Mar 08 2024

NETMANAGEIT

Intelligence Report

New Fakext malware targets Latin American banks

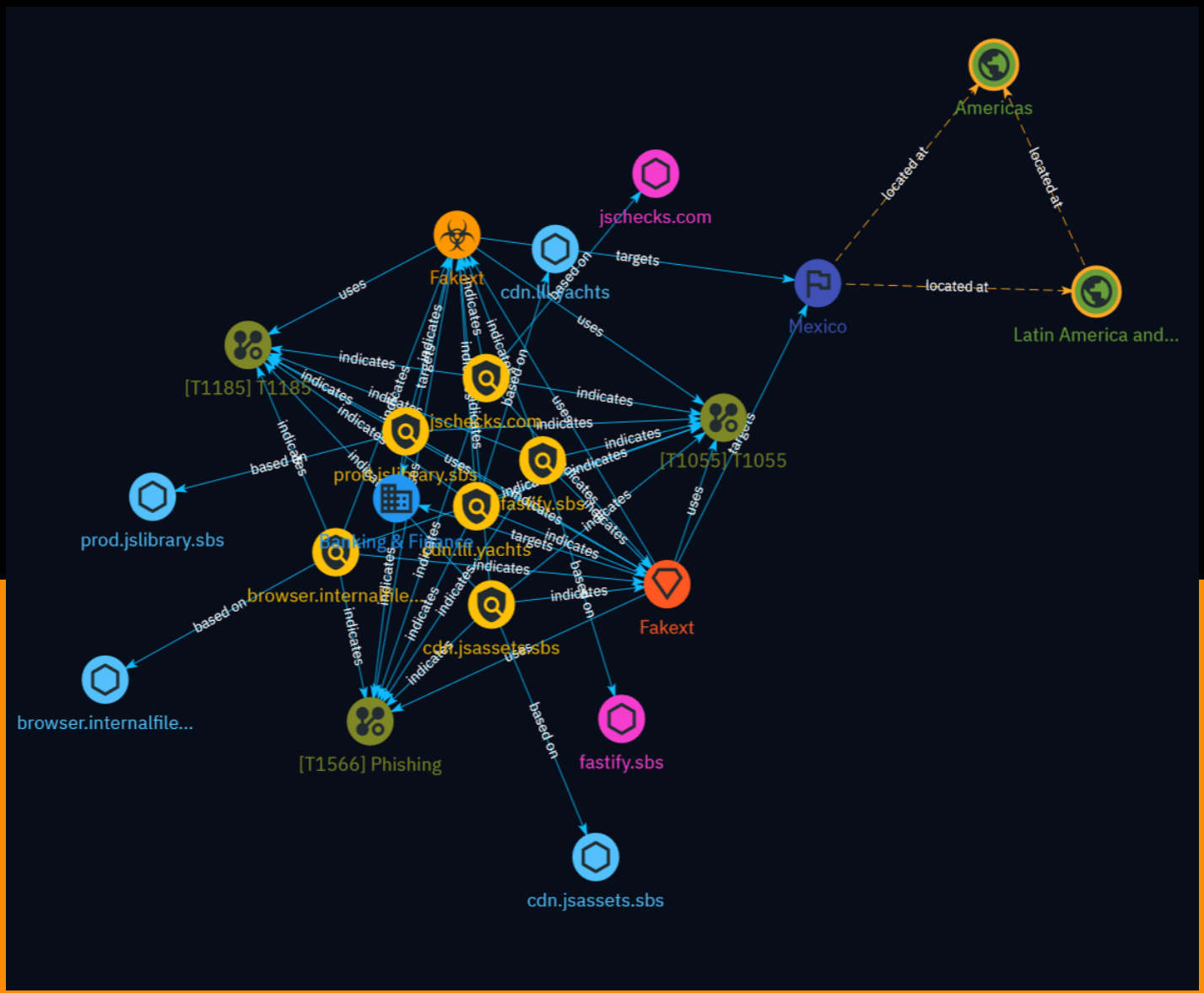

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Indicator 6
- Malware 9
- Intrusion-Set 10
- Sector 11
- Attack-Pattern 12
- Country 15
- Region 16

Observables

- Hostname 17
- Domain-Name 18

External References

- External References 19

Overview

Description

A new malware campaign called Fakext is using malicious browser extensions to steal credentials and install remote access tools on victims' devices. The campaign is primarily targeting banks in Latin America. The malware uses man-in-the-browser attacks and web injections to steal input fields and display fake pages prompting victims to download remote access tools. Technical analysis shows the malware uses evasive techniques like domain spoofing and anti-debugging methods.

Confidence

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

100 / 100

Content

N/A

Indicator

Name
prod.jslibrary.sbs
Pattern Type
stix
Pattern
[hostname:value = 'prod.jslibrary.sbs']
Name
cdn.lll.yachts
Pattern Type
stix
Pattern
[hostname:value = 'cdn.lll.yachts']
Name
cdn.jsassets.sbs

Pattern Type

stix

Pattern

[hostname:value = 'cdn.jsassets.sbs']

Name

browser.internalfiles.sbs

Pattern Type

stix

Pattern

[hostname:value = 'browser.internalfiles.sbs']

Name

jschecks.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 year ago', 'timestamp': 1674096785, 'iso': '2023-01-18T21:53:05-05:00'} - **IPQS: Domain:** jschecks.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'jschecks.com']

Name

fastify.sbs

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1698858787, 'iso': '2023-11-01T13:13:07-04:00'} - **IPQS: Domain:** fastify.sbs - **IPQS: IP Address:** 104.21.20.179

Pattern Type

stix

Pattern

[domain-name:value = 'fastify.sbs']

Malware

Name
Fakext

Intrusion-Set

Name
Fakext

Sector

Name
Banking & Finance

Attack-Pattern

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

T1185

ID

T1185

Description

Adversaries may take advantage of security vulnerabilities and inherent functionality in browser software to change content, modify user-behaviors, and intercept information as part of various browser session hijacking techniques.(Citation: Wikipedia Man in the Browser) A specific example is when an adversary injects software into a browser that allows them to inherit cookies, HTTP sessions, and SSL client certificates of a user then use the browser as a way to pivot into an authenticated intranet.(Citation: Cobalt Strike Browser Pivot)(Citation: ICEBRG Chrome Extensions) Executing browser-based behaviors such as pivoting may require specific process permissions, such as `SeDebugPrivilege` and/or high-integrity/administrator rights. Another example involves pivoting browser traffic from the adversary's browser through the user's browser by setting up a proxy which will redirect web traffic. This does not alter the user's traffic in any way, and the proxy connection can be severed as soon as the browser is closed. The adversary assumes the security context of whichever browser process the proxy is injected into. Browsers typically create a new process for each tab that is opened and permissions and certificates are separated accordingly. With these permissions, an adversary could potentially browse to any resource on an intranet, such as [Sharepoint](https://attack.mitre.org/techniques/T1213/002) or webmail, that is accessible through the browser and which the browser has sufficient permissions. Browser pivoting may also bypass security provided by 2-factor authentication.(Citation: cobaltstrike manual)

Name

T1055

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Country

Name
Mexico

Region

Name
Latin America and the Caribbean

Name
Americas

Hostname

Value
prod.jslibrary.sbs
cdn.lll.yachts
cdn.jsassets.sbs
browser.internalfiles.sbs

Domain-Name

Value
jschecks.com
fastify.sbs

External References

- https://securityintelligence.com/posts/fakext-targeting-latin-american-banks/
- https://otx.alienvault.com/pulse/65eb47e34664fa12510c74c1