Microsoft Exchange servers hacked to deploy Hive ransomware

By Bill Toulas

Published: 2022-04-20 · Archived: 2026-04-05 13:04:58 UTC

A Hive ransomware affiliate has been targeting Microsoft Exchange servers vulnerable to ProxyShell security issues to deploy various backdoors, including Cobalt Strike beacon.

From there, the threat actors perform network reconnaissance, steal admin account credentials, exfiltrate valuable data, ultimately deploying the file-encrypting payload.

The details come from security and analytics company Varonis, who was called in to investigate a ransomware attack on one of its customers.


DIE LINKE.
0:00

A widely abused initial access

ProxyShell is a set of three vulnerabilities in the Microsoft Exchange Server that allow remote code execution without authentication on vulnerable deployments. The flaws have been used by multiple threat actors, including ransomware like Conti, BlackByte, Babuk, Cuba, and LockFile, after exploits became available.

The flaws are tracked as CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207, and their severity rating ranges from 7.2 (high) to 9.8 (critical).

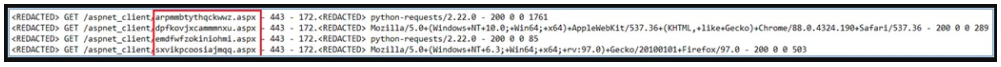
The security vulnerabilities are considered fully patched as of May 2021, but extensive technical details about them were only made available in August 2021, and soon after that, malicious exploitation started [1, 2].

The fact that Hive's affiliate was successful in exploiting ProxyShell in a recent attack shows that there is still room for targeting vulnerable servers.

From access to encryption

Following the exploitation of ProxyShell, the hackers planted four web shells in an accessible Exchange directory, and executed PowerShell code with high privileges to download Cobalt Strike stagers.

The web shells used in this particular attack were sourced from a public Git repository and were merely renamed to evade detection during potential manual inspections.



Randomly-named web shells *(Varonis)*

From there, the intruders used Mimikatz, a credentials stealer, to snatch the password of a domain admin account and perform lateral movement, accessing more assets in the network.

```
mimikatz # sekurlsa::pth /user:Administrator /domain:<REDACTED> /ntlm:<REDACTED> /run:cmd
user    : Administrator
domain  : <REDACTED>
program : cmd
impers. : no
NTLM    : <REDACTED>
  |  PID  7132
  |  TID  10320
  |  LSA Process is now R/W
  |  LUID 6 ; 2617170828 (00000006:9bfedb8c)
  \_ msv1_0   - data copy @ 000001558FB9EA80 : OK !
  \_ kerberos - data copy @ 000001558BE24668
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace @ 000001558EC9F5B8 (32) -> null
```

Launching a new command prompt on the affected system *(Varonis)*

Next, the threat actors performed extensive file search operations to locate the most valuable data to pressure the victim into paying a larger ransom.

Varonis analysts have seen remnants of dropped network scanners, IP address lists, device and directory enumerations, RDPs to backup servers, scans for SQL databases, and more.

One notable case of network scanning software abuse was "SoftPerfect", a lightweight tool that the threat actor used for enumerating live hosts by pinging them and saving the results on a text file.

Finally, and after all files had been exfiltrated, a ransomware payload named "Windows.exe" was dropped and executed on multiple devices.

Before encrypting the organization's files, the Golang payload deleted shadow copies, disabled Windows Defender, cleared Windows event logs, killed file-binding processes, and stopped the Security Accounts Manager to incapacitate alerts.

Command	Description
vssadmin.exe delete shadows /all /quiet	Deleting the shadow copies from the machine to inhibit system recovery
net.exe stop "SamSs" /y	Stops the Security Accounts Manager to prevent sending alerts to SIEM system
reg.exe add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f	Disables Windows Defender to avoid detection
wevtutil.exe cl security	Clearing the Windows Security Event Logs

Commands executed by the final payload *(Varonis)*

Hive evolution

Hive has gone a long way since it was first observed in the wild back in June 2021, having a successful start that prompted the FBI to release a dedicated report on its tactics and indicators of compromise.

In October 2021, the Hive gang added Linux and FreeBSD variants, and in December it became one of the most active ransomware operations in attack frequency.

Last month, researchers at Sentinel Labs reported on a new payload-hiding obfuscation method employed by Hive, which indicates active development.

Source: https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-hive-ransomware/