Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

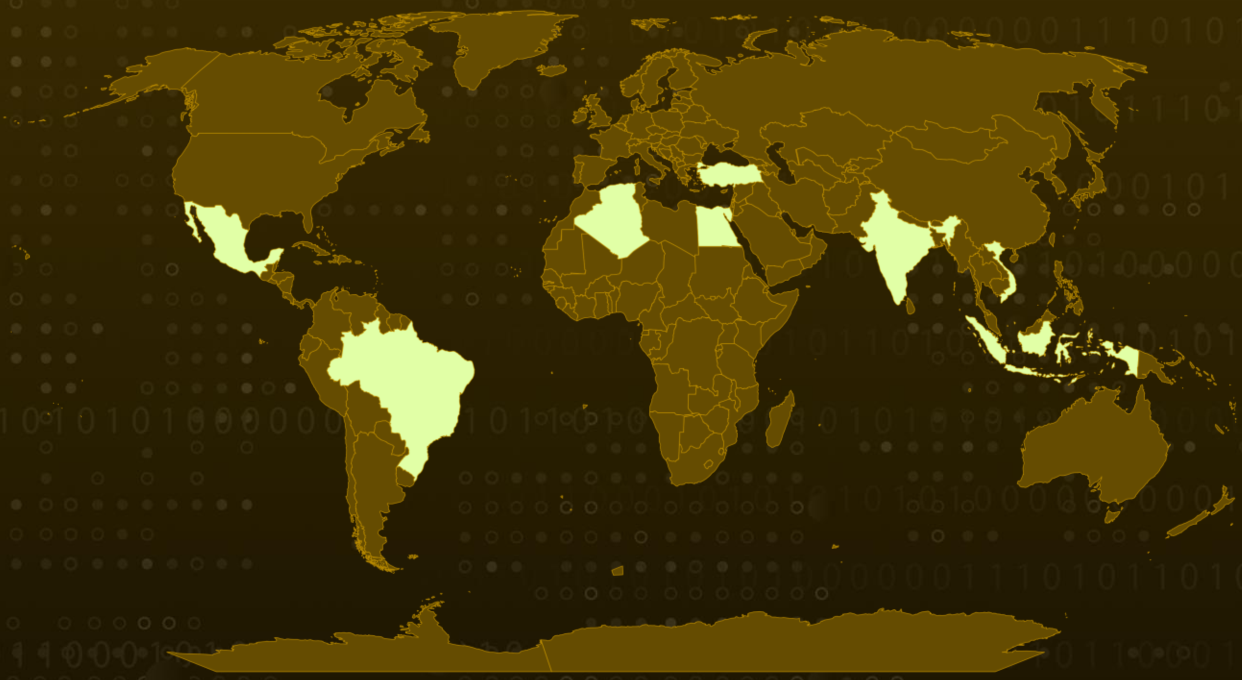
Satacom Malware Campaign Unleashed Crypto-stealing Extension

Date of Publication	Admiralty Code	TA Number
June 8, 2023	A1	TA2023256

Summary

First seen: 2019
Malware: Satacom (aka LegionLoader)
Attack Region: Brazil, Algeria, Turkey, Vietnam, Indonesia, India, Egypt, and Mexico.
Attack: A recently discovered malware campaign has been identified, utilizing the Satacom downloader as a conduit to distribute covert malware designed to illicitly extract cryptocurrency using a deceitful extension tailored for browsers based on the Chromium framework.

Attack Regions



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

Attack Details

#1 A new malware distribution campaign involving the Satacom downloader has emerged. The primary objective of this malware is to pilfer BTC from the victim's account by injecting malicious code into specific cryptocurrency websites. To accomplish this, the malware installs an extension for web browsers based on Chromium.

#2 This extension then establishes communication with a command-and-control (C2) server, the address of which is stored within the BTC transaction data. The infection process commences with the retrieval of a ZIP archive file. This file is obtained from a website designed to mimic a software portal, enticing users with the allure of free downloads for desired software, often illicitly obtained.

#3 The malicious extension incorporates diverse JavaScript (JS) scripts that execute browser manipulations while the user navigates through specifically targeted websites. These manipulations encompass enumeration and tampering with cryptocurrency-oriented platforms.

#4 Additionally, the extension possesses the capability to alter the visual presentation of select email services, such as Gmail, Hotmail, and Yahoo. This enables it to conceal its activities by concealing notifications containing details about the victim's cryptocurrency holdings.

#5 Once the add-on establishes communication with the command-and-control (C2) server, the server reciprocates by providing the web inject script that will be employed on the designated websites. Prominent targets of this campaign encompass users of Coinbase, Bybit, KuCoin, Huobi, and Binance. Another noteworthy feature of the add-on is its proficiency in extracting system metadata, cookies, browser history, screenshots of active tabs, and even accepting commands issued by the C2 server.

Recommendations

Exercise caution when downloading software: Be wary of websites that offer cracked or free software downloads, as they can be potential sources of malware. Stick to reputable sources and avoid suspicious portals that mimic legitimate software platforms.

Cross-Platform Threats: Given the versatility of the malicious extension in targeting different platforms, it is crucial to adopt secure browser practices to protect your devices, regardless of the operating system. While the current malware campaign primarily focuses on Windows-based systems, threat actors could potentially expand their reach to target Linux and macOS users who utilize Chromium-based browsers.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1204 User Execution	T1204.001 Malicious Link
T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1547 Boot or Logon Autostart Execution
T1547.009 Shortcut Modification	T1176 Browser Extensions	T1055 Process Injection	T1055.012 Process Hollowing
T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1539 Steal Web Session Cookie	T1111 Multi-Factor Authentication Interception
T1552 Unsecured Credentials	T1087 Account Discovery	T1518 Software Discovery	T1518.001 Security Software Discovery

T1119 Automated Collection	**T1113** Screen Capture	**T1555** Credentials from Password Stores	**T1185** Browser Session Hijacking
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1071.004** DNS	**T1568** Dynamic Resolution
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	0ac34b67e634e49b0f75cf2be388f244 1aa7ad7efb1b48a28c6ccf7b496c9cfd 199017082159b23decdf63b22e07a7a1 a7f17ed79777f28bf9c9cebaa01c8d70
Domains	dns-beast[.]com don-dns[.]com die-dns[.]com hit-mee[.]com noname-domain[.]com don-die[.]com old-big[.]com tchk-1[.]com you-rabbit[.]com web-lox[.]com ht-specialize[.]xyz ht-input[.]cfd ht-queen[.]cfd ht-dilemma[.]xyz ht-input[.]cfd io-strength[.]cfd fbs-university[.]xyz io-previous[.]xyz io-band[.]cfd io-strength[.]cfd io-band[.]cfd can-nothing[.]cfd scope-chat[.]xyz stroke-chat[.]click

TYPE	VALUE
Domains	icl-surprise[.]xyz new-high[.]click shrimp-clock[.]click oo-knowledge[.]xyz oo-station[.]xyz oo-blue[.]click oo-strategy[.]xyz oo-clearly[.]click economy-h[.]xyz medical-h[.]click hospital-h[.]xyz church-h[.]clickclose-h[.]xyz thousand-h[.]click risk-h[.]xyz current-h[.]click fire-h[.]xyz future-h[.]click moment-are[.]xyz himself-are[.]click air-are[.]xyz teacher-are[.]click force-are[.]xyz enough-are[.]xyz education-are[.]click across-are[.]xyz although-are[.]click punishment-chat[.]click rjjy-easily[.]xyz guy-seventh[.]cfd back-may[.]com post-make[.]com filesend[.]live soft-kind[.]com ee-softs[.]com big-loads[.]com el-softs[.]com

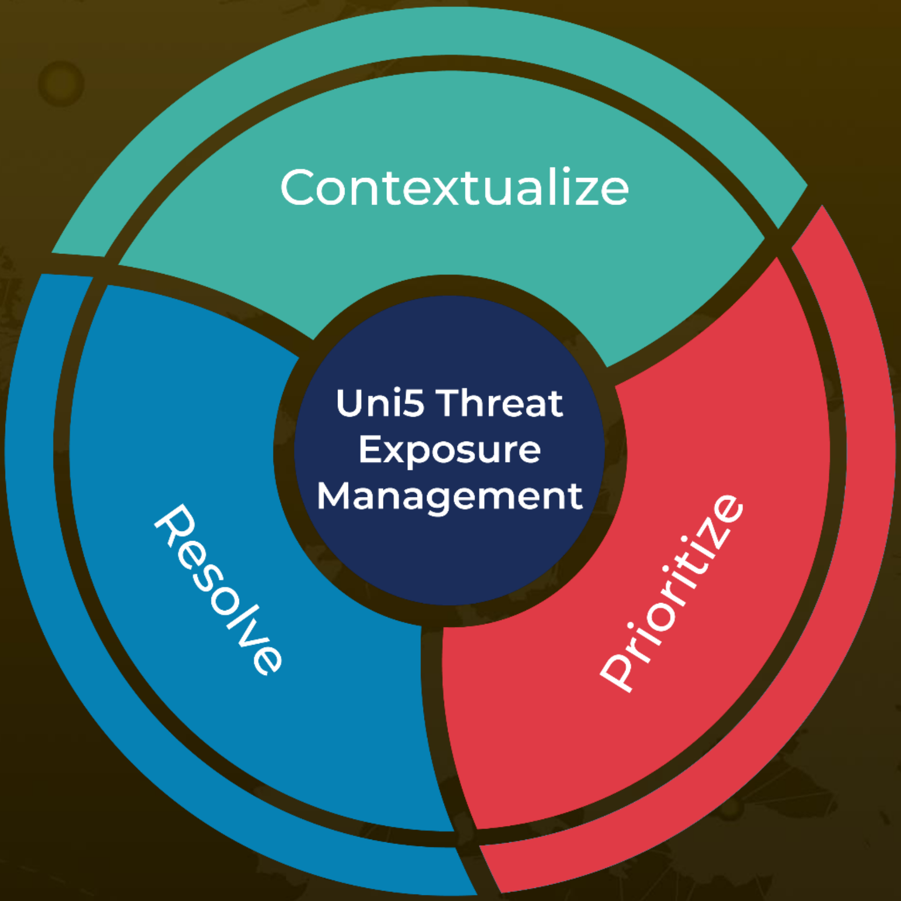
References

https://securelist.com/satacom-delivers-cryptocurrency-stealing-browser-extension/109807/

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

June 8, 2023 • 5:49 AM

More at www.hivepro.com