Hive Pro®

Threat Level

Red

CISA: AA23-284A

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

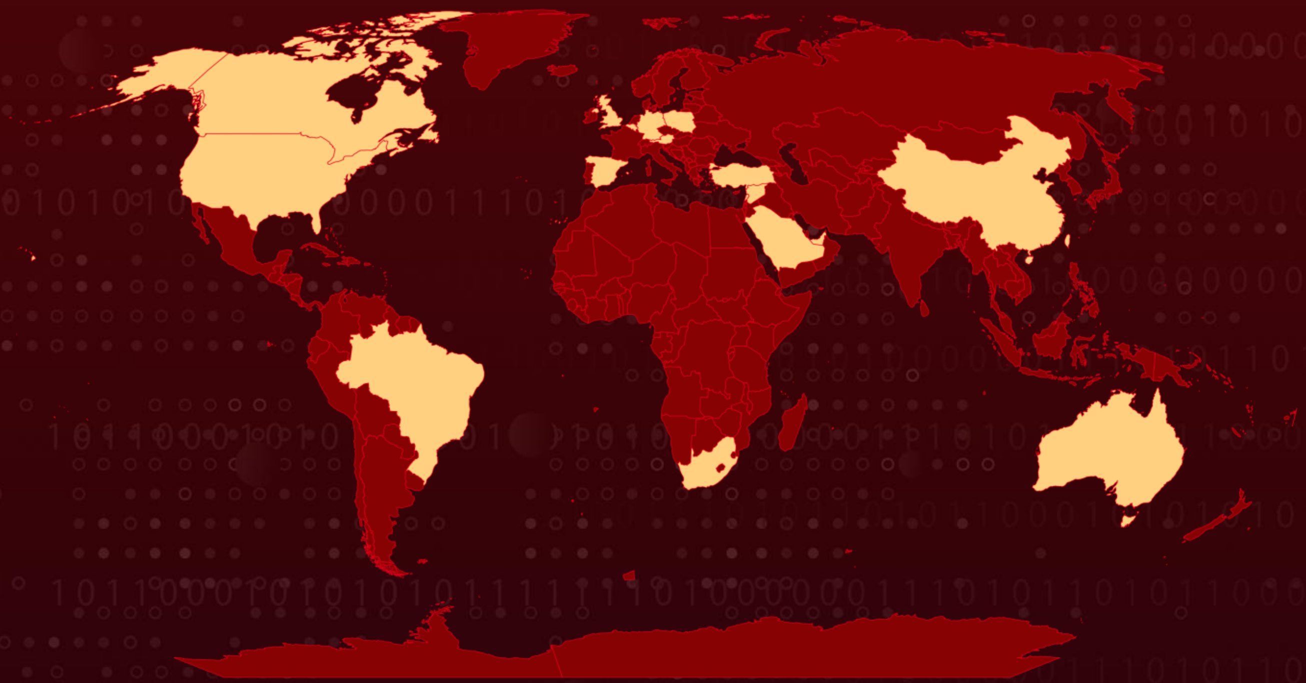
In-Depth Analysis of AvosLocker Ransomware

Date of Publication	Admiralty Code	TA Number
October 12, 2023	A1	TA2023413

Summary

First Appearance: July 4, 2021
Targeted Countries: United States, Syria, Saudi , Arabia, Germany, Spain, Belgium, Turkey, United Arab , Emirates, United Kingdom, Canada, China, Taiwan, Lebanon, Poland, South Africa , United Arab Emirates, Australia, Austria, Brazil, Columbia, Argentina, India, Italy, Philippines, Israel, Saudi Arabia
Affected Platforms: Windows, Linux, and VMware ESXi
Targeted Industries: Real Estate, Education, Financial Services, Food and Beverage, Government, Energy, Healthcare, Manufacturing, Media, Telecommunications, Transportation, Technology
Malware: AvosLocker ransomware
Attack: AvosLocker also known as Avos, is a ransomware-as-a-service that targets critical infrastructure organizations, primarily in the US, and has expanded to target both Windows and Linux systems. Its affiliates use legitimate software, custom scripts, polymorphic techniques, and threaten data leaks if ransoms are not paid

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-31206	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✗	✓
CVE-2021-31207	Microsoft Exchange Server Security Feature Bypass Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-34473	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-34523	Microsoft Exchange Server Privilege Escalation Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2021-26855	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✓	✓	✓
CVE-2021-40539	Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability	Zoho ManageEngine	✓	✓	✓
CVE-2021-44228	Apache Log4j2 Deserialization of Untrusted Data Vulnerability	Apache Log4j2	✓	✓	✓
CVE-2021-45046	Apache Log4j2 Deserialization of Untrusted Data Vulnerability	Apache Log4j2	✗	✗	✓
CVE-2021-45105	Apache Log4j2 Denial of Service Vulnerability	Apache Log4j2	✗	✗	✓
CVE-2021-44832	Apache Log4j2 Remote Code Execution Vulnerability	Apache Log4j2	✗	✗	✓
CVE-2022-26134	Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability	Atlassian Confluence Server and Data Center	✓	✓	✓
CVE-2018-19320	GIGABYTE Multiple Products Unspecified Vulnerability	GIGABYTE Multiple Products	✗	✓	✓

Attack Details

#1

AvosLocker, also known as Avos, was first detected on July 4, 2021, and operates as a ransomware-as-a-service (RaaS), using a double extortion technique. It has compromised organizations in various critical infrastructure sectors primarily in the United States. AvosLocker is written in the C/C++ programming language and was initially compiled to work with Windows systems only. However, in October 2021, it evolved to support Linux systems, including ESXi virtual machines.

#2

AvosLocker affiliates gain access to organizations' networks using legitimate software and open-source tools, and then employ double extortion tactics, threatening to leak or publish stolen data. They gain initial access through compromised RDP/VPN credentials or by exploiting vulnerabilities in public-facing applications.

#3

A total of 12 different vulnerabilities have been found to be exploited by this ransomware. Once initial access is achieved, AvosLocker downloads AnyDesk and a webshell onto the system. It uses a variety of tools, including native Windows tools, for lateral movement and ultimately executes the ransomware payload.

#4

AvosLocker affiliates employ various tools and methods during ransomware operations, such as remote system administration tools, scripts for executing native Windows tools, open-source network tunneling tools, command and control tools, and credential harvesting tools. They also use legitimate software for data exfiltration. Furthermore, AvosLocker affiliates may use custom PowerShell and batch scripts for lateral movement and privilege escalation and may upload custom webshells for network access.

#5

The ransomware encrypts files with the extensions ".avos" and ".avos2" on Windows systems, and for Linux systems, it adds the ".AvosLinux" extension. It employs polymorphic techniques to change its code to evade detection and runs the computer in safe mode after disabling local security programs.

#6

Upon attempting to access the encrypted files, a text file titled "GET_YOUR_FILES_BACK.txt" (ransom note) appears on the desktop. This note guides the victim to an onion site where the victim must provide a specified ID from the .txt file to receive details about the ransom amount and engage in negotiation. If the ransom is not paid, AvosLocker threatens to sell the data.

#7

Phone calls and distributed denial-of-service (DDoS) attacks may be used during negotiations with victims. The ransomware also creates mutex objects to avoid re-infecting systems, encrypts files with specific extensions, and leaves a ransom note in directories.

Recommendations

Conduct Regular Data Backups: Implement a robust data backup strategy that includes regular backups of critical data and systems, ad hoc and periodic backup restoration test. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom. Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection.

Regularly Update and Patch Systems: Keep all software, including operating systems and applications, up to date with the latest security patches and updates. Vulnerabilities in outdated software can be exploited by AvosLocker.

Secure Remote Access: Implement application controls to manage and control the execution of software, including allowlisting remote access programs. Limit the use of Remote Desktop Protocol (RDP) and enforce best practices for its use. Apply phishing-resistant multifactor authentication for remote access. Log RDP login attempts.

Network Segmentation: Use network segmentation to isolate critical systems and data from less critical areas, helping to contain the spread of ransomware.

Endpoint Security: Deploy robust endpoint security solutions, including antivirus and anti-malware software, to detect and prevent AvosLocker infections.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0040 Impact	TA0010 Exfiltration	TA0005 Defense Evasion
TA0010 Exfiltration	TA0001 Initial Access	TA0003 Persistence	TA0006 Credential Access
T1133 External Remote Services	T1059.001 PowerShell	T1059.003 Windows Command Shell	T1059 Command and Scripting Interpreter
T1047 Windows Management Instrumentation	T1505.003 Web Shell	T1505 Server Software Component	T1555 Credentials from Password Stores
T1572 Protocol Tunneling	T1486 Data Encrypted for Impact		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	6cc510a772d7718c95216eb56a84a96201241b264755f28875e685f06e95e1a2, 1198fb9117776809b11a19000161377384957bee846f7b25a610fc8ca082eb37, 794f3d25c42d383fad485f9af1d6d7c0508bcfe8ed80a1afea0e0b51bf92bc81, bff12a83b1fc2e0ad0000ad9b68abc8eada559bb1094caaf5b9f52887df23705, 91ecad5a2010a6d8b6b738a88a1e3db30bd0e4fbc647cd49ecadebdf0a357643, fe23d4b7a9db3c937523afecdbe14969987c27f35b9bb9c90f656bcd897bcb87, df480deb191b335dcbc3d4fc5d59594cb38caee2aaef8d877fbbc573de741301, 01792043e07a0db52664c5878b253531b293754dc6fd6a8426899c1a66ddd61f, e737c901b80ad9ed2cd800fec7c2554178c8afab196fb55a0df36acda1324721, c0a42741eef72991d9d0ee8b6c0531fc19151457a8b59bdcf7b6373d1fe56e02, 29910ea42c8e2abb22d5a88053e1725c93a104e61560a2f8d88716d619bcaa08, 27cd3e759ec4858adaea63050ad1fc22e4850c1e157d88c0943c2589fa39b5a4, 373a791f058539d72983e38ebe68e98132fcf996d04e9a181145f22a96689386, bd88d415032eb24091c352fc0732b31116f44a78d9333037bd7608289608d3cd, e62c0bdf69b88a5bd95872cbcf4da4de4eef226bc9ef0452ee652eeee519b15a, fb544e1f74ce02937c3a3657be8d125d5953996115f65697b7d39e237020706f, 43b7a60c0ef8b4af001f45a0c57410b7374b1d75a6811e0dfc86e4d60f503856, 10ab76cd6d6b50d26fde5fe54e8d80fceeb744de8dbafddff470939fac6a98c4, 7c935dcd672c4854495f41008120288e8e1c144089f1f06a23bd0a0f52a544b1, 0cd7b6ea8857ce827180342a1c955e79c3336a6cf2000244e5cfd4279c5fc1b6, a0b4e3d7e4cd20d25ad2f92be954b95eea44f8f1944118a3194295c5677db749,

TYPE	VALUE
SHA256	e68f9c3314beee640cc32f08a8532aa8dcda613543c54a83680c21d7cd49ca0f, ad5fd10aa2dc82731f3885553763dfd4548651ef3e28c69f77ad035166d63db7, 48dd7d519dbb67b7a2bb2747729fc46e5832c30cafe15f76c1dbe3a249e5e731, 1e21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07db0ff
SHA1	9c8f5c136590a08a3103ba3e988073cfd5779519, 05c63ce49129f768d31c4bdb62ef5fb53eb41b54, dab33aaf01322e88f79ffddcbc95d1ad9ad97374, 6f110f251860a7f6757853181417e19c28841eb4, 67f0c8d81aefcfc5943b31d695972194ac15e9f2, 2d1ce0231cf8ff967c36bbfc931f3807ddba765c, 2f3273e5b6739b844fe33f7310476afb971956dd
MD5	f659d1d15d2e0f3bd87379f8e88c6b42, e09183041930f37a38d0a776a63aa673, 31f8eedc2d82f69ccc726e012416ce33, d3cafcd46dea26c39dec17ca132e5138, 504bd1695de326bc533fde29b8a69319, eb45ff7ea2ccdcceb2e7e14f9cc01397, 829f2233a1cd77e9ec7de98596cd8165, 6ebd7d7473f0ace3f52c483389cab93f, 10ef090d2f4c8001faadb0a833d60089, 8227af68552198a2d42de51cded2ce60, 9d0b3796d1d174080cdfdbd4064bea3a, af31b5a572b3208f81dbf42f6c143f99, 1892bd45671f17e9f7f63d3ed15e348e, cc68eaf36cb90c08308ad0ca3abc17c1, 646dc0b7335cffb671ae3dfd1ebefe47, 609a925fd253e82c80262bad31637f19, c6a667619fff6cf44f447868d8edd681, 3222c60b10e5a7c3158fd1cb3f513640, 90ce10d9aca909a8d2524bc265ef2fa4, 44a3561fb9e877a2841de36a3698abc0, 5cb3f10db11e1795c49ec6273c52b5f1, 122ea6581a36f14ab5ab65475370107e, c82d7be7afdc9f3a0e474f019fb7b0f7
Email Address	keishagrey994@outlook[.]com

TYPE	VALUE
Virtual Currency Wallets	a6dedd35ad745641c52d6a9f8da1fb09101d152f01b4b0e85a64d21c2a0845ee, bfacebcafff00b94ad2bff96b718a416c353a4ae223aa47d4202cdbc31e09c92, 418748c1862627cf91e829c64df9440d19f67f8a7628471d4b3a6cc5696944dd, bc1qn0u8un00nl6uz6uqrw7p50rg86gjrx492jkwfn

Recent Breaches

https://www.bluefield.edu/
https://www.bluefield.edu/
https://www.roseman.edu/
https://www.emmanuel.edu/
https://www.dijones.com.au/
https://cavalierhospital.com/
https://www.laragh.com/
https://sunpowermarine.com/
https://vmedia.ca/
https://maneygordon.com/
https://tiptoppoultry.com/
https://www.hainppc.com/
https://desman.com/
https://acesconn.com/
https://entigrity.com/
https://www.methodistfamily.org/
https://titlecashnow.com/
https://www.openmribala.com/
https://www.cnsu.edu/
https://www.mitchellewis.com/
https://ultralifecorporation.com/
https://www.hamiltonparker.com/
https://schandy.com.uy/
https://cannondesign.com/
https://www.wescoturf.com/
https://buckeyepackaging.com/
https://globalminingproducts.net/
https://memtechacoustical.com/
https://cambiangroup.com/
https://azlaborforce.com/
https://www.corporate-interiors.com/

Patch Details

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31206

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855

https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html

https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/

https://logging.apache.org/log4j/2.x/security.html

https://issues.apache.org/jira/browse/LOG4J2-3293

https://jira.atlassian.com/browse/CONFSERVER-79016

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-284a

https://www.cisa.gov/news-events/alerts/2022/03/22/fbi-and-fincen-release-advisory-avoslocker-ransomware

https://www.hivepro.com/avoslocker-ransomware-group-has-targeted-50-organizations-worldwide/

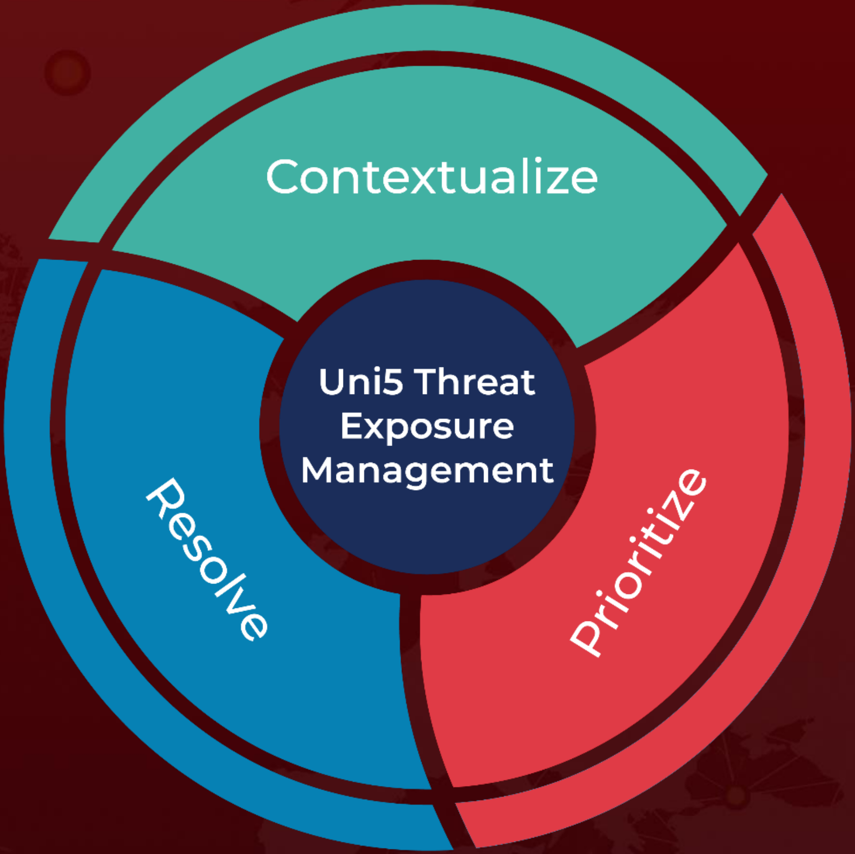
https://www.securin.io/all-about-avoslocker-ransomware/

https://www.securin.io/cve-2022-26134-a-new-rce-atlassian-bug-exploited-by-ransomware-gangs/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 12, 2023 • 8:00 AM

More at www.hivepro.com