KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Dark Pink APT Group Targets South-East Asian Entities

Tracker ID: TN2341 **Date:** March 15, 2023 **Category:** Threat Actor **Industry:** Government **Region**: South-East Asia

Background

The Dark Pink advanced persistent threat (APT) actor has been associated with a new wave of cyberattacks targeting government and military entities in Southeast Asian countries with the "KamiKakaBot" malware. The campaign's malware obfuscation technique has been enhanced to effectively evade anti-malware defenses. Dark Pink, also known as "Saaiwc," use specialized tools such as "TelePowerBot" and "KamiKakaBot" to execute arbitrary commands and steal sensitive data. The threat actor is attributed to Asian origin and has been active since at least mid-2021, with a surge in activity in 2022.

The malware is disseminated by social engineering lures, which are laced in ISO image file attachments in emails. The ISO image includes an executable (Winword.exe), a loader (MSVCR100.dll), and a counterfeit Microsoft Word document with the KamiKakaBot payload. The loader is customized to load the KamiKakaBot malware into the memory of the "Winword.exe" binary via the DLL side-loading mechanism to evade security measures. KamiKakaBot gathers data from web browsers and executes remote commands. The Winlogon Helper library changes malicious Windows Registry entries on the compromised host. The stolen data is later transferred as a ZIP archive to a Telegram bot.

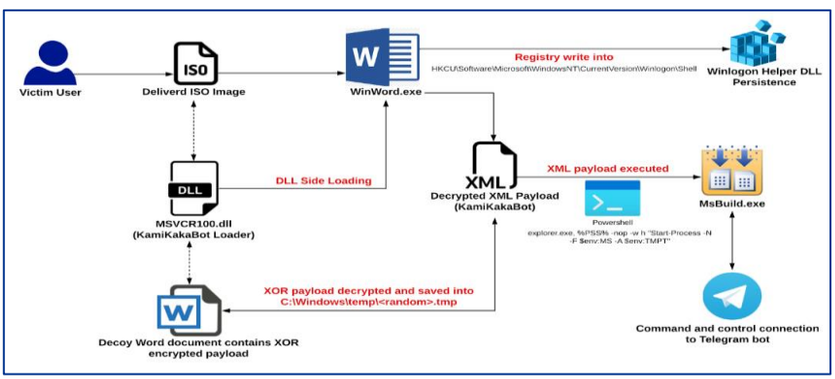

Figure 1 - Execution flow of KamiKakaBot.

The use of legitimate online services, such as Telegram, as a command-and-control (C2) server, remains a preferred choice for numerous threat actors, including advanced persistent groups. The most recent behavior of the Dark Pink APT gang refined its technical ability to circumvent security measures, scale TTPs for, blend in with victim environments, and impede detection throughout all aspects of its operations. The Dark Pink APT group will most likely continue to improve its behavioral evasion strategies based on its ability to creatively deploy TTPs and tools to secure persistent access to targets.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Dark Pink APT Group Targets South-East Asian Entities

Tracker ID: TN2341 **Date:** March 15, 2023 **Category:** Threat Actor **Industry:** Government **Region**: South-East Asia

MITRE ATT&CK Tactics

Initial Access, Execution, Defense Evasion, Persistence, Credential Access and Command and Control.

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Detections

Utilize the shared YARA rule and below detection methods to identify potential threats in the environment:

- Monitor new file creations with double extension ending with executable file extensions (.exe, .vbs, .bat and etc.).
- Monitor modification and creation of Windows registry keys and sub-keys under Winlogon registry locations (HKLM\Software[\Wow6432Node\]\Microsoft\Windows NT\CurrentVersion\Winlogon\ and HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\). Establish a baseline for the values of often abused registry key locations to improve detection accuracy.
- Establish command line baselines for command line commands of common executables, such as powershell, cmd, and other LOLBINs (including MSBuild), to identify potential malicious usage of the built-in tools.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Continuously monitor for suspicious or anomalous activities. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Disable mounting ISO images via group policy (GPO). Add a simple registry key under HKEY_CLASSES_ROOT\Windows.IsoFile\shell\mount called “ProgrammaticAccessOnly” which would remove the context menu item when a user right clicked an ISO. It also removed the functionality of double-clicking to auto-mount ISOs.
- Ensure endpoints have modern next-gen protection capabilities to guard against downloading malicious files from untrusted sources.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Dark Pink APT Group Targets South-East Asian Entities

Tracker ID: TN2341 **Date:** March 15, 2023 **Category:** Threat Actor **Industry:** Government **Region**: South-East Asia

- Disable browser password saving via group policy (GPO), Set the following policies below then close the Group Policy Management Editor:
  - Disable saving browser history: Enabled
  - Enable AutoFill: Disabled
  - Enable saving password to the password manager: Disabled
  - Default cookies setting: Enabled: Keep cookies for the duration of the session
  - Enable saving password to the password manager: Disabled
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

References

- EclecticIQ Threat Research Team, Dark Pink APT Group Strikes Government Entities in South Asian Countries, EclecticIQ, March 14, 2023, External Link (blog.eclecticiq.com).
- Ravie Lakshmanan, KamiKakaBot Malware Used in Latest Dark Pink APT Attacks on Southeast Asian Targets, The Hackers News, March 13, 2023, External Link (thehackernews.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

*

SHA-256
205f6808ab05ff3932ee799f37c227a7a950e07ea97f51d206e0563c83592e60