KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Pakistan-Based APT
‘SideCopy’ Targeting India's Defence Ministry, DRDO

Tracker ID: TN2354 **Date:** March 29, 2023 **Category:** Campaign **Industry:** Government **Region**: Asia - India

Background

The advanced persistent threat (APT) group "SideCopy," which has a history of assaulting India and Afghanistan, is currently linked to a new phishing operation that disseminates "Action RAT." The recent operation is attributed to SideCopy, where they targeted the Defence Research and Development Organization (DRDO), the research and development wing of India's Ministry of Defence. SideCopy is well known for using counterfeits of SideWinder infection networks to spread its malware, which overlaps with Transparent Tribe. It has been operational since 2019.

The Defence Research and Development Organization (DRDO) is an Indian government organization charged with researching and developing advanced technologies used by the Indian Armed Forces. Its primary emphasis is on developing innovative defence systems such as missiles, radars, electronic warfare and communication systems, marine and aircraft systems. The agency plays a critical part in India's defence sector, adding to the country's military power and defence technology self-sufficiency.

The transmission chain of the SideCopy APT is similar to that of the SideWinder APT. According to some accounts, this threat actor shares traits with Transparent Tribe (APT36) and could be a sub-group of that threat actor. The group's attack chains begin with spear-phishing emails to obtain early entry point. These emails include a ZIP package file containing a Windows shortcut file (.LNK) disguised as material about the DRDO's K-4 ballistic missile. When the .LNK file is executed, it retrieves an HTML application from a distant server, which shows a decoy presentation while stealthily installing the Action RAT backdoor.

In addition to collecting information about the target machine, the malware is capable of carrying out instructions sent from a command-and-control (C2) server, such as file harvesting and malware distribution. AuTo Stealer, a novel information-stealing malware that can collect and exfiltrate Microsoft Office files, PDF documents, database and text files, and images via HTTP or TCP is also deployed by the threat actor. This isn't the first time SideCopy has used Action RAT in an assault against India. The SideCopy APT group is constantly evolving its methods and adding new tools to its arsenal. We suggest organizations to adopt cybersecurity best practices to establish the first line of defence against such attackers.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Pakistan-Based APT ‘SideCopy’ Targeting India's Defence Ministry, DRDO

Tracker ID: TN2354 **Date:** March 29, 2023 **Category:** Campaign **Industry:** Government **Region**: Asia - India

MITRE ATT&CK Tactics

Initial Access, Execution, Defense Evasion, Persistence, Discovery, Collection, Command and Control and Exfiltration.

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.
- Organizations conduct phishing awareness training for their employees and partners to stress the importance of caution when opening emails, particularly those messages from unfamiliar senders or with unknown subjects.
- Avoid downloading pirated software from warez/torrent websites. The “Hack Tool” present on sites such as YouTube, torrent sites, etc., mainly contains such malware.
- Implement complex passwords and enforce multi-factor authentication wherever possible.
- Keep applications and software updated. Turn on the automatic software update feature on computer, mobile, and other connected devices.
- Implement a reputed antivirus and internet security software package on connected devices, including PC, laptop, and mobile.
- Educate employees to refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Educate employees on protecting themselves from threats like phishing/untrusted URLs.
- Block URLs that could be used to spread the malware, e.g., Torrent/Warez.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Enable Data Loss Prevention (DLP) Solutions on the employees’ systems.
- Follow multilayered defense solutions and active monitoring to detect threats before operators can launch their attacks.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Pakistan-Based APT ‘SideCopy’ Targeting India's Defence Ministry, DRDO

Tracker ID: TN2354 **Date:** March 29, 2023 **Category:** Campaign **Industry:** Government **Region**: Asia - India

References

- Cyble Blogs, Notorious SideCopy APT group sets sights on India’s DRDO, Cyble, March 21, 2023, External Link (blog.cyble.com).
- Ravie Lakshmanan, Pakistan-Origin SideCopy Linked to New Cyberattack on India's Ministry of Defence, TheHackerNews, March 28, 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

Hash MD5	Hash SHA1	Hash SHA256	URL	IP
0725318b4f5c312eeaf5ec9795a7e919	9902348fc5dffe10a94a3f4be219dc42330ed480	9aed0c5a047959ef38ec0555ccb647688c67557a6f8f60f691ab0ec096833cce	hxxps[:]//www[.]cornerstonebeverly[.]org/js/files/DRDO-K4-Missile-Clean-room[.]zip	144[.]91[.]72[.]17:8080
ab11b91f97d7672da1c5b42c9ecc6d2e	feeadc91373732d65883c8351a6454a77a063ff5	a2e55cbd385971904abf619404be7ee8078ce9e3e46226d4d86d96ff31f6bb9a	hxxps[:]//www[.]cornerstonebeverly[.]org/js/files/docufentososo/doecumentosoneso	
2e19b7a2bbdc8082024d259e27e86911	d7dcea1c35475caa85e9298e44b63d3ce43fb2f0	e88835e21c431d00a9b465d2e8bed746b6369892e33be10bc7ebbda6e8185819	hxxps[:]//www[.]cornerstonebeverly[.]org/js/files/docufentososo/doecumentosoneso/pantomime.hta	
	e612dbb34e01b41e46359019db9340e17e0390b8	85faf414ed0ba9c58b9e7d4dc7388ba5597598c93b701d367d8382717fb485ec		
	3c4c8cbab1983c775e6a76166f7b3c84dde8c8c5	865e041b41b9c370a4eed91a9a407bd44a94e16e236e07be05e87de319a4486c		

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia