Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

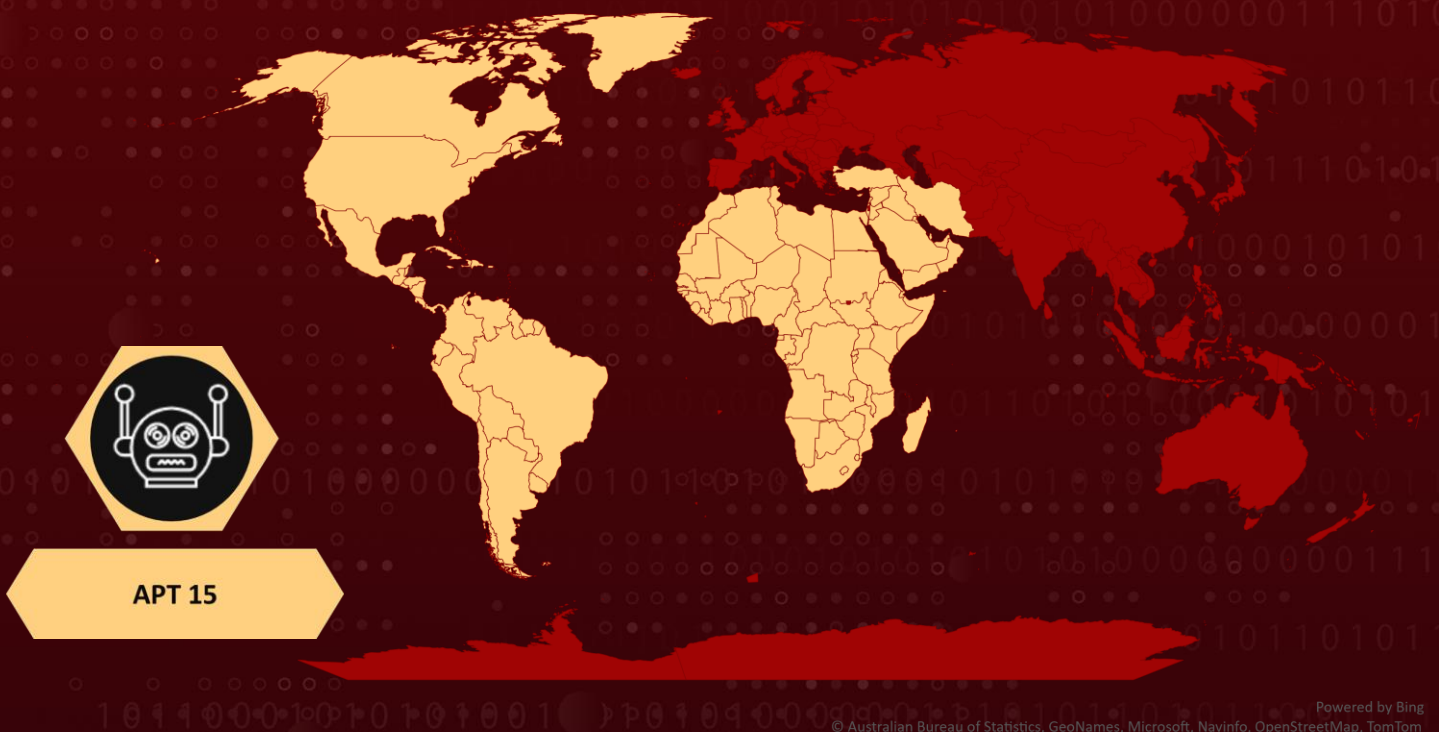
APT15 enhanced its arsenal with an updated variant of the Turian backdoor

Date of Publication	Admiralty Code	TA Number
January 19, 2023	A1	TA2023033

Summary

First appeared: 2010
Attack Region: North and South America, Africa, and the Middle East.
Threat Actor: APT15 (Playful Taurus, BackdoorDiplomacy, Vixen Panda, KeChang, and NICKEL)
Attack: APT15 is a Chinese advanced persistent threat group that regularly conducts cyber espionage attacks. The group has upgraded its Turian backdoor variant and targeted government and diplomatic entities in North and South America, Africa, and the Middle East.

Attack Regions



Attack Details

#1

APT15 has modified its toolkit to include new variants of the Turian backdoor, as well as new command and control infrastructure. The malware contains VMProtect, which obfuscates all API calls within the sample. The final payload is unpacked into the .text, .data, and .rdata sections of the payload, although it is not virtualized.

#2

The network protocol has been modified in this variant to make use of the Security Support Provider Interface (SSPI) instead. The backdoor provides generic capabilities, such as updating the C2 to connect with, command execution, and reverse shell spawning. In this variant, the command IDs appear to be randomized.

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	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0007 Discovery
TA0011 Command and Control	T1106 Native API	T1059 Command and Scripting Interpreter	T1134 Access Token Manipulation
T1049 System Network Connections Discovery	T1102 Web Service	T1553 Subvert Trust Controls	

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA1	cfd9884511f2b5171c00570da837c31094e2ec72 1cf1985aec3dd1f7040d8e9913d9286a52243aca
SHA256	67c911510e257b341be77bc2a88cedc99ace2af852f7825d97100166198 75e80,8549c5bafbfad6c7127f9954d0e954f9550d9730ec2e06d6918c05 0bf3cb19c3,5bb99755924ccb6882fc0bdedb07a482313daeaaa449272dc 291566cd1208ed5,ad22f4731ab228a8b63510a3ab6c1de5760182a7fe9 ff98a8e9919b0cf100c58,6828b5ec8111e69a0174ec14a2563df151559c 3e9247ef55aeaaf8c11ef88bfa
Domains	vpnkerio[.]com update.delldrivers[.]in scm.oracleapps[.]org update.adboeonline[.]net mail.indiarailways[.]net
IP Addresses	152.32.181[.]16 158.247.222[.]6

References

https://unit42.paloaltonetworks.com/playful-taurus/#post-126622-_sert7axmryed

https://www.hivepro.com/backdoordiplomacy-targets-the-telecom-industry-in-the-middle-east/

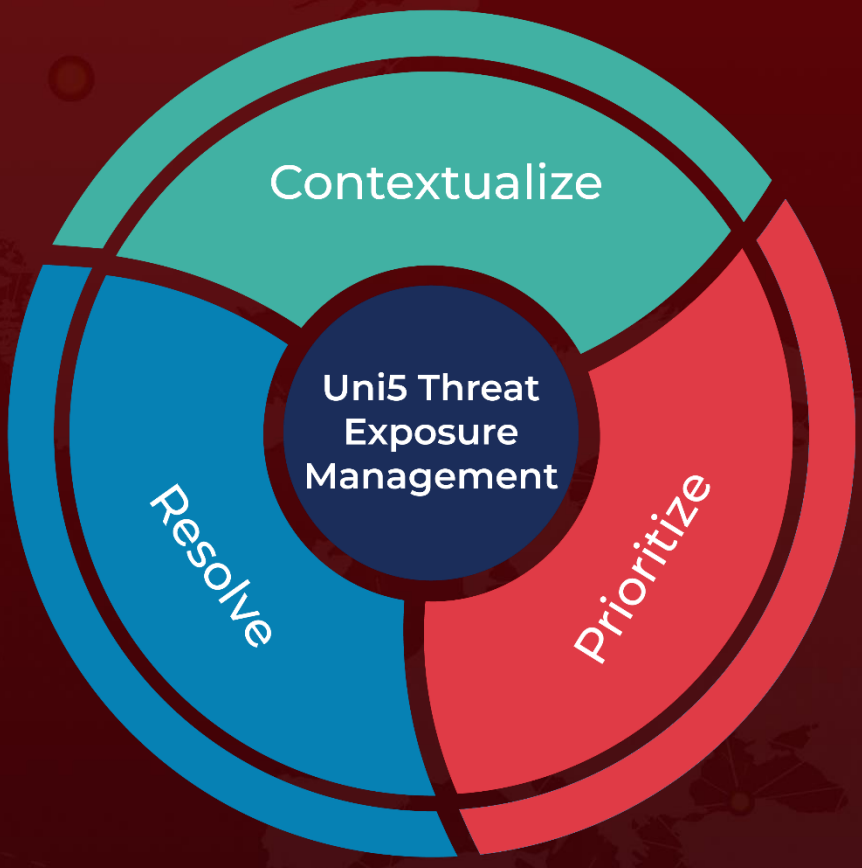
https://attack.mitre.org/groups/G0135/

https://attack.mitre.org/groups/G0004/

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

January 19, 2023 . 3:33 AM

More at www.hivepro.com