Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

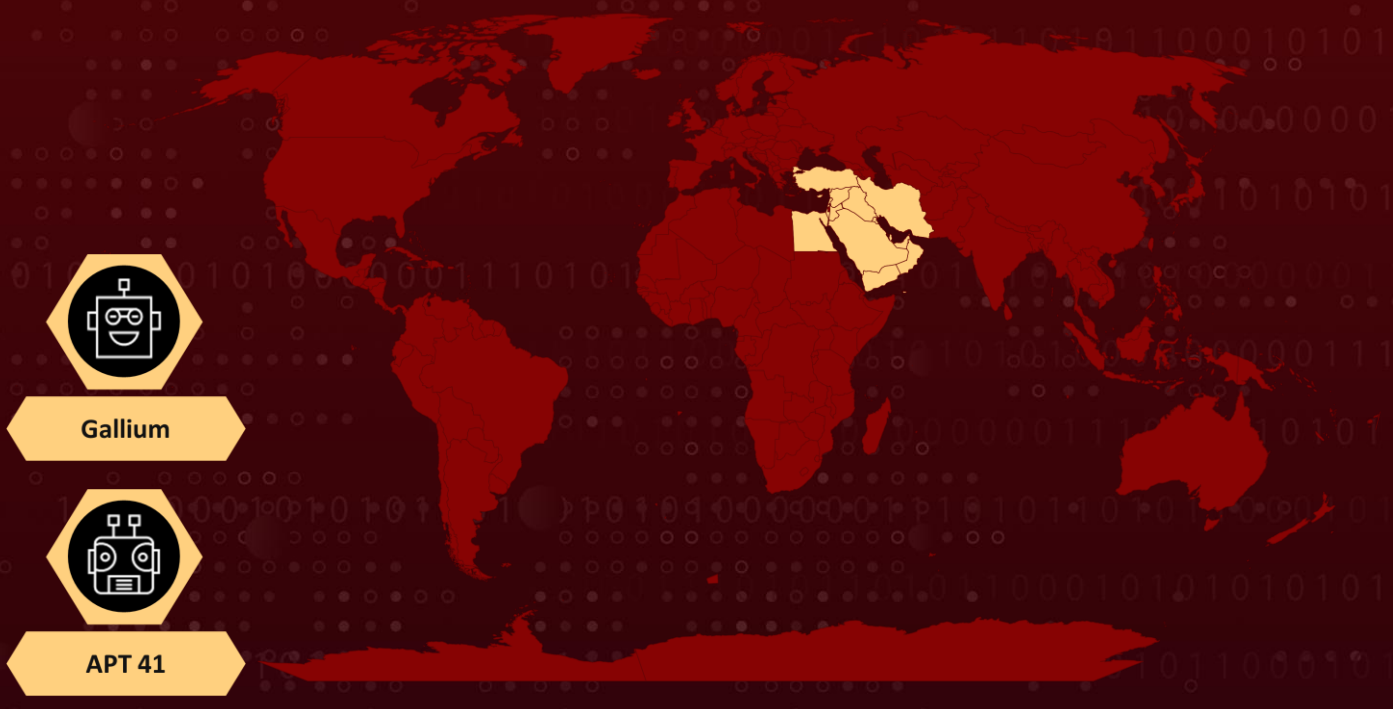
Chinese Cyber Espionage Targets Middle Eastern Telecoms

Date of Publication	Admiralty Code	TA Number
March 28, 2023	A2	TA2023163

Summary

Attack began: March 2023
Malware: mim221
Actor: Gallium and APT 41
Attack Region: Akrotiri and Dhekelia, Bahrain, Cyprus, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen.
Targeted Industries: Telecommunications
Attack: A Chinese cyber espionage group attributed to the Operation Soft Cell campaign, namely Gallium and APT41, has been observed targeting the telecommunications sector in the Middle East.

Attack Regions



Attack Details

#1

Gallium and APT41, Chinese cyber espionage groups connected to Operation Soft Cell campaign, are targeting Middle Eastern telecoms. The attack involves infiltrating Microsoft Exchange servers to deploy webshells for command execution. The attackers are using the mim221, an updated credential theft tool with anti-detection features, and native makecab tool for compressing exfiltrated information. For lateral movement, the attackers are utilizing PsExec tool and net use command to access shared resources on remote machines.

#2

The mim221 architecture comprises pc.exe Windows executable, AddSecurityPackage64.dll, pc.dll, and getHashFlsa64.dll DLLs. The attackers employ it for reconnaissance, credential theft, lateral movement, and data exfiltration. The Chinese cyber espionage actors are consistent in improving their malware to evade detection.

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

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0009 Collection	TA0011 Command and Control	T1055 Process Injection	T1059 Command and Scripting Interpreter
T1049 System Network Connections Discovery	T1003 OS Credential Dumping	T1547 Boot or Logon Autostart Execution	T1106 Native API
T1021 Remote Services	T1074 Data Staged	T1033 System Owner/User Discovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	f54a41145b732d47d4a2b0a1c6e811ddcba48558 1c405ba0dd99d9333173a8b44a98c6d029db8178 df4bd177b40dd66f3efb8d6ea39459648ffd5c0e 814f980877649bc67107d9e27e36fba677cad4e3 508408edda49359247edc7008762079c5ba725d9 97a7f1a36294e5525310f121e1b98e364a22e64d

References

https://www.sentinelone.com/labs/operation-tainted-love-chinese-apts-target-telcos-in-new-attacks/

https://www.cybereason.com/blog/research/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

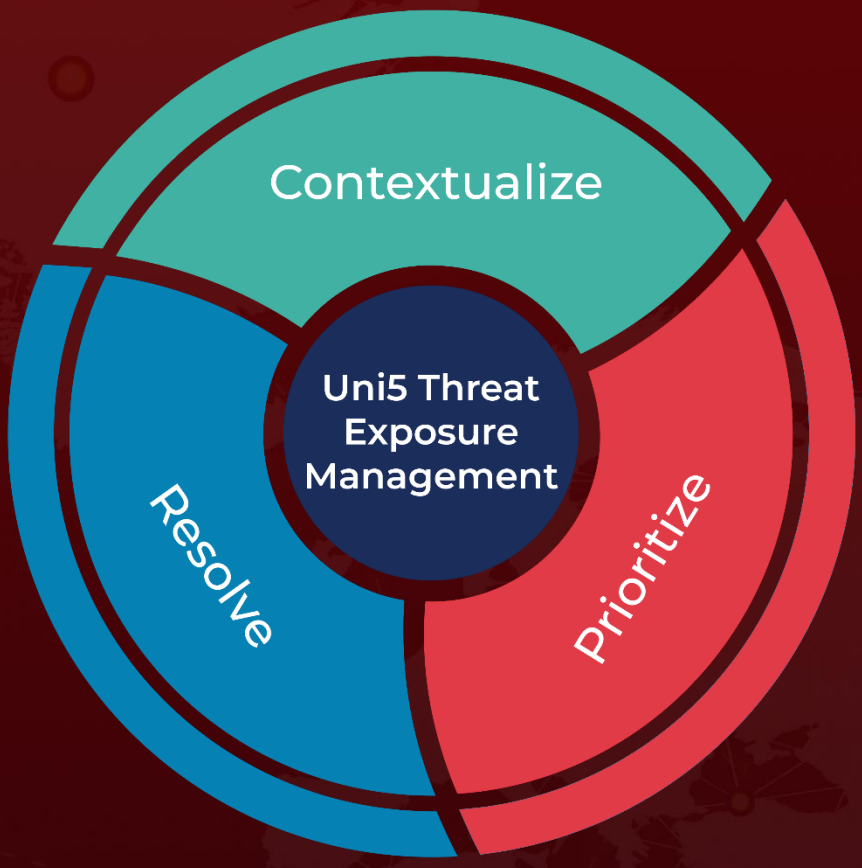
https://attack.mitre.org/groups/G0096/

https://attack.mitre.org/groups/G0093/

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 28, 2023 • 6:25 AM

More at www.hivepro.com