Hive Pro

# THREAT ADVISORY

## Hive Ransomware targets organizations with ProxyShell exploit

**TA2022098**

**Threat Level** RED

**Publish Date –** April 22, 2022

**Hive Ransomware** has been active since its discovery in June 2021, and it is constantly deploying different backdoors, including the **Cobalt Strike** beacon, on Microsoft Exchange servers that are vulnerable to **ProxyShell** (CVE-2021-31207, CVE-2021-34473 and CVE-2021-34523) security flaws. The threat actors then conduct network reconnaissance, obtain admin account credentials, and exfiltrate valuable data before deploying the file-encrypting payload.

Hive and their affiliates access their victims' networks by a variety of methods, including phishing emails with malicious attachments, compromised VPN passwords, and exploiting weaknesses on external-facing assets. Furthermore, Hive leaves a plain-text ransom letter threatening to disclose the victim's data on the TOR website **'HiveLeaks'** if the victim does not meet the attacker's terms.

The Organizations can mitigate the risk by following the recommendations:

- Use multi-factor authentication.
- 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.
- Enable protected files in the Windows Operating System for critical files.

The MITRE ATT&CK TTPs used by **Hive Ransomware** are:
TA0001: Initial Access
TA0002: Execution
TA0003: Persistence
TA0004: Privilege Escalation
TA0005: Defense Evasion
TA0006: Credential Access
TA0007: Discovery
TA0008: Lateral Movement
TA0009: Collection
TA0011: Command and Control
TA0010: Exfiltration
TA0040: Impact
T1190: Exploit Public-Facing Application
T1566: Phishing
T1566.001: Spear-phishing attachment
T1106: Native API
T1204: User Execution
T1204.002: Malicious File
T1059: Command and Scripting Interpreter
T1059.001: PowerShell
T1059.003: Windows Command Shell
T1053: Scheduled Task/Job
T1053.005: Scheduled Task
T1047: Windows Management Instrument
T1136: Create Account
T1136.002: Domain Account
T1078: Valid Accounts
T1078.002: Domain Accounts
T1053: Boot or logon autostart execution
T1068: Exploitation for Privilege Escalation
T1140: Deobfuscate/Decode Files or Information
T1070: Indicator Removal on Host
T1070.001: Clear Windows Event Logs

T1562: Impair Defenses
T1562.001: Disable or Modify Tools
T1003: OS Credential Dumping
T1003.005: Cached Domain Credentials
T1018: Remote System Discovery
T1021: Remote Services
T1021.001: Remote Desktop Protocol
T1021.002: SMB/Windows admin shares
T1021.006: Windows Remote Management
T1083: File and directory discovery
T1057: Process discovery
T1063: Security software discovery
T1049: System Network Connections Discovery
T1135: Network Share Discovery
T1071: Application Layer Protocol
T1071.001: Web Protocols
T1570: Lateral tool transfer
1486: Data Encrypted for Impact
T1005: Data from local system
T1560: Archive Collected Data
T1560.001: Archive via Utility
T1105: Ingress Tool Transfer
T1567: Exfiltration over web service

## Actor Details

| Name | Target Locations | Target sectors | Motive |
|---|---|---|---|
| Hive Ransomware Group | Worldwide | Technology, Healthcare, Transportation, Construction, Media, Professional Services, Retail, Materials, Automotive, Apparel and Fashion, Nonprofits, Retailers, Energy Providers | Financial Gain |

## Vulnerability Details

| CVE ID | Affected Versions | Affected CPE | Vulnerability Name | CWE |
|---|---|---|---|---|
| CVE-2021-34473 | Microsoft Exchange Server 2013 CU23, 2016 CU19, 2016 CU20, 2019 CU8, 2019 CU9 | cpe:2.3:a:microsoft:exchange_server:2013_cu23:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016_cu19:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016_cu20:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019_cu8:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019_cu9:*:*:*:*:*:*:* | Microsoft Exchange Server Remote Code Execution Vulnerability | CWE-94 |
| CVE-2021-34523 | | | Microsoft Exchange Server Elevation of Privilege Vulnerability | CWE-264 |
| CVE-2021-31207 | | | Microsoft Exchange Server Security Feature Bypass Vulnerability | CWE-254 |

## Indicators of Compromise (IoCs)

| Type | Value |
|---|---|
| MD5 | 6c9ad4e67032301a61a9897377d9cff8, 6a58b52b184715583cda792b56a0a1ed, 4fdabe571b66ceec3448939bfb3ffcd1, bb7c575e798ff5243b5014777253635d, 5e1575c221f8826ce55ac2696cf1cf0b, d46104947d8478030e8bcfcc74f2aef7, 2401f681b4722965f82a3d8199a134ed |

| Type | Value |
|---|---|
| File name | Windows.exe,<br>Mimikatz.exe,<br>advanced_port_scanner_2.5.3869.exe,<br>advanced port scanner.exe,<br>scan.exe,<br>p.bat,<br>Psexec,<br>7zip.exe,<br>ac.exe,<br>winlo.e,<br>gmer.exe,<br>Bk74AE.tmp/PCHunter6,<br>Musi,<br>791251-1632642588.ex,<br>nds.d,<br>xxx.000,<br>windows.exe,<br>mmm.exe",<br>xxx.000,<br>"zzz.exe,<br>xxx.exe,<br>main.py |
| IPV4 | 139.60.161[.]228,<br>139.60.161[.]56,<br>91.208.52[.]149,<br>185.70.184[.]8 |
| SHA1 | 655979d56e874fbe7561bb1b6e512316c25cbb19,<br>3477a173e2c1005a81d042802ab0f22cc12a4d55,<br>763499b37aacd317e7d2f512872f9ed719aacae1,<br>2146f04728fe93c393a74331b76799ea8fe0269f,<br>ecf794599c5a813f31f0468aecd5662c5029b5c4,<br>d1ef9f484f10d12345c41d6b9fca8ee0efa29b60,<br>2aee699780f06857bb0fb9c0f73e33d1ac87a385 |
| SHA256 | bdf3d5f4f1b7c90dfc526340e917da9e188f04238e772049b2a97b4f88f711e3,<br>6983ef6e484c0c70356d6f868ac03bc90a1055560642706743511f76aa6f28ad,<br>6a0449a0b92dc1b17da219492487de824e86a25284f21e6e3af056fe3f4c4ec0,<br>5d95bf2518918422a6cac03f90548f02a5848dbc43836868636b61d0a87ed968,<br>47006ed84afb1f1fd761b81f3ae7b6547c0cb4845538301035e1388693fc6f7f,<br>25793a0764a51b38806b7dcf5f5d8df9620f090f72362aa03187c8813e054482,<br>7b7f13ab85bc78849e04a5589c84f0ec1847460106c03ca3db84703c7af054f3,<br>5d95bf2518918422a6cac03f90548f02a5848dbc43836868636b61d0a87ed968,<br>d64f9742539436acba5ff9c4f1c8ca501cad86dfa823828b65418b493c8109ac,<br>5d95bf2518918422a6cac03f90548f02a5848dbc43836868636b61d0a87ed968,<br>bd6d8f7c9e016dd7395ee7f0f8485de622a9b034b7c5d2e1af25cb762dd8d8c9,<br>0e8e6fc94e6eb17cfd8993b3dcfd9acd11ee32f1b4e956df3097ae3259be4f9c,<br>875708f911752bef7e2ef0658d395ebeccef774d5fdb74f6e9ee60b52d86cbf0,<br>5b32ac4754bd5728cc7a68f341bf64cec4a737eb584814bb2099a5f2ff69e584,<br>baa7a6e5a093ee6be47eca86e5acbcba196c7d1d35662eecad23ec870702116a,<br>a2ad0442cebe3e6abb86069a3b66b471b4a7c9d00286da4b8114d17a849128d6,<br>321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f0a78bdac06868136b72c |

Hive Pro

# THREAT ADVISORY

| Type | Value |
|---|---|
| SHA256 | 6bd3adc7e43e20ede1a82ad1469cc7ecd085b324621edbd4ec23db4e4473895f,<br>fd3e7d0f6a31b821604707ef99da281e4fd7d11c7804e46eeed11f66b200a391,<br>321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f0a78bdac06868136b72c,<br>be1565961e123f52e54e350e0ca2666f8ffa42fdc46df18dca6f7c0ac2b43d23,<br>3ec89b737c5b91eb9da0a2d9c6c1f0e637087b4552e26806d959c11f8f06e96f,<br>1e21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07db0ff,<br>fdbc66ebe7af710e15946e1541e2e81ddfd62aa3b35339288a9a244fb56a74cf,<br>c04509c1b80c129a7486119436c9ada5b0505358e97c1508b2cfb5c2a177ed11,<br>88f7544a29a2ceb175a135d9fa221cbfd3e8c71f32dd6b09399717f85ea9afd1,<br>a0b4e3d7e4cd20d25ad2f92be954b95eea44f8f1944118a3194295c5677db749,<br>5954558d43884da2c7902ddf89c0cf7cd5bf162d6feefe5ce7d15b16767a27e5,<br>77a398c870ad4904d06d455c9249e7864ac92dda877e288e5718b3c8d9fc6618,<br>612e5ffd09ca30ca9488d802594efb5d41c360f7a439df4ae09b14bce45575ec,<br>a290ce75c6c6b37af077b72dc9c2c347a2eede4fafa6551387fa8469539409c7,<br>977b2ce598bd6518913fe216d1139c041e159a6510cd71a6a14a49570c1019be,<br>e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173,<br>d1aa0ceb01cca76a88f9ee0c5817d24e7a15ad40768430373ae3009a619e2691,<br>8f3c5f9cd657e3785d751305023cf83a7f27780d5441817614d442e28dbe3ac4,<br>c367ab50c1f103963da0f0404eeda46c9e768711797d638afa1c4cf740575613,<br>fdbc66ebe7af710e15946e1541e2e81ddfd62aa3b35339288a9a244fb56a74cf,<br>ed614cba30f26f90815c28e189340843fab0fe7ebe71bb9b4a3cb7c78ff8e3d2,<br>1e21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07db0ff,<br>fdbc66ebe7af710e15946e1541e2e81ddfd62aa3b35339288a9a244fb56a74cf,<br>c04509c1b80c129a7486119436c9ada5b0505358e97c1508b2cfb5c2a177ed11,<br>a0b4e3d7e4cd20d25ad2f92be954b95eea44f8f1944118a3194295c5677db749,<br>5954558d43884da2c7902ddf89c0cf7cd5bf162d6feefe5ce7d15b16767a27e5,<br>77a398c870ad4904d06d455c9249e7864ac92dda877e288e5718b3c8d9fc6618,<br>e514be3e997895c7e3ece03549c8cb6b5700fe8f814948ed201ca59daa8733fb,<br>7b7f13ab85bc78849e04a5589c84f0ec1847460106c03ca3db84703c7af054f3 |

## Recent Breaches

https://millsgrouponline.com/
https://www.fcch.com/
https://www.konradin.de/de/
https://www.pollmann.at/en
https://www.emilfrey.ch/de
https://rte.com.br/
https://www.friedrich.com/
https://powerhouse1.com/
https://www.hshi.co.kr/eng/
https://www.eurocoininteractive.nl/
https://www.itsinfocom.com/
https://www.pan-energy.com/
https://nsminc.com/
https://www.ucsiuniversity.edu.my/
https://kemlu.go.id/portal/id

## Patch Links

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

### References

https://www.varonis.com/blog/hive-ransomware-analysis
https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-hive