Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

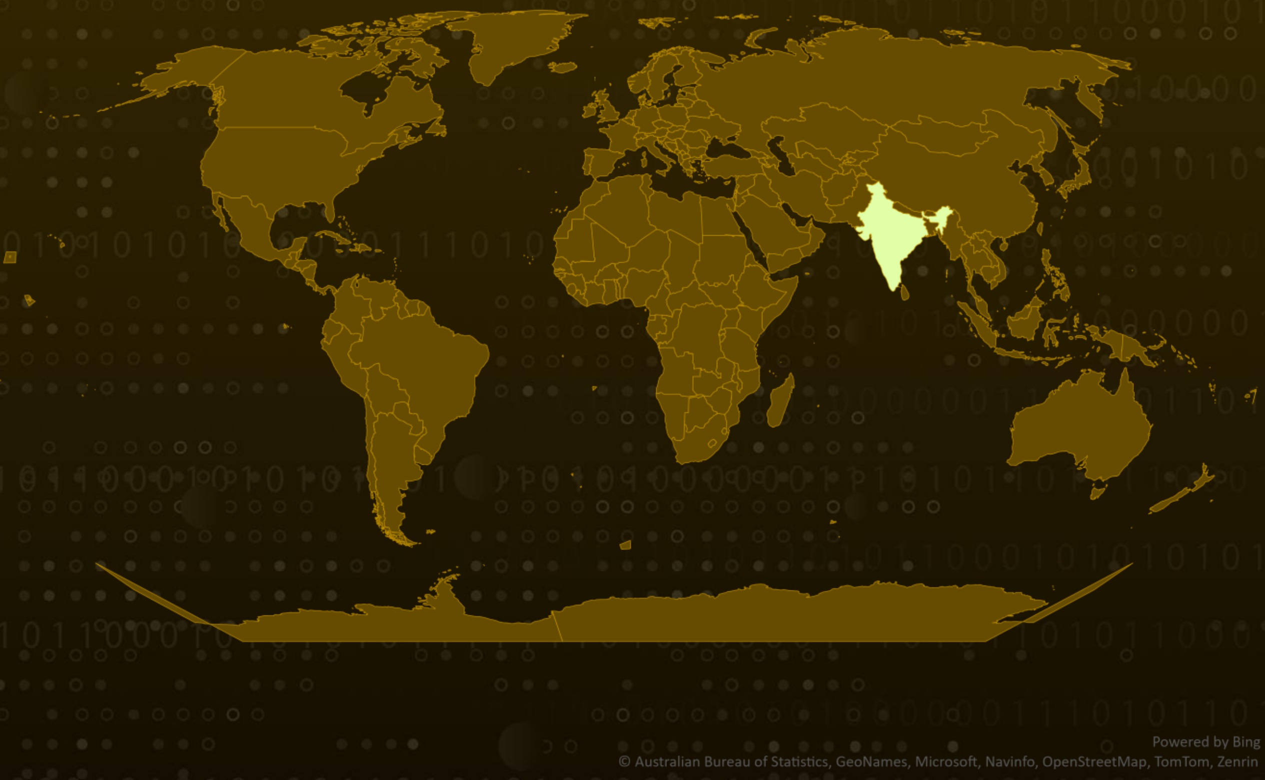
Hackers Employ Updated Ducktail to Target Indian Marketers

Date of Publication	Admiralty Code	TA Number
November 15, 2023	A1	TA2023459

Summary

First appeared: March and early October 2023
Attack Region: India
Targeted Industry: Marketing
Malware: Ducktail
Attack: The threat actors linked to the Ducktail stealer malware have been implicated in a new campaign that focused on marketing professionals in India. The primary goal of this campaign was to compromise and gain control of Facebook business accounts. Notably, this campaign diverged from previous ones by utilizing Delphi as the programming language instead of .NET applications.

Attack Regions


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 The threat actors associated with the Ducktail stealer malware have been identified in a new campaign that took place from March to early October 2023. This campaign specifically targeted marketing professionals in India, with the objective of compromising and taking control of Facebook business accounts.

#2 In the Ducktail attacks, the infostealer propagated by masquerading as documents related to projects and products of well-known companies and brands. A distinctive feature of this campaign was the use of Delphi as the programming language, deviating from the previous approach that relied on .NET applications.

#3 In the Ducktail attacks, the attackers primarily utilized sponsored ads on Facebook to disseminate malicious ads and deploy malware. The malware is capable of extracting victims' login cookies, ultimately enabling the attackers to take control of their accounts. In this campaign, individuals seeking a career change are targeted, receiving archive files containing a malicious executable. The binary is disguised with a PDF icon to deceive users into launching it.

#4 Upon launching the malicious file, it saves a PowerShell script named param.ps1 and a decoy PDF document locally in the "C:\Users\Public" folder on Windows. The script then utilizes the default PDF viewer on the device to open the decoy, introduces a five-minute pause, and subsequently terminates the Chrome browser process. Additionally, the parent executable downloads and executes a rogue library named libEGL.dll.

#5 In the next stage, the browser's LNK shortcut file is modified by appending a command line switch to initiate a rogue extension. This extension disguises itself as the authentic Google Docs Offline add-on to avoid detection. Its purpose is to transmit information about all open tabs to a server controlled by the threat actor and subsequently hijack the targeted Facebook business accounts.

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.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0005 Defense Evasion	TA0006 Credential Access	TA0011 Command and Control
TA0010 Exfiltration	T1589 Gather Victim Identity Information	T1598 Phishing for Information	T1598.002 Spearphishing Attachment
T1583 Acquire Infrastructure	T1583.001 Domains	T1566 Phishing	T1566.001 Spearphishing Attachment
T1176 Browser Extensions	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1129 Shared Modules
T1204 User Execution	T1204.002 Malicious File	T1539 Steal Web Session Cookie	T1027 Obfuscated Files or Information
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1132 Data Encoding	T1132.001 Standard Encoding
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	c82b959d43789d3dbf5115629c3c01fa8dd599fbec36df0f4bc5d0371296545a, 2b3decf08bf9223fb3e3057b5a477d35e62c0b5795a883ceaa9555ca7c28252f, 69257876e2ec5bdbe7114d6ce209f13afbfddb2af0006a6d17e6e91578966870, da13db80b0f3c25b512a1692494f303eff1ff1778a837208f79e2f3c81f8192e, bde696a0ae901864716320e3111d5aa49cba3b1d9375dce2903f7433a287b2f2, 04dd228d0b088c4116b503c31de22c1746054226a533286bec3a3d0606d73119, 89f016d32707f096cc8daf674e5a9fc2ba6cf731d610f5303d997fc848645788, 7da7ca7fcbc6e8bc22b420f82ae5756ecd3ad094b8ebcbd5a78a2362eb87b226, 655a8ea3bc1baff01639dcdc43a294f8a5dc622e543d8f51e9d51c6eaaae6f6e, 1117a93b4b4b78e4d5d6bd79f5f0e04926759558218df30e868464f05bf1bd3d, 554353cda0989c3a141c2ab0d0db06393e4f3fd201727e8cf2ed8d136f87d144, b9a984383a5825868c23bc3afdc70e3af2a56d26d002431940d2429c8e88ace9, c6ae36e28668c6132da4d08bca7ceb13adf576fa1dbdb0a708d9b3b0f140dd03, d03e1a0fce0b112bba4d56380c8d1be671845dd3ed90ec847635ba6015bad84d, ab95f377bf7ae66d26ae7d0d56b71dec096b026b8090f4c5a19ac677a9ffe047, f59e2672f43f327c9c84c057ad3840300a2cd1db1c536834f9e2531c74e5fd1c, ba8eb1a7f18e4cfca7dd178de1546d42ffb50028c8f3f7ba6551f88c11be75db, 06afd110d91419ece0114a7fdeaeba4e79fbc9f2a0450da8b4f264e4ae073a26, 64f6cbe9adf91bc4ed457c79643d764a130b0d25364817c8b6da17b03ff91aa7, bdf8dea28f91adcba7780a26951abc9c32a4a8c205f3207fd4f349f6db290da7, d4f10bd162ee77f4778ecc156921f5949cd2d64aab45b31d6050f446e59aed5a, bdf8dea28f91adcba7780a26951abc9c32a4a8c205f3207fd4f349f6db290da7

TYPE	VALUE
Domains	dauhetdau[.]com, motdanvoi20232023[.]com, voiconprivatesv2083[.]com, cavoisatthu2023asd[.]com

References

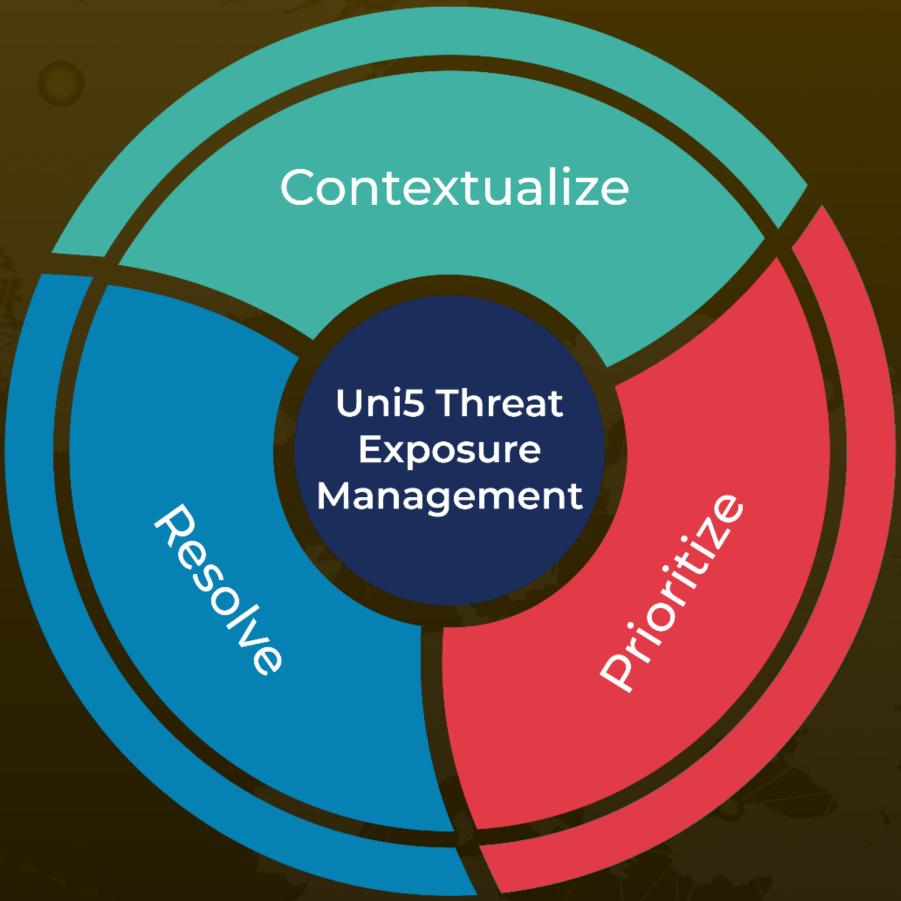
https://securelist.com/ducktail-fashion-week/111017/

https://www.hivepro.com/threat-advisory/ducktail-targets-the-digital-marketers-with-malicious-operations/

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

November 15, 2023 • 3:00 AM

More at www.hivepro.com