

HiveForce Labs

THREAT ADVISORY**ACTOR REPORT****UNC3886 Covert Operations Leveraging Rootkits and Backdoored Applications**

Date of Publication

June 21, 2024

Admiralty code

A1

TA Number

TA2024240

Summary

First Appearance: September 2022

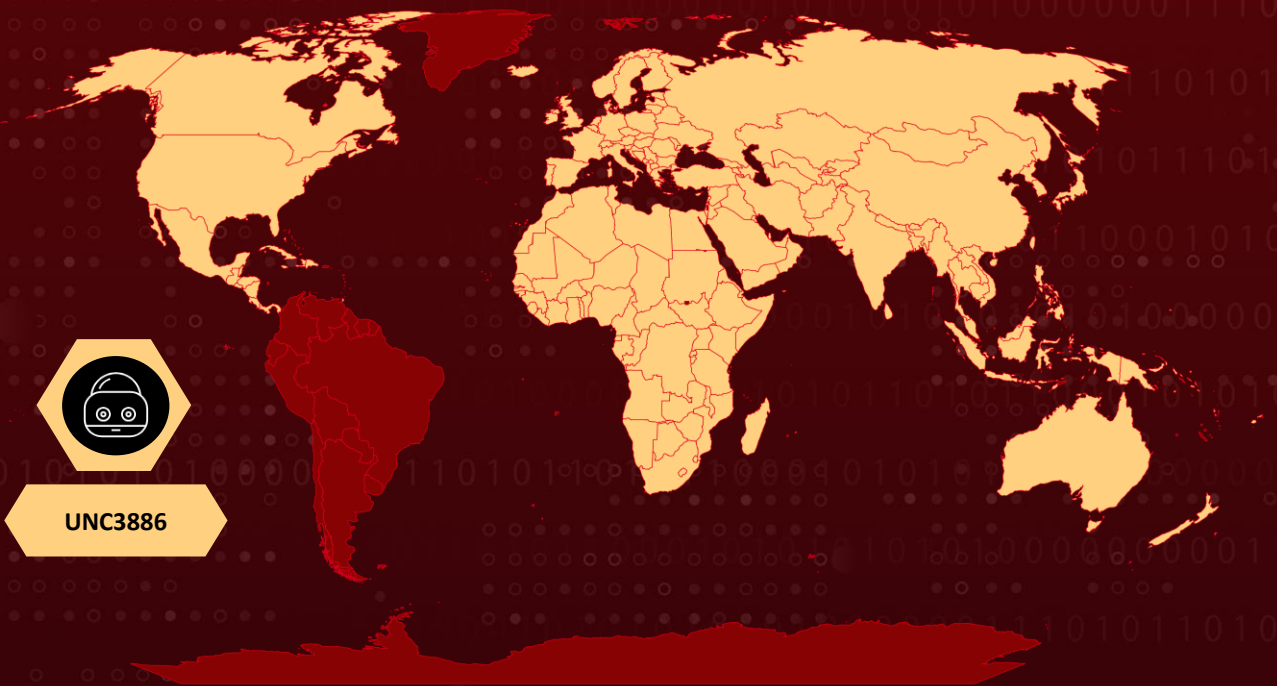
Actor Name: UNC3886

Targeted Countries: North America, Oceania, Europe, Africa, and Asia

Malware: VirtualPita, VirtualPie, VirtualGate, MOPSLIED and RIFLESPINE

Targeted Industries: Government, Telecommunications, Technology, Aerospace, Defense, Energy and Utility

Actor Map



Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

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	✅	✅	✅

Attack 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 employ 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

The increasing appeal of virtual machines as targets due to their widespread use in cloud environments and essential role in IT infrastructure. Overall, UNC3886's operations underscore the importance of securing virtual environments against sophisticated cyber threats.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
UNC3886	China	North America, Oceania, Europe, Africa, and Asia	Government, Telecommunications, Technology, Aerospace, Defense, Energy and Utility
	MOTIVE		
	Espionage		

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

<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation	<u>TA0042</u> Resource Development	<u>TA0005</u> Defense Evasion
<u>TA0006</u> Credential Access	<u>TA0011</u> Command and Control	<u>TA0003</u> Persistence	<u>TA0008</u> Lateral Movement

<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits	<u>T1588</u> Obtain Capabilities	<u>T1059</u> Command and Scripting Interpreter
<u>T1014</u> Rootkit	<u>T1021.004</u> SSH	<u>T1021</u> Remote Services	<u>T1078</u> Valid Accounts
<u>T1202</u> Indirect Command Execution	<u>T1140</u> Deobfuscate/Decode Files or Information	<u>T1095</u> Non-Application Layer Protocol	<u>T1588.004</u> Digital Certificates
<u>T1584</u> Compromise Infrastructure	<u>T1071.001</u> Web Protocols	<u>T1071</u> Application Layer Protocol	<u>T1600</u> Weaken Encryption

✂ 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,

TYPE	VALUE
<p>MD5</p>	<p>f41ad99b8a8c95e4132e850b3663cb40, 48f9bbdb670f89fce9c51ad433b4f200, 4fb72d580241f27945ec187855efd84a, e2cdf2a3380d0197aa11ff98a34cc59e, fd3834d566a993c549a13a52d843a4e1, 4282de95cc54829d7ac275e436e33b78, c9c00c627015bd78fda22fa28fd11cd7, 047ac6aeb0fe80f9f09c5c548233407, bca2ccff0596a9f102550976750e2a89, 3a8a60416b7b0e1aa5d17eefb0a45a16, 6e248f5424810ea67212f1f2e4616aa5, 5d232b72378754f7a6433f93e6380737, 3c7316012cba3bbfa8a95d7277cda873, 9c428a35d9fc1fdaf31af186ff6eec08, 2716c60c28cf7f7568f55ac33313468b, 61ab3f6401d60ec36cd3ac980a8deb75, bd6e38b6ff85ab02c1a4325e8af29ce4, 9ef5266a9fdd25474227c3e33b8e6d77, a7cd7b61d13256f5478feb28ab34be72, cd3e9e4df7e607f4fe83873b9d1142e3, 62bed88bd426f91ddbbbcfcd8508ed6a, 8e80b40b1298f022c7f3a96599806c43, c9f2476bf8db102fea7310abadeb9e01, 2c28ec2d541f555b2838099ca849f965, 2bade2a5ec166d3a226761f78711ce2f, 969d7f092ed05c72f27eef5f2c8158d6, 084132b20ed65b2930129b156b99f5b3</p>
<p>IPv4</p>	<p>8[.]222[.]218[.]20, 8[.]222[.]216[.]144, 8[.]219[.]131[.]77, 8[.]219[.]10[.]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,</p>

TYPE	VALUE
IPv4	149[.]28[.]122[.]119, 155[.]138[.]161[.]147, 154[.]216[.]2[.]149, 103[.]232[.]86[.]217, 103[.]232[.]86[.]210, 103[.]232[.]86[.]209, 58[.]64[.]204[.]165, 58[.]64[.]204[.]142, 58[.]64[.]204[.]139, 165[.]154[.]7[.]145, 165[.]154[.]135[.]108, 165[.]154[.]134[.]140, 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,

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>

References

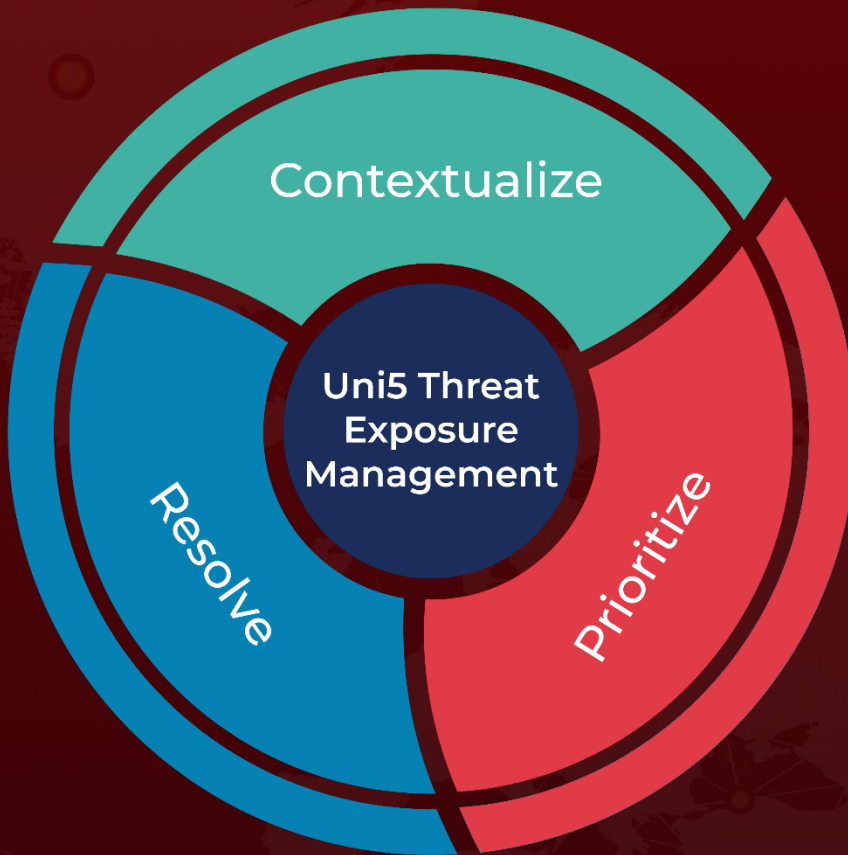
<https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations>

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

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

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com