KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Winter Vivern APT Group Weaponizes MS Office Docs for Espionage Campaigns

Tracker ID: TN2348 **Date:** April 03, 2023 **Category:** Campaign **Industry:** Government, Telecom **Region**: Asia

Background

"Winter Vivern," an advanced persistent threat, has been linked to attacks targeting government figures in India, Lithuania, Slovakia, and the Vatican since 2021. The APT attacks on commercial enterprises, notably telecoms organizations that help Ukraine in the ongoing war, is of particular concern. Winter Vivern, also known as UAC-0114, came to light last month after the Computer Emergency Response Team of Ukraine (CERT-UA) revealed a fresh malware campaign aimed at targeting state authorities in Poland and Ukraine to spread the virus known as "Aperetif."

The underreported group "Winter Vivern" has pro-Russian goals and was first publicized by DomainTools in early 2021. An additional investigation later revealed new behavior connected with Winter Vivern. The threat actor uses a variety of tactics, such as phishing websites, password phishing, and the distribution of malicious documents, that are customized to the specific requirements of the targeted organization. This leads to the distribution of customized loaders and malicious documents, allowing unauthorized access to confidential systems and information.

In the latest campaign, the group has used weaponized Microsoft Excel documents with XLM macros to implant PowerShell on compromised hosts. Although the threat actor's origins are unclear, the cluster appears to be aligned with goals that serve the interests of the governments of Belarus and Russia, according to the attack patterns.

To trick users of the official email service of the Indian government, Winter Vivern set up credential phishing web pages for "email.gov[.]in". Batch scripts that seem to be malware scanners were also used in the attack chains to cause the "Aperetif" malware to be deployed from actor-controlled infrastructure, including infected WordPress websites. Aperetif is malware built on Visual C++ that can gather victim data, keep a backdoor open, and get more payloads from the command-and-control (C2) server.

The cyber espionage group Winter Vivern has been successful in carrying out attacks utilizing simple but efficient attack methodologies and tools. Governments and highly valued private companies are prime targets in their attacks, demonstrating their level of intelligence and strategic aim. They are also skilled at luring targets into assaults and are emerging as a formidable force in cyberspace due to their adaptable collection of TTPs and ability to remain anonymous.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Winter Vivern APT Group Weaponizes MS Office Docs for Espionage Campaigns

Tracker ID: TN2348 **Date:** April 03, 2023 **Category:** Campaign **Industry:** Government, Telecom **Region**: Asia

MITRE ATT&CK Tactics

Initial Access, Exfiltration, Command and Control

Indicators of Compromise *

Please refer to the attached sheet for IOCs.

Recommendations

- Check with your existing AV/EDR vendor to validate the detection scope of identified samples.
- Verify the URL the one is visiting to ensure the site is legitimate before clicking on it or downloading software. The intended URL may be like a legitimate domain name, but it may have errors like a misplaced letter.
- End users should be made aware of the latest phishing tactic employed by the threat actors and ensure not click on any suspicious URLs or emails.
- Organizations should ensure that macros are disabled in Microsoft Office program and users should refrain from enabling them when prompted.
- Before emails arrive in the user's inbox, spam filters should be implemented to automatically remove suspicious or undesired emails.
- In order to prevent malware or TAs from stealing data, keep an eye on the beacon at the network level.
- Continuously monitor for suspicious or anomalous activities. Collect and review relevant logs, data, and artifacts to identify any threat in the network.
- Ensure endpoints have modern next-gen protection capabilities to guard against downloading malicious files from untrusted sources.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

References

- Ravie Lakshmanan, Winter Vivern APT Group Targeting Indian, Lithuanian, Slovakian, and Vatican Officials, The Hackers News, March 17, 2023, External Link (thehackernews.com).
- TOM HEGEL, Winter Vivern | Uncovering a Wave of Global Espionage, SentinelLabs, March 16, 2023, External Link (www.sentinelone.com).

KPMG in India Cyber Response Hotline : +91 9176471471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

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 Cyber Threat Intelligence Platform

Cyber Threat Notification | Winter Vivern APT Group Weaponizes MS Office Docs for Espionage Campaigns

Tracker ID: TN2348 **Date:** April 03, 2023 **Category:** Campaign **Industry:** Government, Telecom **Region**: Asia

*

SHA-256	Domain	URL	IP	SHA1
b60c6945455baa75cadd7b8ca89ae6dd1273aa3b91fd67d0fec8416b8fe9ea1d	bugiplaysec[.]com	hxxps://applesaltbeauty[.]com/wordpress/wp-includes/widgets/classwp/521734i	176.97.66[.]57	0fe3fe479885dc4d9322b06667054f233f343e20
a0bd37a927cfc4a15c502e28614958290e547b430820caeb0f621fdc12645db5	marakanas[.]com	hxxps://marakanas[.]com/Kkdn7862Jj6h2oDASGmpqU4Qq4q4.php	179.43.187[.]175	83f00ee3895043652749976 9db5c7ecb74a9ea41
7ae31d6b2a42edbf32c51baf191db870b45707755e8feefa053371747355b7ac	mfa_it_sec@outlook[.]com	hxxps://natply[.]com/wordpress/wp-includes/fonts/ch/097214o	179.43.187[.]207	a19d46251636fb46a013c7b52361b7340126ab27
72028cff34d33e26bf01e4bf63c8b977ece33b3809bd6dd075bcff343895dc4b	ocs-romastassec[.]com	hxxps://ocs-romastassec[.]com/goog_comredira3cf7ed34f8.php	195.54.170[.]26	a574c5d692b86c6c3ee710af69fccbb908fe1bb8
05457a790782542d3f16c9b8368a077b458ff7349856e6da541223a51e94b9c8	ocspdep[.]com		80.79.124[.]135	c7fa6727fe029c3eaa6d9d8bd860291d7e6e3dd0
a5115118908268569db2b1187b5b13b2cec9480585728d7da0abff38ecd771a6	security-ocsp[.]com			f39b260a9209013d9559173f12fbc2bd5332c52a
	troadsecow[.]com			