Apr 19 2024

NETMANAGEIT

Intelligence Report

Malvertising campaign targeting IT teams with MadMxShell

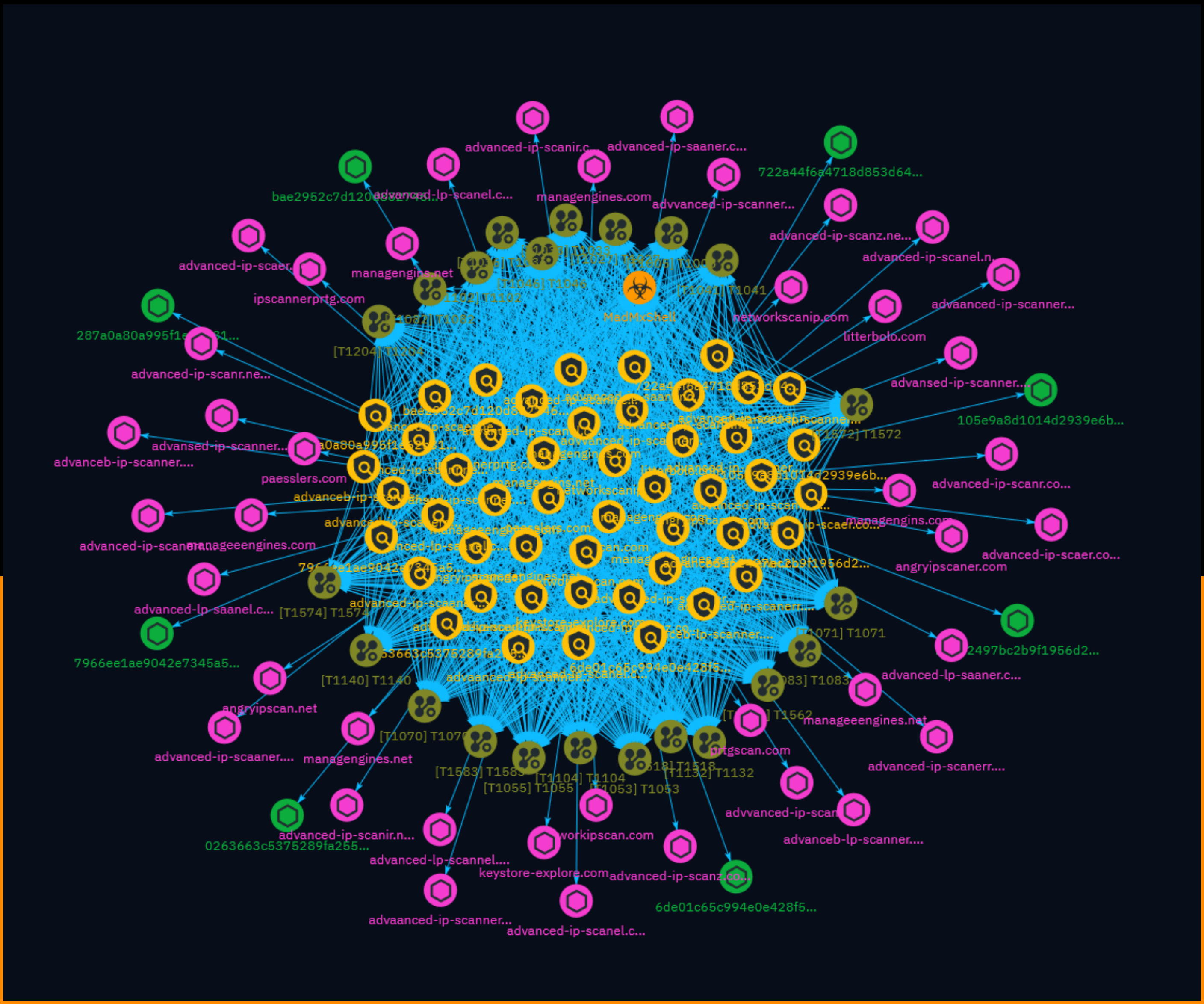

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A threat actor registered typosquatting domains masquerading as legitimate IP scanner software and leveraged Google Ads to distribute a new backdoor named MadMxShell. The backdoor uses techniques like DLL sideloading and DNS tunneling for command and control.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

prtgscan.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1708594384, 'iso': '2024-02-22T04:33:04-05:00'} - **IPQS: Domain:** prtgscan.com - **IPQS: IP Address:** 144.217.117.245

Pattern Type

stix

Pattern

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

Name

paesslers.com

Pattern Type

stix

Pattern

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

Name

networkscanip.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1708594386, 'iso': '2024-02-22T04:33:06-05:00'} - **IPQS: Domain:** networkscanip.com - **IPQS: IP Address:** 144.217.117.245

Pattern Type

stix

Pattern

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

Name

networkipscan.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1708281178, 'iso': '2024-02-18T13:32:58-05:00'} - **IPQS: Domain:** networkipscan.com - **IPQS: IP Address:** 144.217.117.245

Pattern Type

stix

Pattern

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

Name

managengins.net

Description

- **Unsafe:** False - **Server:** N/A - **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 month ago', 'timestamp': 1710451225, 'iso': '2024-03-14T17:20:25-04:00'} - **IPQS: Domain:** managengins.net - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

managengins.com

Description

- **Unsafe:** False - **Server:** N/A - **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 month ago', 'timestamp': 1710451220, 'iso': '2024-03-14T17:20:20-04:00'} - **IPQS: Domain:** managengins.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

managengines.net

Description

- **Unsafe:** False - **Server:** N/A - **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 month ago', 'timestamp': 1710448822, 'iso': '2024-03-14T16:40:22-04:00'} - **IPQS: Domain:** managengines.net - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

managengines.com

Description

- **Unsafe:** False - **Server:** N/A - **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 month ago', 'timestamp': 1710448816, 'iso': '2024-03-14T16:40:16-04:00'} - **IPQS: Domain:** managengines.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

manageeengines.net

Description

- **Unsafe:** False - **Server:** N/A - **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 month ago', 'timestamp': 1710451038, 'iso': '2024-03-14T17:17:18-04:00'} - **IPQS: Domain:** manageeengines.net - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

manageeengines.com

Description

- **Unsafe:** False - **Server:** N/A - **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 month ago', 'timestamp': 1710451032, 'iso': '2024-03-14T17:17:12-04:00'} - **IPQS: Domain:** manageeengines.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

litterbolo.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1703268940, 'iso': '2023-12-22T13:15:40-05:00'} - **IPQS: Domain:** litterbolo.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern
[domain-name:value = 'litterbolo.com']
Name
keystore-explore.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': '2 months ago', 'timestamp': 1709258134, 'iso': '2024-02-29T20:55:34-05:00'} - **IPQS: Domain:** keystore-explore.com - **IPQS: IP Address:** 144.217.123.10
Pattern Type
stix
Pattern
[domain-name:value = 'keystore-explore.com']
Name
ipscannerprtg.com
Description
- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1708594385, 'iso': '2024-02-22T04:33:05-05:00'} - **IPQS: Domain:** ipscannerprtg.com - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

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

Name

angryipscaner.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1709704943, 'iso': '2024-03-06T01:02:23-05:00'} - **IPQS: Domain:** angryipscaner.com - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

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

Name

angryipscan.net

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1709704938, 'iso': '2024-03-06T01:02:18-05:00'} - **IPQS: Domain:** angryipscan.net - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

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

Name

advvanced-ip-scanner.net

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': '3 months ago', 'timestamp': 1704502904, 'iso': '2024-01-05T20:01:44-05:00'} - **IPQS: Domain:** advvanced-ip-scanner.net - **IPQS: IP Address:** 104.21.42.16

Pattern Type

stix

Pattern

[domain-name:value = 'advvanced-ip-scanner.net']

Name

advvanced-ip-scanner.com

Description
- **Unsafe:** False - **Server:** N/A - **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': 1704502893, 'iso': '2024-01-05T20:01:33-05:00'} - **IPQS: Domain:** advvanced-ip-scanner.com - **IPQS: IP Address:** 83.97.73.252
Pattern Type
stix
Pattern
[domain-name:value = 'advvanced-ip-scanner.com']
Name
advansed-ip-scanner.net
Description
- **Unsafe:** False - **Server:** N/A - **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': 1704503004, 'iso': '2024-01-05T20:03:24-05:00'} - **IPQS: Domain:** advansed-ip-scanner.net - **IPQS: IP Address:** 83.97.73.252
Pattern Type
stix
Pattern
[domain-name:value = 'advansed-ip-scanner.net']

Name

advansed-ip-scanner.com

Description

- **Unsafe:** False - **Server:** Bu - **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': 1704502994, 'iso': '2024-01-05T20:03:14-05:00'} - **IPQS: Domain:** advansed-ip-scanner.com - **IPQS: IP Address:** 185.11.61.65

Pattern Type

stix

Pattern

[domain-name:value = 'advansed-ip-scanner.com']

Name

advanced-lp-scannel.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': 1705873183, 'iso': '2024-01-21T16:39:43-05:00'} - **IPQS: Domain:** advanced-lp-scannel.com - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-lp-scannel.com']

Name

advanced-lp-scanel.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1709584255, 'iso': '2024-03-04T15:30:55-05:00'} - **IPQS: Domain:** advanced-lp-scanel.com - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-lp-scanel.com']

Name

advanced-lp-saaner.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1709584243, 'iso': '2024-03-04T15:30:43-05:00'} - **IPQS: Domain:** advanced-lp-saaner.com - **IPQS: IP Address:** 144.217.123.10

Pattern Type
stix
Pattern
[domain-name:value = 'advanced-lp-saaner.com']
Name
advanced-lp-saanel.com
Description
- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1709584231, 'iso': '2024-03-04T15:30:31-05:00'} - **IPQS: Domain:** advanced-lp-saanel.com - **IPQS: IP Address:** 144.217.123.10
Pattern Type
stix
Pattern
[domain-name:value = 'advanced-lp-saanel.com']
Name
advanced-ip-scanz.net
Description
- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 weeks ago', 'timestamp': 1711306471, 'iso': '2024-03-24T14:54:31-04:00'} - **IPQS: Domain:** advanced-ip-scanz.net - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-ip-scanz.net']

Name

advanced-ip-scanz.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 weeks ago', 'timestamp': 1711306526, 'iso': '2024-03-24T14:55:26-04:00'} - **IPQS: Domain:** advanced-ip-scanz.com - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-ip-scanz.com']

Name

advanced-ip-scanr.net

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1710451390, 'iso': '2024-03-14T17:23:10-04:00'} - **IPQS: Domain:** advanced-ip-scanr.net - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-ip-scanr.net']

Name

advanced-ip-scanr.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1710451383, 'iso': '2024-03-14T17:23:03-04:00'} - **IPQS: Domain:** advanced-ip-scanr.com - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-ip-scanr.com']

Name

advanced-ip-scanir.net

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 weeks ago', 'timestamp': 1711306341, 'iso': '2024-03-24T14:52:21-04:00'} - **IPQS: Domain:** advanced-ip-scanir.net - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-ip-scanir.net']

Name

advanced-ip-scanir.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 weeks ago', 'timestamp': 1711306250, 'iso': '2024-03-24T14:50:50-04:00'} - **IPQS: Domain:** advanced-ip-scanir.com - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-ip-scanir.com']

Name

advanced-ip-scanerr.net

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1710309761, 'iso': '2024-03-13T02:02:41-04:00'} - **IPQS: Domain:** advanced-ip-scanerr.net - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-ip-scanerr.net']

Name

advanced-ip-scanerr.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1710309754, 'iso': '2024-03-13T02:02:34-04:00'} - **IPQS: Domain:** advanced-ip-scanerr.com - **IPQS: IP Address:** 144.217.123.10

Pattern Type
stix
Pattern
[domain-name:value = 'advanced-ip-scanerr.com']
Name
advanced-ip-scanel.net
Description
- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1710309755, 'iso': '2024-03-13T02:02:35-04:00'} - **IPQS: Domain:** advanced-ip-scanel.net - **IPQS: IP Address:** 144.217.123.10
Pattern Type
stix
Pattern
[domain-name:value = 'advanced-ip-scanel.net']
Name
advanced-ip-scanel.com
Description
- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1709584218, 'iso': '2024-03-04T15:30:18-05:00'} - **IPQS: Domain:** advanced-ip-scanel.com - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-ip-scanel.com']

Name

advanced-ip-scaer.net

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1710451540, 'iso': '2024-03-14T17:25:40-04:00'} - **IPQS: Domain:** advanced-ip-scaer.net - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-ip-scaer.net']

Name

advanced-ip-scaer.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1710451534, 'iso': '2024-03-14T17:25:34-04:00'} - **IPQS: Domain:** advanced-ip-scaer.com - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-ip-scaer.com']

Name

advanced-ip-scaaner.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1710309755, 'iso': '2024-03-13T02:02:35-04:00'} - **IPQS: Domain:** advanced-ip-scaaner.com - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-ip-scaaner.com']

Name

advanced-ip-saaner.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 month ago', 'timestamp': 1709584205, 'iso': '2024-03-04T15:30:05-05:00'} - **IPQS: Domain:** advanced-ip-saaner.com - **IPQS: IP Address:** 144.217.123.10

Pattern Type

stix

Pattern

[domain-name:value = 'advanced-ip-saaner.com']

Name

advanceb-lp-scanner.com

Description

- **Unsafe:** False - **Server:** Bu - **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': 1705879661, 'iso': '2024-01-21T18:27:41-05:00'} - **IPQS: Domain:** advanceb-lp-scanner.com - **IPQS: IP Address:** 83.97.73.252

Pattern Type

stix

Pattern

[domain-name:value = 'advanceb-lp-scanner.com']

Name

advanceb-ip-scanner.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1705879383, 'iso': '2024-01-21T18:23:03-05:00'} - **IPQS: Domain:** advanceb-ip-scanner.com - **IPQS: IP Address:** 144.217.117.245

Pattern Type

stix

Pattern

[domain-name:value = 'advanceb-ip-scanner.com']

Name

advaanced-ip-scanner.net

Description

- **Unsafe:** False - **Server:** Bu - **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': 1705872738, 'iso': '2024-01-21T16:32:18-05:00'} - **IPQS: Domain:** advaanced-ip-scanner.net - **IPQS: IP Address:** 83.97.73.252

Pattern Type

stix

Pattern

[domain-name:value = 'advaanced-ip-scanner.net']

Name

advaanced-ip-scanner.com

Description

- **Unsafe:** False - **Server:** Bu - **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': 1705872447, 'iso': '2024-01-21T16:27:27-05:00'} - **IPQS: Domain:** advaanced-ip-scanner.com - **IPQS: IP Address:** 185.152.66.243

Pattern Type

stix

Pattern

[domain-name:value = 'advaanced-ip-scanner.com']

Name

bae2952c7d120d882746658e6d128556ae2498005072c4b7d7590a964b93c315

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = 'bae2952c7d120d882746658e6d128556ae2498005072c4b7d7590a964b93c315']

Name
b5162497bc2b9f1956d2145dd32daa5c99d6803544a0254a9090237628168d94

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = 'b5162497bc2b9f1956d2145dd32daa5c99d6803544a0254a9090237628168d94']

Name
7966ee1ae9042e7345a55aa98ddeb4f39133216438d67461c7ee39864292e015

Pattern Type
stix

Pattern
[file:hashes.'SHA-256' = '7966ee1ae9042e7345a55aa98ddeb4f39133216438d67461c7ee39864292e015']

Name
722a44f6a4718d853d640381e77d1b9815d6f1663603859ff758ded896860cba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'722a44f6a4718d853d640381e77d1b9815d6f1663603859ff758ded896860cba']

Name

6de01c65c994e0e428f5043cb496c8adca96ba18dfd2953335d1f3c9b97c60c5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'6de01c65c994e0e428f5043cb496c8adca96ba18dfd2953335d1f3c9b97c60c5']

Name

287a0a80a995f1e62b317cf5faa1db94af6ee9132b0f8483afbd6819aa903d31

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'287a0a80a995f1e62b317cf5faa1db94af6ee9132b0f8483afbd6819aa903d31']

Name
105e9a8d1014d2939e6b0ada3f24ad4bb6bd21f0155c284c90c7675a1de9d193
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '105e9a8d1014d2939e6b0ada3f24ad4bb6bd21f0155c284c90c7675a1de9d193']
Name
0263663c5375289fa2550d0cff3553dfc160a767e718a9c38efc0da3d7a4b626
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '0263663c5375289fa2550d0cff3553dfc160a767e718a9c38efc0da3d7a4b626']

Malware

Name
MadMxShell

Attack-Pattern

Name

T1046

ID

T1046

Description

Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system.(Citation: CISA AR21-126A FIVEHANDS May 2021) Within cloud environments, adversaries may attempt to discover services running on other cloud hosts. Additionally, if the cloud environment is connected to a on-premises environment, adversaries may be able to identify services running on non-cloud systems as well. Within macOS environments, adversaries may use the native Bonjour application to discover services running on other macOS hosts within a network. The Bonjour mDNSResponder daemon automatically registers and advertises a host's registered services on the network. For example, adversaries can use a mDNS query (such as `dns-sd -B _ssh._tcp .`) to find other systems broadcasting the ssh service.(Citation: apple doco bonjour description)(Citation: macOS APT Activity Bradley)

Name

T1132

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

T1574

ID

T1574

Description

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

Name

T1041

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Name

T1104

ID

T1104

Description

Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions. Use of multiple stages may obfuscate the command and control channel to make detection more difficult. Remote access tools will call back to the first-stage command and control server for instructions. The first stage may have automated capabilities to collect basic host information, update tools, and upload additional files. A second remote access tool (RAT) could be uploaded at that point to redirect the host to the second-stage command and control server. The second stage will likely be more fully featured and allow the adversary to interact with the system through a reverse shell and additional RAT features. The different stages will likely be hosted separately with no overlapping infrastructure. The loader may also have backup first-stage callbacks or [Fallback Channels](https://attack.mitre.org/techniques/T1008) in case the original first-stage communication path is discovered and blocked.

Name

T1102

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

T1083

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Name
T1070
ID
T1070
Description
Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary’s actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

Name
T1027
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

T1518

ID

T1518

Description

Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1518) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security measures are present or if the compromised system has a version of software that is vulnerable to [Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068).

Name

T1204

ID
T1204

Description
An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name
T1572

ID
T1572

Description
Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunneling involves explicitly encapsulating a protocol within another. This behavior may conceal malicious traffic by blending in with existing traffic

and/or provide an outer layer of encryption (similar to a VPN). Tunneling could also enable routing of network packets that would otherwise not reach their intended destination, such as SMB, RDP, or other traffic that would be filtered by network appliances or not routed over the Internet. There are various means to encapsulate a protocol within another protocol. For example, adversaries may perform SSH tunneling (also known as SSH port forwarding), which involves forwarding arbitrary data over an encrypted SSH tunnel. (Citation: SSH Tunneling) [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) may also be abused by adversaries during [Dynamic Resolution](https://attack.mitre.org/techniques/T1568). Known as DNS over HTTPS (DoH), queries to resolve C2 infrastructure may be encapsulated within encrypted HTTPS packets.(Citation: BleepingComp Godlua JUL19) Adversaries may also leverage [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) in conjunction with [Proxy](https://attack.mitre.org/techniques/T1090) and/or [Protocol Impersonation](https://attack.mitre.org/techniques/T1001/003) to further conceal C2 communications and infrastructure.

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.
Name

T1036

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

T1562

ID

T1562

Description

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators. Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out of a computer or stopping it from being shut down. These restrictions can further enable malicious operations as well as the continued propagation of incidents.(Citation: Emotet shutdown) Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

Name

T1140

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

T1005

ID

T1005

Description

Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration. Adversaries may do this using a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), such as [cmd](https://attack.mitre.org/software/S0106) as well as a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008), which have functionality to interact with the file system to gather information.(Citation: show_run_config_cmd_cisco) Adversaries may also use [Automated Collection](https://attack.mitre.org/techniques/T1119) on the local system.

Name

T1053

ID

T1053

Description

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

Name

T1082

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Name

T1071

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

T1583

ID

T1583

Description

Adversaries may buy, lease, or rent infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090), including from residential proxy services.(Citation: amnesty_nso_pegasus)(Citation: FBI Proxies Credential Stuffing)(Citation: Mandiant APT29 Microsoft 365 2022) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

Name

T1033

ID

T1033

Description

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

Domain-Name

Value
prtgscan.com
paesslers.com
networkscanip.com
networkipscan.com
managengins.net
managengins.com
managengines.net
managengines.com
manageeengines.net
manageeengines.com
litterbolo.com
keystore-explore.com
ipscannerprtg.com

angryipscaner.com

angryipscan.net

advvanced-ip-scanner.net

advvanced-ip-scanner.com

advansed-ip-scanner.net

advansed-ip-scanner.com

advanced-lp-scannel.com

advanced-lp-scanel.com

advanced-lp-saaner.com

advanced-lp-saanel.com

advanced-ip-scanz.net

advanced-ip-scanz.com

advanced-ip-scanr.net

advanced-ip-scanr.com

advanced-ip-scanir.net

advanced-ip-scanir.com

advanced-ip-scanerr.net

advanced-ip-scanerr.com

advanced-ip-scanel.net
advanced-ip-scanel.com
advanced-ip-scaer.net
advanced-ip-scaer.com
advanced-ip-scaaner.com
advanced-ip-saaner.com
advanceb-lp-scanner.com
advanceb-ip-scanner.com
advaanced-ip-scanner.net
advaanced-ip-scanner.com

StixFile

Value
bae2952c7d120d882746658e6d128556ae2498005072c4b7d7590a964b93c315
b5162497bc2b9f1956d2145dd32daa5c99d6803544a0254a9090237628168d94
7966ee1ae9042e7345a55aa98ddeb4f39133216438d67461c7ee39864292e015
722a44f6a4718d853d640381e77d1b9815d6f1663603859ff758ded896860cba
6de01c65c994e0e428f5043cb496c8adca96ba18dfd2953335d1f3c9b97c60c5
287a0a80a995f1e62b317cf5faa1db94af6ee9132b0f8483afbd6819aa903d31
105e9a8d1014d2939e6b0ada3f24ad4bb6bd21f0155c284c90c7675a1de9d193
0263663c5375289fa2550d0cff3553dfc160a767e718a9c38efc0da3d7a4b626

External References

- https://www.zscaler.com/blogs/security-research/malvertising-campaign-targeting-it-teams-madmxshell
- https://otx.alienvault.com/pulse/66211e47e85b0d25b55155c2