Hive Pro

THREAT ADVISORY

AvosLocker Ransomware group has targeted 50+ Organizations Worldwide

TA2022073

Threat Level RED

Publish Date – Mar 23, 2022

Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency released threat advisories on AvosLocker Ransomware. It is a Ransomware as a Service (RaaS) affiliate-based group that has targeted 50+ organizations in critical infrastructure sectors such as financial services, manufacturing plants, and government facilities in countries such as the United States, Saudi Arabia, the United Kingdom, Germany, Spain, and the United Arab Emirates, among others. After it's affiliates infect targets, AvosLocker claims to handle ransom negotiations, as well as the publishing and hosting of exfiltrated victim data.

The AvosLocker ransomware is a multi-threaded C++ Windows executable that operates as a console application and displays a log of actions performed on victim computers. For the delivery of the ransomware payload, the attackers use spam email campaigns as the initial infection vector. The threat actors exploits Proxy Shell vulnerabilities CVE-2021-31206, CVE-2021-31207, CVE-2021-34523, and CVE-2021-34473, as well as CVE-2021-26855 to gain access to victim's machine and then they deploy Mimikatz to steal passwords. Furthermore, threat actors can use the detected credentials to get RDP access to the domain controller and then exfiltrate data from the compromised machine. Finally, the attacker installs AvosLocker ransomware on the victim's computer and then encrypts the victim's documents and files with the ".avos" extension. The actor then leaves a ransom letter in each directory named "GET YOUR FILES BACK.txt" with a link to an AvosLocker .onion payment site.

The Organizations can mitigate the risk by following the recommendations:

- Keep all operating systems and software up to date.
- Remove unnecessary access to administrative shares.
- Maintain offline backups of data and Ensure all backup data is encrypted and immutable.

The MITRE TTPs commonly used by Avoslocker are:
TA0001: Initial Access
TA0002: Execution
TA0007: Discovery
TA0040: Impact
T1566: Phishing
T1204: User Execution
T1082: System Information Discovery
T1490: Inhibit System Recovery
T1489: Service Stop
T1486: Data Encrypted for Impact

Actor Details

Name	Target Locations	Target sectors	Motive
AvosLocker	United States, Syria, Saudi Arabia, Germany, Spain, Belgium, Turkey, United Arab Emirates, United Kingdom, Canada, China, Taiwan, Lebanon, Poland, South Africa	Professional Services, Logistics, Construction & Engineering, Fashion, Retail, Government, Technology, Oil and Gas, Hospitality, Electrical Equipment	Ecrime, Information theft, and Financial gain

Hive Pro

THREAT ADVISORY

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-31206	Exchange 2013 CU23 versions before 15.0.1497.15, Exchange 2016 CU19 versions before 15.1.2176.12, Exchange 2016 CU20 versions before 15.1.2242.5, Exchange 2019 CU8 versions before 15.2.792.13, and Exchange 2019 CU9 versions before 15.2.858.9	cpe:2.3:a:microsoft:*:*:*:*:*:*:*:*	ProxyShell Remote Code Execution	CWE-94
CVE-2021-31207				CWE-254
CVE-2021-34523				CWE-269
CVE-2021-34473				CWE-94
CVE-2021-26855	Exchange 2013 Versions before 15.00.1497.012, Exchange 2016 CU18 before 15.01.2106.013, Exchange 2016 CU19 before 15.01.2176.009, Exchange 2019 CU7 before 15.02.0721.013, and Exchange 2019 CU8 before 15.02.0792.010			CWE-918

Indicators of Compromise (IoCs)

Type	Value
SHA-256	10ab76cd6d6b50d26fde5fe54e8d80fceeb744de8dbafddff470939fac6a98c4, 7c935dcd672c4854495f41008120288e8e1c144089f1f06a23bd0a0f52a544b1, e737c901b80ad9ed2cd800fec7c2554178c8afab196fb55a0df36acda1324721, 0cd7b6ea8857ce827180342a1c955e79c3336a6cf2000244e5cfd4279c5fc1b6, a0b4e3d7e4cd20d25ad2f92be954b95eea44f8f1944118a3194295c5677db749, 1e21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07db0ff
SHA-1	9c8f5c136590a08a3103ba3e988073cfd5779519, 05c63ce49129f768d31c4bdb62ef5fb53eb41b54, dab33aaf01322e88f79ffddcbc95d1ad9ad97374, 6f110f251860a7f6757853181417e19c28841eb4, 67f0c8d81aefcfc5943b31d695972194ac15e9f2, 2f3273e5b6739b844fe33f7310476afb971956dd
MD5	f659d1d15d2e0f3bd87379f8e88c6b42, e09183041930f37a38d0a776a63aa673, 31f8eedc2d82f69ccc726e012416ce33, d3cafcd46dea26c39dec17ca132e5138, 504bd1695de326bc533fde29b8a69319, eb45ff7ea2ccdcceb2e7e14f9cc01397

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31206
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31207
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855

Recent Breaches

https://www.unical.com/
https://www.paccity.net/
https://www.gigabyte.com/

References

https://www.cisa.gov/uscert/ncas/current-activity/2022/03/22/fbi-and-fincen-release-advisory-avoslocker-ransomware