KPMG Cyber Threat Intelligence Platform

Sidecopy APT– Exploiting Multi-Platform Intrusions

TLP : Clear

KPMG. Make the Difference.

SideCopy is a Pakistan-linked APT group, active since 2019. It operates as a sub-cluster of Transparent Tribe (APT36), a known threat actor group engaged in cyber espionage across South Asia. APT36 typically targets Linux-based environments, while SideCopy focuses on Windows systems, using a range of Remote Access Trojans (RATs) and plugins to maintain persistence and extract sensitive data. SideCopy has shifted from HTA files to MSI packages for malware delivery and expanded its focus to critical infrastructure sectors in India and Afghanistan, including railways, oil and gas, and foreign ministries.

Sidecopy APT gains initial access through spear-phishing emails containing malicious ZIP attachments or links to spoofed domains, impersonating as trusted entities. Post access, it deploys payload through RAT to capture sensitive information, user account enumeration, keystroke logging, audio capture etc. The payload embedded in the attachment is executed using MSI installers and DLL side-loading is performed via LOLBins. Persistence is achieved through registry modifications and scheduled task creation, ensuring access across system reboots. To evade detection, it uses AES encryption to obscure payloads and scripts, and reflective loading to inject malicious code into memory, avoiding disk-based detection. For C2 communication, it establishes secure communication channels that mimic legitimate traffic patterns, incorporating UUID-based registration and use CURL to enable reliable data transfer over HTTP. The sensitive data including credentials and documents is exfiltrated using RAT functionalities.

SideCopy leverages social engineering, stealthy persistence mechanisms, and data exfiltration techniques, underscoring the need for enhanced email security, endpoint monitoring, and the implementation of geo-filtering on network devices to counter these threats.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected 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

B V, Raghavendra
Partner
T: +91 98455 45202
E: raghavendrabv@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

Sidecopy APT - Exploiting Multi-Platform Intrusions

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
144.91.72[.]17	64.188.27[.]144

Indicators of Compromise: Domains	
scigov[.]cn	tzdpt[.]com
zx176[.]com	m.zx176[.]com
hcmindia[.]net	egovservice[.]in
tzbs.tzdpt[.]com	egovservice[.]in
nhp.mowr.gov[.]in	hcmvip-india[.]com
hcmvip-india[.]net	cmc.egovservice[.]in
dss.egovservice[.]in	cmc.egovservice[.]in
dss.egovservice[.]in	pen.egovservice[.]in
pmshriggssssiwan[.]in	educationportals[.]in
reviewassignment[.]in	mail.egovservice[.]in
drjagrutichavan[.]com	dns1.indianblog[.]xyz
pakora.egovservice[.]in	cpanel.egovservice[.]in
pakola.egovservice[.]in	pakola.egovservice[.]in
modspaceinterior[.]com	webdisk.egovservice[.]in
reviewassignment[.]online	webmail.egovservice[.]in
cpcontacts.egovservice[.]in	gadchiroli.egovservice[.]in
updates.biossysinternal[.]com	cpcalendars.egovservice[.]in
updates.widgetservicecenter[.]com	

Indicators of Compromise: Hashes
68c7c14b9ac69491b23b3c3ad88f3a1e
6af1776a02536f72f810ca0fa21f38ff
74334bc0a9b02032a5a91f7a30d455d6

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Sidecopy APT - Exploiting Multi-Platform Intrusions

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
a3d8e4f55c50bc916f6410f31a811e2d
b6ef8bb7e47ddc55131990e21d2519a7
e321f5efca5fbe7ea23a168b6c550698
f78ef3ce842241a692a831f1f601628f
fbd5257ef2f7befbdcb77f3bef137091
0690116134586d41a23baed300fc6355
0a67bfda993152c93a212087677f9b60
0e57890a3ba16b1ac0117a624f262e61
0eb9e8bec7cc70d603d2d8b6efdd6bb5
1d65fa0457a9917809660fff782689fe
320bc4426f4f152d009b6379b5257c78
32a44a8f7b722b078b647e82cb9e85cf
53eebedc3846b7cf5e29a90a5b96c803
57c2f8b4bbf4037439317a44c2263346
589a65e0f3fe6777d17d0ac36ab07f6f
7637cbfa99110fe8e1074e7ead66710e
83ce6ee6ad09a466eb96f347a8b0dc20
8ceeeec0e33026114f028cbb006cb7fc
97c3328427b72f05f120e9a98b6f9b09
9d189e06d3c4cefdd226e645a0b8bdb9
9de50f9357187b623b06fc051e3cac4f
b5e71ff3932c5ef6319b7ca70f7ba8da
e165114280204c39e99cf0c650477bf8
ef40f484e095f0f6f207139cb870a16e
9f1f11a708d393e0a4109ae189bc64f1f3e312653dcf317a2bd406f18ffcc507
93fb036e65c0683af5ffb98e2b61e30499dec068a4e15bf3bec8066d3e246852

KPMG

KPMG Cyber Threat Intelligence Platform

Sidecopy APT - Exploiting Multi-Platform Intrusions

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
bc1acdca196f1ff72722243be2afe1429b88122afb9d4852d6d6e57689411d3d
a31f222fc283227f5e7988d1ad9c0aecd66d58bb7b4d8518ae23e110308dbf91
d777bcb6fba73faf96cb422383404c3b81a8afa5aebbc8ed70076081de7daa0c
81038a217237afd16d80da7fc9219cbd145f9698bb512e2b625559a47ba73fec