JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP: WHITE

Product ID: CU-000164-MW

March 17, 2022

Indicators of Compromise Associated with AvosLocker Ransomware

SUMMARY

AvosLocker is a Ransomware as a Service (RaaS) affiliate-based group that has targeted victims across multiple critical infrastructure sectors in the United States including, but not limited to, the Financial Services, Critical Manufacturing, and Government Facilities sectors. AvosLocker claims to directly handle ransom negotiations, as well as the publishing and hosting of exfiltrated victim data after their affiliates infect targets. As a result, AvosLocker indicators of compromise (IOCs) vary between indicators specific to AvosLocker malware and indicators specific to the individual affiliate responsible for the intrusion.

TECHNICAL DETAILS

AvosLocker ransomware encrypts files on a victim's server and renames them with the ".avos" extension. AvosLocker actors then place ransom notes on the victim server and include a link to an AvosLocker .onion payment site (Figure 1). Depending upon the affiliate, payments in Monero are preferred; however, they accept Bitcoin for a 10-25% premium. We have also observed alleged AvosLocker representatives make phone calls to the victims to direct them to the payment site to negotiate. Multiple victims have also reported that AvosLocker negotiators have been willing to negotiate reduced ransom payments.

The AvosLocker leak site claims to have targeted victims in the United States, Syria, Saudi Arabia, Germany, Spain, Belgium, Turkey, the United Arab Emirates, the United Kingdom, Canada, China, and Taiwan. The leak site includes samples of stolen victim data and threatens to sell the data to unspecified third parties, if a victim does not pay the ransom.

AvosLocker ransomware is a multi-threaded Windows executable written in C++ that runs as a console application and shows a log of actions performed on victim systems. AvosLocker

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

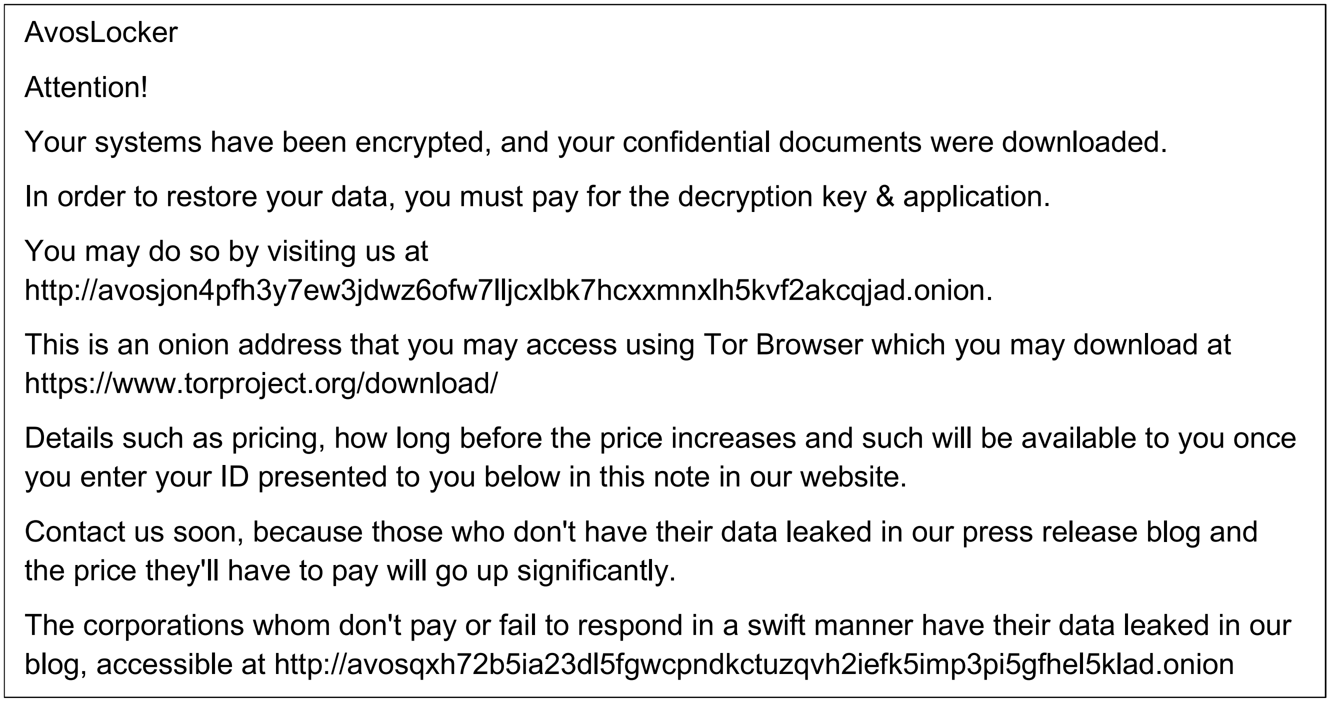
ransomware samples contained optional command line arguments that could be supplied by an attacker to enable/disable certain features.

Indicators of compromise specific to AvosLocker malware

Encryption and the ransom demand

AvosLocker ransomware creates a mutex object for use as an infection marker to avoid infecting a system twice. Prior to encryption, the ransomware maps accessible drives and enumerated files in directories. It then encrypts files while creating a ransom note named "GET_YOUR_FILES_BACK.txt" in every directory.

In observed cases, encrypted files have the file extension ".avos", ".avos2", or "AvosLinux". Infected directories have a text file entitled "GET_YOUR_FILES_BACK.txt". In some cases, the text from the text file reproduces on the desktop wallpaper of infected servers. The "GET_YOUR_FILES_BACK.txt" file directs victims to an onion site accessible via a TOR browser, where the victim is prompted to enter an ID provided to them in the ransom note.



AvosLocker

Attention!

Your systems have been encrypted, and your confidential documents were downloaded.

In order to restore your data, you must pay for the decryption key & application.

You may do so by visiting us at
http://avosjon4pfh3y7ew3jdwz6ofw7lljcxlbk7hcxxmnxlh5kvf2akcqjad.onion.

This is an onion address that you may access using Tor Browser which you may download at
https://www.torproject.org/download/

Details such as pricing, how long before the price increases and such will be available to you once you enter your ID presented to you below in this note in our website.

Contact us soon, because those who don't have their data leaked in our press release blog and the price they'll have to pay will go up significantly.

The corporations whom don't pay or fail to respond in a swift manner have their data leaked in our blog, accessible at http://avosqxh72b5ia23dl5fgwcpndkctuzqvh2iefk5imp3pi5gfhel5klad.onion

(U) Figure 1 - AvosLocker Ransom Note circa December 2021

Indicators of compromise specific to the victim's actions

Data published on the leak site

AvosLocker actors publish victim exfiltrated data on the AvosLocker public leak site if victims do not negotiate or pay the ransom. The AvosLocker public leak site is separate from the site

AvosLocker directs victims to in the “GET_YOUR_FILES_BACK.txt” file. The public leak site lists victims of AvosLocker, along with a sample of data allegedly stolen from the victim’s network. The leak site gives visitors an opportunity to view a sample of victim data and to purchase victim data.

Phone calls and DDOS attacks

In some cases, AvosLocker victims receive phone calls from an AvosLocker representative. The caller encourages the victim to go to the onion site to negotiate and threatens to post stolen data online. In some cases, AvosLocker actors will threaten and execute distributed denial-of-service (DDoS) attacks during negotiations.

Indicators of compromise specific to the affiliate

Persistence mechanisms on victim systems include the modification of Windows Registry 'Run' keys and the use of scheduled tasks.

Other tools associated with AvosLocker ransomware attacks:

- Cobalt Strike
- Encoded PowerShell scripts (publicly available tool)
- PuTTY Secure Copy client tool “pscp.exe”
- Rclone
- AnyDesk
- Scanner
- Advanced IP Scanner
- WinLister

Vulnerabilities

Multiple victims have reported on premise Microsoft Exchange Server vulnerabilities as the likely intrusion vector.

Some victims pointed to specific vulnerabilities: including the Proxy Shell vulnerabilities associated to CVE-2021-31207, CVE-2021-34523, and CVE-2021-34473, in addition to CVE-2021-26855.

Intrusion vectors are likely dependent on the skillsets of the AvosLocker affiliate who infiltrated the victim’s network.

MITIGATIONS

- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).

- Implement network segmentation and maintain offline backups of data to ensure limited interruption to the organization.
- Regularly back up data, password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Install and regularly update antivirus software on all hosts, and enable real time detection.
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind. Do not give all users administrative privileges.
- Disable unused ports.
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.
- Use multifactor authentication where possible.
- Use strong passwords and regularly change passwords to network systems and accounts, implementing the shortest acceptable timeframe for password changes. Avoid reusing passwords for multiple accounts.
- Require administrator credentials to install software.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Focus on cyber security awareness and training. Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e., ransomware and phishing scams).

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 official one-stop location for resources to tackle ransomware more effectively.

Financial Institutions must also ensure compliance with any applicable Bank Secrecy Act requirements, including suspicious activity reporting obligations. Indicators of compromise, such as suspicious email addresses, file names, hashes, domains, and IP addresses can be provided under Item 44 of the Suspicious Activity Report (SAR) form. For more information on mandatory and voluntary reporting of cyber events via suspicious activity reports (SARs), see FinCEN Advisory FIN-2016-A005, “Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime,” October 25, 2016, and FinCEN Advisory FIN-2021-A004, “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,” November 8, 2021, which updates FinCEN Advisory FIN-2020-A006.

CISA's Ransomware Readiness Assessment is a no-cost self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.

CISA offers a range of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.