FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

5 JUNE 2019

Alert Number
MC-000104-MW

WE NEED YOUR HELP!
If you find any of these indicators on your networks, or have related information, please contact
FBI CYWATCH immediately.
Email:
cywatch@fbi.gov

Phone:
1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Indicators of Compromise Associated with RobbinHood Ransomware

Summary

Between 7 April and 7 May 2019, three US cities were victims of RobbinHood Ransomware attacks. These attacks represent the first observed instances of RobbinHood Ransomware in the United States. RobbinHood encrypts the files on the victim's network using RSA-4096, an asymmetric cryptographic algorithm. Once a machine has been infected, the RobbinHood actors issue a ransom note, providing the victim with two options to recover their data. The first option requires the victim to send 3 Bitcoin (BTC) for each affected system. The second option requires the victims to send 13 BTC for all affected systems. The note also states the ransom amount will increase by $10,000 per day, after the fourth day, if payment is not received.

Technical Details

Initial technical analysis indicates the malware encrypted files on each victim's network using the same file extension ".enc_robbinhood". The victims were presented with directions to pay the ransom and communicate with the attackers via the same top-level .onion domain. The only variation was a different directory on the .onion site was created for each attack.

It is currently unknown how the executable file containing the ransomware is dropped onto the system. On one infected machine, the system logs showed the creation of a service named “WindowsEventsLog32.” The service file name included the path to Robbinhood executable file at c:\windows\temp\winlogon.exe. This file is not part of the payload functionality – it is intended to execute the payload.

The ransomware will attempt to read “C:\windows\temp\pub.key” and will terminate if the file does not exist. There is logging functionality built into the malware that is located in “C:\windows\temp\rbf.log” but is currently disabled in the samples observed. The ransomware will attempt to stop hundreds of potential services running on the victim machine relating to antivirus, security, and database software in the form of “cmd.exe /c sc.exe stop <service>”

The following indicators of compromise have been observed in samples of the Robbinhood Ransomware:

MD5 Indicators:

- MD5: 73d43cf4aecf2dc55ef61ab17dfbb147
- MD5: a6d61654e6af6f1fa417229aa2da76f2
- MD5: aace43af8d0932a7b01c5b8fb71c8199
- MD5: edfec708d2b6686beb55e449fb55d11e
- MD5: 5c9c205c7767472abb8bc112f79afd7e

SHA1 Indicators:

- SHA1: 3e73d8b77f4364377506fb9fea06aaf0702bbdd2
- SHA1: aaccd5b3c438a1d0e0daa62c58477feb9e7f6d77
- SHA1: b7cbdabf4832bf2343bebc4fbb7896c1ac02b27e
- SHA1: f926c3e916fa7c499a7ca0c5bdbf9a05d9924348
- SHA1: 56422e5cc2abe198198003d2c5bf009c8652a983

SHA256 Indicators:

- 3bc78141ff3f742c5e942993adfbef39c2127f9682a303b5e786ed7f9a8d184b
- bfc39ca9a223a731fb6d9ffb29923844904cb842435cde0c640ba79818b5e728
- 9977ba861016edef0c3fb38517a8a68dbf7d3c17de07266cfa515b750b0d249e
- 4e58b0289017d53dda4c912f0eadf567852199d044d2e2bda5334eb97fa0b67c
- e128d5aa0b5a9c6851e69cbf9d2c983eefd305a10cba7e0c8240c8e2f79a544f

imphash:

- 1c2a6fbef41572f4c9ce8acb5a63cde7
- 406f4cbdf82bde91761650ca44a3831a

Recommended Mitigations

The FBI recommends the incorporation of the following Yara rule into your network defenses to detect the RobbinHood Ransomware:

```
rule robbinhood

{

meta:description = "Robbinhood Ransomware"

date = "05/09/2019"

strings:

$go1 = "go.buildid"

$go2 = "Go build ID:"

$rh1 = "c:/users/valery/go/src/oldboy/config.go" nocase

$rh2 = "c:\\windows\\temp\\pub.key" nocase

$rh3 = ".enc_robbinhood" nocase

$rh4 = "cmd.exe /c net use * /DELETE /Y" nocase

$rh5 = "ServiceFuck"

$rh6 = "RecoveryFCK"

$rh7 = "ShadowFucks"
$rh8 = "CoolMaker"

condition:

uint16(0) == 0x5A4D and

all of ($go*) and

any of ($rh*)

}
```

Defending Against Ransomware Generally

Precautionary measures to mitigate ransomware threats include, but are not limited to:

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Only download software – especially free software – from sites you know and trust.
- Enable automated patches for your operating system and Web browser(s).

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:GREEN**. Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.