Feb 01 2024

NETMANAGEIT

Intelligence Report

An Evasive Large-Scale Scareware and PUP Delivery Campaign

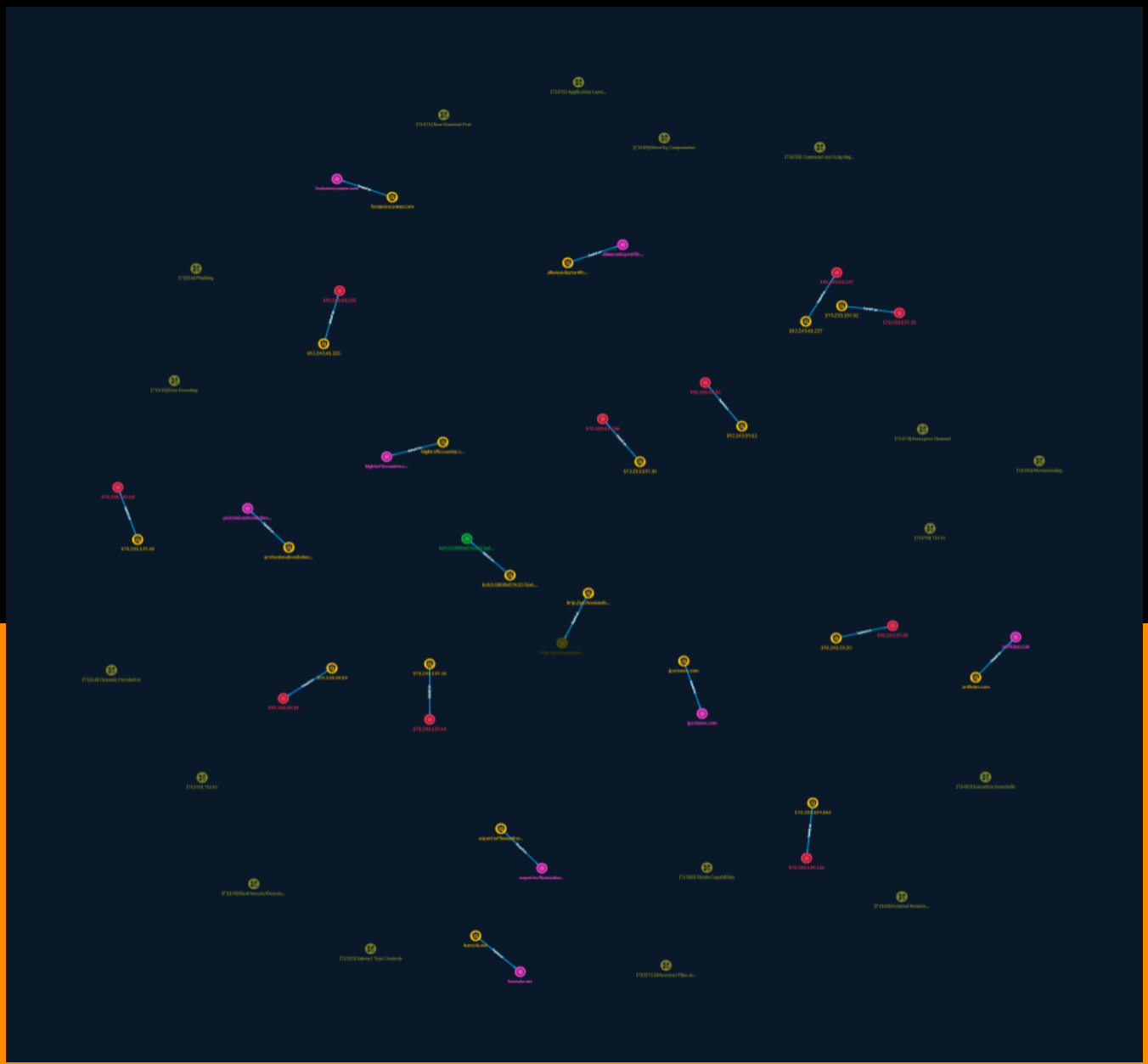

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Indicator 6
- Attack-Pattern 29

Observables

- Domain-Name 50
- IPv4-Addr 52
- StixFile 54
- Url 55

External References

- External References 56

Overview

Description

Researchers discovered a large-scale campaign called ApateWeb that uses over 130,000 domains to deliver scareware, potentially unwanted programs, and scam pages. The campaign has complex infrastructure with multiple layers of redirection between the entry point and final payload delivery. A group controls the entry point, tracking victims before forwarding traffic. They use evasive tactics like cloaking and wildcard DNS. Since August 2022 there has been increased activity, though it has been active throughout 2022-2024. Hundreds of sites involved rank in Tranco's top 1 million websites. Millions of monthly hits come from around the world. The campaign spreads via deceptive emails and JavaScript embedded on sites. Customers using Advanced URL Filtering and DNS Security are better protected.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

professionalswebcheck.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 84706 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Missing Content - **Domain Age:** {'human': '2 years ago', 'timestamp': 1648802359, 'iso': '2022-04-01T04:39:19-04:00'} - **IPQS: Domain:** professionalswebcheck.com - **IPQS: IP Address:** 146.148.34.125

Pattern Type

stix

Pattern

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

Name

experttrafficmonitor.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago',

'timestamp': 1700133846, 'iso': '2023-11-16T06:24:06-05:00'} - **IPQS: Domain:** experttrafficmonitor.com - **IPQS: IP Address:** 3.216.175.245

Pattern Type

stix

Pattern

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

Name

192.243.61.227

Description

- **Zip Code:** N/A - **ISP:** DataWeb Global Group - **ASN:** 39572 - **Organization:** DataWeb Global Group - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 192.243.61.227 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Virginia - **City:** Ashburn - **Latitude:** 39.02 - **Longitude:** -77.54

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.243.61.227']

Name

192.243.59.20

Description

- **Zip Code:** N/A - **ISP:** DataWeb Global Group - **ASN:** 39572 - **Organization:** DataWeb Global Group - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 192.243.59.20 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Virginia - **City:** Ashburn - **Latitude:** 39.02 - **Longitude:** -77.54

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.243.59.20']

Name

192.243.61.225

Description

- **Zip Code:** N/A - **ISP:** DataWeb Global Group - **ASN:** 39572 - **Organization:** DataWeb Global Group - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 192.243.61.225 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Virginia - **City:** Ashburn - **Latitude:** 39.02 - **Longitude:** -77.54

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.243.61.225']

Name

192.243.59.13

Description

- **Zip Code:** N/A - **ISP:** DataWeb Global Group - **ASN:** 39572 - **Organization:** DataWeb Global Group - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 192.243.59.13 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Virginia - **City:** Ashburn - **Latitude:** 39.02 - **Longitude:** -77.54

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.243.59.13']

Name

192.243.59.12

Description

- **Zip Code:** N/A - **ISP:** DataWeb Global Group - **ASN:** 39572 - **Organization:** DataWeb Global Group - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 192.243.59.12 - **Proxy:** True - **VPN:** True - **TOR:** True - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Virginia - **City:** Ashburn - **Latitude:** 39.01800156 - **Longitude:** -77.53900146

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.243.59.12']

Name

173.233.137.52

Description

- **Zip Code:** N/A - **ISP:** Servers-com - **ASN:** 7979 - **Organization:** Servers-com - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 173.233.137.52 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Texas - **City:** Dallas - **Latitude:** 32.79 - **Longitude:** -96.82

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.233.137.52']

Name

173.233.139.164

Description

- **Zip Code:** N/A - **ISP:** Servers-com - **ASN:** 7979 - **Organization:** Servers-com - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 173.233.139.164 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Texas - **City:** Dallas - **Latitude:** 32.79 - **Longitude:** -96.82

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.233.139.164']

Name

173.233.137.60

Description

- **Zip Code:** N/A - **ISP:** Servers-com - **ASN:** 7979 - **Organization:** Servers-com - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 173.233.137.60 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Texas - **City:** Dallas - **Latitude:** 32.79 - **Longitude:** -96.82

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.233.137.60']

Name

173.233.137.44

Description

- **Zip Code:** N/A - **ISP:** Servers-com - **ASN:** 7979 - **Organization:** Servers-com - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 173.233.137.44 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Texas - **City:** Dallas - **Latitude:** 32.79 - **Longitude:** -96.82

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.233.137.44']

Name

173.233.137.36

Description

- **Zip Code:** N/A - **ISP:** Servers-com - **ASN:** 7979 - **Organization:** Servers-com - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 173.233.137.36 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Texas - **City:** Dallas - **Latitude:** 32.79 - **Longitude:** -96.82

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.233.137.36']

Name

jpadsnow.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 23 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Search Engines - **Domain Age:** {'human': '3 months ago', 'timestamp': 1698757864, 'iso': '2023-10-31T09:11:04-04:00'} - **IPQS: Domain:** yahoo.com - **IPQS: IP Address:** 98.137.11.164

Pattern Type

stix

Pattern

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

Name

hightrafficcounter.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 174436 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Malicious websites - **Domain Age:**

{'human': '4 weeks ago', 'timestamp': 1704309556, 'iso': '2024-01-03T14:19:16-05:00'} - **IPQS: Domain:** hightrafficcounter.com - **IPQS: IP Address:** 204.11.56.48

Pattern Type

stix

Pattern

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

Name

hanoola.net

Pattern Type

stix

Pattern

[domain-name:value = 'hanoola.net']

Name

featuresscanner.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 1 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Search Engines - **Domain Age:** {'human': '5 months ago', 'timestamp': 1693565015, 'iso': '2023-09-01T06:43:35-04:00'} - **IPQS: Domain:** google.com - **IPQS: IP Address:** 192.243.59.12

Pattern Type

stix

Pattern

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

Name

artificius.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '11 months ago', 'timestamp': 1678351405, 'iso': '2023-03-09T03:43:25-05:00'} - **IPQS: Domain:** artificius.com - **IPQS: IP Address:** 172.67.132.219

Pattern Type

stix

Pattern

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

Name

allureoutlayterrific.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 1 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Search Engines - **Domain Age:**

{'human': '8 months ago', 'timestamp': 1687082053, 'iso': '2023-06-18T05:54:13-04:00'} - **IPQS: Domain:** google.com - **IPQS: IP Address:** 172.240.108.68

Pattern Type

stix

Pattern

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

Name

http://professionalswebcheck.com/stats

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 84706 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Missing Content - **Domain Age:** {'human': '2 years ago', 'timestamp': 1648802359, 'iso': '2022-04-01T04:39:19-04:00'} - **IPQS: Domain:** professionalswebcheck.com - **IPQS: IP Address:** 146.148.34.125

Pattern Type

stix

Pattern

[url:value = 'http://professionalswebcheck.com/stats']

Name

bd62d3808ef29c557da64b412c4422935a641c22e2bdcfe5128c96f2ff5b5e99

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd62d3808ef29c557da64b412c4422935a641c22e2bdcfe5128c96f2ff5b5e99']

Name

professionalswebcheck.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 84706 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Missing Content - **Domain Age:** {'human': '2 years ago', 'timestamp': 1648802359, 'iso': '2022-04-01T04:39:19-04:00'} - **IPQS: Domain:** professionalswebcheck.com - **IPQS: IP Address:** 146.148.34.125

Pattern Type

stix

Pattern

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

Name

experttrafficmonitor.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago',

'timestamp': 1700133846, 'iso': '2023-11-16T06:24:06-05:00'} - **IPQS: Domain:** experttrafficmonitor.com - **IPQS: IP Address:** 3.216.175.245

Pattern Type

stix

Pattern

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

Name

192.243.61.227

Description

- **Zip Code:** N/A - **ISP:** DataWeb Global Group - **ASN:** 39572 - **Organization:** DataWeb Global Group - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 192.243.61.227 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Virginia - **City:** Ashburn - **Latitude:** 39.02 - **Longitude:** -77.54

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.243.61.227']

Name

192.243.59.20

Description

- **Zip Code:** N/A - **ISP:** DataWeb Global Group - **ASN:** 39572 - **Organization:** DataWeb Global Group - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 192.243.59.20 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Virginia - **City:** Ashburn - **Latitude:** 39.02 - **Longitude:** -77.54

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.243.59.20']

Name

192.243.61.225

Description

- **Zip Code:** N/A - **ISP:** DataWeb Global Group - **ASN:** 39572 - **Organization:** DataWeb Global Group - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 192.243.61.225 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Virginia - **City:** Ashburn - **Latitude:** 39.02 - **Longitude:** -77.54

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.243.61.225']

Name

192.243.59.13

Description

- **Zip Code:** N/A - **ISP:** DataWeb Global Group - **ASN:** 39572 - **Organization:** DataWeb Global Group - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 192.243.59.13 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Virginia - **City:** Ashburn - **Latitude:** 39.02 - **Longitude:** -77.54

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.243.59.13']

Name

192.243.59.12

Description

- **Zip Code:** N/A - **ISP:** DataWeb Global Group - **ASN:** 39572 - **Organization:** DataWeb Global Group - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 192.243.59.12 - **Proxy:** True - **VPN:** True - **TOR:** True - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Virginia - **City:** Ashburn - **Latitude:** 39.01800156 - **Longitude:** -77.53900146

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.243.59.12']

Name

173.233.137.52

Description

- **Zip Code:** N/A - **ISP:** Servers-com - **ASN:** 7979 - **Organization:** Servers-com - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 173.233.137.52 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Texas - **City:** Dallas - **Latitude:** 32.79 - **Longitude:** -96.82

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.233.137.52']

Name

173.233.139.164

Description

- **Zip Code:** N/A - **ISP:** Servers-com - **ASN:** 7979 - **Organization:** Servers-com - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 173.233.139.164 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Texas - **City:** Dallas - **Latitude:** 32.79 - **Longitude:** -96.82

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.233.139.164']

Name

173.233.137.60

Description

- **Zip Code:** N/A - **ISP:** Servers-com - **ASN:** 7979 - **Organization:** Servers-com - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 173.233.137.60 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Texas - **City:** Dallas - **Latitude:** 32.79 - **Longitude:** -96.82

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.233.137.60']

Name

173.233.137.44

Description

- **Zip Code:** N/A - **ISP:** Servers-com - **ASN:** 7979 - **Organization:** Servers-com - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 173.233.137.44 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Texas - **City:** Dallas - **Latitude:** 32.79 - **Longitude:** -96.82

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.233.137.44']

Name

173.233.137.36

Description

- **Zip Code:** N/A - **ISP:** Servers-com - **ASN:** 7979 - **Organization:** Servers-com - **Is Crawler:** False - **Timezone:** America/Chicago - **Mobile:** False - **Host:** 173.233.137.36 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Texas - **City:** Dallas - **Latitude:** 32.79 - **Longitude:** -96.82

Pattern Type

stix

Pattern

[ipv4-addr:value = '173.233.137.36']

Name

jpadsnow.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 23 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Search Engines - **Domain Age:** {'human': '3 months ago', 'timestamp': 1698757864, 'iso': '2023-10-31T09:11:04-04:00'} - **IPQS: Domain:** yahoo.com - **IPQS: IP Address:** 98.137.11.164

Pattern Type

stix

Pattern

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

Name

hightrafficcounter.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 174436 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Malicious websites - **Domain Age:**

{'human': '4 weeks ago', 'timestamp': 1704309556, 'iso': '2024-01-03T14:19:16-05:00'} - **IPQS: Domain:** hightrafficcounter.com - **IPQS: IP Address:** 204.11.56.48

Pattern Type

stix

Pattern

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

Name

hanoola.net

Pattern Type

stix

Pattern

[domain-name:value = 'hanoola.net']

Name

featuresscanner.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 1 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Search Engines - **Domain Age:** {'human': '5 months ago', 'timestamp': 1693565015, 'iso': '2023-09-01T06:43:35-04:00'} - **IPQS: Domain:** google.com - **IPQS: IP Address:** 192.243.59.12

Pattern Type

stix

Pattern

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

Name

artificius.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '11 months ago', 'timestamp': 1678351405, 'iso': '2023-03-09T03:43:25-05:00'} - **IPQS: Domain:** artificius.com - **IPQS: IP Address:** 172.67.132.219

Pattern Type

stix

Pattern

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

Name

allureoutlayterrific.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 1 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Search Engines - **Domain Age:**

{'human': '8 months ago', 'timestamp': 1687082053, 'iso': '2023-06-18T05:54:13-04:00'} - **IPQS: Domain:** google.com - **IPQS: IP Address:** 172.240.108.68

Pattern Type

stix

Pattern

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

Name

http://professionalswebcheck.com/stats

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 84706 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Missing Content - **Domain Age:** {'human': '2 years ago', 'timestamp': 1648802359, 'iso': '2022-04-01T04:39:19-04:00'} - **IPQS: Domain:** professionalswebcheck.com - **IPQS: IP Address:** 146.148.34.125

Pattern Type

stix

Pattern

[url:value = 'http://professionalswebcheck.com/stats']

Name

bd62d3808ef29c557da64b412c4422935a641c22e2bdcfe5128c96f2ff5b5e99

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd62d3808ef29c557da64b412c4422935a641c22e2bdcfe5128c96f2ff5b5e99']

Attack-Pattern

Name
T1193
ID
T1193
Name
T1192
ID
T1192
Name
Drive-by Compromise
ID
T1189
Description
Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for

exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

Name

Obtain Capabilities

ID

T1588

Description

Adversaries may buy and/or steal capabilities that can be used during targeting. Rather than developing their own capabilities in-house, adversaries may purchase, freely download, or steal them. Activities may include the acquisition of malware, software (including licenses), exploits, certificates, and information relating to vulnerabilities. Adversaries may obtain capabilities to support their operations throughout numerous phases of the adversary lifecycle. In addition to downloading free malware, software, and exploits from the internet, adversaries may purchase these capabilities from third-party entities. Third-party entities can include technology companies that specialize in malware and exploits, criminal marketplaces, or from individuals.(Citation: NationsBuying)(Citation: PegasusCitizenLab) In addition to purchasing capabilities, adversaries may steal capabilities from third-party entities (including other adversaries). This can include stealing software licenses, malware, SSL/TLS and code-signing certificates, or raiding closed databases of vulnerabilities or exploits.(Citation: DiginotarCompromise)

Name

Data Encoding

ID

T1132

Description

Adversaries may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system. Use of data encoding may adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems.(Citation: Wikipedia Binary-to-text Encoding) (Citation: Wikipedia Character Encoding) Some data encoding systems may also result in data compression, such as gzip.

Name

Encrypted Channel

ID

T1573

Description

Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

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

Non-Standard Port

ID

T1571

Description

Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data. Adversaries may also make changes to victim systems to abuse non-standard ports. For example, Registry keys and other configuration settings can be used to modify protocol and port pairings.(Citation: change_rdp_port_conti)

Name

Execution Guardrails

ID

T1480

Description

Adversaries may use execution guardrails to constrain execution or actions based on adversary supplied and environment specific conditions that are expected to be present on the target. Guardrails ensure that a payload only executes against an intended target and reduces collateral damage from an adversary's campaign.(Citation: FireEye Kevin Mandia Guardrails) Values an adversary can provide about a target system or environment to use as guardrails may include specific network share names, attached physical devices, files, joined Active Directory (AD) domains, and local/external IP addresses.(Citation: FireEye Outlook Dec 2019) Guardrails can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. This use of guardrails is distinct from typical [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497). While use of [Virtualization/Sandbox Evasion](https://

attack.mitre.org/techniques/T1497) may involve checking for known sandbox values and continuing with execution only if there is no match, the use of guardrails will involve checking for an expected target-specific value and only continuing with execution if there is such a match.

Name

Dynamic Resolution

ID

T1568

Description

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control. Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer

systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

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

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

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) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack

against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

External Remote Services

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms

allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management] (https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Name

T1193

ID

T1193

Name

T1192

ID

T1192

Name

Drive-by Compromise

ID

T1189

Description

Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising] (https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

Name

Obtain Capabilities

ID

T1588

Description

Adversaries may buy and/or steal capabilities that can be used during targeting. Rather than developing their own capabilities in-house, adversaries may purchase, freely download, or steal them. Activities may include the acquisition of malware, software (including licenses), exploits, certificates, and information relating to vulnerabilities. Adversaries may obtain capabilities to support their operations throughout numerous phases of the adversary lifecycle. In addition to downloading free malware, software, and exploits from the internet, adversaries may purchase these capabilities from third-party entities. Third-party entities can include technology companies that specialize in malware and exploits, criminal marketplaces, or from individuals.(Citation: NationsBuying)(Citation: PegasusCitizenLab) In addition to purchasing capabilities, adversaries may steal capabilities from third-party entities (including other adversaries). This can include stealing software licenses, malware, SSL/TLS and code-signing certificates, or raiding closed databases of vulnerabilities or exploits.(Citation: DiginotarCompromise)

Name

Data Encoding

ID

T1132

Description

Adversaries may encode data to make the content of command and control traffic more difficult to detect. Command and control (C2) information can be encoded using a standard data encoding system. Use of data encoding may adhere to existing protocol specifications and includes use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems.(Citation: Wikipedia Binary-to-text Encoding) (Citation:

Wikipedia Character Encoding) Some data encoding systems may also result in data compression, such as gzip.

Name

Encrypted Channel

ID

T1573

Description

Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Despite the use of a secure algorithm, these implementations may be vulnerable to reverse engineering if secret keys are encoded and/or generated within malware samples/configuration files.

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

Non-Standard Port

ID

T1571

Description

Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data. Adversaries may also make changes to victim systems to abuse non-standard ports. For example, Registry keys and other configuration settings can be used to modify protocol and port pairings.(Citation: change_rdp_port_conti)

Name

Execution Guardrails

ID

T1480

Description

Adversaries may use execution guardrails to constrain execution or actions based on adversary supplied and environment specific conditions that are expected to be present on the target. Guardrails ensure that a payload only executes against an intended target

and reduces collateral damage from an adversary's campaign.(Citation: FireEye Kevin Mandia Guardrails) Values an adversary can provide about a target system or environment to use as guardrails may include specific network share names, attached physical devices, files, joined Active Directory (AD) domains, and local/external IP addresses.(Citation: FireEye Outlook Dec 2019) Guardrails can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. This use of guardrails is distinct from typical [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497). While use of [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) may involve checking for known sandbox values and continuing with execution only if there is no match, the use of guardrails will involve checking for an expected target-specific value and only continuing with execution if there is such a match.

Name

Dynamic Resolution

ID

T1568

Description

Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control. Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

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

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

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) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [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)

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

External Remote Services

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Domain-Name

Value
professionalswebcheck.com
experttrafficmonitor.com
jpadsnow.com
hightrafficcounter.com
allureoutlayterrific.com
hanoola.net
featuresscanner.com
artificius.com
professionalswebcheck.com
experttrafficmonitor.com
jpadsnow.com
hightrafficcounter.com
allureoutlayterrific.com

hanoola.net

featuresscanner.com

artificius.com

IPv4-Addr

Value
192.243.61.227
192.243.61.225
192.243.59.20
192.243.59.13
192.243.59.12
173.233.139.164
173.233.137.60
173.233.137.52
173.233.137.44
173.233.137.36
192.243.61.227
192.243.61.225
192.243.59.20

192.243.59.13

192.243.59.12

173.233.139.164

173.233.137.60

173.233.137.52

173.233.137.44

173.233.137.36

StixFile

Value
bd62d3808ef29c557da64b412c4422935a641c22e2bdcfe5128c96f2ff5b5e99
bd62d3808ef29c557da64b412c4422935a641c22e2bdcfe5128c96f2ff5b5e99

Url

Value
http://professionalswebcheck.com/stats
http://professionalswebcheck.com/stats

External References

- https://unit42.paloaltonetworks.com/apateweb-scareware-pup-delivery-campaign/
- https://otx.alienvault.com/pulse/65bb916e3b058b7d29fad39a