libraries\_Decryption_ReadMe.html
C:\Users\Public\Libraries\_Help_Help_Help.html
C:\Users\Public\Libraries\_Help_Important.html
C:\Users\Public\Music\Sample Music\_Decrypt_Files.html
C:\Users\Public\Music\Sample Music\_Decryption_ReadMe.html
C:\Users\Public\Music\Sample Music\_Help_Help_Help.html
C:\Users\Public\Music\Sample Music\_Help_Important.html
C:\Users\Public\Pictures\Sample Pictures\_Decrypt_Files.html
C:\Users\Public\Pictures\Sample Pictures\_Decryption_ReadMe.html
C:\Users\Public\Pictures\Sample Pictures\_Help_Help_Help.html
C:\Users\Public\Pictures\Sample Pictures\_Help_Important.html
C:\Users\Public\Recorded TV\Sample Media\_Decrypt_Files.html
C:\Users\Public\Recorded TV\Sample Media\_Decryption_ReadMe.html
C:\Users\Public\Recorded TV\Sample Media\_Help_Help_Help.html
C:\Users\Public\Recorded TV\Sample Media\_Help_Important.html
```

Example logfile for RobbinHood ransom note creation

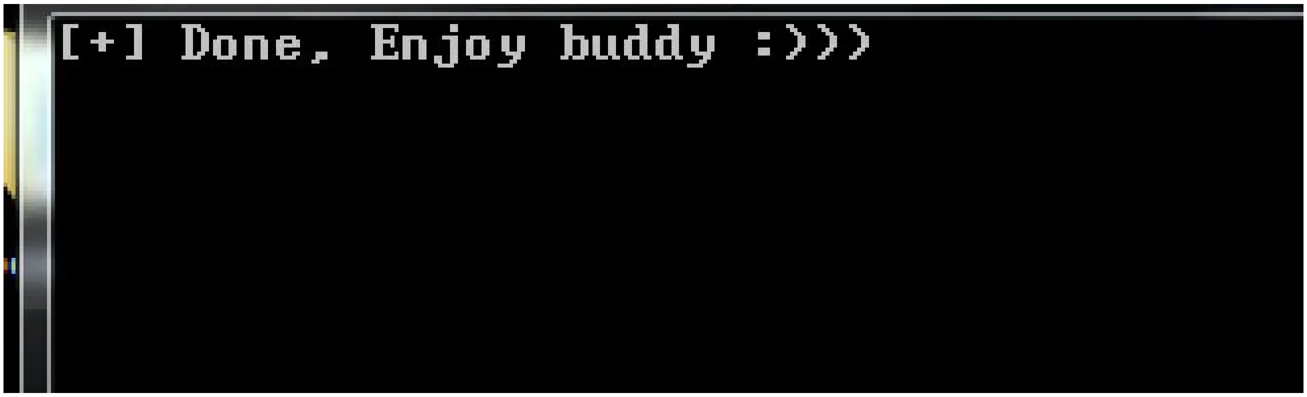
After encryption has been completed, these log files will be deleted. Below is an example of some of the debug messages that would be displayed during this cleanup stage if console output was enabled.



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

Cleaning up Logs

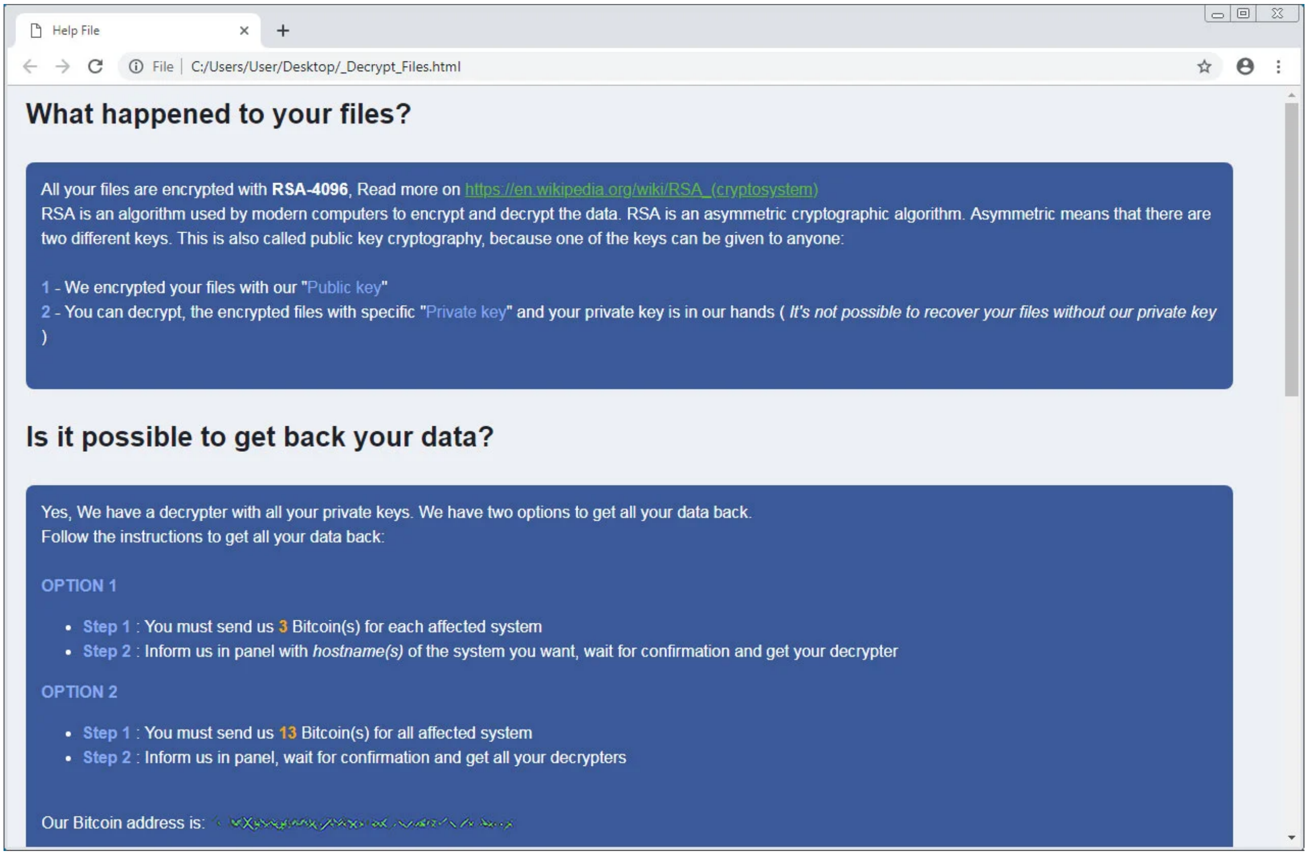
Furthermore, if console output is enabled in the ransomware, when done encrypting a computer it will display a final message stating "Enjoy buddy :)))" as shown below.



```
[+] Done, Enjoy buddy :)))
```

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.



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. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone:

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 possible to recover your files without our private key*)

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: [redacted]

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, DCAgent, ESHASRV, KAVFSGT, MySQL80, POP3Svc,
SMTPSvc, Smcinst, SstpSvc, TrueKey, mfefire, EhttpSrv, IISAdmin, IMAP4Svc, McShield,
MySQL57, kavfsslp, klnagent, macmnsvc, ntrtscan, tmlisten, wbengine, Antivirus,
MSSQL$TPS, SQLWriter, ShMonitor, UI0Detect, sophossps, MSOLAP$TPS, MSSQL$PROD,
SAVService, SQLBrowser, SmcService, swi_filter, swi_update, AcrSch2Svc, EsgShKernel,
MBAMService, MSSQLSERVER, MsDtsServer, SntpService, VeeamNFSSvc, swi_service,
AcronisAgent, FA_Scheduler, MSExchangeES, MSExchangeIS, MSExchangeSA, MSSQL$ECWDB2,
MSSQL$SOPHOS, MSSQL$TPSAMA, PDVFSService, ReportServer, SQLAgent$TPS, SQLTELEMETRY,
VeeamRESTSvc, MSExchangeMTA, MSExchangeSRS, MSOLAP$TPSAMA, McTaskManager,
SQLAgent$CXDB, SQLAgent$PROD, VeeamCloudSvc, VeeamMountSvc, SQL Backups,
mozyprobackup, msftesql$PROD, swi_update_64, EraserSvc11710, MSExchangeMGMT,
MSSQL$BKUPEXEC, MSSQL$SQL_2008, MsDtsServer100, MsDtsServer110, SQLSERVERAGENT,
VeeamBackupSvc, VeeamBrokerSvc, VeeamDeploySvc, Sophos Agent, svcGenericHost,
EPUpdateService, MBEndpointAgent, MSOLAP$SQL_2008, MSSQLFDLauncher, McAfeeFramework,
SAVAdminService, SQLAgent$ECWDB2, SQLAgent$SOPHOS, SQLAgent$TPSAMA, VeeamCatalogSvc,
MSSQL$SHAREPOINT, MSSQL$SQLEXPRESS, MSSQL$SYSTEM_BGC, NetMsmqActivator,
ReportServer$TPS, SepMasterService, TrueKeyScheduler, EPSecurityService,
MSOLAP$SYSTEM_BGC, MSSQL$PRACTICEMGT, SQLAgent$BKUPEXEC, SQLAgent$SQL_2008,
SQLSafeOLRService, VeeamTransportSvc, Zoolz 2 Service, MSSQL$PRACTTICEBGC,
MSSQL$VEEAMSQL2012, Sophos MCS Agent, BackupExecJobEngine, MSSQL$SBSMONITORING,
MSSQLFDLauncher$TPS, MSSQLServerADHelper, McAfeeEngineService, OracleClientCache80,
ReportServer$TPSAMA, SQLAgent$SHAREPOINT, SQLAgent$SQLEXPRESS, SQLAgent$SYSTEM_BGC,
SQLTELEMETRY$ECWDB2, Sophos MCS Client, BackupExecRPCService, MSSQL$VEEAMSQL2008R2,
TrueKeyServiceHelper, BackupExecVSSProvider, MSSQL$PROFXENGAGEMENT,
ReportServer$SQL_2008, SQLAgent$PRACTTICEBGC, SQLAgent$PRACTTICEMGT,
SQLAgent$VEEAMSQL2012, BackupExecAgentBrowser, MSSQLFDLauncher$TPSAMA,
MSSQLServerADHelper100, MSSQLServerOLAPService, SQLAgent$SBSMONITORING,
VeeamDeploymentService, VeeamHvIntegrationSvc, Acronis VSS Provider, Sophos Clean
Service, ReportServer$SYSTEM_BGC, SQLAgent$VEEAMSQL2008R2, Sophos Health Service,
Sophos Message Router, MSSQLFDLauncher$SQL_2008, SQLAgent$PROFXENGAGEMENT, SQLsafe
Backup Service, SQLsafe Filter Service, SQLAgent$CITRIX_METAFRAME,
VeeamEnterpriseManagerSvc, BackupExecAgentAccelerator, MSSQLFDLauncher$SHAREPOINT,
MSSQLFDLauncher$SYSTEM_BGC, Sophos Safestore Service, Symantec System Recovery,
BackupExecManagementService, Enterprise Client Service, Sophos AutoUpdate Service,
BackupExecDeviceMediaService, Sophos Web Control Service,
MSSQLFDLauncher$SBSMONITORING, Sophos File Scanner Service,
McAfeeFrameworkMcAfeeFramework, MSSQLFDLauncher$PROFXENGAGEMENT, Sophos Device
Control Service, Sophos System Protection Service, Veeam Backup Catalog Data
Service,
```

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. Asymmetric means that there are two different
keys. This is also called public key cryptography, because one of the keys can be
given to anyone:

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 possible to recover your files without our
private key )

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 data back as a demo.
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
```

- Ransomware
- RobbinHood

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

-

  Amigo-A - 3 years ago

    -
    -

  Thanks for the details!
  If we look closely at antivirus detections on VT, we will notice that almost all of antiviruses write the word Robin with one letter 'B'. But the extortionists decided to write it with two letters 'B'. This should be a funny. But there are two more Ransomware named RobinHood, which were before.

-

  Lawrence Abrams - 3 years ago

  Yes, writing it with one B is incorrect and companies should stop doing it.

-

  Iconera - 3 years ago

  Great analysis. Have you tried making a read only folder C:\Windows\Temp\pub.key which will prevent the file of the same name being created to see if that is a preventitive method on clean systems

-
  [Lawrence Abrams](#) - 3 years ago
    -
    -
  No, but those types of tricks last only as long as the developer doesn't know about it. As these are targeted installs, the dev will prob notice something is amiss and work around it.
-
  gooolero - 2 years ago
    -
    -

  Thanks for the details!

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: