Hive Pro

THREAT ADVISORY

UNC2596 exploits Microsoft's ProxyShell and ProxyLogon vulnerabilities to distribute Cuba Ransomware

TA2022042

Threat Level RED

Published Date – Feb 28, 2022

Threat actor UNC2596 popularly known for their Ecrime business has targeted more than 50 organizations in 11+ countries. The threat actors increased their initial attack vector by exploiting proxyshell and proxylogon vulnerabilities to deploy Cuba ransomware.

The UNC2596 threat actor has used web shells to load the TERMITE in-memory dropper during intrusions, with further activity involving various backdoors and built-in Windows tools. The threat actor has also employed new malware, such as WEDGECUT to enumerate active hosts, BURNTCIGAR to disable endpoint security, and the BUGHATCH custom downloader, in addition to familiar tools such as Cobalt Strike BEACON and NetSupport. UNC2596 employed a multi-pronged extortion technique in which data was stolen and leaked on the group's shame website, in addition to encrypting with Cuba ransomware.

Organizations can mitigate the risk by following the recommendations:

- Have an effective backup strategy that ensures the backup are inaccessible from the endpoint.
- Keep all operating systems and software up to date.
- Implement a user training program and phishing exercises.

The Mitre TTPs used by UNC2596 in the current attack are:

TA0001: Initial Access
TA0007: Discovery
TA0040: Impact
TA0009: Collection
TA0005: Defense Evasion
TA0003: Persistence
TA0011: Command and Control
TA0042: Resource Development
TA0002: Execution
TA0008: Lateral Movement
TA0006: Credential Access
T1190: Exploit Public-Facing Application
T1010: Application Window Discovery
T1012: Query Registry
T1016: System Network Configuration Discovery
T1018: Remote System Discovery
T1033: System Owner/User Discovery
T1057: Process Discovery
T1082: System Information Discovery
T1083: File and Directory Discovery
T1087: Account Discovery
T1518: Software Discovery
T1486: Data Encrypted for Impact
T1489: Service Stop
T1056.001: Keylogging
T1021.004: SSH
T1555.003: Credentials from Web Browsers
T1021.001: Remote Desktop Protocol

T1112: Modify Registry
T1134: Access Token Manipulation
T1134.001: Token Impersonation/Theft
T1140: Deobfuscate/Decode Files or Information
T1497.001: System Checks
T1553.002: Code Signing
T1564.003: Hidden Window
T1574.011: Services Registry Permissions Weakness
T1620: Reflective Code Loading
T1098: Account Manipulation
T1136: Create Account
T1136.001: Local Account
T1543.003: Windows Service
T1071.001: Web Protocols
T1071.004: DNS
T1095: Non-Application Layer Protocol
T1105: Ingress Tool Transfer
T1573.002: Asymmetric Cryptography
T1583.003: Virtual Private Server
T1587.003: Digital Certificates
T1588.003: Code Signing Certificates
T1608.001: Upload Malware
T1608.002: Upload Tool
T1608.003: Install Digital Certificate
T1608.005: Link Target
T1053: Scheduled Task/Job
T1059: Command and Scripting Interpreter
T1059.001: PowerShell
T1129: Shared Modules
T1569.002: Service Execution

Actor Details

Name	Target Locations	Target sectors	Motive
UNC2596	Australia, Belgium, Canada, Germany, India, UK, USA, Austria, Colombia, Jordan, Poland	Construction & Engineering, Education, manufacturing, Oil &Gas, Transportation, Defense, Energy, Financial, Government, Healthcare, High-Tech, IT, Media, Pharmaceutical, Telecommunications and MSPs	Ecrime

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

Hive Pro

THREAT ADVISORY

CVE ID	Affected Versions	Affected CPE	Vulnerability Name	CWE
CVE-2021-26855	Microsoft Exchange Server 2013, Microsoft Exchange Server 2016, Microsoft Exchange Server 2019	cpe:2.3:a:microsoft:exchange_server:2013_cu23:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016_cu18:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2016_cu19:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019_cu7:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:exchange_server:2019_cu8:*:*:*:*:*:*:*	SSRF vulnerability in Microsoft Exchange Server	CWE-918
CVE-2021-26857			An insecure deserialization vulnerability in Microsoft Exchange	CWE-20
CVE-2021-26858			An arbitrary file write vulnerabilities in Microsoft Exchange	CWE-20
CVE-2021-27065			An arbitrary file write vulnerabilities in Microsoft Exchange	CWE-20

Indicators of Compromise (IoCs)

Type	Value
IPv4	64.235.39[.]82, 64.52.169[.]174, 144.172.83[.]13, 190.114.254[.]116, 185.153.199[.]164, 45.32.229[.]66, 23.227.197[.]229
MD5	72a60d799ae9e4f0a3443a2f96fb4896, bda33efc53c202c99c1e5afb3a13b30c, e78ed117f74fd7441cadc3ea18814b3e, ba83831700a73661f99d38d7505b5646, c47372b368c0039a9085e2ed437ec720, c5e3b725080712c175840c59a37a5daa, c9d3b29e0b7662dafc6a1839ad54a6fb, 9ca2579117916ded7ac8272b7b47bb98, 26c09228e76764a2002ba643afeb9415, 98a2e05f4aa648b02540d2e17946da7e, ddf2e657a89ae38f634c4a271345808b, 95820d16da2d9c4fbb07130639be2143, 896376ce1bbca1ed73a70341896023e0, f51c4b21445a0ece50b1f920648ed726, 7d4307d310ad151359b025fc5a7fca1a, b62eec21d9443f8f66b87dd92ba34e85, df0e5d91d0986fde9bc02db38eef5010, 46b977a0838f4317425df0f2e1076451, 8c4341a4bde2b6faa76405f57e00fc48, d5679f47d22c7c0647038ce6f54352e4, e77af544cc9d163d81e78b3c4da2eee5, 98b2fff45a9474d61c1bd71b7a60712b, 9a0a2f1dc7686983843ee38d3cab448f, fb6da2aa2aca0ce2e0af22b2c3ba2668, 3e96efd37777cc01cabb3401485297aa, 73c0f0904105b4c220c25f64506ea986, 20a04e7fc12259dfd4172f5232ed5ccf, becdcaa3a4d933c13427bb40f9c1cfbb, 48f8cd5e42cdf06d5a520ab66a5ae576

Hive Pro

THREAT ADVISORY

Type	Value
SHA-1	6d5ca42906c60caa7d3e0564b011d20b87b175cbd9d44a96673b46a82b07df68, 101b3147d404150b3c0c882ab869a18eb6eeb79e8b7b2df81fb4be1a8b58f1bf, 9ab05651daf9e8bf3c84b14613cd98e8479018bbcf3543521e94458012eba96e, 79d6b1b6b1ecb446b0f49772bf4da63fcec6f6bfc7c2e1f4924cb7acbb3b4f53, c443df1ddf8fd8a47af6fbfd0b597c4eb30d82efd1941692ba9bb9c4d6874e14, f68cea99e6887739cd82865f9b973664117af14c1a25d4917eec25ce4b26a381, 4306c5d152cdd86f3506f91633ef3ae7d8cf0dd25f3e37bec43423c4742f4c42, aeb044d310801d546d10b247164c78afde638a90b6ef2f04e1f40170e54dec03, 6ce206a1e1224e0a9d296d5fabffee7fe5ab45ef00299a21e8df66e8c6ba5a27, 811bb84e1e9f59279f844a040bf68d25ad29a756fbc07cffd7308f8490a15329, d1e14b5f02fb020db4e215cb5c3abc6a7b1589443bccd6f03b77ee124ca72b5c, a722615c2ee101cde88c7f44fb214eccfe2d06752be751db066018a3244bce62, 671e049f3e2f6b7851ca4e8eed28ba5c9bf209eb4ad44aab081a9871b06f2833, ea5de5558396f66af8382afd98f2a7118a6bcabf8f9612c7e35b121a8d1f230c, ad12f38308a85c8792f2f7e1e46afc3d9f1a9017edc2cbfbb28ae0191477ab3a, 9cec82bebe1637c50877ff11de5bd4db1db4999d1bd764a772a5620388843c5f, 6cd25067316f8fe013792697f2f5da298318e2047ea4c5da525955799f66726f, 13d333d5e3c1dd6c33dfa8fc76def6109b5187d4ce6bb82a34a8bf311b027d79, df89d3d1f795a77eefc14f0356816d8b40934e40697f8190f76e0f5664f33fd3, 728a2d5dd2bf9c707431ff68e94c0d7a7ace9508241051c02344d9e9c556e015, 7f357ab4ac225e14a6967f89f20926e9e0db15dca5b8fe058c120a365570b783, 7b2144f2b5d722a1a8a0c47a43ecaf029b434bfb34a5cffe651fda2adf401131, 03249bf622c3ae1dbed8b14cfaa8332442a41c4592d325ad93b6a8cb6d4b29f8, 1842ddc55b4bf9c71606451d404a21f7f3da8e54c56318010c80ba4f571bd8f5, bcf0f202db47ca671ed6146040795e3c8315b7fb4f886161c675d4ddf5fdd0c4, e35593fab92606448ac4cac6cd2bd6b4df5d7ab3b733ba4b9472994cf0e3d87d, 482b160ee2e8d94fa6e4749f77e87da89c9658e7567459bc633d697430e3ad9a, 6c4b57fc995a037a0d60166deadfb869a07b4bb382651b9c4ea9e59fb347c3d1, 44a4ce7b5d2e154ec802a67ef14c613298cafc00b1ca3a15b302195f2686a186, 6e66caaa12c3cafd1dc3f8c6305354fcbb958ed7f9a4e5e5bf3a2dc2216b5915, d8df1a4d59a0382b367fd6936cce538201e9b93a2850dbc66a4dd575fbeb8c42
Domain	irrislaha[.]com, leptengthinete[.]com, siagevewilin[.]com, surnbuithe[.]com

Recent Breaches

http://www.get-integrated.com
https://www.muntons.com/
https://www.cmmcpas.com

Patch Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26855
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26857
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26858
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-27065
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.mandiant.com/resources/unc2596-cuba-ransomware