Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

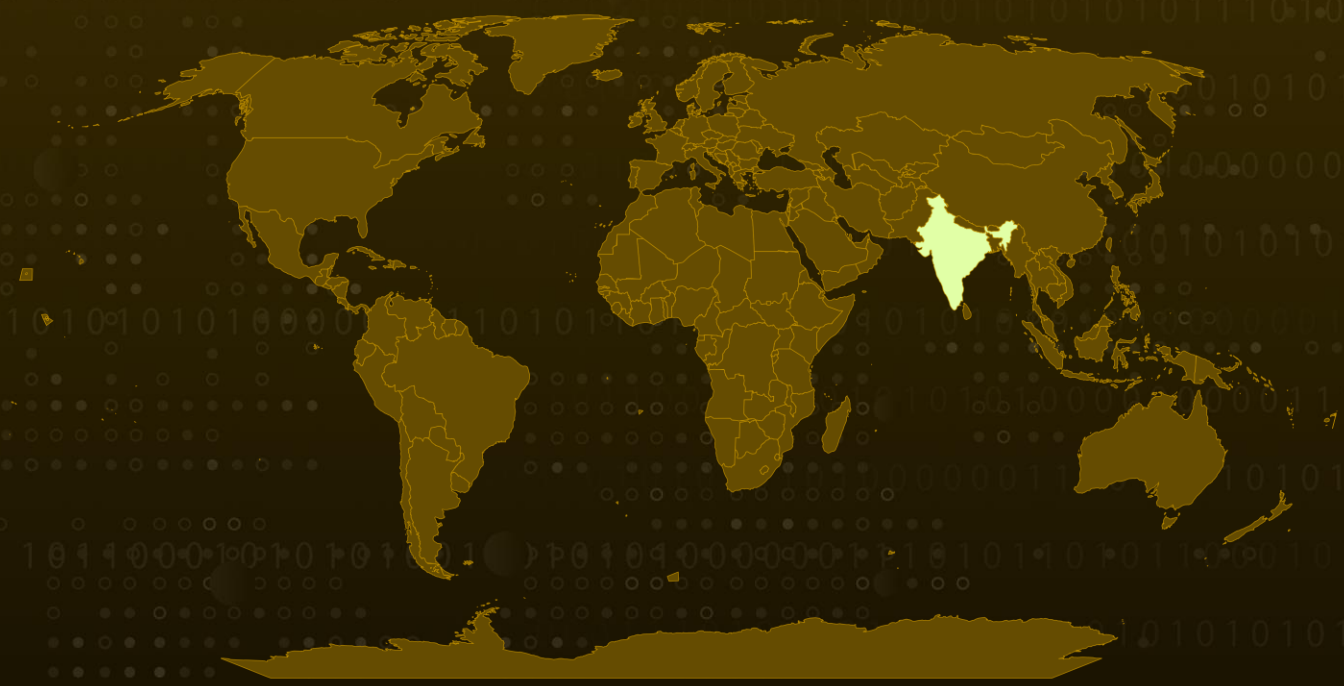
‘Operation FlightNight’ Targeting India with Deceptive Air Force Invitations

Date of Publication	Admiralty Code	TA Number
March 28, 2024	A1	TA2024123

Summary

Attack Began: March 2024
Attack Region: India
Affected Industries: Government entities and Energy companies, National defense
Campaign: Operation FlightNight
Malware: HackBrowserData
Attack: In a campaign dubbed Operation FlightNight, unidentified threat actors have focused on Indian government agencies and energy companies, aiming to deploy a modified variant of an open-source information stealer malware known as HackBrowserData. The threat actors have been observed exfiltrating sensitive data through Slack channels.

Attack Regions



Attack Details

#1 An anonymous threat actor used the open-source information stealer HackBrowserData in an attack against Indian government organisations and the energy sector. The attacker used Slack channels as access points to upload private emails, sensitive documents, and browser cache. This operation, known as "Operation FlightNight," was directed towards several Indian government departments.

#2 Initially the threat actor employed a decoy PDF document disguised as an invitation letter from the Indian Air Force to deceive victims into downloading malware from an ISO file. Upon execution of a shortcut link within the PDF, the malware was activated, initiating the exfiltration of documents and cached web browser data to Slack channels.

#3 HackBrowserData, originally an open-source tool for stealing browser login credentials, cookies, and history, has been modified for more nefarious purposes. In Operation FlightNight, a variant of this tool was observed, the modified variant includes new functionalities such as communication via Slack channels, document stealing capabilities, and obfuscation techniques to evade detection.

#4 Upon execution, the malware creates a mutex file to ensure singular execution and stores browser cache data in a zip file, which is then uploaded to Slack channels. Specific file types like Microsoft Office documents and PDFs are targeted for quick data theft.

#5 The attackers are leveraging previously exfiltrated data to craft decoy PDFs for the ongoing campaign, intending to trick individuals into believing they are accessing authentic documents. The **similarities** between Operation FlightNight and the Go-Stealer campaign suggest that the same threat actor, likely targeting Indian government entities, is behind both attacks.

#6 The Operation FlightNight and Go-Stealer campaign demonstrate how threat actors utilize open-source tools for cyber espionage, showcasing the dynamic nature of cyber threats as they switch their malware within a span of two months. Attackers adapt these tools to streamline their operations and minimize resource expenditure, employing Slack servers for data exfiltration to obscure their actions.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0010** Exfiltration	**TA0011** Command and Control	**T1567** Exfiltration Over Web Service
T1539 Steal Web Session Cookie	**T1217** Browser Information Discovery	**T1071** Application Layer Protocol	**T1071.001** Web Protocols
T1083 File and Directory Discovery	**T1566** Phishing	**T1566.002** Spearphishing Link	**T1036** Masquerading
T1036.008 Masquerade File Type	**T1140** Deobfuscate/Decode Files or Information	**T1204** User Execution	**T1204.002** Malicious File

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	4455ca4e12b5ff486c466897522536ad753cd459d0eb3bfb1747ffc79a2ce5dd, 69c3a92757f79a0020cf1711cda4a724633d535f75bbef2bd74e07a902831d59, 0ac787366bb435c11bf55620b4ba671b710c6f8924712575a0e443abd9922e9f, a811a2dea86dbf6ee9a288624de029be24158fa88f5a6c10acf5bf01ae159e36, 4fa0e396cda9578143ad90ff03702a3b9c796c657f3bdaaf851ea79cb46b86d7, 4a287fa02f75b953e941003cf7c2603e606de3e3a51a3923731ba38eef5532ae, dab645ecb8b2e7722b140ffe1fd59373a899f01bc5d69570d60b8b26781c64fb
Domains	solucionesgeofisicas.slack[.]com, swiftrecruiters.slack[.]com, telcomprodicci.slack[.]com, alfarabischoolgroup.slack[.]com, tucker-group.slack[.]com

References

https://blog.eclecticiq.com/operation-flightnight-indian-government-entities-and-energy-sector-targeted-by-cyber-espionage-campaign

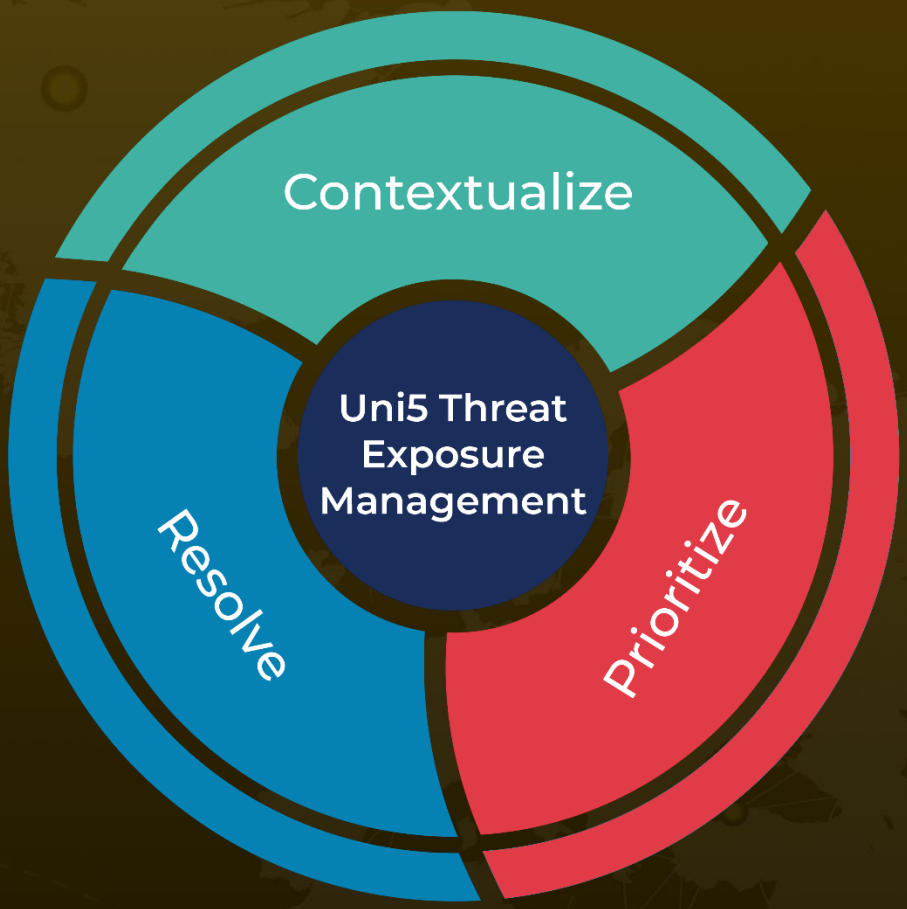
https://www.eclecticiq.com/hubfs/_blogs/corporate-blog/2024/Operation%20FlightNight/Operation%20NightFlight_5.png

https://xelemental.github.io/Golang-based-credential-stealer-targets-Indian-Airforce-Officials/

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

March 28, 2024 • 5:50 AM

More at www.hivepro.com