Table of Contents

Avos Group Threat Brief

AvosLocker, Avos2, AvosLinux

The AvosLocker ransomware, developed by the Avos Group, was first advertised on dark web forums in June 2021 under a subscription-based Ransomware-as-a-Service (RaaS) model. Since its launch, Avos Group affiliates have predominantly targeted US-based companies across a range of industries.

To better ensure payment from their victims, Avos Group and its affiliates employ the 'Double Extortion' method where they first exfiltrate sensitive data from victim networks and threaten to auction the data via Avos Group's dedicated leaks site if the ransom is not paid.

In late October 2021, Avos Group announced an update to the AvosLocker ransomware, named 'Avos2', as well as a Linux-targeting and VMware Elastic Sky X Integrated (ESXi)-targeting variant, named 'AvosLinux'. The Avos Group developers claim high-performance encryption through the use of multithreading and claim to encrypt a higher amount of each file compared to their competitors.

Like many other ransomware groups, Avos Group wants to ensure victims know their files have been encrypted by their ransomware. To achieve this, the ransomware drops the ransom note titled "GET_YOUR_FILES_BACK.txt" and changes the desktop wallpaper to display the ransom note. Files encrypted by the new variants also have '.avos2' or '.avoslinux' appended to their filename.

Targeting of ESXi by ransomware actors has risen since late 2021, with other ransomware groups such as LockBit and ALPHV/BlackCat also releasing variants able to encrypt ESXi virtual machines. Targeting is likely due to the popularity of ESXi in businesses, where virtual machines often host critical services such as databases and web servers.

Victimology

A conversation between a prospective partner and Avos Group was posted on the RAMP forum on February 3, 2022, which gave insight into how Avos Group vets potential partners and how they validate potential victims.

In the conversation, Avos Group explicitly stated they only target corporations, not individuals and requested to see the "zoom" page (likely ZoomInfo, a service that sells information on businesses) of the victim the prospective partner stated they had access to. This is an interesting insight into the Avos Group's vetting process to ensure candidates are technically capable and have valid targets and those who fail may be outright rejected or required to pay a large deposit as security.

In their partnership advertisements, Avos Group states attacking Post-Soviet/Commonwealth of Independent States (CIS) countries is not allowed. This is a common rule among ransomware and cybercrime groups likely put in place to prevent action from Russian authorities.

The following graphs outline known victims of Avos Group and its affiliates since the cybercriminal group began operating in June 2021. This data is sourced from Avos Group's own leaks site and as such, this data is likely not a true reflection of all victims as some may have paid the ransom before having their data published to the leaks site.

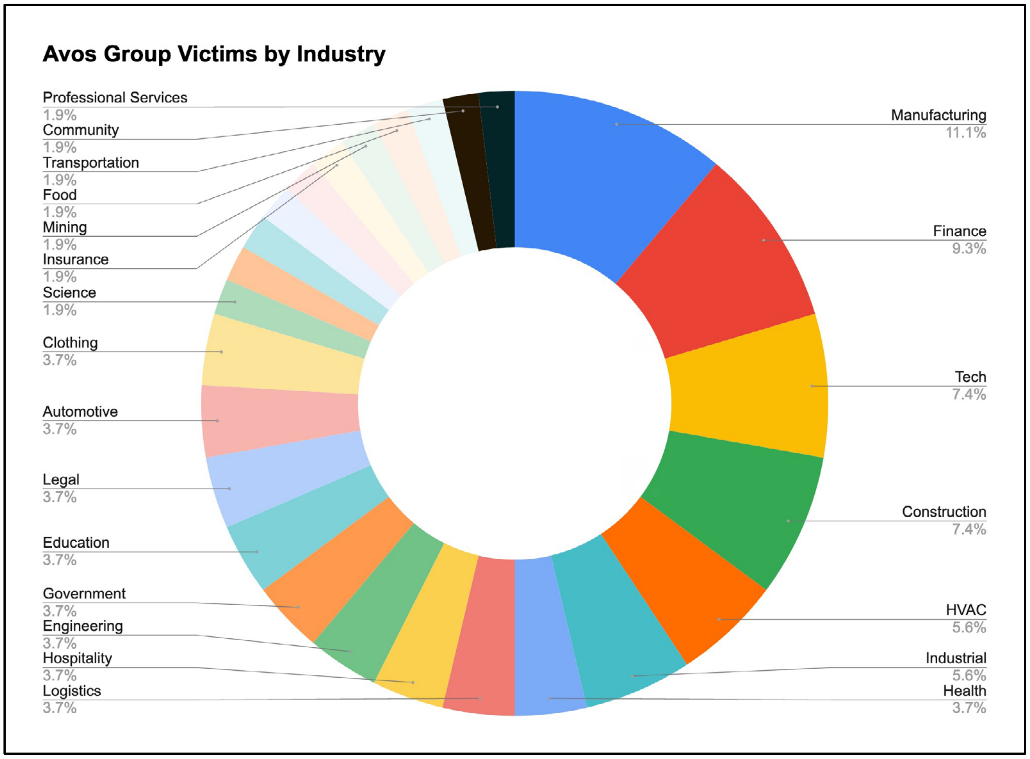
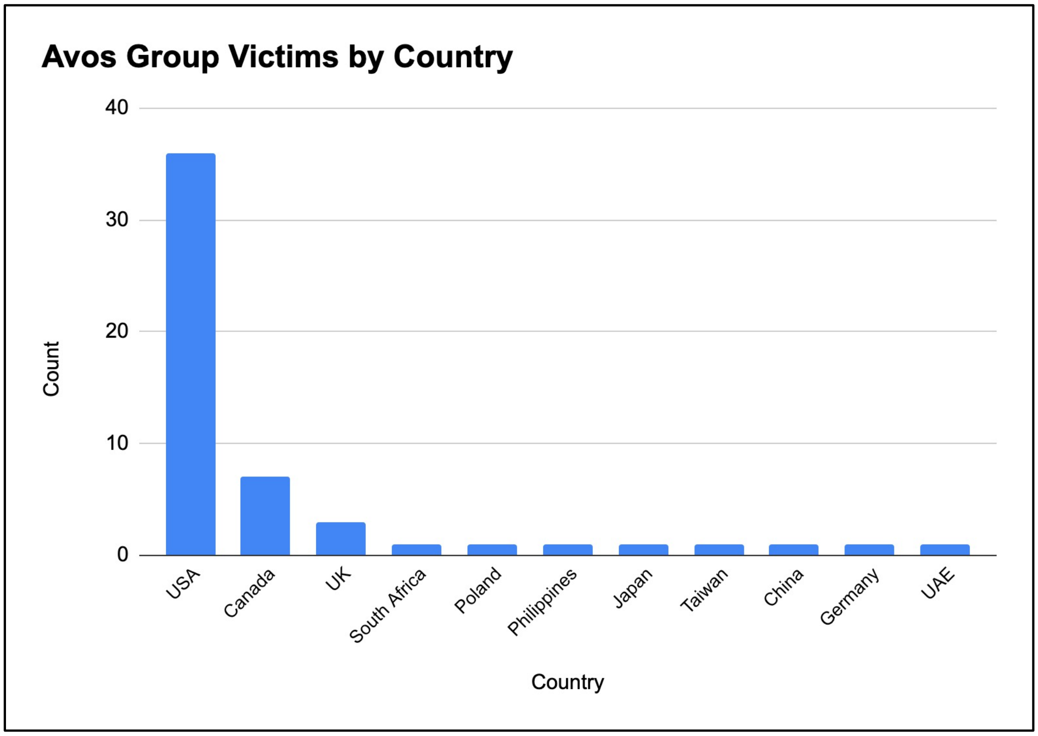


Table of Contents



Tactics, Techniques, and Procedures (TTPs)

Avos Group affiliates have been known to exploit the ProxyShell exploit to gain initial access to victim networks. ProxyShell is the name given to a group of three Microsoft Exchange vulnerabilities that allow attackers to perform unauthenticated remote code execution and upload arbitrary files with elevated privileges.

Avos Group affiliates are known to exfiltrate sensitive data from victim networks before encrypting endpoints. However, there is no confirmed technique consistently utilized by the actors in this phase of the attack.

Before encrypting Windows machines, Avos Group affiliates have been observed utilizing a unique defense evasion technique. The actors will reboot Windows machines into Safe Mode using the legitimate desktop support and remote access tool AnyDesk. Safe Mode prevents many programs, including third-party security tools, from running and increases the chance of AvosLocker ransomware successfully encrypting the victim device.

AnyDesk also allows the remote attackers to keep a foothold in the network and perform further command and control actions on the victim device as needed.

Before encryption, the Windows-targeting AvosLocker ransomware deletes volume shadow copies from the victim device and kills processes that could prevent execution before encrypting files on the device.

The ransomware also drops the ransom note named "GET_YOUR_FILES_BACK.txt" in each directory it encrypts and changes the desktop wallpaper of the encrypted device to the ransom note.

Table of Contents

Before encrypting ESXi-related files, AvosLinux kills ESXi VMs with the following command:

```
esxcli --formatter=csv --format-param=fields==”WorldID,DisplayName”
vm process list | tail -n +2 | awk -F $’,’ ‘{system(“esxcli vm
process kill -- type=force --world-id=” $1)}’
```

Once devices are encrypted and the ransom notes have been dropped, victims are required to navigate to Avos Group's TOR site and enter their unique ID provided in the ransom note. Failure to do so will result in the victim's data being auctioned or published on Avos Group's leaks site.

Mitre ATT&CK

The following maps known AvosLocker ransomware attack TTPs to MITRE ATT&CK:

Initial Access

- **Exploit Public-Facing Application (T1190) -** AvosLocker actors have exploited the ProxyShell vulnerabilities on Microsoft Exchange servers to gain initial access.

Execution

- **Command and Scripting Interpreter-** Windows Command Shell (T1059.003) - AvosLocker actors have used Windows Command Shell to perform actions on victim devices.
- **Command and Scripting Interpreter-** Unix Shell (T1059.004) - AvosLocker actors have used the Unix shell to perform actions on victim devices.

Persistence

- **External Remote Services (T1133) -** AvosLocker actors have used RDP software to maintain access to devices in victim networks..

Defense Evasion

- **Hide Artifacts: Hidden Window (T1564.003) -** AvosLocker launches processes with a hidden window.
- **Impair Defenses: Safe Mode Boot (T1562.009) -** AvosLocker reboots Windows machines into Safe Mode before executing the ransomware to evade defensive tools.
- **Modify Registry (T1112) -** AvosLocker modifies the registry to change the desktop wallpaper of infected devices.
- **Signed Binary Proxy Execution: Rundll32 (T1218.011) -** AvosLocker has used 'rundll32.exe' to prevent the desktop wallpaper from automatically updating from the ransom note.

Discovery

- **System Information Discovery (T1082) -** AvosLocker is able to collect information on infected machines.

Command and Control

- **Remote Access Software (T1219) -** AvosLocker actors have been observed using the RDP tool AnyDesk for command and control of victim devices.

Impact

- **Service Stop (T1489) -** AvosLocker has the ability to stop services and processes.
- **Inhibit System Recovery (T1490) -** AvosLocker can delete shadow copies to prevent victims from restoring files without paying the ransom.
- **Defacement: Internal Defacement (T1491.001) -** AvosLocker changes the background wallpaper of encrypted devices with a ransom note.
- **Data Encrypted for Impact (T1486) -** AvosLocker encrypts files and appends the '.avos2' file extension during the process.

Table of Contents

Mitigations/Defenses

Implementing a strong foundation of security controls is recommended to defend your network against AvosLocker.

The Center for Internet Security (CIS) Controls are a prioritized set of safeguards designed to defend against cyber attacks. The CIS Controls have three tiers, known as Implementation Groups, that build on each other.

The following table maps AvosLocker's MITRE ATT&CK techniques to CIS v8 Safeguards:

— IG1 — IG2 — IG3

MITRE ATT&CK	CIS Safeguards
Exploit Public-Facing Application (T1190)	**IG1** 4.4: Implement and Manage a Firewall on Servers 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process 7.1: Establish and Maintain a Vulnerability Management Process 7.2: Establish and Maintain a Remediation Process 7.3: Perform Automated Operating System Patch Management 7.4: Perform Automated Application Patch Management 12.1: Ensure Network Infrastructure is Up-to-Date
Command and Scripting Interpreter: Windows Command Shell (T1059.003)	**IG2** 2.5: Allowlist Authorized Software **IG3** 2.7: Allowlist Authorized Scripts
Command and Scripting Interpreter: Unix Shell (T1059.004)	**IG2** 2.5: Allowlist Authorized Software **IG3** 2.7: Allowlist Authorized Scripts

External Remote Services (T1133)	**IG1** 2.3: Address Unauthorized Software 4.1: Establish and Maintain a Secure Configuration Process 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers 6.3: Require MFA for Externally-Exposed Applications 6.4: Require MFA for Remote Network Access 6.5: Require MFA for Administrative Access
Hide Artifacts: Hidden Window (T1564.003)	**IG2** 2.5: Allowlist Authorized Software
Modify Registry (T1112)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process
Signed Binary Proxy Execution: Rundll32 (T1218.011)	**IG2** 10.5: Enable Anti-Exploitation Features
Remote Access Software (T1219)	**IG1** 4.2 :Establish and Maintain a Secure Configuration Process for Network Infrastructure 4.4: Implement and Manage a Firewall on Servers
Service Stop (T1489)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 4.7: Manage Default Accounts on Enterprise Assets and Software 5.3: Disable Dormant Accounts 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts 6.1: Establish an Access Granting Process 6.2: Establish an Access Revoking Process
Inhibit System Recovery (T1490)	**IG1** 4.1: Establish and Maintain a Secure Configuration Process 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data
Defacement: Internal Defacement (T1491.001)	**IG1** 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data
Data Encrypted for Impact (T1486)	**IG1** 11.1: Establish and Maintain a Data Recovery Process 11.2: Perform Automated Backups 11.3: Protect Recovery Data 11.4: Establish and Maintain an Isolated Instance of Recovery Data

Table of Contents

Detection Opportunities

The following detection opportunities are mapped to MITRE ATT&CK v9 methods, CIS v8 Safeguards, and provide appropriate Red Canary Atomic Red Team tests to undertake for validation:

Detection Opportunity 1: Shadow Copy and System State Backup Deletion

MITRE ATT&CK: Inhibit System Recovery (T1490)

CIS Control(s): 4.1, 4.2, 4.7, 5.3, 5.4, 7.1, 7.2, 7.3, 11.1, 11.2, 11.3, 11.4

Red Canary Atomic Red Team Test(s): T1490 - Inhibit System Recovery Test #1

ILike many other ransomware variants, AvosLocker and its successor, Avos2, deletes volume shadow copies from endpoints before encrypting files. This is intended to prevent victims from recovering their devices without paying the ransom.

Insight into PowerShell commands will allow you and your team to defend against malicious actors utilizing PowerShell to perform their activities. This can be done in a number of ways including enabling PowerShell Transcription and exporting the transcripts to a remote location for analysis or by deploying an Endpoint Detection and Response (EDR) solution to your corporate environment.

Searching for the following command within PowerShell logs will allow you to detect potentially malicious pre-deployment activity on your endpoints:

Command: vssadmin.exe delete shadow*

The Sigma rule 'Shadow Copies Deletion Using Operating Systems Utilities' covers malicious vssadmin commands as well as other similar commands known to be used by malicious actors. Using this Sigma rule for improving defenses is highly recommended.

Detection Opportunity 2: Detect AnyDesk

MITRE ATT&CK: T1219

CIS Control(s): 4.2, 4.4

Red Canary Atomic Red Team Test(s): Atomic Test #2 - AnyDesk Files Detected Test on Windows

AnyDesk is legitimate desktop support and remote access tool that has been used by various malicious actors, including Avos actors. Avos Group actors have been observed installing AnyDesk on victim devices to use as a Command-and-Control tool as well as utilizing its ability to remotely reboot Windows devices into Safe Mode in order to disable security applications that could prevent the AvosLocker ransomware from successfully deploying.

By regularly auditing endpoints in your network for the installation of AnyDesk you are preventing unauthorized access to your network from malicious actors, including Avos Group affiliates. Given AnyDesk is a legitimate tool, it is important to understand whether the application is installed for legitimate reasons before removing it from endpoints.

Red Canary's T1219 Atomic Test #2 - AnyDesk Files Detected Test on Windows is a helpful and easy-to-run validation to ensure your detection for AnyDesk installations is functioning properly.

Table of Contents

Indicators of Compromise (IOCs)

IOC	Notes
.avos	File extension
.avos2	File extension
.avoslinux	File extension
7c935dcd672c4854495f41008120288e8e1c144089f1f06a23bd0a0f52a544b1	ELF SHA256 hash
10ab76cd6d6b50d26fde5fe54e8d80fceeb744de8dbafddff470939fac6a98c4	ELF SHA256 hash
c0a42741eef72991d9d0ee8b6c0531fc19151457a8b59bdcf7b6373d1fe56e02	ELF SHA256 hash
f810deb1ba171cea5b595c6d3f816127fb182833f7a08a98de93226d4f6a336f	ELF SHA256 hash
http://avosqxh72b5ia23dl5fgwcpndkctuzqvh2iefk5imp3pi5gfhel5klad.onion	AvosLocker TOR domain hardcoded in ELF samples
http://avosjon4pfh3y7ew3jdwz6ofw7lljcxlbk7hcxxmnxlh5kvf2akcqjad.onion	AvosLocker TOR domain hardcoded in ELF samples

References/Appendix/Resources

https://www.sophos.com/en-us/press-office/press-releases/2021/12/avoslocker-ransomware-uses-anydesk-in-safe-mode-to-launch-attacks

https://www.cyber.gov.au/acsc/view-all-content/alerts/microsoft-exchange-proxyshell-targeting-australia

https://blog.cyble.com/2022/01/17/avoslocker-ransomware-linux-version-targets-vmware-esxi-servers/

https://therecord.media/avoslocker-ransomware-gang-to-auction-the-data-of-victims-who-dont-pay/

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_shadow_copies_deletion.yml