JOINT
CYBERSECURITY
ADVISORY

Product ID: AA23_284A

October 11, 2023

#StopRansomware: AvosLocker Ransomware (Update)

SUMMARY

Note: *This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

Actions to take today to mitigate cyber threats from AvosLocker ransomware:

- Securing remote access tools
- Restricting RDP and other remote desktop services
- Securing PowerShell and/or restrict usage
- Update software to latest version and apply patching updates regularly.

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint Cybersecurity Advisory (CSA) to disseminate known IOCs, TTPs, and detection methods associated with the AvosLocker variant identified through FBI investigations as recently as May 2023. AvosLocker operates under a ransomware-as-a-service (RaaS) model. AvosLocker affiliates have compromised organizations across multiple critical infrastructure sectors in the United States, affecting Windows, Linux, and VMware ESXi environments. AvosLocker affiliates compromise organizations' networks by using legitimate software and open-source remote system administration tools. AvosLocker affiliates then use exfiltration-based data extortion tactics with threats of leaking and/or publishing stolen data.

This joint CSA updates the March 17, 2022, AvosLocker ransomware joint CSA, Indicators of Compromise Associated with AvosLocker ransomware, released by FBI and the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). This update includes IOCs

U.S. organizations: To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at 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 Report@cisa.dhs.gov.

and TTPs not included in the previous advisory and a YARA rule FBI developed after analyzing a tool associated with an AvosLocker compromise.

FBI and CISA encourage critical infrastructure organizations to implement the recommendations in the Mitigations section of this CSA to reduce the likelihood and impact of AvosLocker ransomware and other ransomware incidents.

TECHNICAL DETAILS

Note: *This advisory uses the MITRE ATT&CK for Enterprise framework, version 13. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.*

AvosLocker affiliates use legitimate software and open-source tools during ransomware operations, which include exfiltration-based data extortion. Specifically, affiliates use:

- Remote system administration tools—Splashtop Streamer, Tactical RMM, PuTTy, AnyDesk, PDQ Deploy, and Atera Agent—as backdoor access vectors [T1133].
- Scripts to execute legitimate native Windows tools [T1047], such as PsExec and Nltest.
- Open-source networking tunneling tools [T1572] Ligolo[1] and Chisel.[2]
- Cobalt Strike and Sliver[3] for command and control (C2).
- Lazagne and Mimikatz for harvesting credentials [T1555].
- FileZilla and Rclone for data exfiltration.
- Notepad++, RDP Scanner, and 7zip.

FBI has also observed AvosLocker affiliates:

1) Use custom PowerShell [T1059.001] and batch (`.bat`) scripts [T1059.003] for lateral movement, privilege escalation, and disabling antivirus software.
2) Upload and use custom webshells to enable network access [T1505.003].

For additional TTPs, see joint CSA Indicators of Compromise Associated with AvosLocker Ransomware.

Indicators of Compromise (IOC)

See Tables 1 and 2 below for IOCs obtained from January 2023–May 2023.

Table 1: Files, Tools, and Hashes as of May 2023

Files and Tools	MD5
psscriptpolicytest_im2hdxqi.g0k.ps1	829f2233a1cd77e9ec7de98596cd8165
psscriptpolicytest_lysyd03n.o10.ps1	6ebd7d7473f0ace3f52c483389cab93f

Files and Tools	MD5
psscriptpolicytest_1bokrh3l.2nw.ps1	10ef090d2f4c8001faadb0a833d60089
psscriptpolicytest_nvuxllhd.fs4.ps1	8227af68552198a2d42de51cded2ce60
psscriptpolicytest_2by2p21u.4ej.ps1	9d0b3796d1d174080cdfdbd4064bea3a
psscriptpolicytest_te5sbsfv.new.ps1	af31b5a572b3208f81dbf42f6c143f99
psscriptpolicytest_v3etgbxw.bmm.ps1	1892bd45671f17e9f7f63d3ed15e348e
psscriptpolicytest_fqa24ixq.dtc.ps1	cc68eaf36cb90c08308ad0ca3abc17c1
psscriptpolicytest_jzjombgn.sol.ps1	646dc0b7335cffb671ae3dfd1ebefe47
psscriptpolicytest_rdm5qyy1.phg.ps1	609a925fd253e82c80262bad31637f19
psscriptpolicytest_endvm2zz.qlp.ps1	c6a667619fff6cf44f447868d8edd681
psscriptpolicytest_s1mgcgdk.25n.ps1	3222c60b10e5a7c3158fd1cb3f513640
psscriptpolicytest_xnjvzu5o.fta.ps1	90ce10d9aca909a8d2524bc265ef2fa4
psscriptpolicytest_satzbifj.oli.ps1	44a3561fb9e877a2841de36a3698abc0
psscriptpolicytest_grjck50v.nyg.ps1	5cb3f10db11e1795c49ec6273c52b5f1
psscriptpolicytest_0bybivfe.x1t.ps1	122ea6581a36f14ab5ab65475370107e
psscriptpolicytest_bzoicrns.kat.ps1	c82d7be7afdc9f3a0e474f019fb7b0f7
Files and Tools	**SHA256**
BEACON.PS1	e68f9c3314beee640cc32f08a8532aa8dcda613543c54a83680c21d7cd49ca0f
Encoded PowerShell script	ad5fd10aa2dc82731f3885553763dfd4548651ef3e28c69f77ad035166d63db7
Encoded PowerShell script	48dd7d519dbb67b7a2bb2747729fc46e5832c30cafe15f76c1dbe3a249e5e731
Files and Tools	**SHA1**
PowerShell backdoor	2d1ce0231cf8ff967c36bbfc931f3807ddba765c

Table 2: Email Address and Virtual Currency Wallets

Email Address
keishagrey994@outlook[.]com

Virtual Currency Wallets
a6dedd35ad745641c52d6a9f8da1fb09101d152f01b4b0e85a64d21c2a0845ee
bfacebcafff00b94ad2bff96b718a416c353a4ae223aa47d4202cdbc31e09c92
418748c1862627cf91e829c64df9440d19f67f8a7628471d4b3a6cc5696944dd
bc1qn0u8un00nl6uz6uqrw7p50rg86gjrx492jkwfn

DETECTION

Based on an investigation by an advanced digital forensics group, FBI created the following YARA rule to detect the signature for a file identified as enabling malware. `NetMonitor.exe` is a malware masquerading as a legitimate process and has the appearance of a legitimate network monitoring tool. This persistence tool sends pings from the network every five minutes. The NetMonitor executable is configured to use an IP address as its command server, and the program communicates with the server over port 443. During the attack, traffic between NetMonitor and the command server is encrypted, where NetMonitor functions like a reverse proxy and allows actors to connect to the tool from outside the victim's network.

YARA Rule

```
rule NetMonitor
{
  meta:
    author = "FBI"
    source = "FBI"
    sharing = "TLP:CLEAR"
    status = "RELEASED"
    description = "Yara rule to detect NetMonitor.exe"
    category = "MALWARE"
    creation_date = "2023-05-05"
  strings:
    $rc4key = {11 4b 8c dd 65 74 22 c3}
    $op0 = {c6 [3] 00 00 05 c6 [3] 00 00 07 83 [3] 00 00 05 0f 85 [4] 83 [3] 00
00 01 75 ?? 8b [2] 4c 8d [2] 4c 8d [3] 00 00 48 8d [3] 00 00 48 8d [3] 00 00 48
89 [3] 48 89 ?? e8}
  condition:
    uint16(0) == 0x5A4D
    and filesize < 50000
    and any of them
}
```

MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 3-7 for all referenced threat actor tactics and techniques in this advisory.

Table 3: AvosLocker Affiliates ATT&CK Techniques for Initial Access

Initial Access		
Technique Title	**ID**	**Use**
External Remote Services	T1133	AvosLocker affiliates use remote system administration tools—Splashtop Streamer, Tactical RMM, PuTTy, AnyDesk, PDQ Deploy, and Atera Agent—to access backdoor access vectors.

Table 4: AvosLocker Affiliates ATT&CK Techniques for Execution

Execution		
Technique Title	**ID**	**Use**
Command and Scripting Interpreter: PowerShell	T1059.001	AvosLocker affiliates use custom PowerShell scripts to enable privilege escalation, lateral movement, and to disable antivirus.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	AvosLocker affiliates use custom `.bat` scripts to enable privilege escalation, lateral movement, and to disable antivirus.
Windows Management Instrumentation	T1047	AvosLocker affiliates use legitimate Windows tools, such as PsExec and Nltest in their execution.

Table 5: AvosLocker Affiliates ATT&CK Techniques for Persistence

Persistence		
Technique Title	**ID**	**Use**
Server Software Component	T1505.003	AvosLocker affiliates have uploaded and used custom webshells to enable network access.

Table 6: AvosLocker Affiliates ATT&CK Techniques for Credential Access

Credential Access		
Technique Title	**ID**	**Use**
Credentials from Password Stores	T1555	AvosLocker affiliates use open-source applications Lazagne and Mimikatz to steal credentials from system stores.

Table 7: AvosLocker Affiliates ATT&CK Techniques for Command and Control

Command and Control		
Technique Title	**ID**	**Use**
Protocol Tunneling	T1572	AvosLocker affiliates use open source networking tunneling tools like Ligolo and Chisel.

MITIGATIONS

FBI and CISA recommend organizations implement the mitigations below to improve your cybersecurity posture on the basis of the threat actor activity and to reduce the risk of compromise by AvosLocker ransomware. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

> These mitigations apply to all critical infrastructure organizations and network defenders. The FBI and CISA recommend that software manufactures incorporate secure-by-design and -default principles and tactics into their software development practices to limit the impact of ransomware techniques (such as threat actors leveraging backdoor vulnerabilities into remote software systems), thus, strengthening the secure posture for their customers.
>
> For more information on secure by design, see CISA's Secure by Design and Default webpage and joint guide.

- Secure remote access tools by:
  - **Implementing application controls** to manage and control execution of software, including allowlisting remote access programs. Application controls should prevent installation and execution of portable versions of unauthorized remote access and other software. A properly configured application allowlisting solution will block any unlisted application execution. Allowlisting is important because antivirus solutions may fail to detect the execution of malicious portable executables when the files use any combination of compression, encryption, or obfuscation.
  - Applying recommendations in CISA's joint Guide to Securing Remote Access Software.
- **Strictly limit the use of RDP and other remote desktop services**. If RDP is necessary, rigorously apply best practices, for example [CPG 2.W]:
  - Audit the network for systems using RDP.
  - Close unused RDP ports.
  - Enforce account lockouts after a specified number of attempts.
  - Apply phishing-resistant multifactor authentication (MFA).
  - Log RDP login attempts.
- **Disable command-line and scripting activities and permissions** [CPG 2.N].
- **Restrict the use of PowerShell**, using Group Policy, and only grant access to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows operating systems (OSs) should be permitted to use PowerShell [CPG 2.E].

- **Update Windows PowerShell or PowerShell Core** to the latest version and uninstall all earlier PowerShell versions. Logs from Windows PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities [CPG 1.E, 2.S, 2.T].
- **Enable enhanced PowerShell logging** [CPG 2.T, 2.U].
  - PowerShell logs contain valuable data, including historical OS and registry interaction and possible TTPs of a threat actor's PowerShell use.
  - Ensure PowerShell instances, using the latest version, have module, script block, and transcription logging enabled (enhanced logging).
  - The two logs that record PowerShell activity are the PowerShell Windows Event Log and the PowerShell Operational Log. FBI and CISA recommend turning on these two Windows Event Logs with a retention period of at least 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as possible.

  Configure the Windows Registry to require User Account Control (UAC) approval for any PsExec operations requiring administrator privileges to reduce the risk of lateral movement by PsExec.

In addition, FBI and CISA recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the impact and risk of compromise by ransomware or data extortion actors:

- **Disable File and Printer sharing services.** If these services are required, use strong passwords or Active Directory authentication.
- **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 (e.g., hard drive, storage device, or the cloud).
- **Maintain offline backups of data,** and regularly maintain backup and restoration (daily or weekly at minimum). By instituting this practice, an organization minimizes the impact of disruption to business practices as they will not be as severe and/or only have irretrievable data [CPG 2.R]. Recommend organizations follow the 3-2-1 backup strategy in which organizations have three copies of data (one copy of production data and two backup copies) on two different media such as disk and tape, with one copy kept off-site for disaster recovery.
- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) **to comply** with NIST's standards for developing and managing password policies.
  - Use longer passwords consisting of at least 15 characters [CPG 2.B].
  - Store passwords in hashed format using industry-recognized password managers.
  - Add password user "salts" to shared login credentials.
  - Avoid reusing passwords [CPG 2.C].
  - Implement multiple failed login attempt account lockouts [CPG 2.G].
  - Disable password "hints".

  - Refrain from requiring password changes more frequently than once per year. **Note:** NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.
  - Require administrator credentials to install software.
- **Require phishing-resistant multifactor authentication** for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems [CPG 2.H].
- **Keep all operating systems, software, and firmware 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. Organizations should patch vulnerable software and hardware systems within 24 to 48 hours of vulnerability disclosure. Prioritize patching known exploited vulnerabilities in internet-facing systems [CPG 1.E].
- **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, restricting further lateral movement [CPG 2.F].
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.** To aid in detecting 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 [CPG 3.A].
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Disable unused ports** [CPG 2.V].
- **Consider adding an email banner to emails** received from outside your organization [CPG 2.M].
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.K, 2.L, 2.R].

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, FBI and CISA recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. FBI and CISA recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Table 3-7).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.

5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

FBI and CISA recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

RESOURCES

- Stopransomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts.
- The Joint Ransomware Guide provides preparation, prevention, and mitigation best practices as well as a ransomware response checklist.
- Cyber Hygiene Services and Ransomware Readiness Assessment provide no-cost cyber hygiene and ransomware readiness assessment services.

REPORTING

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with AvosLocker affiliates, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file. The FBI and CISA do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to the FBI Internet Crime Complaint Center (IC3) at ic3.gov, local FBI Field Office, or CISA via the agency's Incident Reporting System or its 24/7 Operations Center at report@cisa.gov or (888) 282-0870.

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. CISA and FBI do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA and FBI.

REFERENCES

[1] GitHub sysdream | ligolo repository

[2] GitHub jpillora | chisel repository

[3] GitHub BishopFox | sliver repository