Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

A Financially Motivated Threat Group UNC961 Targeting North American Organizations

Date of Publication	Admiralty code	TA Number
March 24, 2023	A1	TA2023158

Summary

First Appearance: 2016
Actor Name: UNC961(Prophet Spider)
Target Region: North America, India, United Kingdom, United States
Target Sectors: Energy, Financial Services, Healthcare, Manufacturing, Media, Retail, Technology, Telecommunications

Actor Map

CVEs

CVE	NAME	PATCH	CISA KEV
CVE-2021-44228*	Apache Log4j2 Remote Code Execution Vulnerability	✓	✓
CVE-2021-26084	Atlassian Confluence Server Arbitrary Code Execution	✓	✓
CVE-2019-19781	Citrix Application Delivery Controller and Citrix Gateway Vulnerability	✓	✓
CVE-2020-14750	Oracle WebLogic Server Remote Code Execution Vulnerability	✓	✓
CVE-2021-22205	GitLab Community and Enterprise Editions From 11.9 Remote Code Execution Vulnerability	✓	✓
CVE-2017-7504	JbossMQ HTTP Invocation Layer deserialization vulnerability	✗	✗

* Zero-day Vulnerability

Actor Details

#1

UNC961 is a financially motivated cyber threat group that targets organizations in North America, with a focus on exploiting vulnerable Internet-facing servers during periods of vulnerability and exploit code disclosure. Their main goals include stealing sensitive data and providing access to ransomware-affiliated threat clusters. One instance of their attacks involved exploiting the Log4Shell vulnerability to gain access to MobileIron Core infrastructure. Another attack involved exploiting a vulnerability in Atlassian Confluence to access the victim's network, where they used a Linux-based backdoor to maintain persistence.

#2

In another incident, UNC961 compromised a victim and transferred access to another threat group, UNC3966. UNC961 has been observed targeting other Internet-facing application servers such as Citrix ADC, Oracle WebLogic, Gitlab, and Atlassian Confluence. They have also been observed exfiltrating sensitive data including network reconnaissance and credential information.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
UNC961(Prophet Spider)	Unknown **MOTIVE** Information theft and espionage; Financial Gain	North America, India, United Kingdom, United States	Energy, Financial Services, Healthcare, Manufacturing, Media, Retail, Technology, Telecommunications

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 actor 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	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1505 Server Software Component	T1505.003 Web Shell

T1083 File and Directory Discovery	**T1018** Remote System Discovery	**T1069** Permission Groups Discovery	**T1069.001** Local Groups
T1069.002 Domain Groups	**T1016** System Network Configuration Discovery	**T1033** System Owner/User Discovery	**T1049** System Network Connections Discovery
T1140 Deobfuscate/Decode Files or Information	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.003** Windows Command Shell
T1059.004 Unix Shell	**T1543** Create or Modify System Process	**T1543.003** Windows Service	**T1053** Scheduled Task/Job
T1053.005 Scheduled Task	**T1105** Ingress Tool Transfer	**T1197** BITS Jobs	**T1112** Modify Registry
T1070 Indicator Removal	**T1070.007** Clear Network Connection History and Configurations	**T1047** Windows Management Instrumentation	**T1569** System Services
T1569.002 Service Execution	**T1560** Archive Collected Data	**T1560.001** Archive via Utility	**T1048** Exfiltration Over Alternative Protocol
T1071 Application Layer Protocol	**T1071.002** File Transfer Protocols	**T1021** Remote Services	**T1021.004** SSH
T1572 Protocol Tunneling	**T1135** Network Share Discovery	**T1003** OS Credential Dumping	**T1003.001** LSASS Memory
T1003.003 NTDS	**T1482** Domain Trust Discovery	**T1087** Account Discovery	**T1087.002** Domain Account

Indicator of Compromise (IOCs)

TYPE	VALUE
MD5	c55f4b123c645f9c5a1d00205ab2e61e 31c49b87463f4e4ce6ae4c442319d3a2
IPV4	104.149.170[.]183 23.227.203[.]214 37.1.209[.]20 107.181.187[.]184 45.61.136[.]39 209.141.61[.]225 107.181.187[.]182 136.244.69[.]29 5.149.250[.]214
URLs	hxxps[:]//ms-prod19-live[.]com/rehjhj8785780923853/abc hxxps[:]//ms-prod19-live[.]com/rehjhj8785780923853/cdef

Patch Link

https://logging.apache.org/log4j/2.x/security.html

https://jira.atlassian.com/browse/CONFSERVER-67940

https://support.citrix.com/article/CTX267027

https://www.oracle.com/security-alerts/alert-cve-2020-14750.html

https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22205.json

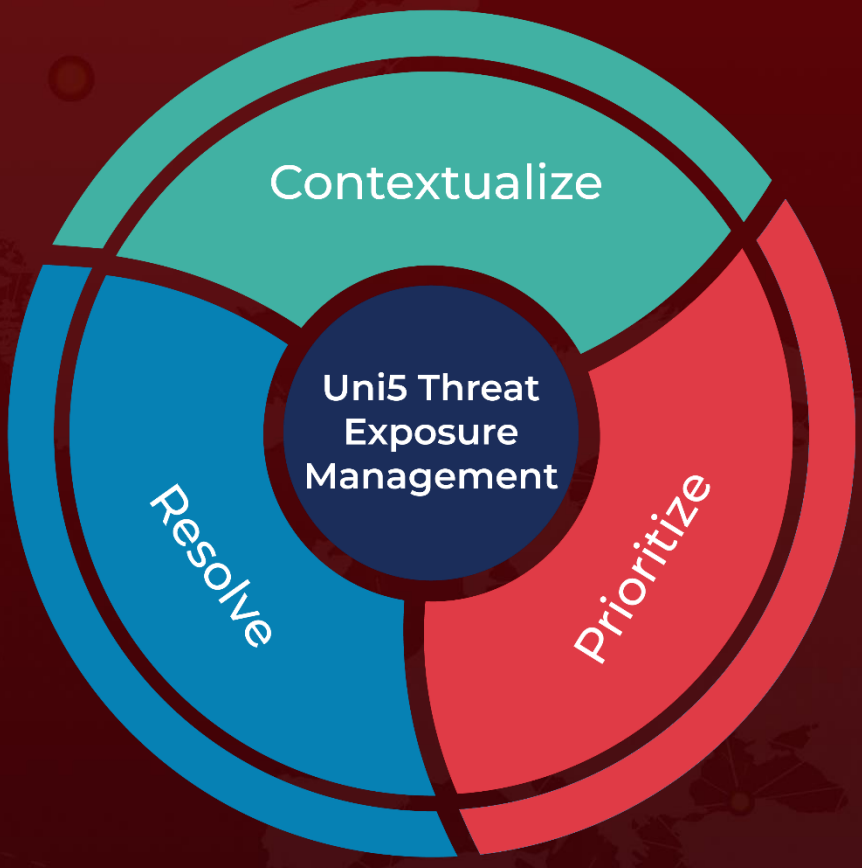
References

https://www.mandiant.com/resources/blog/unc961-multiverse-financially-motivated

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 24, 2023 • 3:00 AM

More at www.hivepro.com