Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

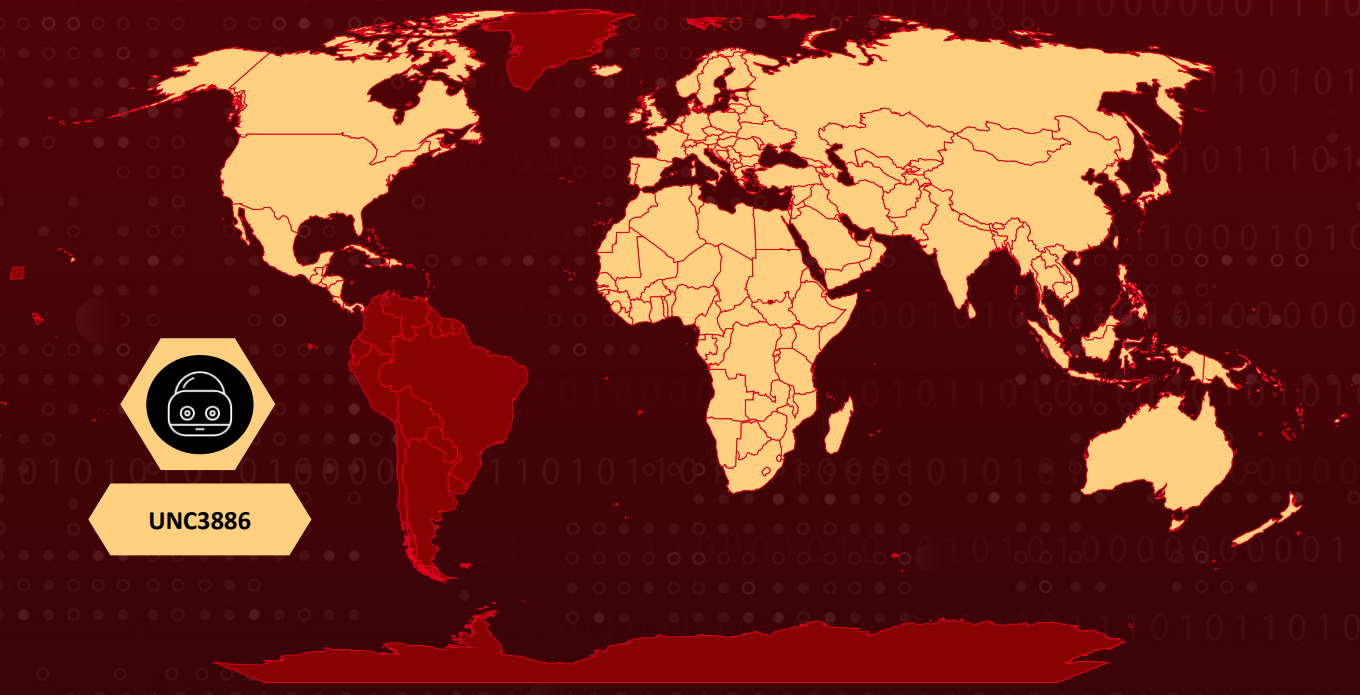
UNC3886 Covert Operations Leveraging Rootkits and Backdoored Applications

Date of Publication	Last Update Date	Admiralty code	TA Number
June 21, 2024	July 25, 2025	A1	TA2024240

Summary

First Appearance: September 2022
Actor Name: UNC3886
Targeted Countries: North America, Oceania, Europe, Africa, and Asia
Malware: VirtualPita, VirtualPie, VirtualGate, MOPSLED, RIFLESPINE, TINYSHELL
Targeted Industries: Government, Telecommunications, Technology, Aerospace, Defense, Energy, Utility, Critical Infrastructure

Actor Map



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-34048	VMware vCenter Server Out-of-Bounds Write Vulnerability	VMware vCenter Server	✓	✓	✓
CVE-2022-41328	Fortinet FortiOS Path Traversal Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2022-22948	Vmware vCenter Server Information Disclosure Vulnerability	Vmware vCenter Server	✗	✓	✓
CVE-2023-20867	VMware Tools Authentication Bypass Vulnerability	VMware Tools	✓	✓	✓
CVE-2022-42475	Fortinet FortiOS Heap-Based Buffer Overflow Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2025-21590	Juniper Junos OS Improper Isolation or Compartmentalization Vulnerability	Juniper Junos OS	✓	✓	✓

Actor Details

#1

A China-linked cyber espionage group, tracked as UNC3886, has been employing various techniques to evade detection and maintain access to compromised systems after initial zero-day attacks. UNC3886 has exploited vulnerabilities in Fortinet, and VMware systems to gain access. To sustain long-term access, the group uses multiple layers of persistence across network devices, hypervisors, and virtual machines. Their attacks focus on entities in North America, Southeast Asia, Oceania, and other regions, including industries like government, telecommunications, technology, aerospace, defense, and energy.

#2

UNC3886 utilize publicly available rootkits like REPTILE and MEDUSA to maintain access and evade detection, bypassing security software to infiltrate networks. They employs malware such as MOPSLED and RIFLESPINE, using trusted third-party services like GitHub and Google Drive as command-and-control (C2) channels. They also acquire and use valid credentials to move laterally between virtual machines on compromised VMware ESXi systems, sometimes utilizing backdoored SSH executables.

#3

Additionally, UNC3886 uses backdoored SSH clients and custom SSH servers to harvest credentials and employs LOOKOVER to decrypt TACACS+ authentication packets. Other malware used includes a trojanized TACACS daemon, VIRTUALSHINE (a VMware VMCI sockets-based backdoor), VIRTUALPIE (a Python backdoor), and VIRTUALSPHERE (a VMCI-based controller module).

#4

One of the defining characteristics of UNC3886 is its focus on environments lacking Endpoint Detection and Response (EDR) solutions. This includes virtualized infrastructures and certain types of network devices, which are often less monitored and protected compared to traditional endpoints. By targeting these environments, UNC3886 can operate with a lower risk of detection, leveraging advanced persistence techniques to maintain long-term access to compromised systems.

#5

In recent operations, UNC3886 has been actively targeting critical infrastructure. As of July 2025, Singapore's Coordinating Minister for National Security confirmed a "significant and ongoing attack campaign" by UNC3886 against the nation's vital services, warning of potential impacts on business operations and supply chains. This follows a mid-2024 campaign where UNC3886 exploited CVE-2025-21590 in end-of-life Juniper Networks MX Series routers running Junos OS, deploying custom TINYSHELL-based backdoors and utilizing advanced process injection techniques, to maintain covert, long-term access and disable logging mechanisms.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
UNC3886	China **MOTIVE** Information theft and espionage	North America, Oceania, Europe, Africa, and Asia	Government, Telecommunications, Technology, Aerospace, Defense, Energy, Utility, Critical Infrastructure

Recommendations

Implement Robust Endpoint Protection: Deploy advanced endpoint protection solutions that include behavior-based detection, machine learning algorithms, and threat intelligence. These solutions can detect and block malicious activities associated with UNC3886. Regularly update endpoint security software to ensure protection against the latest threats.

Patch and Update Software: Keep all operating systems, applications, and firmware up to date with the latest security patches and updates. UNC3886 threat actors often exploit known vulnerabilities to gain initial access to systems. By promptly applying patches, organizations can mitigate the risk of these vulnerabilities being exploited and prevent unauthorized access to their networks.

Advanced Threat Detection and Response: Deploying advanced threat detection and response solutions is essential for identifying and mitigating sophisticated attacks. This includes using Endpoint Detection and Response (EDR) tools, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). These tools can detect unusual activity and provide alerts on potential intrusions, allowing for quicker response times.

Network Segmentation: Segmenting the network can limit the spread of an attack and protect sensitive information. By creating isolated network segments for different parts of the infrastructure, organizations can control access more effectively and contain potential breaches. Implementing strict access controls and monitoring traffic between segments can further enhance security.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation	TA0042 Resource Development
TA0005 Defense Evasion	TA0006 Credential Access	TA0003 Persistence	TA0008 Lateral Movement
TA0011 Command and Control	TA0010 Exfiltration	T1600 Weaken Encryption	T1041 Exfiltration Over C2 Channel

T1588.006 Vulnerabilities	T1588.005 Exploits	T1588 Obtain Capabilities	T1059 Command and Scripting Interpreter
T1014 Rootkit	T1021.004 SSH	T1021 Remote Services	T1078 Valid Accounts
T1078.001 Default Accounts	T1068 Exploitation for Privilege Escalation	T1562 Impair Defenses	T1090 Proxy
T1202 Indirect Command Execution	T1140 Deobfuscate/Decode Files or Information	T1095 Non-Application Layer Protocol	T1588.004 Digital Certificates
T1584 Compromise Infrastructure	T1071.001 Web Protocols	T1071 Application Layer Protocol	

Indicator of Compromise (IOCs)

TYPE	VALUE
MD5	381b7a2a6d581e3482c829bfb542a7de, 876787f76867ecf654019bd19409c5b8, 827d8ae502e3a4d56e6c3a238ba855a7, 9ea86dccd5bbde47f8641b62a1eeff07, fcb742b507e3c074da5524d1a7c80f7f, 129ba90886c5f5eb0c81d901ad10c622, 0f76936e237bd87dfa2378106099a673, d18a5f1e8c321472a31c27f4985834a4, 4ddca39b05103aeb075ebb0e03522064, 0e43a0f747a60855209b311d727a20bf, 1d89b48548ea1ddf0337741ebdb89d92, ecb34a068eeb2548c0cbe2de00e53ed2, 89339821cdf6e9297000f3e6949f0404, c870ea6a598c12218e6ac36d791032b5, 1079d416e093ba40aa9e95a4c2a5b61f, ed9be20fea9203f4c4557c66c5b9686c, 568074d60dd4759e963adc5fe9f15eb1, 4d5e4f64a9b56067704a977ed89aa641, 1b7aee68f384e252286559abc32e6dd1, b754237c7b5e9461389a6d960156db1e, f41ad99b8a8c95e4132e850b3663cb40, 48f9bbdb670f89fce9c51ad433b4f200, 4fb72d580241f27945ec187855efd84a, e2cdf2a3380d0197aa11ff98a34cc59e, fd3834d566a993c549a13a52d843a4e1,

TYPE	VALUE
MD5	4282de95cc54829d7ac275e436e33b78, c9c00c627015bd78fda22fa28fd11cd7, 047ac6aebe0fe80f9f09c5c548233407, bca2ccff0596a9f102550976750e2a89, 3a8a60416b7b0e1aa5d17eefb0a45a16, 6e248f5424810ea67212f1f2e4616aa5, 5d232b72378754f7a6433f93e6380737, 3c7316012cba3bbfa8a95d7277cda873, 9c428a35d9fc1fdaf31af186ff6eec08, 2716c60c28cf7f7568f55ac33313468b, 61ab3f6401d60ec36cd3ac980a8deb75, bd6e38b6ff85ab02c1a4325e8af29ce4, 9ef5266a9fdd25474227c3e33b8e6d77, a7cd7b61d13256f5478feb28ab34be72, cd3e9e4df7e607f4fe83873b9d1142e3, 62bed88bd426f91ddbbbcfcd8508ed6a, 8e80b40b1298f022c7f3a96599806c43, c9f2476bf8db102fea7310abadeb9e01, 2c28ec2d541f555b2838099ca849f965, 2bade2a5ec166d3a226761f78711ce2f, 969d7f092ed05c72f27eef5f2c8158d6, 084132b20ed65b2930129b156b99f5b3, 2c89a18944d3a895bd6432415546635e, aac5d83d296df81c9259c9a533a8423a, 8023d01ffb7a38b582f0d598afb974ee, 5724d76f832ce8061f74b0e9f1dcad90, e7622d983d22e749b3658600df00296d, b9e4784fa0e6283ce6e2094426a02fce, bf80c96089d37b8571b5de7cab14dd9f, 3243e04afe18cc5e1230d49011e19899
IPv4	8[.]222[.]218[.]20, 8[.]222[.]216[.]144, 8[.]219[.]131[.]77, 8[.]219[.]0[.]112, 8[.]210[.]75[.]218, 8[.]210[.]103[.]134, 47[.]252[.]54[.]82, 47[.]251[.]46[.]35, 47[.]246[.]68[.]13, 47[.]243[.]116[.]155, 47[.]241[.]56[.]157, 45[.]77[.]106[.]183, 45[.]32[.]252[.]98, 207[.]246[.]64[.]38, 149[.]28[.]122[.]119, 155[.]138[.]161[.]47, 154[.]216[.]2[.]149, 103[.]232[.]86[.]217, 103[.]232[.]86[.]210, 103[.]232[.]86[.]209,

TYPE	VALUE
IPv4	58[.]64[.]204[.]165, 58[.]64[.]204[.]142, 58[.]64[.]204[.]139, 165[.]154[.]7[.]145, 165[.]154[.]135[.]108, 165[.]154[.]134[.]40, 152[.]32[.]231[.]251, 152[.]32[.]205[.]208, 152[.]32[.]144[.]15, 152[.]32[.]129[.]162, 123[.]58[.]207[.]86, 123[.]58[.]196[.]34, 118[.]193[.]63[.]40, 118[.]193[.]61[.]71, 118[.]193[.]61[.]178
IPv4:Port	129[.]126[.]109[.]50[:]22, 116[.]88[.]34[.]184[:]22, 223[.]25[.]78[.]136[:]22, 45[.]77[.]39[.]28[:]22, 101[.]100[.]182[.]122[:]22, 118[.]189[.]188[.]122[:]22, 158[.]140[.]135[.]244[:]22, 8[.]222[.]225[.]8[:]22
SHA1	0962e10dc34256c6b31509a5ced498f8f6a3d6b6, 93d5c4ebec2aa45dcbd6ddbaad5d80614af82f84, a3cc666e0764e856e65275bd4f32a56d76e51420, abff003edf67e77667f56bbcfc391e2175cb0f8a, e35733db8061b57b8fcdb83ab51a90d0a8ba618c, E9cbac1f64587ce1dc5b92cde9637affb3b58577, 50520639cf77df0c15cc95076fac901e3d04b708, 1a6d07da7e77a5706dd8af899ebe4daa74bbbe91, 06a1f879da398c00522649171526dc968f769093, f8697b400059d4d5082eee2d269735aa8ea2df9a, cf7af504ef0796d91207e41815187a793d430d85, 01735bb47a933ae9ec470e6be737d8f646a8ec66, cec327e51b79cf11b3eeffebf1be8ac0d66e9529, 2e9215a203e908483d04dfc0328651d79d35b54f
SHA256	13f11c81331bdce711139f985e6c525915a72dc5443fbbfe99c8ec1dd7ad2209, 4a6f559426493abc0d056665f23457e2779abd3482434623e1f61f4cd5b41843, 4cf3e0b60e880e6a6ba9f45187ac5454813ae8c2031966d8b264ae0d1e15e70d, 505eb3b90cd107cf7e2c20189889afdff813b2fbb98bbdeab65cde520893b168, 5731d988781c9a1d2941f7333615f6292fb359f6d48498f32c29878b5bedf00f, c2ef08af063f6d416233a4b2b2e991c177fc72d70a76c24bca9080521d41040f,

TYPE	VALUE
SHA256	1893523f2a4d4e7905f1b688c5a81b069f06b3c3d8c0ff9d16620468d117edbb, 98380ec6bf4e03d3ff490cdc6c48c37714450930e4adf82e6e14d244d8373888, 5bef7608d66112315eefff354dae42f49178b7498f994a728ae6203a8a59f5a2, c0ec15e08b4fb3730c5695fb7b4a6b85f7fe341282ad469e4e141c40ead310c3, 5995aaff5a047565c0d7fe3c80fa354c40e7e8c3e7d4df292316c8472d4ac67a, 905b18d5df58dd6c16930e318d9574a2ad793ec993ad2f68bca813574e3d854b, e1de05a2832437ab70d36c4c05b43c4a57f856289224bbd41182deea978400ed, 3751997cfcb038e6b658e9180bc7cce28a3c25dbb892b661bcd1065723f11f7e, 7ae38a27494dd6c1bc9ab3c02c3709282e0ebcf1e5fcf59a57dc3ae56cfd13b4

Patch Links

https://www.vmware.com/security/advisories/VMSA-2023-0023.html

https://fortiguard.com/psirt/FG-IR-22-369

https://www.vmware.com/security/advisories/VMSA-2022-0009.html

https://www.vmware.com/security/advisories/VMSA-2023-0013.html

https://fortiguard.com/psirt/FG-IR-22-398

https://supportportal.juniper.net/s/article/2025-03-Out-of-Cycle-Security-Bulletin-Junos-OS-A-local-attacker-with-shell-access-can-execute-arbitrary-code-CVE-2025-21590?language=en_US

References

https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations

https://www.hivepro.com/threat-advisory/unc3886-targets-technologies-with-custom-malware-and-exploits-zero-day-vulnerabilities/

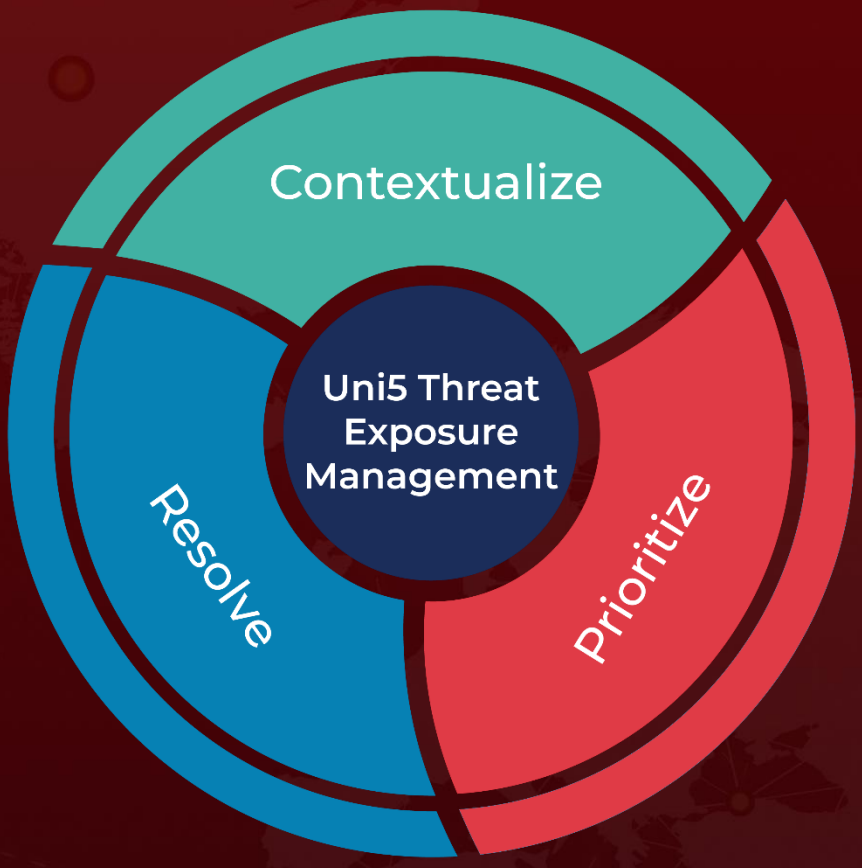
https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-targets-juniper-routers

https://www.straitstimes.com/singapore/who-is-unc3886-the-group-that-attacked-spores-critical-information-infrastructure

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 21, 2024 • 6:30 AM

More at www.hivepro.com