Dec 19 2023

NETMANAGEIT

Intelligence Report

Toward Ending the Domain Wars: Early Detection of Malicious Stockpiled Domains

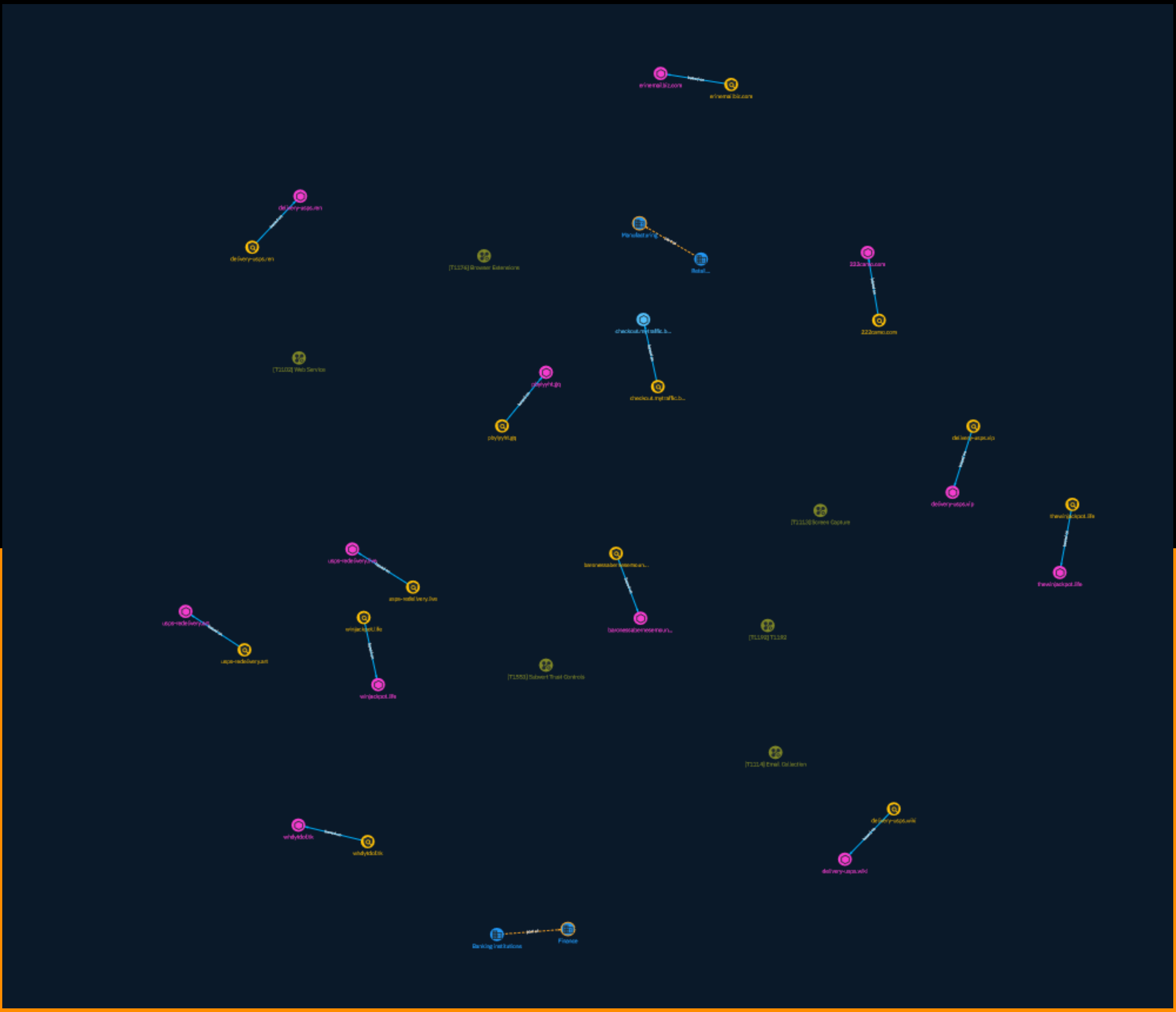

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Palo Alto Networks has developed an automated detector to detect malicious domain names that are being used by cybercriminals to make it harder for law enforcement to take down their botnets, or domain wars.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
T1192
ID
T1192
Name
Subvert Trust Controls
ID
T1553
Description
Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls.

(Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

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

Email Collection

ID

T1114

Description

Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including trade secrets or personal information, that can prove valuable to adversaries. Adversaries can collect or forward email from mail servers or clients.

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).

Name

Screen Capture

ID
T1113

Description
Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

Sector

Name
Finance
Description
Public and private entities involved in the allocation of assets and liabilities over space and time.
Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name
Retail (distribution)
Description
Distribution and sale of goods directly to the consumer.
Name

Banking institutions
Description
Credit institutions whose business consists in receiving repayable funds from the public and granting credit. As the bank of banks, central banks are included in this scope.

Indicator

Name
usps-redelivery.art
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix
Pattern
[domain-name:value = 'usps-redelivery.art']
Name
winjackpot.life
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix

Pattern
[domain-name:value = 'winjackpot.life']

Name
222camo.com

Pattern Type
stix

Pattern
[domain-name:value = '222camo.com']

Name
checkout.mytraffic.biz

Pattern Type
stix

Pattern
[hostname:value = 'checkout.mytraffic.biz']

Name
delivery-usps.vip

Description
Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'delivery-usps.vip']

Name

usps-redelivery.live

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'usps-redelivery.live']

Name

delivery-usps.ren

Pattern Type

stix

Pattern

[domain-name:value = 'delivery-usps.ren']

Name

thewinjackpot.life

Description

Created by VirusTotal connector as the positive count was >= 10

Pattern Type

stix

Pattern

[domain-name:value = 'thewinjackpot.life']

Name

whdytdof.tk

Pattern Type

stix

Pattern

[domain-name:value = 'whdytdof.tk']

Name

baronessabernesemountaindogpuppies.com

Pattern Type

stix

Pattern
[domain-name:value = 'baronessabernesemountaindogpuppies.com']
Name
delivery-usps.wiki
Pattern Type
stix
Pattern
[domain-name:value = 'delivery-usps.wiki']
Name
pbyiyyht.gq
Pattern Type
stix
Pattern
[domain-name:value = 'pbyiyyht.gq']
Name
erinemailbiz.com
Pattern Type
stix

Pattern
[domain-name:value = 'erinemailbiz.com']

Domain-Name

Value
baronessabernesemountaindogpuppies.com
delivery-usps.ren
thewinjackpot.life
whdytdof.tk
222camo.com
delivery-usps.wiki
usps-redelivery.live
pbyiyyht.gq
winjackpot.life
erinemailbiz.com
delivery-usps.vip
usps-redelivery.art

Hostname

Value
checkout.mytraffic.biz

External References

- https://otx.alienvault.com/pulse/658181bc828850f35f6b26c7
- https://unit42.paloaltonetworks.com/detecting-malicious-stockpiled-domains/