FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

05 May 2021

Alert Number
CU-000145-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 to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP:GREEN**: The information in this product may be shared with peers and partner organizations within your sector or community, but not via publicly accessible channels.

Indicators Associated with Avaddon Ransomware

Summary

The FBI has received notifications of unidentified cyber actors using Avaddon ransomware against US and foreign private sector companies, manufacturing organizations, and healthcare agencies. Avaddon ransomware was first advertised on Russian-language hacking forums as a ransomware-as-a-service (RaaS).

Avaddon ransomware actors have compromised victims through remote access login credentials [e.g., remote desktop protocol (RDP) and virtual private network (VPN)] with single-factor authentication or improperly configured RDP. After Avaddon actors gain access to a victim's network, they map the network and identify backups for deletion and/or encryption. The malware escalates privileges, contains anti-analysis protection code, enables persistence on a victim system, and verifies the victim is not located in the Commonwealth of Independent States (CIS).[1]

[1] (U) The Commonwealth of Independent States is composed of Russia and 11 former Soviet Union countries.

Avaddon ransomware actors not only encrypt victims' data for a ransom but also exfiltrate data from their victims. The actors threaten to leak the victims' data to The Onion Router (TOR) network unless their ransom demand is paid in virtual currency within days of infection. Avaddon's extortion tactics progress from a warning, to a partial data leak, and finally to a full data leak of all exfiltrated files. The extortion/data leak process typically follows these steps:

- **Leak Warning**: After initially gaining access to a victim network, Avaddon actors leave a ransom note on the victim's network and post a "leak warning" to the Avaddon TOR leak website (avaddongun7rngel.onion). The warning consists of screenshots from files (e.g., sensitive documents) and proof of access to the victim's network (e.g., screenshots of network folders).

- **5 Percent Leak**: If the victim does not quickly pay the ransom within 3 to 5 days, Avaddon actors increase the pressure on victims by leaking a portion of the files (as opposed to screenshots). The Avaddon actors leak this data by uploading a small .ZIP file to Avaddon's TOR leak website.

- **Full Leak**: If the ransom is not paid after the 5 percent leak, Avaddon actors post all their exfiltrated data in large .ZIP files in the "Full dumps" section of the Avaddon TOR leak website.

In January 2021, Avaddon actors stated they would attack victims who do not pay the ransom with distributed denial-of service (DDoS) attacks. As of April 2021, the FBI has not identified DDoS attacks following Avaddon ransomware events.

Ransom Note Details and TOR Websites

Avaddon ransom notes typically contain a unique victim ID and a link to the TOR website at *avaddonbotrxmuyl.onion*, which victims must access by downloading and using a TOR browser. This website is used to provide technical support, negotiate with victims via an online chat functionality, post data leaks, and receive ransomware payments from victims. When victims enter their IDs on the site, they receive instructions on how to pay the ransom and decrypt their data.

File Names and Tools used by Attackers

The following applications are leveraged by Avaddon actors to compromise victims. While these applications support legitimate purposes, they can also be used by threat actors to aid in system compromise or exploration of an enterprise:

- PowerShell
- WMIC.exe (WMI -Windows Management Instrumentation)
- Svchost.exe (Service host system process)
- Taskhost.exe (Host protocol)

Technical Details

Avaddon was written in C++ and encrypts data using a unique AES256 encryption key. During the infection process, Avaddon checks the operating system language and keyboard layouts. If a potential victim's operating system language is set to specific languages normally used in the CIS, the malware ceases operation without harming the system.

Analysis of Avaddon ransomware reveals common capabilities of ransomware, such as encryption (e.g. CryptEncrypt), persistence through registry keys (e.g., RegCreateKeyW, StartServiceW), anti-analysis (e.g., IsDebuggerPresent), and activity control (e.g., DeleteService or TerminateProcess or "EventDisable UAC").

Registry Changes

The following registry keys are changed during system compromise:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System EnableLUA=0 (disables the "administrator in Admin Approval Mode" user type

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System EnableLinkedConnections=1 (makes the user mapped drives available to the administrator)

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System ConsentPromptBehaviorAdmin=0 (this option allows the actors to perform an operation that requires elevation without consent or credentials)

Avaddon ransomware adds the following registry entries to enable its automatic execution at system startup:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run update = %Application Data%\{malware filename}.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run update = %Application Data%\{malware filename}.exe

Modification of Registry Keys

Avaddon ransomware changes the desktop wallpaper by modifying the following registry entries:

- HKEY_CURRENT_USER\Control Panel\Desktop Wallpaper = %User Profile%\bckgrd.bmp

Other Observed System Modifications:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000 Owner = {HEX VALUES}
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000 SessionHash = {HEX VALUES}
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000 Sequence = {VALUE}
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000 RegFiles0000 = {Target File Name}
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\RestartManager\Session0000 RegFilesHash = {Hex Values}

Avaddon ransomware also terminates services and processes related to backup and antivirus running in system memory before encrypting victim's data (e.g. RTVscan.exe, 360se.exe etc.).

Avaddon's Affiliates' Varied TTPs: Avaddon victims are identified and compromised by affiliates, not ransomware developers. Affiliates customize the ransomware's code and use diverse tactics, techniques, and procedures (TTPs) to deploy the ransomware. The wide variety of actors and their associated TTPs adds a layer of difficulty in identifying common indicators (e.g., IP addresses, file names) associated with Avaddon activity. The information listed below is derived from limited victim reporting.

File Storage

Victim reporting has indicated executable files and/or PowerShell scripts are stored in the following locations:

- %Application Data%\{malware filename}.exe
- C:\Users\{user name} \Documents\My Received Files\My Received Files\

Indicators of Compromise

Potential malicious IP addresses (used during remote access connections):

- 185.216.33.0/24
- 45.145.67.0/23
- 193.27.229.0/23
- 217.8.117.63

Potential malicious domain names:

- myphotoload.com
- Tldrnet.top

Ransom Note File Name:

- readme.txt

File Extension on Encrypted Files

Initially, the Avaddon ransomware used the extension .avdn when encrypting files. In fall 2020, the ransomware started using an extension composed of a combination of nine or ten characters of the letters A through E. (e.g., .BEaBeBecdA, .BAAcbdCDbb, .DDAbAAcae).

Information Requested

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. Regardless of whether you or your organization decide to pay the ransom, the FBI urges you to report ransomware incidents to your local field office. Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under US law, and prevent future attacks.

The FBI may seek the following information that you determine you can legally share, including:

- Recovered executable file
- Live memory (RAM) capture
- Images of infected systems
- Malware samples
- IP addresses identified as malicious or suspicious
- Email addresses of the attackers
- A copy of the ransom note
- Ransom amount
- Bitcoin wallets used by the attackers
- Bitcoin wallets used to pay the ransom
- Post-incident forensic reports

Recommended Mitigations

- Back-up critical data offline.
- Ensure copies of critical data are in the cloud or on an external hard drive or storage device.
- Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the data resides.
- Use two-factor authentication with strong passwords, including for remote access services.

- Monitor cyber threat reporting regarding the publication of compromised VPN login credentials and change passwords/settings if applicable.
- Regularly change passwords to critical systems.
- Keep computers, devices, and applications patched and up-to-date.
- Install and regularly update anti-virus or anti-malware software on all hosts.

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@ic.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@ic.fbi.gov or (202) 324-3691.

Administrative Note

This product is marked TLP:GREEN. The information in this product may be shared with peers and partner organizations within your sector or community, but not via publicly accessible channels.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

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.