FBI FLASH

FEDERAL BUREAU OF INVESTIGATION ♦ CYBER DIVISION

02 Dec 2021

FLASH Number

CU-000156-MW



**WE NEED YOUR HELP!** If you identify any suspicious activity within your enterprise or have related information, please contact your local FBI Cyber Squad immediately with respect to the procedures outlined in the Reporting Notice section of this message.

**Note: By reporting any related information to FBI Cyber Squads, 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.*

# Indicators of Compromise Associated with Cuba Ransomware

## Summary

The FBI has identified, as of early November 2021 that Cuba ransomware actors have compromised at least 49 entities in five critical infrastructure sectors, including but not limited to the financial, government, healthcare, manufacturing, and information technology sectors. Cuba ransomware is distributed through Hancitor malware, a loader known for dropping or executing stealers, such as Remote Access Trojans (RATs) and other types of ransomware, onto victims' networks. Hancitor malware actors use phishing emails, Microsoft Exchange vulnerabilities, compromised credentials, or legitimate Remote Desktop Protocol (RDP) tools to gain initial access to a victim's network. Subsequently, Cuba ransomware actors use legitimate Windows services—such as PowerShell, PsExec, and other unspecified services—and then leverage Windows Admin privileges to execute their ransomware and other processes remotely. Cuba ransomware actors compromise a victim network through the encryption of target files with the ".cuba" extension. Cuba ransomware actors have demanded at least US $74 million and received at least US $43.9 million in ransom payments.

## Technical Details

Cuba ransomware, upon compromise, installs and executes a CobaltStrike beacon as a service on the victim's network via PowerShell. Once installed, the ransomware downloads two executable files, which include "pones.exe" for password acquisition and "krots.exe," also known as KPOT, enabling the Cuba ransomware actors to write to the compromised system's temporary (TMP) file. Once the TMP file is uploaded, the "krots.exe" file is deleted and the TMP file is executed in the compromised network. The TMP file includes Application Programming Interface (API) calls related to memory injection that, once executed, deletes itself from the system. Upon deletion of the TMP file, the compromised network begins communicating with a reported malware repository located at Montenegro-based Uniform Resource Locator (URL) teoresp.com.

Further, Cuba ransomware actors use MimiKatz malware to steal credentials, and then use RDP to log into the compromised network host with a specific user account. Once an RDP connection is complete, the Cuba ransomware actors use the CobaltStrike server to communicate with the compromised user account. One of the initial PowerShell script functions allocates memory space to run a base64-encoded payload. Once this payload is loaded into memory, it can be used to reach the remote command-and-control (C2) server and then deploy the next stage of files for the ransomware. The remote C2 server is located at the malicious URL kurvalarva.com

## Indicators

The following are characteristics of a Cuba ransomware compromise, as of mid-October 2021:

| **Cuba Ransomware Associated Files and Hashes, as of Mid-October 2021** | | |
|---|---|---|
| **File Name** | **File Path** | **File Hash** |
| qcklo.aspx | c:\inetput\wwwroot\aspnet_client | MD5: 7b6f996cc1ad4b5e131e7bf9b1c33253<br>SHA-1: 2841848ef59dfe7137e15119e4c9ce5e873e3607<br>SHA-256: b14341b1ffe9e2730394b9066c6829b4e2f59a4234765ae2e97cfc6d4593730a |
| haqdu.aspx | c:\inetput\wwwroot\aspnet_client | MD5: 7b6f996cc1ad4b5e131e7bf9b1c33253<br>SHA-1: 2841848ef59dfe7137e15119e4c9ce5e873e3607<br>SHA-256: b14341b1ffe9e2730394b9066c6829b4e2f59a4234765ae2e97cfc6d4593730a |
| komar.ps1 | c:\windows\temp | MD5: ba83831700a73661f99d38d7505b5646<br>SHA-1: 209ffbc8ba1e93167bca9b67e0ad3561c065595d<br>SHA-256: |

| | | |
|---|---|---|
| | | 79d6b1b6b1ecb446b0f49772bf4da63fcec6f6bfc7c2e1f4924cb7acbb3b4f53 |
| aa.bat | c:\windows\temp | MD5: 3fe1a3aaca999a5db936843c9bdfea14<br>SHA-1: 25ebe54beb3c422ccd2d90aa8ae89087f71b0bed<br>SHA-256:<br>e82cc49c03320a0fb6ec3512c0ca3332eb1b40070cc53a78bc80b77b4aba975c |
| aa.dll | c:\windows\temp | MD5: d907be57b5ef2af8a8b45d5f87aa4773<br>SHA-1: 867d41458d94e985f6b3e2bae1dfb75e14cbc57f<br>SHA-256:<br>4b5eefa1727b97b6f773be3937a8cc390f0434ddc2f01dc24b68b690fafbcc93 |
| netping.dll | c:\windows\temp | |
| check.txt | c:\windows\temp | |
| result.txt | c:\windows\temp | |
| protoping.exe | c:\windows\temp | |
| agent32.ps1 | c:\windows\temp | MD5: ba83831700a73661f99d38d7505b5646<br>SHA-1: 209ffbc8ba1e93167bca9b67e0ad3561c065595d<br>SHA-256:<br>79d6b1b6b1ecb446b0f49772bf4da63fcec6f6bfc7c2e1f4924cb7acbb3b4f53 |
| new.dll | c:\programdata | MD5: ee2f71faced3f5b5b202c7576f0f52b9<br>SHA-1: d1ff26ea3d2d2ced4b7e76d971a60533817048d7<br>SHA-256:<br>5cd95b34782ca5acf8a34d9dc184cb880a19b6edcaf4a4553fa0619b597c2f50 |
| run.txt | c:\windows\temp | MD5: 99c7cad7032ec5add3a21582a64bb149<br>SHA-1: 4de5d433af5701462517719ce097bb4c0e5676c9<br>SHA-256:<br>7f4bdf94a0e0457f41bdd1a8d8d9fc39fc383d3d0a331048828d391bbf727a1e |
| agent32.bin | c:\windows\temp | MD5: 72a60d799ae9e4f0a3443a2f96fb4896<br>SHA-1: a304497ff076348e098310f530779002a326c264<br>SHA-256:<br>6d5ca42906c60caa7d3e0564b011d20b87b175cbd9d44a96673b46a82b07df68 |
| dc.exe | | |
| iv.exe | | |
| ivnet.exe | | |
| shar.bat | | |
| psexesrv.exe | | |
| 82.ps1 | | |
| process 66-87.dll; | | |
| install.cmd | | |
| | | ce3a6224dae98fdaa712cfa6495cb72349f333133dbfb339c9e90699cbe4e8e |

| | | |
|---|---|---|
| | | 141b2190f51397dbd0dfde0e3904b264c91b6f81febc823ff0c33da980b69944 |
| | | 1d142c36c6cdd393fe543a6b7782f25a9cbafca17a1cfa0f3fc0f5a9431dbf3f |
| | | 81bdd622f0cb9d7e2ac5325a74606fa7818bd4205f37184eba68cdcbe96942f6 |
| | | d010fbb1afeb610338c49ae2425b6b7c4a9f4c469aedd096a15b32527565d7db |
| | | 7e765942d89cd3bfaca41034cd959b8d741085bd8bcedbb741e15ed685227a5e |
| | | 05f90cad3627f5253e1a03156793bc6cada7f4ce0d510f55139f0285fcff589d |
| | | EEDC68C92C50BE88C5935651D6B772D4728C3566581BE1F24D4CE7EF63A76D2E |
| | | 3468C6DEB3827F5C161A8622E7D794444C7B38225F6F15002193D2572A4D132E |
| | | 02B17677BEC8A4FBB77FDDB347BFDCC651FF2B25187131CCE45C326E3CF42FE5 |
| | | 188E66158E0F96AD1FFD3F090E2570B8644CD80733C7AAFB931E893A4F280165 |

| **Cuba Ransomware Associated Email Addresses, as of Mid-October 2021** | |
|---|---|
| **Email Provider** | **Email Addresses** |
| **Protonmail** | ad_default@protonmail.com |
| | admansmit001@protonmail.com |
| | afts_agent@protonmail.com |
| | helpadmin1@protonmail.com |
| | helpallen@protonmail.com |
| | helpallen@protonmail.com |
| | mail_supportRG@protonmail.com |
| | roselondon@protonmail.com |
| | system_admC@protonmail.com |
| **Protonmail.ch** | dark_sysadmin@protonmail.ch |
| | iracomp1@protonmail.ch |
| | iracomp3@protonmail.ch |
| | LR_FWS_H2M_ET@protonmail.ch |
| | under_amur@protonmail.ch |
| **Cock.li** | cloudkey@cock.li |
| | fiaadministrator@cock.li |
| | frankstore@cock.li |
| | helpallen@cock.li |
| | iracomp@cock.li |
| | ivantisupport@cock.li |

| | |
|---|---|
| | logme@cock.li |
| | mfra@cock.li |
| | morebeerplease@cock.li |
| | roselondon@cock.li |
| **Cuba-supp.com** | admin@cuba-supp.com |

| **Cuba Ransomware Associated Jabber Address, as of Mid-October 2021** |
|---|
| cuba_support@exploit.im |

| **IP Addresses Associated with Cuba Ransomware, as of Mid-October 2021** |
|---|
| 37.120.193.123 |
| 40.115.162.72 |
| 157.245.70.127 |
| 31.44.184.82 |
| 185.153.199.176 |

| **Bitcoin Wallet Receiving Ransom Payments, as of Mid-October 2021** |
|---|
| bc1qvpk8ksl3my6kjezjss9p28cqj4dmpmmjx5yl3y |
| bc1qhtwfcysclc7pck2y3vmjtpzkaezhcm6perc99x |
| bc1qft3s53ur5uq5ru6sl3zyr247dpr55mnggwucd3 |
| bc1qp7h9fszlqxjwyfhv0upparnsgx56x7v7wfx4x7 |

| **Sample Cuba Ransom Note, as of Mid-October 2021** |
|---|
| Good day. All your files are encrypted. For decryption contact us.<br>Write here iracomp3@protonmail.com<br>We also inform that your databases, ftp server and file server were downloaded by us to our servers.<br><br>* Do not rename encrypted files<br>* Do not try to decrypto your data using third party software,<br>it may cause permanent data loss. |

## Information Requested:

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, Bitcoin wallet information, the decryptor file, and/or a benign sample of an encrypted file. The FBI does not encourage paying ransoms. Payment does not guarantee files will be recovered. It may also embolden adversaries to target

additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. However, the FBI understands that when victims are faced with an inability to function, all options are evaluated to protect shareholders, employees and customers. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to promptly report ransomware incidents to your local field office. Doing so provides the FBI with critical information needed to prevent future attacks by identifying and tracking ransomware attackers and holding them accountable under US law.

## Recommended Mitigations:

FBI recommends network defenders to apply the following mitigations to reduce the risk of compromise by Cuba ransomware:

- **Require all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to have strong, unique passwords.** Passwords should not be reused across multiple accounts or stored on the system where an adversary may have access. Note: Devices with local administrative accounts should implement a password policy that requires strong, unique passwords for each individual administrative account.
- **Require multi-factor authentication** for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
- **Keep all operating systems and software up to date**. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats.
- **Remove unnecessary access to administrative shares**, especially ADMIN$ and C$. If ADMIN$ and C$ are deemed operationally necessary, restrict privileges to only the necessary service or user accounts and perform continuous monitoring for anomalous activity.
- **Use a host-based firewall** to only allow connections to administrative shares via server message block (SMB) from a limited set of administrator machines.

Adversaries use system and network discovery techniques for network and system visibility and mapping. To limit an adversary from learning the organization's enterprise environment, limit common system and network discovery techniques by taking the following actions:

- **Segment networks** to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral

movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.

- **Implement time-based access for accounts set at the admin level and higher**. For example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the AD level when the account is not in direct need. When the account is needed, individual users submit their requests through an automated process that enables access to a system, but only for a set timeframe to support task completion.
- **Disable command-line and scripting activities and permissions**. Privilege escalation and lateral movement often depend on software utilities that run from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.
- **Maintain offline backups of data**, and regularly maintain backup and restoration. This practice will ensure the organization will not be severely interrupted, have irretrievable data.
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure.

## Additional Resources

For additional resources related to the prevention and mitigation of ransomware, go to https://www.stopransomware.gov as well as the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide. Stopransomware.gov is the Government's new, official one-stop location for resources to tackle ransomware more effectively.

## Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. 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.

## Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, the information in this product may be shared without restriction.