Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

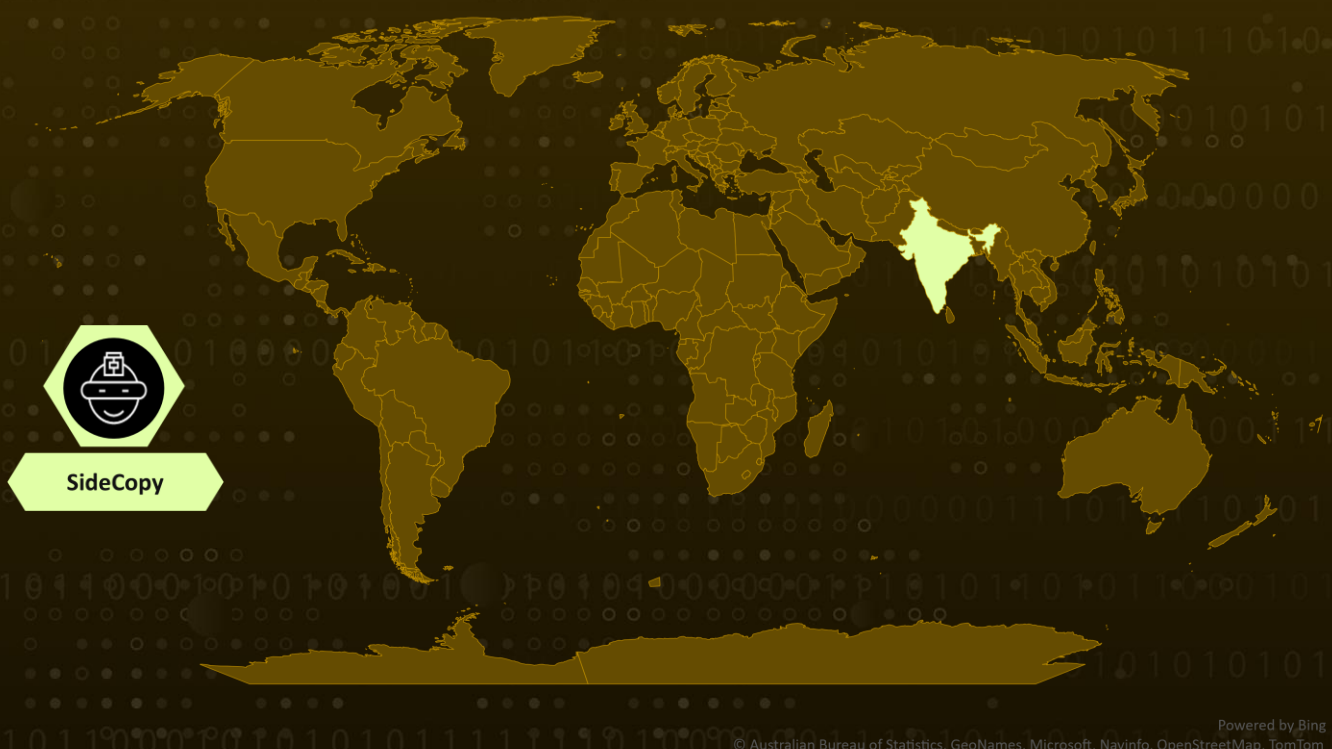
SideCopy Resurfaces to Target Indian Defense

Date of Publication	Admiralty Code	TA Number
May 5, 2023	A2	TA2023214

Summary

Attack Began: 2023
Actor: SideCopy
Framework: SILENTTRINITY
Affected Platform: Windows, Mac, and Linux
Attack Region: India
Targeted Sector: Defense, Embassies, Government
Attack: SideCopy's recent campaign utilizes SILENTTRINITY and targets the Indian defense industry, warranting attention from SideCopy threat actors.

Attack Regions



Attack Details

#1

While SideCopy's primary focus lies on Windows platforms, there have been reports of their deployment of malware on vulnerable Mac and Linux machines. The mode of initial infiltration is believed to be through phishing emails. Specifically, a Zip file bearing the name "DRDO-K4-Missile-Clean-room.zip" was identified as a probable attachment. Within this Zip file, three files were discovered, two of which were designed for installation in a subdirectory of the extraction destination.

#2

In prior instances of SideCopy incidents, CACTUSTORCH was utilized to surreptitiously install code through the use of obfuscated JavaScript and VBScript. However, this present campaign displays a divergence in the method of payload delivery, wherein the tool SILENTTRINITY is utilized. SILENTTRINITY is a newer and more comprehensive tool, functioning as a post-exploitation framework with the same capabilities as those of Empire or CobaltStrike. The specific payload that SideCopy delivers appears to hold relevance only to a select group within the Indian defense industry.

Recommendations

- Ensure all systems, including those running Mac and Linux, are equipped with the necessary security measures and anti-virus software to mitigate the risk of being compromised.
- Educate employees on identifying and avoiding phishing emails, particularly those with suspicious attachments, to prevent the initial infiltration vector of SideCopy's attacks.
- The Indian defense industry should prioritize safeguarding sensitive information and promptly implement measures to detect and respond to potential cyber threats. Additionally, consider implementing proactive security measures, such as blocking indicators of compromise (IoCs), to stay ahead of potential threats.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
T1047 Windows Management Instrumentation	**T1543** Create or Modify System Process	**T1543.002** Systemd Service	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder	**T1574** Hijack Execution Flow	**T1574.002** DLL Side-Loading	**T1036** Masquerading
T1070 Indicator Removal	**T1070.006** Timestomp	**T1112** Modify Registry	**T1497** Virtualization/Sandbox Evasion
T1562 Impair Defenses	**T1562.001** Disable or Modify Tools	**T1564** Hide Artifacts	**T1564.001** Hidden Files and Directories
T1056 Input Capture	**T1010** Application Window Discovery	**T1018** Remote System Discovery	**T1057** Process Discovery
T1082 System Information Discovery	**T1083** File and Directory Discovery	**T1518** Software Discovery	**T1518.001** Security Software Discovery
T1114 Email Collection	**T1071** Application Layer Protocol	**T1095** Non-Application Layer Protocol	**T1105** Ingress Tool Transfer
T1571 Non-Standard Port	**T1573** Encrypted Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	9aed0c5a047959ef38ec0555ccb647688c67557a6f8f60f691ab0ec096833cce bf34077c8b22759b28dcc458dc1b7bba3810c1c30b050b26a26e8d9f64e77971 c7753ffb7f66b0dfb05a24955324182cb92bbf41dd8fccb308c3f04d497a16da a2e55cbd385971904abf619404be7ee8078ce9e3e46226d4d86d96ff31f6bb9a e88835e21c431d00a9b465d2e8bed746b6369892e33be10bc7ebbda6e8185819 68ec4461653ae682eeace1bff583307ec521a3ee23873a991c031cc49dc8132f b9514ed1566c8ce46ab5bfd665f8b997f2d5624740f298699df43bb108e08c4d 85faf414ed0ba9c58b9e7d4dc7388ba5597598c93b701d367d8382717fb485ec 1c2399674713d2a3fc19b841e979eed61d73d1b7ca8fd6f29ba95a41f5a7684d f0cc9b18ba32f95085d5f9a3539dc08832c19e7d3124a5febbdc3bae47deab24 17eabfb88a164aa95731f198bd69a7285cc7f64acd7c289062cd3979a4a2f5bf 865e041b41b9c370a4eed91a9a407bd44a94e16e236e07be05e87de319a4486c
URLs	hXXp://cornerstonebeverly[.]org hXXp://cornerstonebeverly[.]org/js/files/docufentososo/doecumentosoneso/pantomime[.]hta hXXps://cornerstonebeverly[.]org/js/files/ntfonts/avena/ hXXp://cornerstonebeverly[.]org/js/files/ntfonts/jquery[.]txt hXXp://144.91.72[.]17:8080/user_details hXXp://144.91.72[.]17:8080/streamcmd?AV=Unknown&OS=6.1.7601.17932&Vesrion=1&detail=Wfstzepn_Admin

References

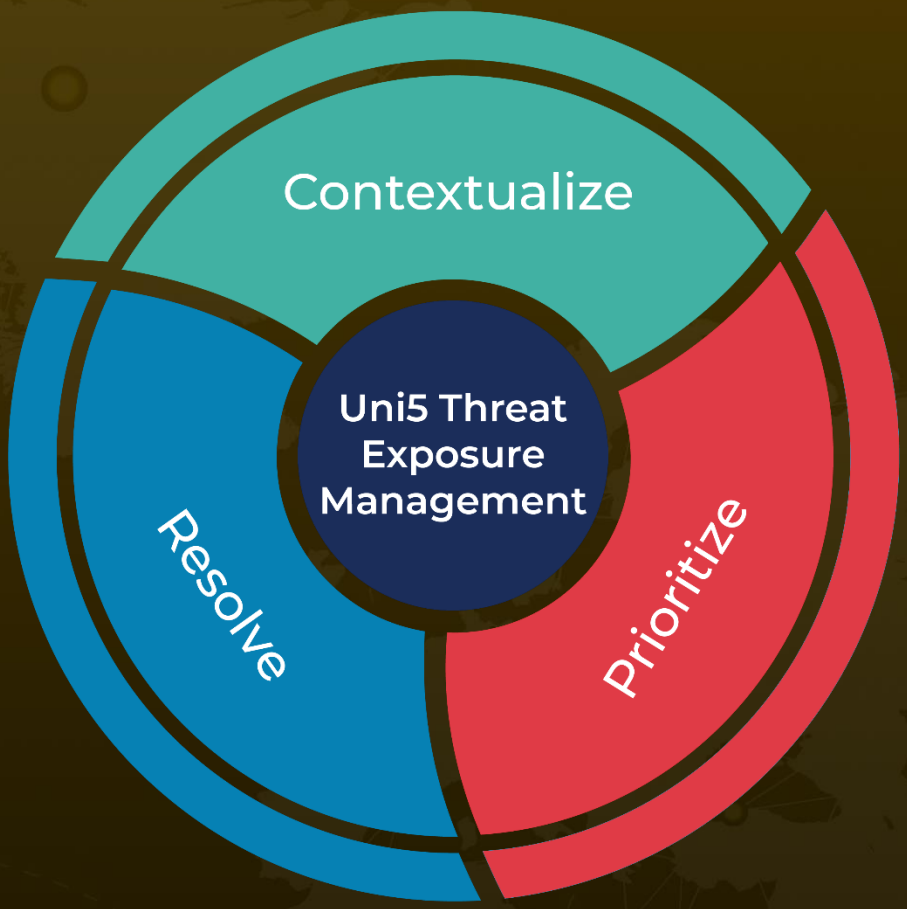
https://www.fortinet.com/blog/threat-research/clean-rooms-nuclear-missiles-and-sidecopy

https://www.hivepro.com/sidecopy-apt-launches-phishing-campaign-against-indian-government/

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

May 5, 2023 • 7:08 AM

More at www.hivepro.com