Mar 28 2024

NETMANAGEIT

Intelligence Report

Operation FlightNight: Indian Government Entities and Energy Sector Targeted by Cyber Espionage Campaign

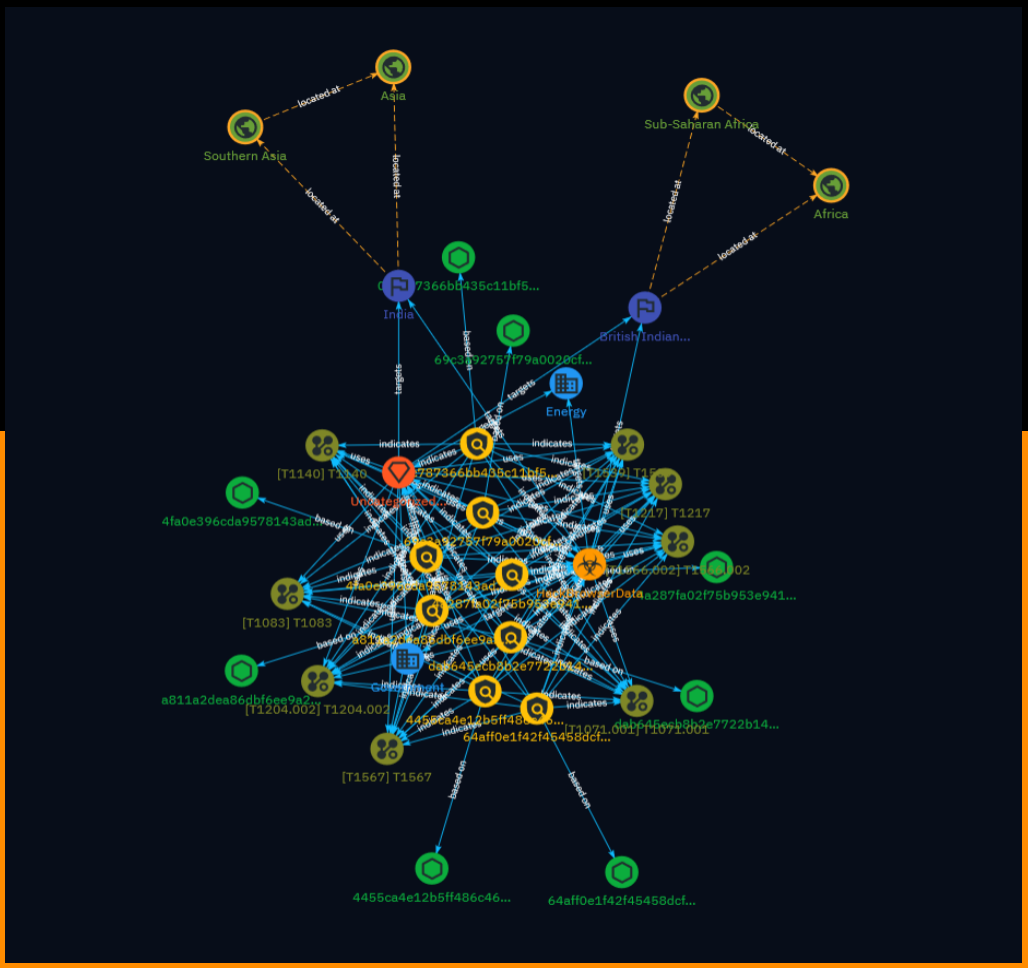

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Beginning March 2024, a threat actor used phishing emails with ISO files containing malware to target Indian government agencies and energy companies. The malware exfiltrated documents and browser data to attacker-controlled Slack channels. Analysts assess the campaign was cyber espionage, likely by the same actor behind a January 2024 attack. The incident highlights the use of open-source tools and Slack for low-cost, hard-to-detect data theft.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name

dab645ecb8b2e7722b140ffe1fd59373a899f01bc5d69570d60b8b26781c64fb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dab645ecb8b2e7722b140ffe1fd59373a899f01bc5d69570d60b8b26781c64fb']

Name

a811a2dea86dbf6ee9a288624de029be24158fa88f5a6c10acf5bf01ae159e36

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a811a2dea86dbf6ee9a288624de029be24158fa88f5a6c10acf5bf01ae159e36']

Name

69c3a92757f79a0020cf1711cda4a724633d535f75bbef2bd74e07a902831d59

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '69c3a92757f79a0020cf1711cda4a724633d535f75bbef2bd74e07a902831d59']

Name

64aff0e1f42f45458dcf3174b69d284d558f7dac24a902438e332e05d0d362ef

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '64aff0e1f42f45458dcf3174b69d284d558f7dac24a902438e332e05d0d362ef']

Name

4fa0e396cda9578143ad90ff03702a3b9c796c657f3bdaaf851ea79cb46b86d7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4fa0e396cda9578143ad90ff03702a3b9c796c657f3bdaaf851ea79cb46b86d7']

Name

4a287fa02f75b953e941003cf7c2603e606de3e3a51a3923731ba38eef5532ae

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4a287fa02f75b953e941003cf7c2603e606de3e3a51a3923731ba38eef5532ae']

Name

4455ca4e12b5ff486c466897522536ad753cd459d0eb3bfb1747ffc79a2ce5dd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4455ca4e12b5ff486c466897522536ad753cd459d0eb3bfb1747ffc79a2ce5dd']

Name

0ac787366bb435c11bf55620b4ba671b710c6f8924712575a0e443abd9922e9f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0ac787366bb435c11bf55620b4ba671b710c6f8924712575a0e443abd9922e9f']

Malware

Name
HackBrowserData

Intrusion-Set

Name
Uncategorized Threat Actor

Attack-Pattern

Name
T1071.001
ID
T1071.001
Description
Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Protocols such as HTTP/S(Citation: CrowdStrike Putter Panda) and WebSocket(Citation: Brazking-Websockets) that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.
Name
T1083
ID
T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Name

T1217

ID

T1217

Description

Adversaries may enumerate information about browsers to learn more about compromised environments. Data saved by browsers (such as bookmarks, accounts, and browsing history) may reveal a variety of personal information about users (e.g., banking sites, relationships/interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.(Citation: Kaspersky Autofill) Browser information may also highlight additional targets after an adversary has access to valid credentials, especially [Credentials In Files](https://attack.mitre.org/techniques/T1552/001) associated with logins cached by a browser. Specific storage locations vary based on platform and/or application, but browser information is typically stored in local files and databases (e.g., `%APPDATA%/Google/Chrome`).(Citation: Chrome Roaming Profiles)

Name

T1567

ID

T1567

Description

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services. Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Name

T1140

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/

encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

T1566.002

ID

T1566.002

Description

Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Spearphishing may also involve social engineering techniques, such as posing as a trusted source. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](https://attack.mitre.org/techniques/T1204). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly. Additionally, adversaries may use seemingly benign links that abuse special characters to mimic legitimate websites (known as an "IDN homograph attack").(Citation: CISA IDN ST05-016) URLs may also be obfuscated by taking advantage of quirks in the URL schema, such as the acceptance of integer- or hexadecimal-based hostname formats and the automatic discarding of text before an “@” symbol: for example, `hxxp://google.com@1157586937`.(Citation: Mandiant URL Obfuscation 2023) Adversaries may also utilize links to perform consent phishing, typically with OAuth 2.0 request URLs that when accepted by the user provide permissions/access for malicious applications, allowing adversaries to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s.(Citation: Trend Micro Pawn Storm OAuth 2017) These stolen access tokens allow the adversary to perform various actions on behalf of the user via API calls. (Citation: Microsoft OAuth 2.0 Consent Phishing 2021)

Name

T1204.002

ID

T1204.002

Description

An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001). Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl. Adversaries may employ various forms of [Masquerading](https://attack.mitre.org/techniques/T1036) and [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to increase the likelihood that a user will open and successfully execute a malicious file. These methods may include using a familiar naming convention and/or password protecting the file and supplying instructions to a user on how to open it.(Citation: Password Protected Word Docs) While [Malicious File](https://attack.mitre.org/techniques/T1204/002) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534).

Name

T1539

ID

T1539

Description

An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website. Cookies are often valid for an extended period of time, even if the web application is not actively used. Cookies can be found on disk, in the process memory of the browser, and in network traffic to remote systems. Additionally, other applications on the targets machine might store sensitive authentication cookies in memory (e.g. apps which authenticate to cloud services). Session cookies can be used to bypasses some multi-factor authentication protocols.(Citation: Pass The Cookie) There are several examples of malware targeting cookies from web browsers on the local system.(Citation: Kaspersky TajMahal April 2019)(Citation: Unit 42 Mac Crypto Cookies January 2019) There are also open source frameworks such as `Evilginx2` and `Muraena` that can gather session cookies through a malicious proxy (ex: [Adversary-in-the-Middle](https://attack.mitre.org/techniques/T1557)) that can be set up by an adversary and used in phishing campaigns.(Citation: Github evilginx2)(Citation: GitHub Mauraena) After an adversary acquires a valid cookie, they can then perform a [Web Session Cookie] (https://attack.mitre.org/techniques/T1550/004) technique to login to the corresponding web application.

Country

Name
India

Name
British Indian Ocean Territory

Region

Name
Southern Asia
Name
Asia
Name
Sub-Saharan Africa
Name
Africa

Sector

Name
Government
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.
Name
Energy
Description
Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.

StixFile

Value
dab645ecb8b2e7722b140ffe1fd59373a899f01bc5d69570d60b8b26781c64fb
a811a2dea86dbf6ee9a288624de029be24158fa88f5a6c10acf5bf01ae159e36
69c3a92757f79a0020cf1711cda4a724633d535f75bbef2bd74e07a902831d59
64aff0e1f42f45458dcf3174b69d284d558f7dac24a902438e332e05d0d362ef
4fa0e396cda9578143ad90ff03702a3b9c796c657f3bdaaf851ea79cb46b86d7
4a287fa02f75b953e941003cf7c2603e606de3e3a51a3923731ba38eef5532ae
4455ca4e12b5ff486c466897522536ad753cd459d0eb3bfb1747ffc79a2ce5dd
0ac787366bb435c11bf55620b4ba671b710c6f8924712575a0e443abd9922e9f

External References

- https://blog.eclecticiq.com/operation-flightnight-indian-government-entities-and-energy-sector-targeted-by-cyber-espionage-campaign
- https://otx.alienvault.com/pulse/660564a7aa39593bdabd1c8b