AvosLocker ransomware targets vulnerable Microsoft Exchange Servers

17th March 2022

Orpheus severity score: 63

Affiliates of AvosLocker have been actively targeting Microsoft Exchange Servers vulnerable to CVE-2021-34473, CVE-2021-34523, CVE-2021-31207 (collectively known as ProxyShell), and CVE-2021-26855 to gain a foothold on US company networks across the financial services, manufacturing and government sectors.

AvosLocker is a ransomware-as-a-service (RaaS) group active since June 2021. Like many other RaaS variants, AvosLocker:

- engages in double extortion, leaking files stolen from non-compliant victims on a dedicated leak website
- threatens victims to stage distributed-denial-of-service attacks during negotiations as further leverage
- deliberately pursues high-profile organisations to maximise ransom returns – a tactic known as “big game hunting”
- features a module designed to target VMware EsXi hypervisor servers
- The targeting of Microsoft Exchange Servers vulnerable to ProxyShell and CVE-2021-26855 showcases how AvosLocker operators and affiliates conform with tactics, techniques and procedures widely used by ransomware extortionists and other threat actor groups.

CVE-2021-26855 (CVSS 9.8|OVSS: 100) has been actively exploited since at least March 2021 by a plethora of nation-state and criminal groups. Similarly, the ProxyShell vulnerabilities (CVE-2021-34473 [CVSS 9.8|OVSS: 93], CVE-2021-34523 [CVSS 9.8|OVSS: 74], CVE-2021-31207 [CVSS 7.2|OVSS: 65]), also saw extensive exploitation, which includes efforts from ransomware extortionists.

+44 (0)203 8232 999
info@secrutiny.com
www.secrutiny.com

It also reiterates the ongoing attractiveness of the vulnerabilities within the threat landscape and the need for companies relying on Microsoft Exchange Servers to ensure these are running with the latest available patches.

Threat Subcategory	Ransomware
Sectors	Manufacturing | Financial Services | Government
Objective	Extortion ransomware | Extortion data leak | Extortion DDoS
Target System	Servers
Countries & Target	United States of America
Malware & Tools	AvosLocker
Target Software	Microsoft Exchange
CVE	CVE-2021-34473 | CVE-2021-34523 | CVE-2021-31207 | CVE-2021-26855
Infection Vectors	Scanning/Enumeration
Sources	https://www.ic3.gov/Media/News/2022/220318.pdf