Dec 22 2023

NETMANAGEIT

Intelligence Report

Why Is an Australian Footballer Collecting My Passwords? The Various Ways Malicious JavaScript Can Steal Your Secrets

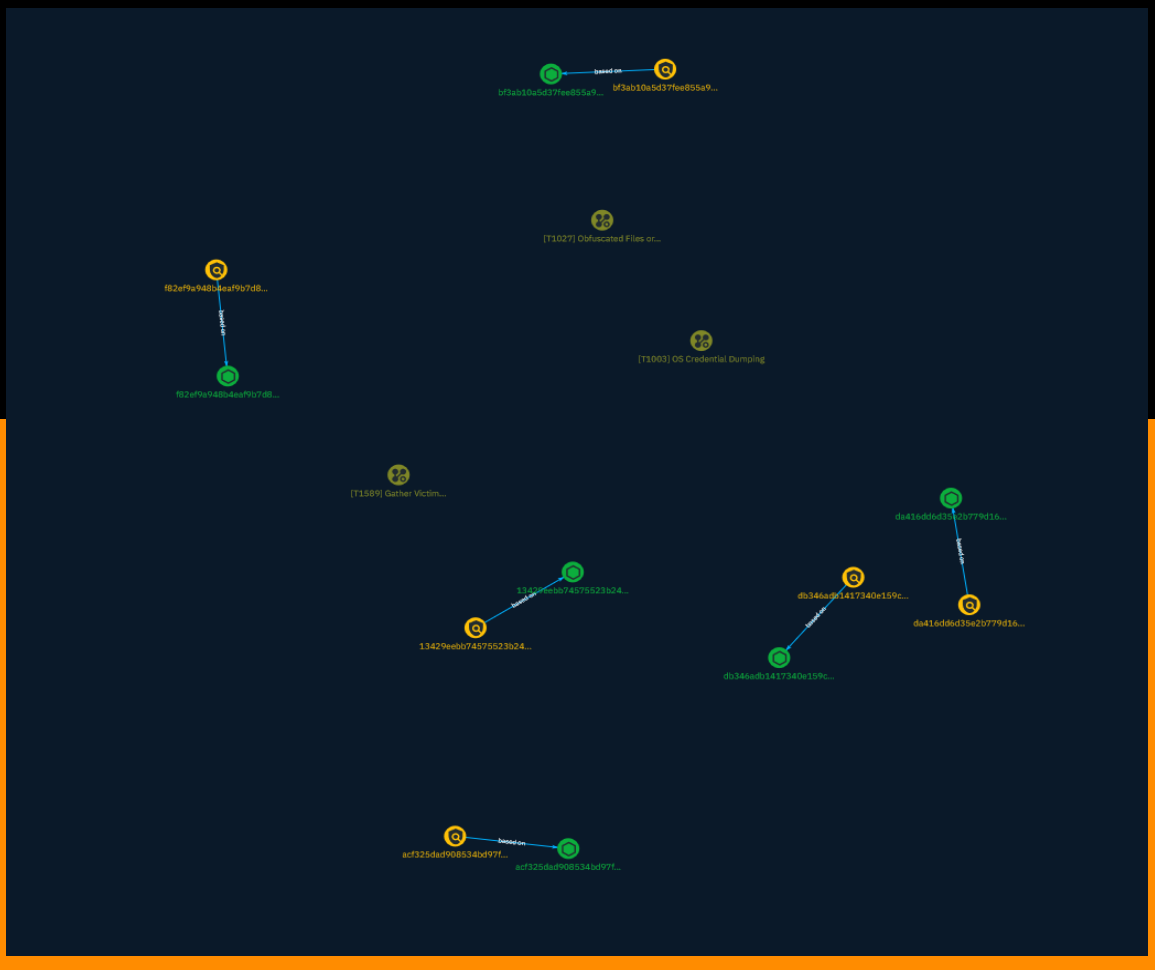

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Malicious JavaScript is increasingly being used to steal sensitive information including passwords and credit card numbers, according to research carried out by Palo Alto Networks Unit 42 and the University of California, Los Angeles (UCLA).

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
OS Credential Dumping
ID
T1003
Description
Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.
Name
Gather Victim Identity Information
ID
T1589
Description
Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal

data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials. Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about users could also be enumerated via other active means (i.e. [Active Scanning](https://attack.mitre.org/techniques/T1595)) such as probing and analyzing responses from authentication services that may reveal valid usernames in a system. (Citation: GrimBlog UsernameEnum) Information about victims may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: OPM Leak)(Citation: Register Deloitte)(Citation: Register Uber)(Citation: Detectify Slack Tokens)(Citation: Forbes GitHub Creds)(Citation: GitHub truffleHog)(Citation: GitHub Gitrob)(Citation: CNET Leaks) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

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)

Indicator

Name
13429eebb74575523b242e16b51eacf287a351c6de04557ec3cc343812aae0cb
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '13429eebb74575523b242e16b51eacf287a351c6de04557ec3cc343812aae0cb']
Name
bf3ab10a5d37fee855a9336669839ce6ad3862ad32f97207d4e959faaba0a3ed
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'bf3ab10a5d37fee855a9336669839ce6ad3862ad32f97207d4e959faaba0a3ed']
Name

da416dd6d35e2b779d164f06d4798ca2d9a3d3867e7708b11bf6a863a5e7ffc2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'da416dd6d35e2b779d164f06d4798ca2d9a3d3867e7708b11bf6a863a5e7ffc2']

Name

f82ef9a948b4eaf9b7d8cda13c5fa8170c20b72fde564f7d3a0f271644c73b92

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f82ef9a948b4eaf9b7d8cda13c5fa8170c20b72fde564f7d3a0f271644c73b92']

Name

db346adb1417340e159c45c5e4fdaea039c0edbca6e62ad46aa9aec1cf1273a1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'db346adb1417340e159c45c5e4fdaea039c0edbca6e62ad46aa9aec1cf1273a1']

Name

acf325dad908534bd97f6df0926f30fc7938a1ac6af1cec00aa45bcf63699e24

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'acf325dad908534bd97f6df0926f30fc7938a1ac6af1cec00aa45bcf63699e24']

StixFile

Value
acf325dad908534bd97f6df0926f30fc7938a1ac6af1cec00aa45bcf63699e24
f82ef9a948b4eaf9b7d8cda13c5fa8170c20b72fde564f7d3a0f271644c73b92
da416dd6d35e2b779d164f06d4798ca2d9a3d3867e7708b11bf6a863a5e7ffc2
db346adb1417340e159c45c5e4fdaea039c0edbca6e62ad46aa9aec1cf1273a1
bf3ab10a5d37fee855a9336669839ce6ad3862ad32f97207d4e959faaba0a3ed
13429eebb74575523b242e16b51eacf287a351c6de04557ec3cc343812aae0cb

External References

- https://otx.alienvault.com/pulse/658439e86a451e98d57ca3d8
- https://unit42.paloaltonetworks.com/malicious-javascript-steals-sensitive-data/