Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

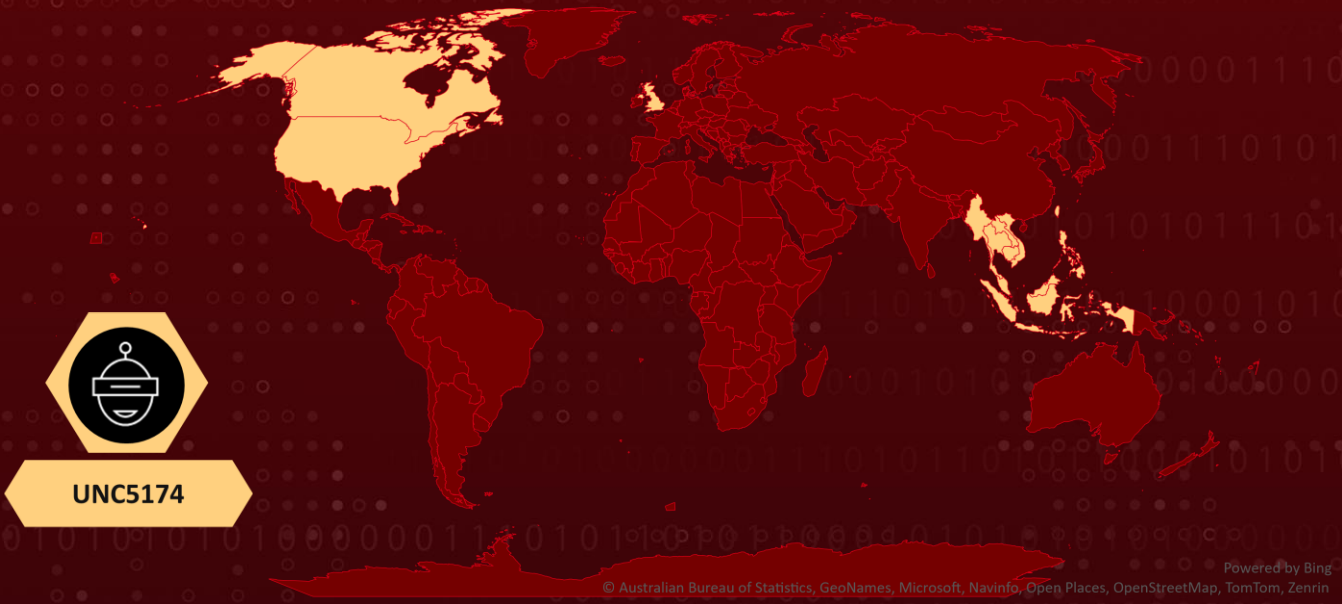
UNC5174 Functions as an Initial Access Broker, Exploiting Vulnerabilities

Date of Publication	Admiralty Code	TA Number
March 27, 2024	A1	TA2024121

Summary

Attack Commenced: October 2023
Attack Region: Southeast Asia, US, Hong Kong, UK, Canada, Taiwan
Threat Actor: UNC5174 (aka Uteus)
Affected Industries: Research, Education institutions, Charities and Non-governmental organizations (NGOs), Government organizations, Think Tanks
Malware: SNOWLIGHT, GOHEAVY, GOREVERSE, and SUPERSHELL
Attack: UNC5174, a threat actor believed to be associated with China, has been identified exploiting various vulnerabilities and deploying custom tools such as SNOWLIGHT, GOHEAVY, and GOREVERSE for post-exploitation activities. These tools enable UNC5174 to carry out sophisticated cyber operations, potentially aligned to infiltration and espionage operations.

Attack Regions



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

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-46747	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability	F5 BIG-IP Configuration Utility	✗	✓	✓
CVE-2024-1709	ConnectWise ScreenConnect Authentication Bypass Vulnerability	ConnectWise ScreenConnect	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-22518	Atlassian Confluence Improper Authorization Vulnerability	Confluence Data Center, Confluence Server	✗	✓	✓
CVE-2022-0185	Linux Kernel Vulnerability	FAS/AFF BMC, NetApp HCI BMC	✗	✗	✓
CVE-2022-30525	Zyxel Multiple Firewalls OS Command Injection Vulnerability	USG FLEX, ATP series, VPN series	✗	✓	✓

Attack Details

#1

UNC5174 (aka Uteus), a threat actor associated with China, has been observed exploiting vulnerabilities such as CVE-2023-46747 affecting F5 BIG-IP Traffic Management UI since October 2023 and CVE-2024-1709 in ConnectWise ScreenConnect instances since February 2024. They utilize custom tools like SNOWLIGHT, GOHEAVY, GOREVERSE for post-exploitation activities.

#2

Leveraging F5 BIG-IP flaw, UNC5174 created administrative user accounts and executed bash commands via TMSH. This malicious activity was evident in the "/var/log/restjavad-audit.log" and "/var/log/audit" log file showing illegimitate requests to the REST API. Subsequently, they leveraged their TMSH access to download and execute "/tmp/watchsys" using a cURL command, identified as SNOWLIGHT, a new 64-bit ELF downloader.

#3

SNOWLIGHT, a C-based Linux downloader, performs various actions such as file deletion, process killing, file downloading from a remote URL, permission modification, and in-memory payload execution. It connects to an IP address over TCP port 443 utilizing raw sockets, and a uses binary protocol to communicate with C2 sever, further decoding and executing a secondary ELF file. The secondary ELF file known as GOHEAVY serves several purposes, including establishing covert communication channels and potentially enabling lateral movement within compromised networks.

#4

UNC5174 also deployed GOREVERSE, a publicly available reverse shell, to connect to the C2 infrastructure hosting the SUPERSHELL framework. Additionally, they used GOHEAVY, a Golang-based tunneler tool obfuscated using GOBFUSCATE, to establish covert communication channels and facilitate lateral movement within compromised networks. UNC5174 even attempted to self-patch vulnerabilities using mitigation scripts to limit future exploitation by other threat actors.

#5 UNC5174 was previously associated with Chinese hacktivist collectives such as "Dawn Calvary," "Genesis Day," and "Teng Snake." However, in mid-2023, they shifted their focus to access brokering for compromised environments and are suspected to be linked with PRC MSS (Ministry of State Security). UNC5174 shares similarities with UNC302 in terms of exploit usage and operational priorities. The organizations targeted by UNC5174, including U.S. defense and UK government entities, were concurrently targeted by UNC302.

#6 UNC5174's exploitation of multiple vulnerabilities and its usage of novel malwares underscores their comprehensive approach to infiltration, espionage operations. Their activities reflect a sophisticated approach to targeting vulnerabilities in edge equipment, highlighting the emergence of an initial access broker ecosystem utilized by PRC MSS to target multinational corporations, posing a significant threat globally.

Recommendations

Apply Patch: Install the security patch provided by vendors to address the exploited vulnerabilities. This patch closes the security gap that allows attackers to exploit the vulnerability.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Access Permissions and Logs: Begin by examining access permissions on critical system directories and files. Look for any discrepancies or unauthorized changes in permissions. Check system logs, including security logs, for any suspicious activities related to account creation or modification.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0011 Command and Control
TA0040 Impact	T1190 Exploit Public-Facing Application	T1027 Obfuscated Files or Information	T1070 Indicator Removal
T1070.004 File Deletion	T1140 Deobfuscate/Decode Files or Information	T1222 File and Directory Permissions Modification	T1222.002 Linux and Mac File and Directory Permissions Modification
T1601 Modify System Image	T1601.001 Patch System Image	T1016 System Network Configuration Discovery	T1049 System Network Connections Discovery
T1082 System Information Discovery	T1083 File and Directory Discovery	T1095 Non-Application Layer Protocol	T1105 Ingress Tool Transfer
T1572 Protocol Tunneling	T1573 Encrypted Channel	T1573.002 Asymmetric Cryptography	T1059 Command and Scripting Interpreter
T1059.004 Unix Shell	T1136 Create Account	T1136.001 Local Account	T1531 Account Access Removal
T1003 OS Credential Dumping	T1003.008 /etc/passwd and /etc/shadow	T1608 Stage Capabilities	T1608.003 Install Digital Certificate

Indicators of Compromise (IOCs)

TYPE	VALUE
IP	118.140.151[.]242, 61.239.68[.]73, 172.245.68[.]110
URL	http://172.245.68[.]110:8888
MD5	c867881c56698f938b4e8edafe76a09b, df4603548b10211f0aa77d0e9a172438, 0951109dd1be0d84a33d52c135ba9c97, 9c3bf506dd19c08c0ed3af9c1708a770, 0ba435460fb7622344eec28063274b8a, a78bf3d16349eba86719539ee8ef562d

Patch Link

https://my.f5.com/manage/s/article/K000137353

https://screenconnect.connectwise.com/download

https://www.atlassian.com/software/confluence/download-archives

https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=722d94847de2

https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-os-command-injection-vulnerability-of-firewalls

References

https://www.mandiant.com/resources/blog/initial-access-brokers-exploit-f5-screenconnect

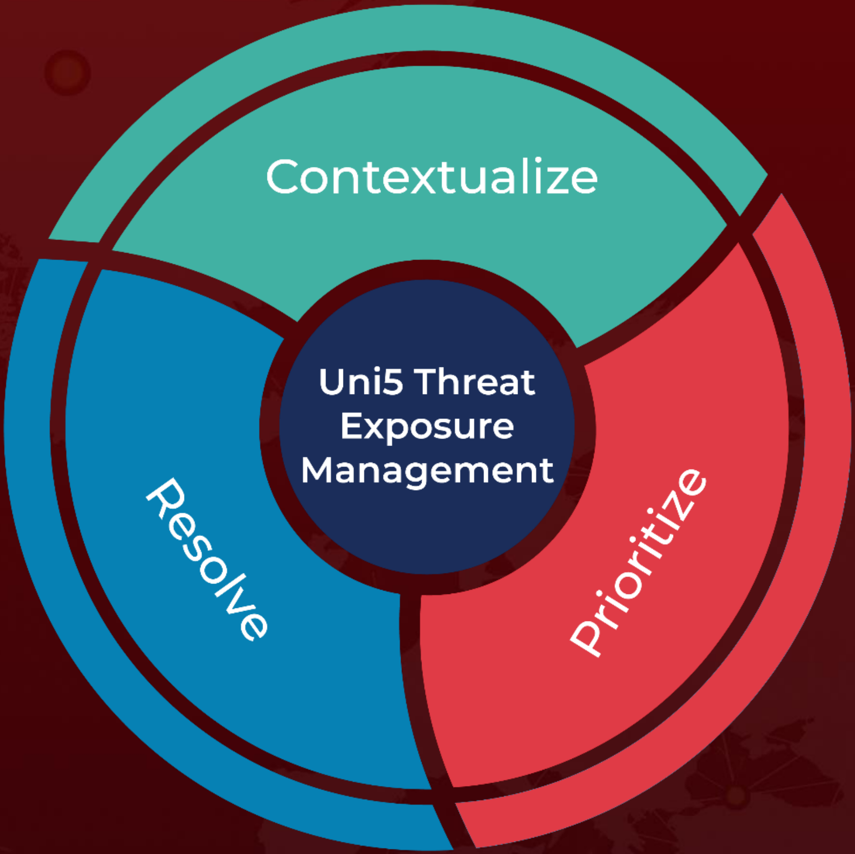
https://www.hivepro.com/threat-advisory/critical-vulnerabilities-in-screenconnect-under-active-exploitation/

https://www.hivepro.com/threat-advisory/atlassians-critical-confluence-flaw-risk-of-data-loss/

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 27, 2024 • 7:45 AM

More at www.hivepro.com