Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

Tropic Trooper Targets Middle East with New Web Shell

Date of Publication	Admiralty code	TA Number
September 6, 2024	A1	TA2024344

Summary

Attack Began: 2011
Actor Name: Tropic Trooper (aka Pirate Panda, APT 23, KeyBoy, Iron, Bronze Hobart, Earth Centaur)
Targeted Regions: The Middle East, and Malaysia
Malware: China Chopper, Crowdoor
Targeted Industries: Government

Actor Map

Tropic
Trooper
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-2021-34473	PROXYSHELL (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✗	✓	✓
CVE-2021-34523	PROXYSHELL (Microsoft Exchange Server Privilege Escalation Vulnerability)	Microsoft Exchange Server	✗	✓	✓
CVE-2021-31207	PROXYSHELL (Microsoft Exchange Server Security Feature Bypass Vulnerability)	Microsoft Exchange Server	✗	✓	✓
CVE-2023-26360	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability	Adobe ColdFusion	✓	✓	✓

Actor Details

#1

Tropic Trooper, also known as KeyBoy or Pirate Panda, is a Chinese-speaking advanced persistent threat (APT) group that has been active since 2011. This group is notorious for targeting government institutions, military agencies, healthcare, and high-tech industries, particularly in regions like Taiwan, the Philippines, and Hong Kong. Recently, they have shifted their focus towards government entities in the Middle East, especially those involved in human rights studies, marking a strategic expansion of their operations.

#2

In June 2024, researchers identified a new cyber campaign involving Tropic Trooper, which began in June 2023. The attack utilized several known vulnerabilities in widely used applications, including Microsoft Exchange and Adobe ColdFusion, to deliver the web shell.

#3

The campaign was characterized by the deployment of a web shell variant known as China Chopper on a public web server running the Umbraco content management system (CMS). This web shell was compiled as a .NET module and allowed the attackers to remotely control the compromised server. The exploitation chain led to the introduction of a malware implant named Crowdoor, a variant of the SparrowDoor backdoor, which was designed for network scanning, lateral movement, and evasion of defenses.

#4

Tropic Trooper's techniques included DLL side-loading and the use of post-exploitation tools to maintain persistence and exfiltrate sensitive information while bypassing traditional security defenses. The group has also been linked to the USBferry attack, which targets air-gapped environments by delivering malicious payloads through USB devices. This method has been active since at least 2014, primarily focusing on military and government users in Asia.

#5

The recent activities of Tropic Trooper highlight their evolving tactics and the growing sophistication of their cyber espionage efforts, particularly in sensitive geopolitical contexts. Their targeting of human rights-related entities in the Middle East suggests a deliberate strategy to gather intelligence on critical issues, indicating the potential for significant implications for regional security and human rights advocacy.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Tropic Trooper (aka Pirate Panda, APT 23, KeyBoy, Iron, Bronze Hobart, Earth Centaur)	China	The Middle East and Malaysia	Government
	MOTIVE		
	Information theft and espionage		

Recommendations

Strengthen Public-Facing Applications: Regularly update and patch public-facing applications to close vulnerabilities that could be exploited for initial access, particularly those exploited by Tropic Trooper (e.g., Microsoft Exchange and Adobe ColdFusion vulnerabilities).

Implement Robust Access Controls: Enforce the principle of least privilege, restricting access to critical systems and data, and closely monitor user permissions to prevent lateral movement by attackers.

Enhance Incident Response Capabilities: Develop and regularly test a proactive incident response plan that includes scenarios involving sophisticated malware, persistence mechanisms, and data exfiltration techniques.

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.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0042 Resource Development	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0001 Initial Access	TA0003 Persistence	TA0043 Reconnaissance	TA0011 Command and Control
TA0006 Credential Access	TA0007 Discovery	T1588.006 Vulnerabilities	T1218.007 Msiexec
T1218 System Binary Proxy Execution	T1068 Exploitation for Privilege Escalation	T1588.005 Exploits	T1218.011 Rundll32
T1059 Command and Scripting Interpreter	T1059.007 JavaScript	T1027 Obfuscated Files or Information	T1055 Process Injection

T1505.003 Web Shell	T1574.001 DLL Search Order Hijacking	T1574 Hijack Execution Flow	T1543.003 Windows Service
T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1543 Create or Modify System Process	T1090 Proxy
T1046 Network Service Discovery	T1003.001 LSASS Memory	T1003 OS Credential Dumping	T1018 Remote System Discovery
T1190 Exploit Public-Facing Application	T1588 Obtain Capabilities		

Indicator of Compromise (IOCs)

TYPE	VALUE
MD5	0b9ae998423a207f021f8e61b93bc849, 103e4c2e4ee558d130c8b59bfd66b4fb, 149a9e24dbe347c4af2de8d135aa4b76, 1dd03936baf0fe95b7e5b54a9dd4a577, 27c558bd42744cddc9edb3fa597d0510, 2c7ebd103514018bad223f25026d4db3, 3b7721715b2842cdff0ab72bd605a0ce, 3f15c4431ad4573344ad56e8384ebd62, 4f950683f333f5ed779d70eb38cdadcf, 78b47dda664545542ed3abe17400c354, 868b8a5012e0eb9a48d2daf7cb7a5d87, 8a900f742d0e3cd3898f37dbc3d6e054, c10643b3fb304972c650e593b69faaa1, dd7593e9ba80502505c958b9bbbf2838, e0d9215f64805e0bff03f4dc796fe52e, e845563ba35e8d227152165b0c3e769f, fca94b8b718357143c53620c6b360470, fd8382efb0a16225896d584da56c182c
SHA1	311d1d50673fbfc40b84d94239cd4fa784269465, 69112c87f67dd2a0be79e57323aeb28874d5fb08, c944e49a476b7a2b50e4f2b3ac681e08d118f8fe

TYPE	VALUE
SHA256	8df9fa495892fc3d183917162746ef8fd9e438ff0d639264236db553b09629dc, 9ba6c63e29b26174e52a519c1afe7a4401e65485fd6ce6a2d574d910dd1d8d22
IPv4	162[.]19[.]135[.]182, 51[.]195[.]37[.]155
Domains	techmersion[.]com, blog[.]techmersion[.]com
File path	c:\sql\tools\attunitycdcoracle\x64\1033, c:\microsoft.net\framework64\v4.0.30319\temporary asp.net files\root\fc88e889\b64f0276, c:\microsoft.net\framework64\v4.0.30319\temporary asp.net files\root\5b841946\ca5a9bf5

Patch Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html

References

https://securelist.com/new-tropic-trooper-web-shell-infection/113737/

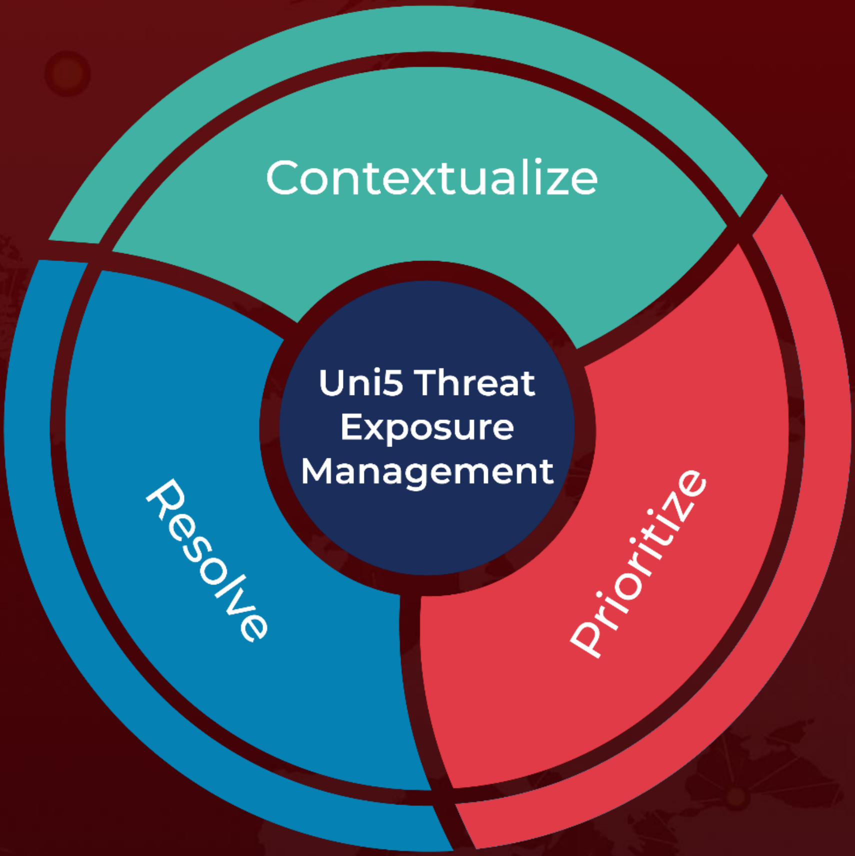
https://www.trendmicro.com/en_in/research/20/e/tropic-troopers-back-usbferry-attack-targets-air-gapped-environments.html

https://attack.mitre.org/groups/G0081/

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

September 6, 2024 • 5:30 AM

More at www.hivepro.com