Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

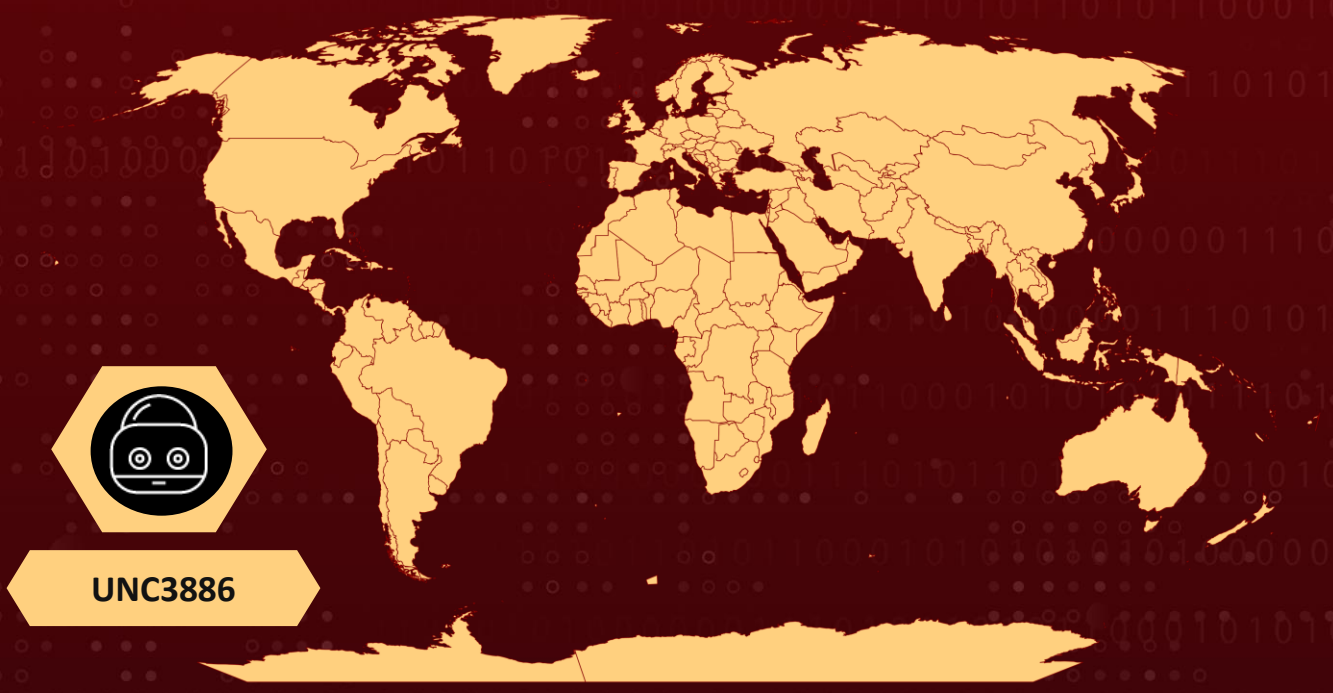
UNC3886 targets technologies with custom malware and exploits zero-day vulnerabilities

Date of Publication	Admiralty Code	TA Number
March 21, 2023	A1	TA2023150

Summary

First appeared: September 2022
Attack Region: Worldwide
Actor Name: UNC3886
Targeted Products: Firewalls, IoT devices, hypervisors, and VPN
Attack: UNC3886 is a cyber espionage Chinese group that targets technologies without EDR solutions and exploits zero-day vulnerabilities to steal user credentials and maintain access.

Attack Regions



CVEs

CVE	NAME	PATCH	CISA KEV
CVE-2022-41328*	Privilege escalation in FortiOS	✓	✓

* Represents Zero-day Vulnerability

Attack Details

#1

UNC3886 is a cyber espionage Chinese threat actor that targets technologies that do not support endpoint detection and response (EDR) solutions. The group has exploited zero-day vulnerabilities and deployed custom malware to steal user credentials and maintain long-term access to the victim environments. UNC3886 is associated with the novel VMware ESXi hypervisor malware framework and has deployed backdoors onto Fortinet and VMware solutions to maintain persistent access to the environments.

#2

Fortinet firewalls involved the exploitation of a path traversal vulnerability (CVE-2022-41328) through the execute wireless-controller hs20-icon upload-icon command. The vulnerability allowed the attacker to upload a file smaller than 65,535 bytes to any location on the file system, enabling the attacker to replace any legitimate system file on the FortiGate firewall. The evidence of attempted exploitation in FortiGuard logs events and the creation of a persistent backdoor named CASTLETAP, which was identified in a forensic image of the compromised FortiGate firewalls.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery
TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control	TA0040 Impact
T1565 Data Manipulation	T1565.001 Stored Data Manipulation	T1027 Obfuscated Files or Information	T1070 Indicator Removal
T1070.003 Clear Command History	T1070.004 File Deletion	T1078 Valid Accounts	T1140 Deobfuscate/Decode Files or Information
T1202 Indirect Command Execution	T1218 System Binary Proxy Execution	T1218.011 Rundll32	T1222 File and Directory Permissions Modification
T1497 Virtualization/Sandbox Evasion	T1497.001 System Checks	T1620 Reflective Code Loading	T1552 Unsecured Credentials
T1555 Credentials from Password Stores	T1555.005 Password Managers	T1016 System Network Configuration Discovery	T1033 System Owner/User Discovery
T1057 Process Discovery	T1082 System Information Discovery	T1083 File and Directory Discovery	T1087 Account Discovery
T1518 Software Discovery	T1074 Data Staged	T1074.001 Local Data Staging	T1560 Archive Collected Data
T1560.001 Archive via Utility	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.003 Windows Command Shell
T1059.004 Unix Shell	T1059.006 Python	T1129 Shared Modules	T1095 Non-Application Layer Protocol
T1102 Web Service	T1102.001 Dead Drop Resolver	T1105 Ingress Tool Transfer	T1571 Non-Standard Port
T1573 Encrypted Channel	T1573.001 Symmetric Cryptography	T1021 Remote Services	T1021.004 SSH

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	9ce2459168cf4b5af494776a70e0feda b6e92149efaf78e9ce7552297505b9d5 53a69adac914808eced2bf8155a7512d a388ebaef45add5da503e4bf2b9da546 88711ebc99e1390f1ce2f42a6de0654d e2d2884869f48f40b32fb27cc3bdefff 53a69adac914808eced2bf8155a7512d 64bdf7a631bc76b01b985f1d46b35ea6 a86a8fe875a89816e5808588154a067e 3e43511c4f7f551290292394c4e21de7
SHA1	86f3623b3fb8d5303b6c9d8295292a5c2ceb2889 75c092098e3409d366a46fdde6a92ff97d29cee1 9dca7f1af5752bb007e5cc55acd2511f03049ee5 8c40fc87fa3b25a559585b10a8ca11c81fb09f75 3109b890901499f7ebb90f8870a7d1617d27e7c9 b8bdaa1bd204a6c710875b0c4265655d1fd37d52 1a077212735617a665a6b631e34a6aedcbc41713 d5f8436e9815358e33b8243abda76c9b398943e2 8ef5159944d048fe84e51a818c9b11ebcfa98517
SHA256	245e4646e5d984c2da4cfe223bb2fae679441bcf42b254fc193ae97dc32af7ad 9fb09fe6db61fbdd19ac9c368e2f64fb9606119649830762fa467719c480ed44 18afbad17dee0e4330a85b782e8e580c6125d8a7127cda69ad0e2728d505a6f5 a00fed53b1ece4610c8b52934c20af3667d455f092a77f8d9bc46fdb9047e41a eb6af99148f0ce5b58e414162ff2b7567b4cf08953862a088996365ff306014b 33c22b2db8c0948c67204485972d2eb856e13dca16132371337fc3534e3df16d abefe121e5c895bf63be80152ccbe2d7bb5ad985aa3ab989bcb7c0804b90d004 2266667af7532a32b9c21c330a9fe56356ca66610e39654804a7262f2af61017 4e4c5e5ca588bd84b67a37b654ec522768fa83e535ff795a5c196da8f8b9737d

Patch Link

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

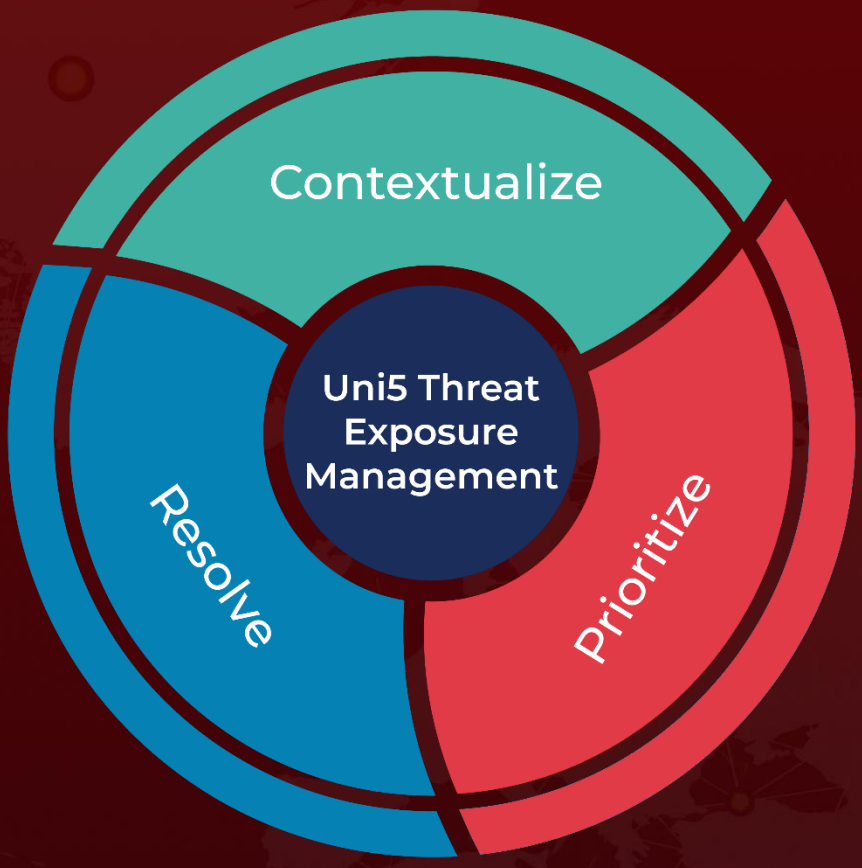
References

https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem

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

March 21, 2023 • 6:00 AM

More at www.hivepro.com