Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

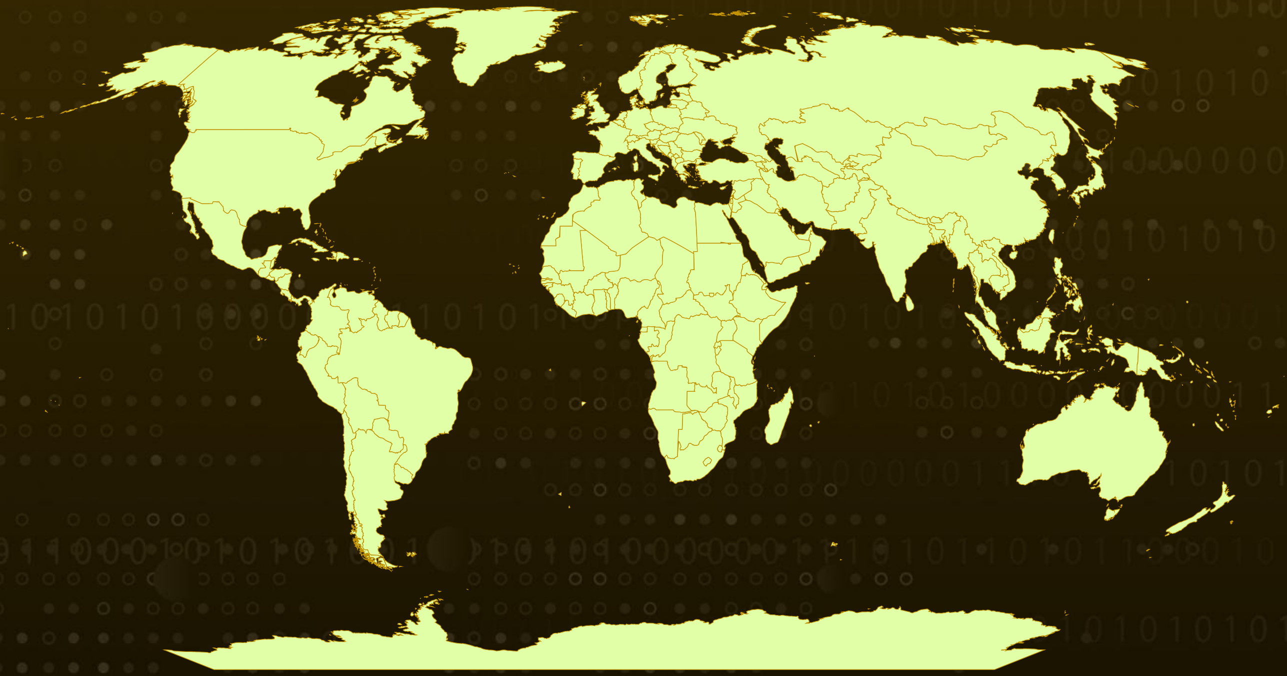
NodeStealer Reloaded: Targeting Facebook Ads and Credit Cards with New Tactics

Date of Publication	Admiralty Code	TA Number
November 22, 2024	A1	TA2024441

Summary

Attack Discovered: 2023
Targeted Countries: Worldwide
Malware: NodeStealer
Attack: A new and enhanced version of the Python-based NodeStealer malware has emerged, with expanded capabilities designed to inflict even greater damage. This iteration not only targets credentials stored in web browsers but also harvests sensitive credit card information. Additionally, it has been refined to extract more data from victims' Facebook Ads Manager accounts, further amplifying its potential impact on businesses and individuals.

Attack Regions



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

Attack Details

#1 The Python-based NodeStealer malware has evolved significantly over the past year, with multiple variants introducing new tactics and expanding their capabilities. Initially designed to steal browser-stored credentials and cookies, NodeStealer now targets Facebook Ads Manager accounts and harvests credit card data stored in web browsers.

#2 By stealing cookies and login credentials, the malware generates access tokens to interact with Ads Manager using the Facebook Graph API. This allows it to extract budget details and retrieve information about businesses linked to the account. The stolen credentials are likely used to create or hijack ad campaigns for malicious purposes. Interestingly, the attackers, believed to be Vietnamese speaking, avoids malware execution in Vietnamese region.

#3 The malware uses the Windows Restart Manager DLL to unlock browser database files, enabling the extraction of sensitive information even when files are in use. By copying browser databases into temporary folders, the malware queries specific details using Python's SQLite3 library. Credit card theft is a key feature of newer variants. This database contains autofill information, including cardholder names, card numbers, and expiration dates, which the malware extracts with precision.

#4 Persistence and evasion are core elements of NodeStealer's design. It uses run registry keys to maintain its presence on infected systems, executing malicious scripts via PowerShell during startup. The latest variant of NodeStealer abandons external payload sources, embedding its entire malicious script within a batch file that echoes the Python code line-by-line, a tactic aimed at streamlining execution and bypassing traditional defenses.

#5 Data exfiltration remains consistent across all NodeStealer variants, with stolen information sent to attackers via Telegram. Compiled text files containing credentials, IP addresses, country codes, and hostnames are transmitted to NodeStealer's evolution illustrates the growing complexity of cyber threats targeting both individuals and businesses. By analyzing its tactics, security teams can adapt their defenses to detect and mitigate similar threats.

Recommendations

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.

Enable Multi-Factor Authentication (MFA): Strengthen account security by enabling MFA for Facebook Ads Manager and other sensitive accounts. This extra layer of protection makes it significantly harder for attackers to access your accounts, even if credentials are compromised.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0009** Collection
TA0010 Exfiltration	**T1190** Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1059.006** Python
T1555 Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1539** Steal Web Session Cookie	**T1074** Data Staged
T1590 Gather Victim Network Information	**T1218** System Binary Proxy Execution	**T1606** Forge Web Credentials	**T1606.001** Web Cookies

T1217 Browser Information Discovery	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1560** Archive Collected Data
T1592 Gather Victim Host Information			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	4613225317e768d6d69b412843a314e2af64960856a0cfd798ed52285867bc36, AE0712C02E750C35219214437D8794DA3BCD9FF608C3F59CDCA0934A958189D3, C6C0000ECF6AF93D0750C45FBD8AF0F8E2289F051DFD523C9550675017F27B53, 58ED336B7AB7B84BA05892F9839ADCB13390D66B53532B62EC37CBCD6A7DE3FF, C5D4E4D9FA2C201D74A14FD1972B670FDE243F087451A3A7DC52A9A6DB61A1CB, 641F2DB9E9FB8255337672FB8DA9226225FA8E393B651C7C7EBBB5B555D4B755, EA25DD47B43DDAA3DF11E6D16544702A8FABBCD0031BA11D1DF51461704A8973, 4613225317e768d6d69b412843a314e2af64960856a0cfd798ed52285867bc36, 8dcced38514c8167c849c1bba9c3c6ef20f219a7439d2fc1f889410e34d8f6c9, ea25dd47b43ddaa3df11e6d16544702a8fabbcd0031ba11d1df51461704a8973

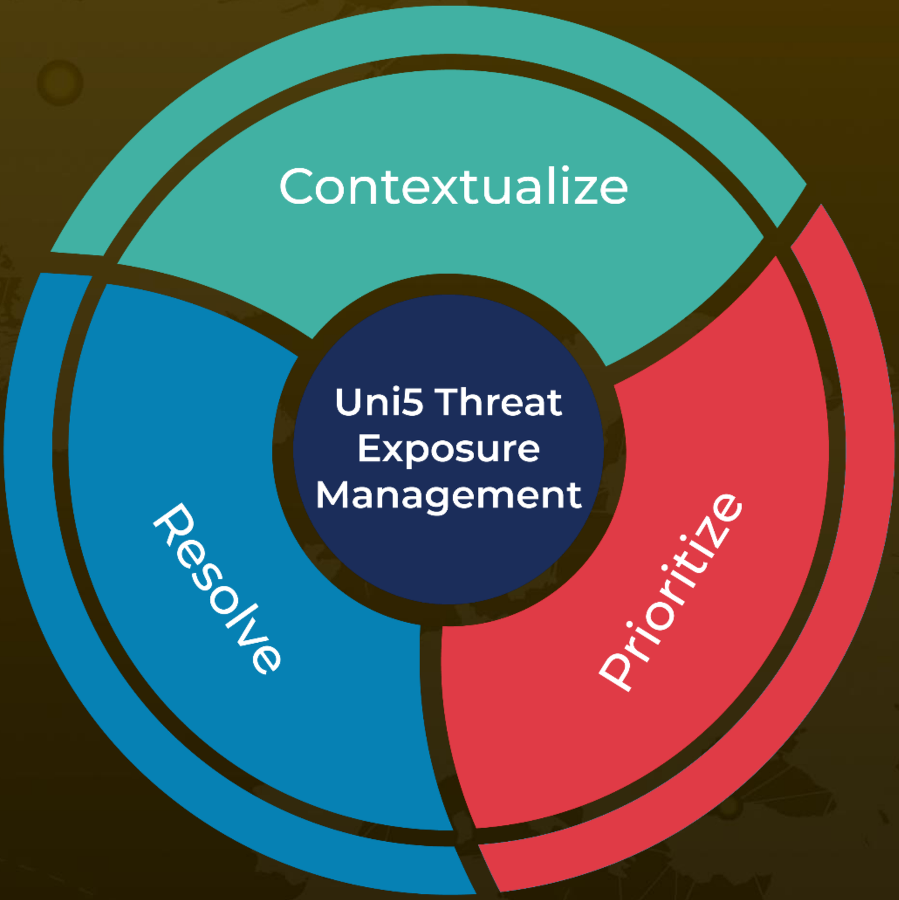
References

https://www.netskope.com/blog/python-nodestealer-targets-facebook-ads-manager-with-new-techniques

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 22, 2024 • 5:50 AM

More at www.hivepro.com