Jul 06 2023

Intelligence Report

Malicious ad for USPS fishes for banking credentials

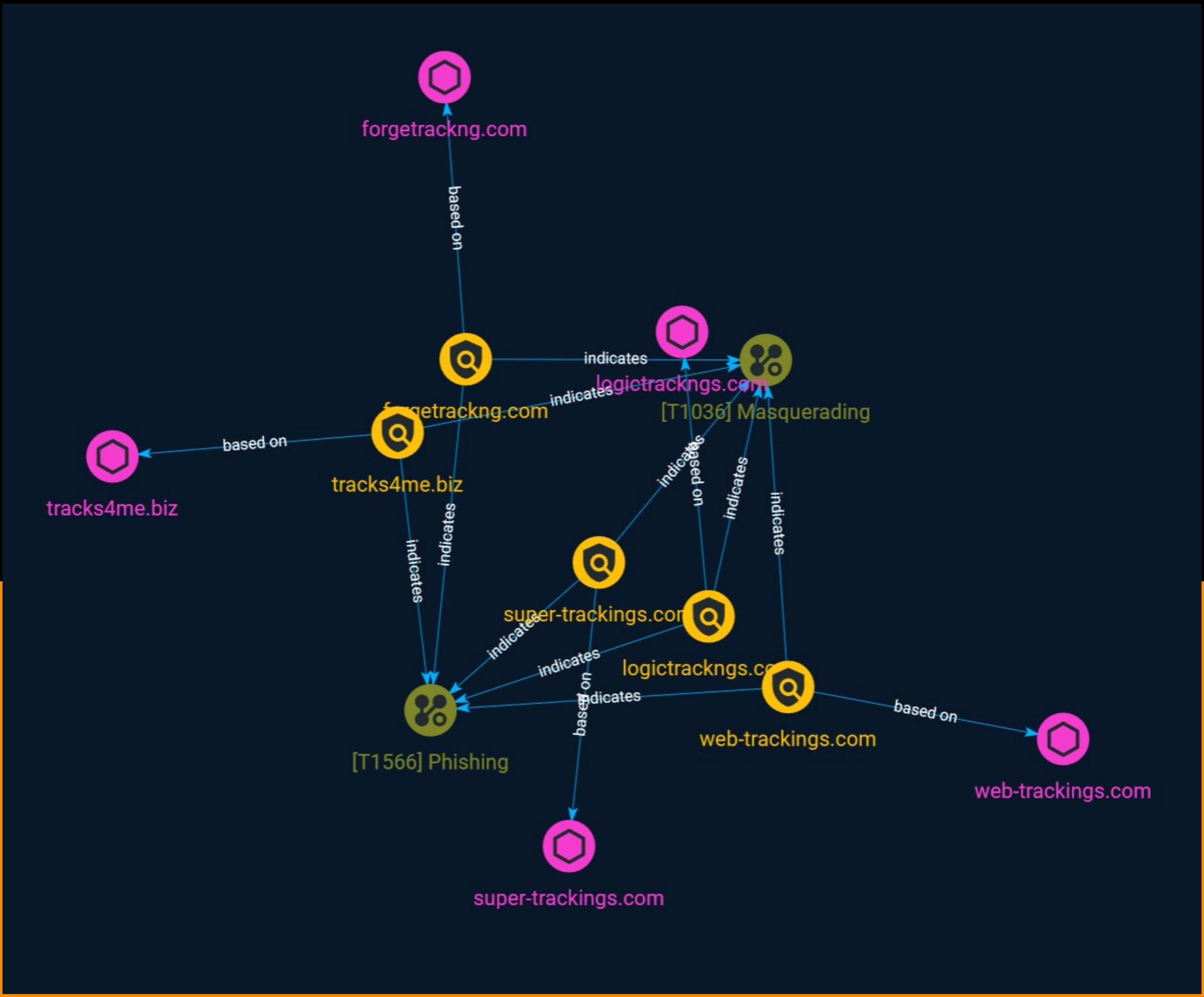

Table of contents

Overview

Entities

Observables

External References

Overview

Description

We often think of malvertising as being malicious ads that push malware or scams, and quite rightly so these are probably the most common payloads. However, malvertising is also a great vehicle for phishing attacks which we usually see more often via spam emails.

Confidence

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

15 / 100

Indicator

Name

logictrackngs.com

Pattern Type

stix

Pattern

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

Name

super-trackings.com

Pattern Type

stix

Pattern

[domain-name:value = 'super-trackings.com']

Name

forgetrackng.com

Pattern Type

stix

Pattern

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

Name

web-trackings.com

Pattern Type

stix

Pattern

[domain-name:value = 'web-trackings.com']

Name

tracks4me.biz

Pattern Type

stix

Pattern

[domain-name:value = 'tracks4me.biz']

Attack-Pattern

Name
Masquerading
ID
T1036
Description
Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)
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)

Domain-Name

Value
logictrackngs.com
web-trackings.com
tracks4me.biz
forgetrackng.com
super-trackings.com

External References

- https://otx.alienvault.com/pulse/64a715ea971d76ba344ffe4f
- https://www.malwarebytes.com/blog/threat-intelligence/2023/07/malicious-ad-for-usps-phishes-for-jpmorgan-chase-credentials