KPMG Cyber Threat Intelligence Platform

UNC2814 - Stealth Espionage via GRIDTIDE Backdoor

TLP : Clear

KPMG. Make the Difference.

UNC2814 is a PRC-aligned cyber espionage group active since at least 2017. It primarily targets telecommunications and government sectors to obtain strategic surveillance data, including communications intelligence and personally identifiable information (PII). The group has confirmed intrusions in 42 countries and suspected targeting in over 70 across Africa, Asia, and the Americas.

Initial access is gained by exploiting or compromising internet-facing web servers and edge systems. After gaining access, it uses a service account with elevated permissions to move laterally through the environment via SSH. The attackers deploy the GRIDTIDE backdoor, which allows them to run shell commands and transfer files while using Google Sheets as a high-availability command-and-control (C2) channel, hiding malicious traffic inside normal cloud API requests. LOLBins are used for reconnaissance, privilege escalation, and maintaining persistence. The backdoor is launched using the command nohup ./xapt, ensuring it keeps running in the background even if the session closes. Persistence is maintained through a custom systemd unit named xapt.service, which disguises itself as a legacy Debian utility and allows systemd to automatically restart the malware from /usr/sbin/xapt. SoftEther VPN is deployed to establish an encrypted outbound tunnel to an attacker-controlled IP. For C2 communication, a cell-based polling method is used in which cell A1 receives attacker commands and is overwritten with status messages, cells A2 onward contain command output and file data, and cell V1 holds host fingerprint details from the compromised system. To avoid detection, all transmitted data is encoded using a URL-safe Base64 scheme that replaces the standard “+” and “/” characters with “–” and “_”.

UNC2814’s low-noise and Living-off-the-land-heavy tactics show the group’s mature capabilities while highlighting the need for behavior driven detection and strong defense-in-depth.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Patch your Windows environment with the latest version as per the OEM and secure it with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context.

The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

Atul Gupta
Partner
Head of Cyber Security
T: +91 98100 81050
E: atulgupta@kpmg.com

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

UNC2814 - Stealth Espionage via GRIDTIDE Backdoor

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
5.34.176[.]6	207.148.73[.]18
38.54.82[.]69	38.180.205[.]14
38.60.194[.]21	38.54.112[.]184
65.20.104[.]91	38.60.171[.]242
130.94.6[.]228	45.76.157[.]113
38.54.31[.]146	45.76.184[.]214
38.54.32[.]244	149.28.128[.]128
38.54.37[.]196	139.84.236[.]237
38.60.224[.]25	149.28.139[.]125
38.60.252[.]66	178.79.188[.]181
45.90.59[.]129	195.123.211[.]70
202.59.10[.]122	139.180.219[.]115
45.77.254[.]168	195.123.226[.]235

Indicators of Compromise: Domains	
kozow[.]com	ddnsgeek[.]com
ooguy[.]com	accesscam[.]org
camdvr[.]org	theworkpc[.]com
mywire[.]org	loseyourip[.]com
casacam[.]net	webredirect[.]org
ddnsfree[.]com	bumbleshrimp[.]com
freeddns[.]org	

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

UNC2814 - Stealth Espionage via GRIDTIDE Backdoor

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
2d261e232233eb8027dc8c1fcc128682
2d873e91ac1a0423b186bd4fbf8e50d0
be0a15969da42365acc8cbc91c9e8bed9b6362f5
852c068dca060ab0268a920d52704888abf17e9a
4eb994b816a1a24cf97bfd7551d00fe14b810859170dbf15180d39e05cd7c0f9
ce36a5fc44cbd7de947130b67be9e732a7b4086fb1df98a5afd724087c973b47