Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

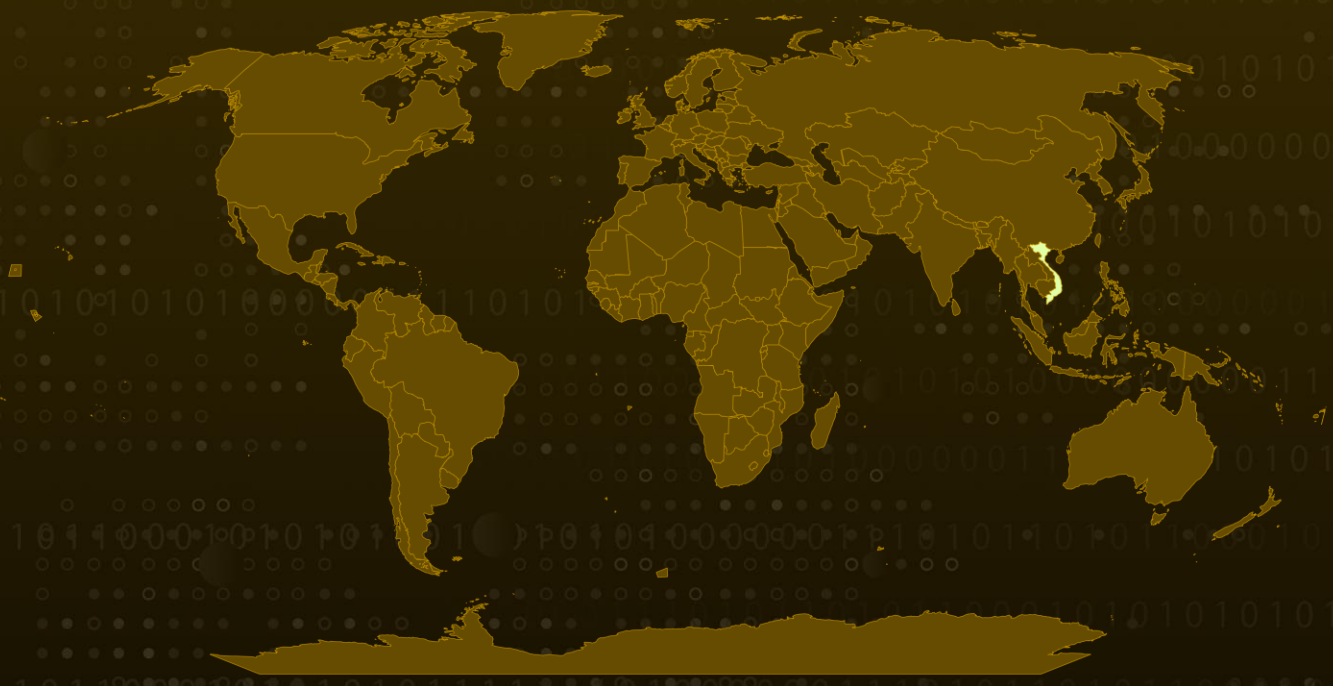
VietCredCare Operates As Stealer-as-a-Service, Targeting Meta Sessions

Date of Publication	Admiralty Code	TA Number
February 22, 2024	A1	TA2024070

Summary

Attack Began: August 2022
Attack Region: Vietnam
Malware: VietCredCare
Attack: Since August 2022, a previously unidentified information stealer known as VietCredCare has emerged. This stealer is notable for its capability to automatically sort through credentials specifically for the service it targets. The primary objective of threat actors employing VietCredCare is to compromise and completely takeover Facebook accounts of prominent businesses and organizations.

Attack Regions



Attack Details

#1 Since at least August 2022, there has been an emergence of VietCredCare, an information-stealing malware previously unrecognized. This malware is distributed through the "stealer-as-a-service" model. In Vietnam, VietCredCare primarily targets individuals, especially those responsible for managing the online presence of prominent companies and organizations. Phishing attacks are a common method used to distribute VietCredCare, often by disguising it as legitimate files or applications.

#2 VietCredCare is a type of Facebook-targeting malware specifically aimed at accounts holding a balance of Meta ad credits or those actively running advertisements. Its primary function is to filter out credentials and session cookies. The objectives of the threat actors employing this malware include spreading politically charged posts, executing phishing scams, and facilitating the sale of stolen credentials to other sophisticated actors.

#3 The Windows version of the VietCredCare information stealer, created in .NET, tricked users into launching a phony payload. VietCredCare uses command-and-control servers to self-replicate and run without human input. It can retrieve information from widely used browsers such as MS Edge, Chromium, Chrome, and the Vietnamese-specific Cốc Cốc. The threat actor can access a Telegram bot that receives data extracted from compromised devices.

#4 The malware demonstrates a number of sophisticated features, such as the capacity to create botnets and encrypt it, in order to avoid detection by antivirus software. It can also change file icons to look like genuine files and covertly embed the bot inside other programs or tools. Moreover, VietCredCare has the capability to circumvent Facebook's two-factor authentication mechanism, allowing it to steal data stored in the victim's browser.

#5 The utilization of the stealer-as-a-service business model by the malware is particularly alarming as it lowers the barrier for entry for threat actors with limited technical skills and escalates the overall threat landscape. Remarkably, over 20 distinct threat actors have employed the same VietCredCare sample in their nefarious operations, rendering it a noteworthy threat.

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	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	T1566 Phishing
T1566.002 Spearphishing Link	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1574 Hijack Execution Flow
T1134 Access Token Manipulation	T1497 Virtualization/Sandbox Evasion	T1497.001 System Checks	T1497.003 Time Based Evasion
T1027 Obfuscated Files or Information	T1027.001 Binary Padding	T1027.002 Software Packing	T1552 Unsecured Credentials

T1555 Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1036** Masquerading	**T1204** User Execution
T1204.002 Malicious File			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	bd9eb106e265c5d0ae7a9e9d2d5925d558128599b1ba4a4cbc29b6fc7b3f48f0, 71c4d0fc03bc4e083f64b2f80b2242618fb725efd64f362446f98c6d2051834f, b5621b540d1ca1dd802397822145ae4f80e96e59b81fdc8d0a7b18919ceadd12, 17598536cf0bac6cb0d589410682e2cd9f813ea52bc931fe85292b149dbeb659, 20ac10ea3a964c25f09b0008406388cf4195828eed6daaeda139c55ce84986f4, 8c6e6faa28f67ac56587a4dcea49c820b466113604900c3f829185a096c6df47, aababe351df7fc27a8d9a227f75850adc1fc3fe86248e59953def5b3fa9b8822, 67b095896e09acff1b2140c933d5efff0dd2a10c920b5db6518531f2304a8838, 1d92dd2e8b04e715954d2bf99e053f9b05eb89986e2b13651d17498f51d2de5d, e2b4e099b70a213f27a84b8534964a7dfd870004ebee3c5eb6601f239c5fd3a1, b3eaa35baecf562a018df53066e8ec438cac854b0bb30eba7aa34a9d8230aacb, 74ab0c6b96cffa75b474ba1fbf69b9cd8502981f85a89642c0b3aa35399a4bda, e0b00681a57457af72fc53866316fc2ba1b0c99d79685ca3a4e8973d023b6426, 071001dcdf87312fece26c4f9bec92f0e0c651eb88786d6ac4ea7ee128fe0aba, 83d3c0e4b813020aa8c2e917be86bbf8b48336960a7ac65f973e88fc05575263, 596f86cf3d2911f2817289be25621d9a1f93bd0d861b66f0fec2a9092b9eff3c,

TYPE	VALUE
SHA256	f1b430bed2b7c1c10f66d8551713c3bcc06c689f0c55a57129703feeab58927f, c4616a07ab285f8a124079e6d2afd30ea1c552804c4ac689510e5a0e85e6dd3b, 3a56c8b9269a6dd225bc150dfd6bcf058aeadd2d5196ed02cec5bf00521238d9, f791d75904f434461c0bcccc0ff3d39ab4eb04eb208e9b7eed3e71376b6820b8, 5c1ef4b5e5a8cd2a80fd5e5aee0d29eb44fedcb9dd5e73e6b5c74f17e83a19cb, 1f28712c2fabfd21aa286fa70e6191f4265d808b3880b897f4c8df5778c1b785, d305ec61046d4470559480cf724b16584e65752a37c7817b8a06b208247b2ac5, aa2ce3666ff4ede662c071d07b16d4e2fadc6c2dd9fe76eb9fb4dc82817a5ec8, a2ac7a96a14f855caa520ce2862dbdb83d1cb278d0f9171e116926c5a40196aa, 27f377560d2ada287cb134b1d350eaa2fc15799a3845fe35c06e6d208e63bb71, d26634062b44a009eaf0cc024fd24e7d32d4117664904b86b925b2d5639e527b, 2eeb5b0e3d6e3e1f1422b6d8115a48c0fb6953e42e974a2754e079ea0de0819f, dafdfdf54ec92cf126f676947fb708f6354326ebf5f6e3fbd84022df179a1c85, ffc70cddcfdbdda5a941d53a2307567da14853442e00282c7e0bd57bc9f963a1, c1fb24f868d17673b41da5aaa8738730963f4a8e3d208420a0cd21a8f2a5470f, 257146b44136f54e976273759e3f3f671d1622797259091a37312d58933a4ea8, 987863291c7025bef2e2a7d8b5081f4bde9d1ca38172a99567004c1c44599010, 22b462e4e852a4f5b668c941780e4d01af7f9e645b6cf50a6f9154ce9d96ebe4, 14b8e34338e445d15d901f3b39fea324ef66eab686877d520a4b3a5cc86632ef

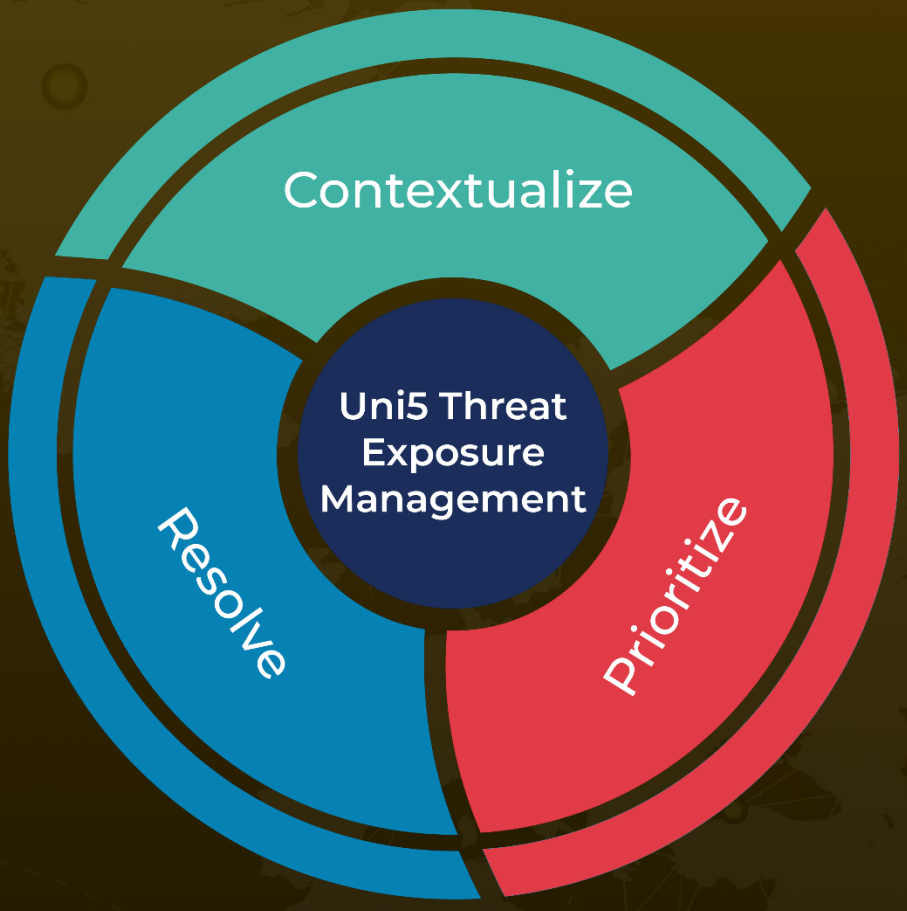
References

https://www.group-ib.com/blog/vietcredcare-stealer/

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

February 22, 2024 • 5:00 AM

More at www.hivepro.com