Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

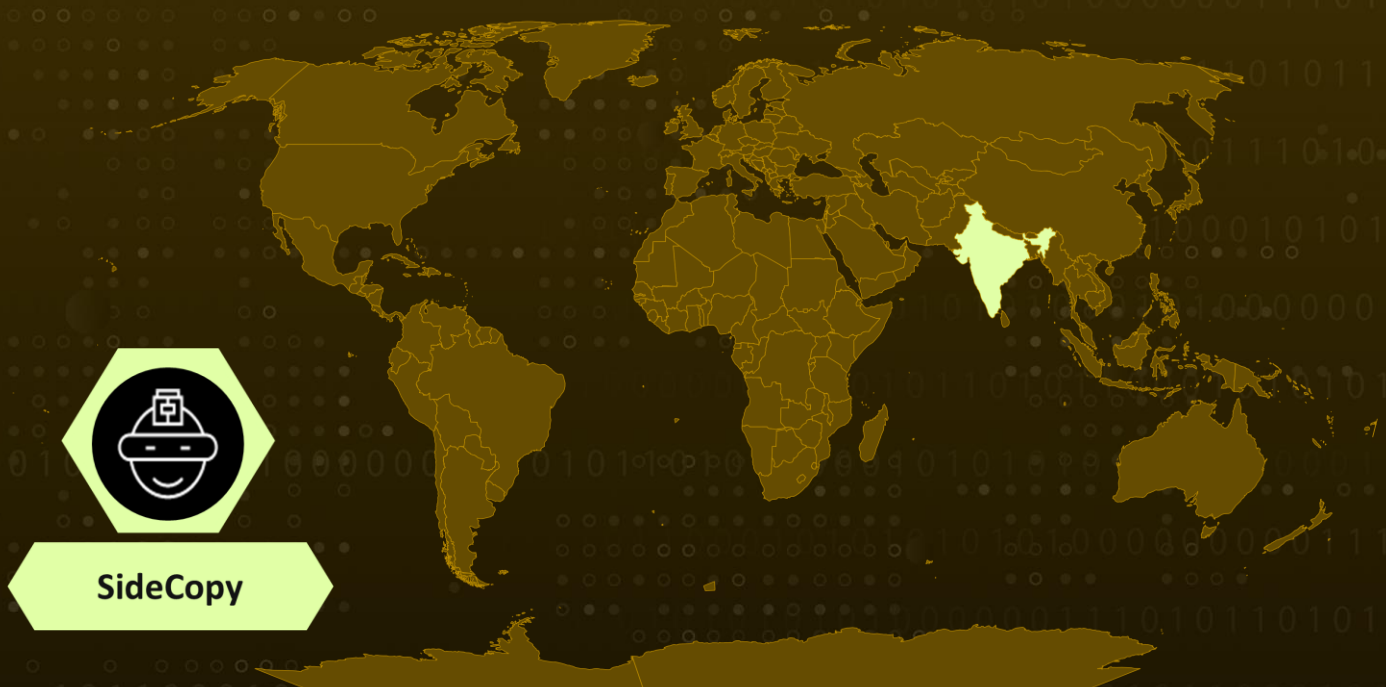
SideCopy APT Launches Phishing Campaign Against Indian Government

Date of Publication	Admiralty Code	TA Number
December 27, 2022	A1	TA2022318

Summary

First Appearance: 2019
Actor Name: SideCopy
Target Region: India
Target Sectors: Defense, Embassies, Government

Actor Map



Actor Details

#1 The new malicious activity of the SideCopy threat actors is the attack campaign STEPPY#KAVACH, which was notably active in 2021 and was originally related to Pakistan. The most recent malicious attack campaign we observed began with infection via a targeted phishing attempt.

#2 LNK files are used to initiate code execution, which then downloads and executes a malicious C# payload that acts as a remote access trojan (RAT). This current SideCopy attack effort has targeted a two-factor authentication solution called Kavach that is used by Indian government officials and appears to be identical to previous campaigns launched by APT36 and TransparentTribe.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
SideCopy	Pakistan **MOTIVE** Information theft and Espionage	India	Defense, Embassies, Government

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0011 Command and Control	TA0010 Exfiltration	T1566 Phishing	T1566.001 Spearphishing Attachment
T1204 User Execution	T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1059.001 PowerShell
T1059.003 Windows Command Shell	T1059.007 JavaScript	T1218 System Binary Proxy Execution	T1218.005 Mshta
T1036 Masquerading	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1573 Encrypted Channel
T1573.001 Symmetric Cryptography	T1105 Ingress Tool Transfer	T1571 Non-Standard Port	T1041 Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	889dd2abc6aa85863d6ea46c86d95050ac702c5743523ef5aeec63a8ff356d34 e56cbac2134c6bcb67cf25428f8d7db959d341a26d81e4eb4f9f77e7186e5906 36eda255b689e66fbc70ae0264eed7b79ed99022e4b3409748474d9bb73ae64e 66c4f5b3702cc76b6ae67851835e078c16c88f716eae8375c1ba797c6eaa375f df16aab18a13f16fa272555e6aa762f5098b0c4f06cb26bfbcc23a5f4f8668db 6484088f132efbd416eba7ac3f3339a41500f28bf8d58b18b4da75258c8a2fb4 d47a36fe2490e0e480dd59827495da93abe997cf20302aaedadca5988295c526 5ad783061390d75d7d947b6801b0e0b8d677b656ae6508bf6d355a32ab5c2fdf

TYPE	VALUE
SHA256	c7c6ea40ce0f0f540dae8512b1b26f32f465eb70ec248aa540d119e86356afb4 c8127216d74724b9bbad1cffe2d00acd908c2ba664e37fe2f97f397ada5e75d6 0eb2da6e6905e46ceb2a7c50500e9a5cb2a35cd4879ad3ad78d11d6e60a82a69 3a6ab95138ee9bd3a74f7c8dce93469e78588ddbfc6a44d85e9b1b849fa13ba7 fb4a2bac3e60b6a84c7ae19e73e57f3677673823da3ce8c90dfe697313b7438c 963f1895a44f94c995b901a8ce896efacce0c1a8662a20ba1348eb7c6325cc19 cb9ab35ec79e0ccb2b567f424d4e0e7a69732ccfd0c3cdb0b06580922aa06c35 d2bfc378333fe73770c459f5f509626991e90ea5a53f5207a2d018bd82a8fed7
URLs	hxxps://www.incometaxdelhi[.]org/gallery/thumnails/mix/sit.hta hxxps://www.incometaxdelhi[.]org/gallery/thumnails/mix/b.php hxxp://155.133.23[.]244/d.php
IP Address	155.133.23[.]244

References

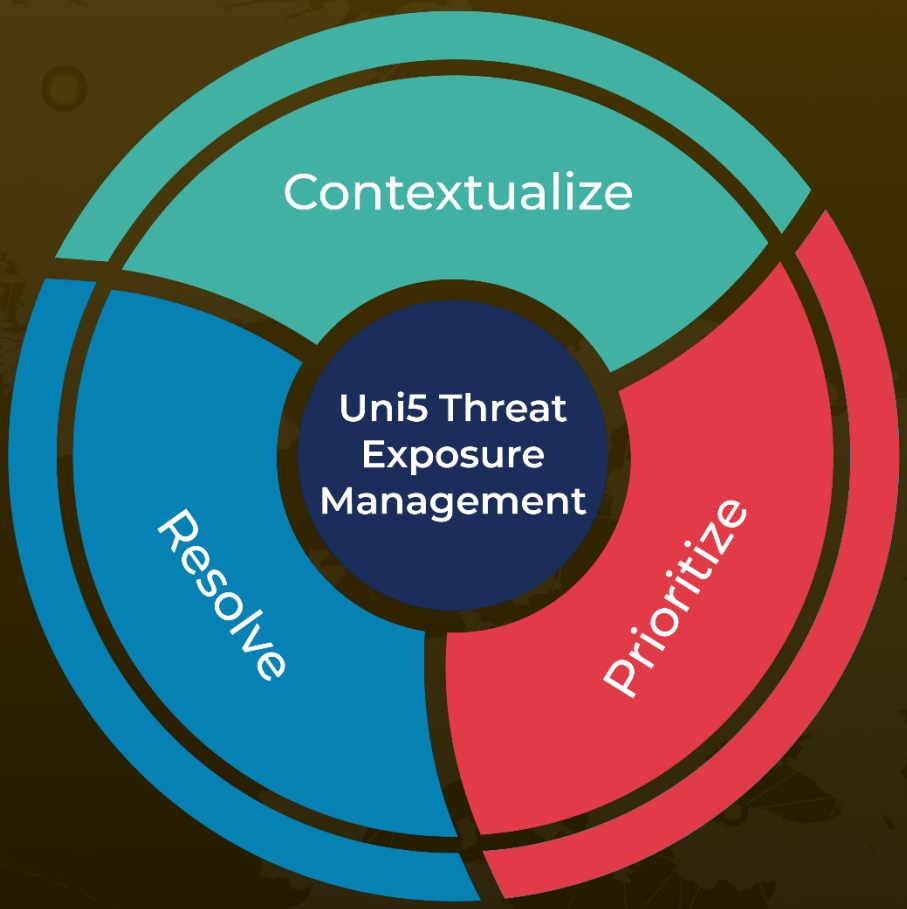
https://www.securonix.com/blog/new-steppykavach-attack-campaign/?&web_view=true

https://attack.mitre.org/groups/G1008/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 27, 2022 • 3:10 AM

More at www.hivepro.com