Sep 18 2023

NETMANAGEIT

Intelligence Report

New Python NodeStealer Goes Beyond Facebook Credentials, Now Stealing All Browser Cookies and Login Credentials

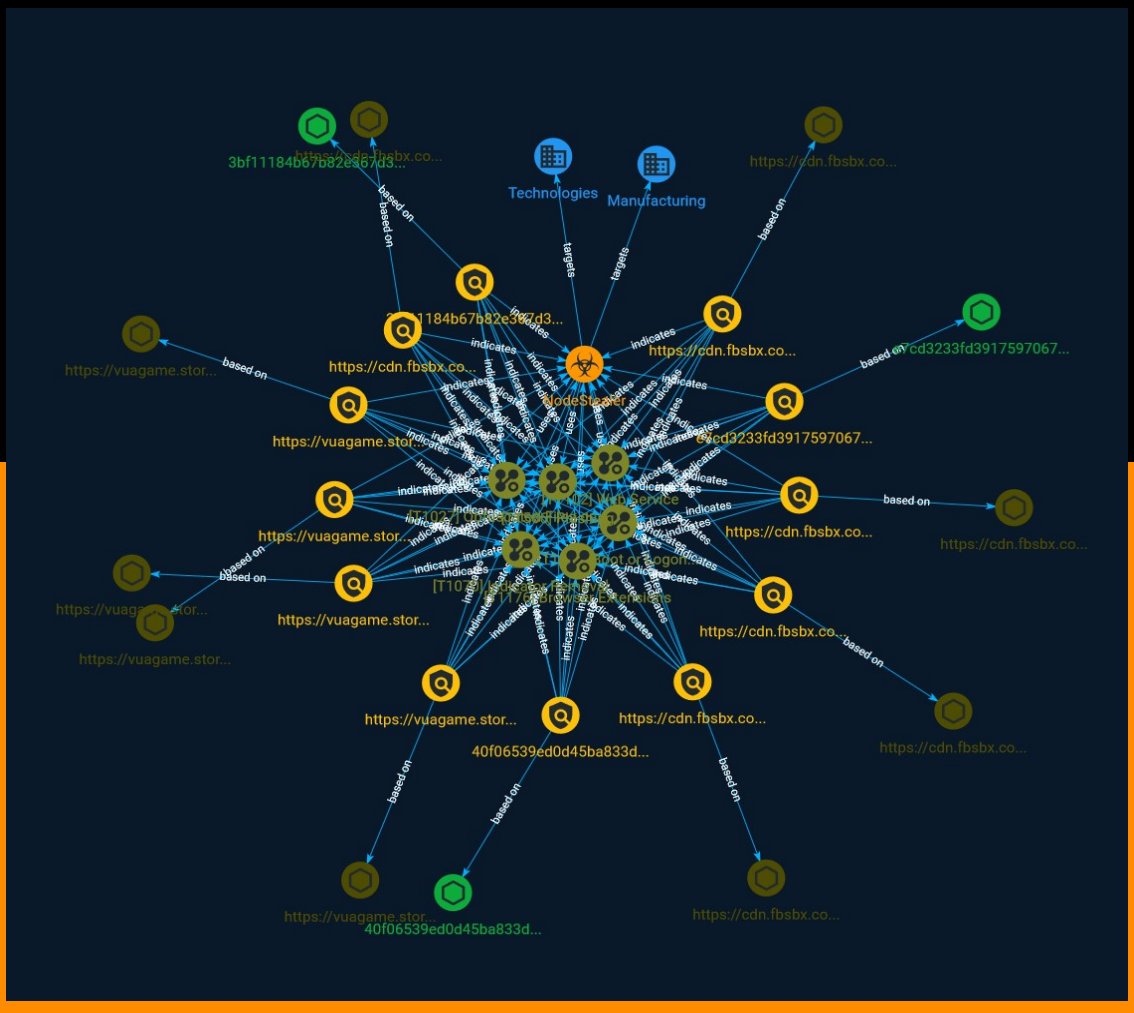

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers have been tracking a campaign that uses malicious Python scripts to steal Facebook users' credentials and browser data. This campaign targets Facebook business accounts with bogus Facebook messages with a malicious file attached. The attacks are reaching victims mainly in Southern Europe and North America across different segments, led by the manufacturing services and technology sectors.

Confidence

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

15 / 100

Attack-Pattern

Name
Boot or Logon Autostart Execution
ID
T1547
Description
Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.
Name
Indicator Removal
ID
T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL,

download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Browser Extensions

ID

T1176

Description

Adversaries may abuse Internet browser extensions to establish persistent access to victim systems. Browser extensions or plugins are small programs that can add functionality and customize aspects of Internet browsers. They can be installed directly or through a browser's app store and generally have access and permissions to everything that the browser can access.(Citation: Wikipedia Browser Extension)(Citation: Chrome Extensions Definition) Malicious extensions can be installed into a browser through malicious app store downloads masquerading as legitimate extensions, through social engineering, or by an adversary that has already compromised a system. Security can be limited on browser app stores so it may not be difficult for malicious extensions to defeat automated scanners.(Citation: Malicious Chrome Extension Numbers) Depending on the browser, adversaries may also manipulate an extension's update url to install updates from an adversary controlled server or manipulate the mobile configuration file to silently install additional extensions. Previous to macOS 11, adversaries could silently install browser extensions via the command line using the `profiles` tool to install malicious `.mobileconfig` files. In macOS 11+, the use of the `profiles` tool can no longer install configuration profiles, however `.mobileconfig` files can be planted and installed with user interaction.(Citation: xorrior chrome extensions macOS) Once the extension is installed, it can browse to websites in the background, steal all information that a user enters into a browser (including credentials), and be used as an installer for a RAT for persistence. (Citation: Chrome Extension Crypto Miner)(Citation: ICEBRG Chrome Extensions)(Citation: Banker Google Chrome Extension Steals Creds)(Citation: Catch All Chrome Extension) There have also been instances of botnets using a persistent backdoor through malicious Chrome extensions.(Citation: Stantinko Botnet) There have also been similar examples of extensions being used for command & control.(Citation: Chrome Extension C2 Malware)

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [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) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Sector

Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Indicator

Name
https://vuagame.store/rmv
Pattern Type
stix
Pattern
[url:value = 'https://vuagame.store/rmv']
Name
https://cdn.fbsbx.com/v/t59.2708-21/366541252_307708121731913_2867761615862616633_n.rar/image-produit-103c3gdfe2d22c19d3f47611e2e.rar
Pattern Type
stix
Pattern
[url:value = 'https://cdn.fbsbx.com/v/t59.2708-21/366541252_307708121731913_2867761615862616633_n.rar/image-produit-103c3gdfe2d22c19d3f47611e2e.rar']

Name

https://cdn.fbsbx.com/v/t59.2708-21/366736184_272143855551717_1974995500254017245_n.rar/imagem-produto-103c3e2e43234ed22c19d3f47611e2e.rar

Pattern Type

stix

Pattern

[url:value = 'https://cdn.fbsbx.com/v/t59.2708-21/366736184_272143855551717_1974995500254017245_n.rar/imagem-produto-103c3e2e43234ed22c19d3f47611e2e.rar']

Name

https://vuagame.store/4HA

Pattern Type

stix

Pattern

[url:value = 'https://vuagame.store/4HA']

Name

https://cdn.fbsbx.com/v/t59.2708-21/367434252_826968952391881_4583268091682907143_n.rar/image-product-103c3e2d4se43234ed22c19d3f47611e2e.rar

Pattern Type

stix

Pattern

[url:value = 'https://cdn.fbsbx.com/v/t59.2708-21/367434252_826968952391881_4583268091682907143_n.rar/image-product-103c3e2d4se43234ed22c19d3f47611e2e.rar']

Name

https://vuagame.store/document.zip

Pattern Type

stix

Pattern

[url:value = 'https://vuagame.store/document.zip']

Name

3bf11184b67b82e367d36cb9ed3380a43814b000d84aef0bb89d4e08e4fcd581

Description

RAR_Archive SHA256 of 13f94cda395bfdd2c87a024ee497e576

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3bf11184b67b82e367d36cb9ed3380a43814b000d84aef0bb89d4e08e4fcd581']

Name

https://cdn.fbsbx.com/v/t59.2708-21/366790602_1527838844638580_5700504415987597148_n.rar/Bild-Produkt-1615448759625_19599_4e232787b5053ac7f631b0c701d2159c_1.rar

Pattern Type

stix

Pattern

[url:value = 'https://cdn.fbsbx.com/v/t59.2708-21/366790602_1527838844638580_5700504415987597148_n.rar/Bild-Produkt-1615448759625_19599_4e232787b5053ac7f631b0c701d2159c_1.rar']

Name

https://vuagame.store/4HAI.zip

Pattern Type

stix

Pattern

[url:value = 'https://vuagame.store/4HAI.zip']

Name

e7cd3233fd39175970675135dac2c582382747b328b3786f8a833ae2ab8f4239

Description

RAR_Archive SHA256 of 173b17e195b0a80611c22f333c3d2ec2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e7cd3233fd39175970675135dac2c582382747b328b3786f8a833ae2ab8f4239']

Name

40f06539ed0d45ba833d6ff0b9ef8165b8bebf407abcf17f27ec27951de0d513

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '40f06539ed0d45ba833d6ff0b9ef8165b8bebf407abcf17f27ec27951de0d513']

Name

https://cdn.fbsbx.com/v/t59.2708-21/366774494_655373353219514_2097719301301827427_n.rar/photo-product-103c3e2d22c19d3f47611e2e.rar

Pattern Type

stix

Pattern

[url:value = 'https://cdn.fbsbx.com/v/t59.2708-21/366774494_655373353219514_2097719301301827427_n.rar/photo-product-103c3e2d22c19d3f47611e2e.rar']

Malware

Name
NodeStealer

StixFile

Value
3bf11184b67b82e367d36cb9ed3380a43814b000d84aef0bb89d4e08e4fcd581
40f06539ed0d45ba833d6ff0b9ef8165b8bebf407abcf17f27ec27951de0d513
e7cd3233fd39175970675135dac2c582382747b328b3786f8a833ae2ab8f4239

Url

Value
https://cdn.fbsbx.com/v/t59.2708-21/367434252_826968952391881_4583268091682907143_n.rar/image-product-103c3e2d4se43234ed22c19d3f47611e2e.rar
https://vuagame.store/4HA
https://cdn.fbsbx.com/v/t59.2708-21/366790602_1527838844638580_5700504415987597148_n.rar/Bild-Produkt-1615448759625_19599_4e232787b5053ac7f631b0c701d2159c_1.rar
https://cdn.fbsbx.com/v/t59.2708-21/366736184_272143855551717_1974995500254017245_n.rar/imagem-produto-103c3e2e43234ed22c19d3f47611e2e.rar
https://cdn.fbsbx.com/v/t59.2708-21/366541252_307708121731913_2867761615862616633_n.rar/image-produit-103c3gdfe2d22c19d3f47611e2e.rar
https://cdn.fbsbx.com/v/t59.2708-21/366774494_655373353219514_2097719301301827427_n.rar/photo-product-103c3e2d22c19d3f47611e2e.rar
https://vuagame.store/4HAI.zip
https://vuagame.store/rmv
https://vuagame.store/document.zip

External References

- https://otx.alienvault.com/pulse/65080ead21f8e49d8badcccb
- https://www.netskope.com/blog/new-python-nodestealer-goes-beyond-facebook-credentials-now-stealing-all-browser-cookies-and-login-credentials