Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

New KamiKakaBot Malware Targeting Government Entities in ASEAN Countries

Date of Publication	Admiralty Code	TA Number
March 14, 2023	A1	TA2023132

Summary

First appeared: February 2023
Attack Region: ASEAN countries
Targeted Industries: Government
Actor Name: Dark Pink APT (Saaiwc Group, APT-LY-005)
Malware: KamiKakaBot
Attack: The new KamiKakaBot malware has been discovered targeting government entities in ASEAN countries, with the Dark Pink APT group believed to be behind the campaign.

Attack Regions

Attack Details

#1

In February 2023, a new cyberattack campaign using the KamiKakaBot malware being used to target government entities in ASEAN countries. This malware is designed to steal data from web browsers such as Chrome, Edge, and Firefox, including saved credentials, browsing history, and cookies. It can also allow the attackers to execute remote code on infected devices.

#2

The campaign is believed to be the work of the Dark Pink APT group, the malware is delivered via phishing emails containing a malicious ISO file as an attachment. The ISO file contains a decoy Word document, as well as a legitimate WinWord.exe file that is used for DLL side-loading. The KamiKakaBot loader is then executed into the memory of WinWord.exe.

#3

The malware uses various evasion techniques, such as Living-off-the-Land binaries, to remain undetected while executing its malicious actions. The attackers communicate with the malware using a Telegram bot controlled by the threat actor. The campaign has exploited the increasing digitization of economies and relationships between Europe and the ASEAN region.

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	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0001 Initial Access
TA0011 Command and Control	T1574 Hijack Execution Flow	T1059 Command and Scripting Interpreter	T1059.001 Powershell
T1574.002 DLL Side-Loading	T1204 User Execution	T1204.002 Malicious File	T1566 Phishing
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1036 Masquerading	T1112 Modify Registry
T1423 Network Service Scanning	T1055 Credentials from Password Stores	T1055.003 Credentials from Web Browsers	T1539 Steal Web Session Cookie
T1185 Browser Session Hijacking	T1203 Exploitation for Client Execution	T1218 System Binary Proxy Execution	T1102.002 Bidirectional Communication
T1102 Web Service	T1566.001 Spearphishing Attachment	T1547.004 Winlogon Helper DLL	T1036.007 Masquerading Double File Extension
T1140 Deobfuscate/Decode Files or Information	T1027 Obfuscated Files or Information		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	eae05a0d4468f865219130740dfe41bb
SHA1	c320963f3f64ce27a0c340807583b5bdb4d8fe27
SHA256	06ecb4ae52acd132706830e3f1d4885dfb1a89b2925130d62a55b635e8ef36fd

References

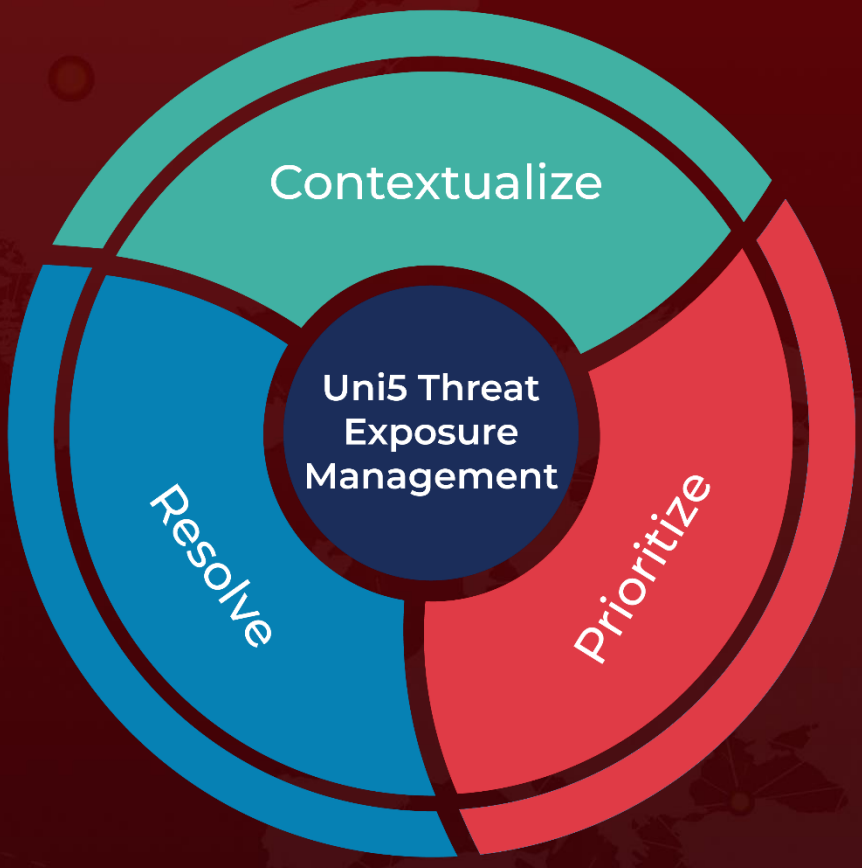
https://blog.eclecticiq.com/dark-pink-apt-group-strikes-government-entities-in-south-asian-countries

https://www.hivepro.com/southeast-asian-apt-group-saaiwc-targets-military-and-financial-departments-with-powerdism-backdoor/

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 14, 2023 • 12:03 AM

More at www.hivepro.com