May 02 2024

NETMANAGEIT

Intelligence Report

Nearly 20% of Docker Hub Repositories Spread Malware & Phishing Scams

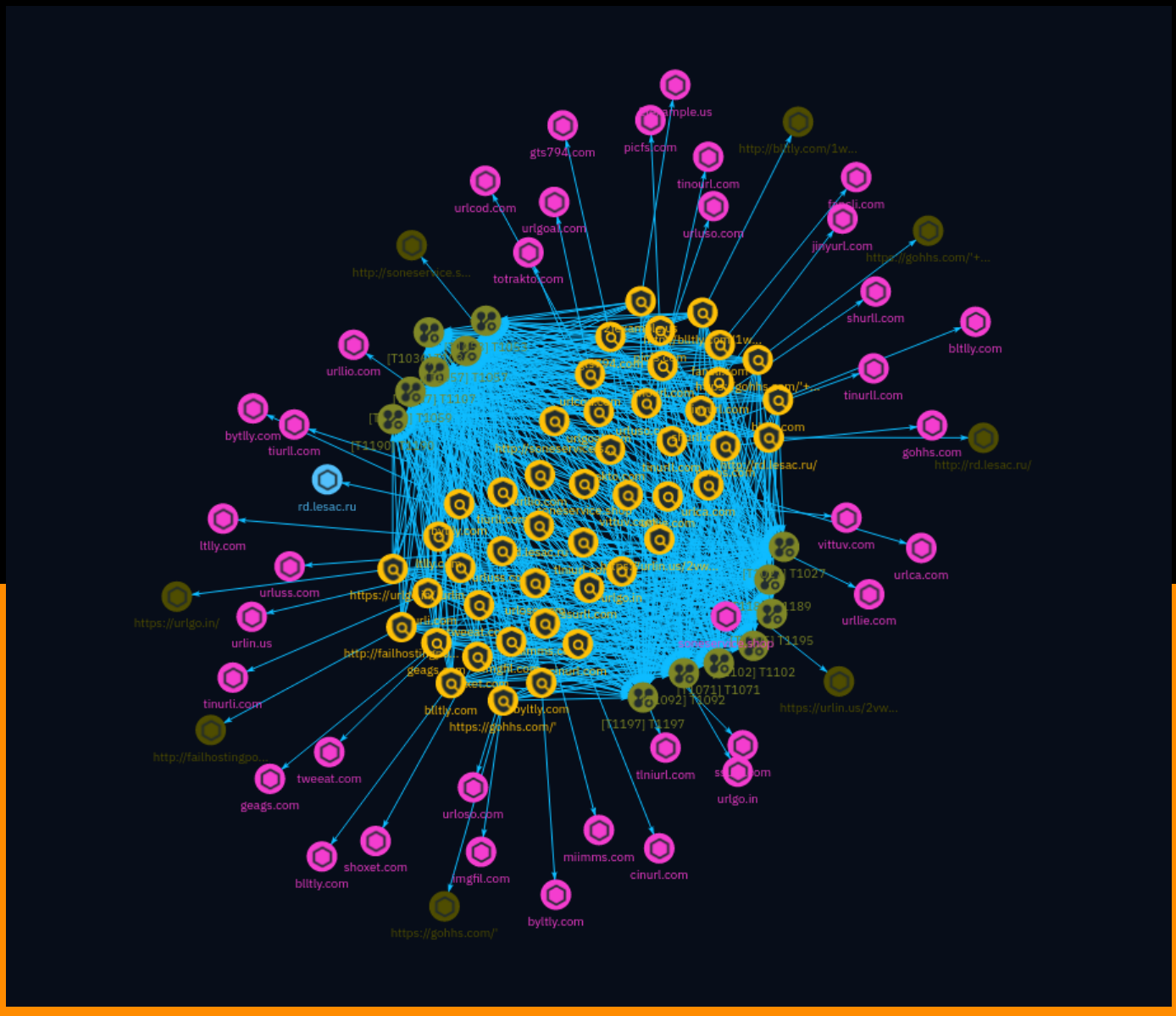

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report details an investigation by JFrog Security researchers on a coordinated attack on Docker Hub, where millions of malicious repositories were planted to spread malware and phishing scams. It analyzes three major malware campaigns, dubbed 'Downloader', 'eBook Phishing', and 'Website SEO', that exploited Docker Hub's repository documentation feature. The report provides insights into the attackers' tactics, techniques, and infrastructure, highlighting the challenges of moderating open platforms.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

rd.lesac.ru

Pattern Type

stix

Pattern

[hostname:value = 'rd.lesac.ru']

Name

vittuv.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': '1 year ago', 'timestamp': 1681117533, 'iso': '2023-04-10T05:05:33-04:00'} - **IPQS: Domain:** vittuv.com - **IPQS: IP Address:** 172.67.132.79

Pattern Type

stix

Pattern

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

Name

urluss.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 784790 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5 years ago', 'timestamp': 1561137345, 'iso': '2019-06-21T13:15:45-04:00'} - **IPQS: Domain:** urluss.com - **IPQS: IP Address:** 172.67.141.129

Pattern Type

stix

Pattern

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

Name

urluso.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': '3 years ago', 'timestamp': 1625741598, 'iso': '2021-07-08T06:53:18-04:00'} - **IPQS: Domain:** urluso.com - **IPQS: IP Address:** 172.67.165.252

Pattern Type

stix

Pattern

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

Name

urloso.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 755377 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & Internet - **Domain Age:** {'human': '3 years ago', 'timestamp': 1625741598, 'iso': '2021-07-08T06:53:18-04:00'} - **IPQS: Domain:** urloso.com - **IPQS: IP Address:** 172.67.187.254

Pattern Type

stix

Pattern

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

Name

urllio.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 985219 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '6 years ago', 'timestamp': 1535695304, 'iso': '2018-08-31T02:01:44-04:00'} - **IPQS: Domain:** urllio.com - **IPQS: IP Address:** 104.21.54.250

Pattern Type

stix

Pattern

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

Name

urllie.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 944349 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '6 years ago', 'timestamp': 1528141676, 'iso': '2018-06-04T15:47:56-04:00'} - **IPQS: Domain:** urllie.com - **IPQS: IP Address:** 172.67.142.174

Pattern Type

stix

Pattern

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

Name

urlin.us

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 936727 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '11 years ago', 'timestamp': 1371223152, 'iso': '2013-06-14T11:19:12-04:00'} - **IPQS: Domain:** urlin.us - **IPQS: IP Address:** 104.21.1.102

Pattern Type

stix

Pattern

[domain-name:value = 'urlin.us']

Name

urlgoal.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': '6 years ago', 'timestamp': 1525331773, 'iso': '2018-05-03T03:16:13-04:00'} - **IPQS: Domain:** urlgoal.com - **IPQS: IP Address:** 172.67.142.17

Pattern Type

stix

Pattern

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

Name

urlgo.in

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** ECommerce - **Domain Age:** {'human': '4 years ago', 'timestamp': 1587107943, 'iso': '2020-04-17T03:19:03-04:00'} - **IPQS: Domain:** urlgo.in - **IPQS: IP Address:** 172.67.157.94

Pattern Type

stix

Pattern

[domain-name:value = 'urlgo.in']

Name

urlcod.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:** Web Tracker - **Domain Age:** {'human': '1 year ago', 'timestamp': 1671736977, 'iso': '2022-12-22T14:22:57-05:00'} - **IPQS: Domain:** urlcod.com - **IPQS: IP Address:** 104.21.70.193

Pattern Type

stix

Pattern

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

Name

urlca.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:** Web Tracker - **Domain Age:** {'human': '4 years ago', 'timestamp': 1583492493, 'iso': '2020-03-06T06:01:33-05:00'} - **IPQS: Domain:** urlca.com - **IPQS: IP Address:** 172.67.139.236

Pattern Type

stix

Pattern

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

Name

tweeat.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': '4 years ago', 'timestamp': 1583492489, 'iso': '2020-03-06T06:01:29-05:00'} - **IPQS: Domain:** tweeat.com - **IPQS: IP Address:** 172.67.211.140

Pattern Type

stix

Pattern

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

Name

totrakto.com

Description

- **Unsafe:** True - **Server:** Apache - **Domain Rank:** 547341 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Downloads - **Domain Age:** {'human': '10 years ago', 'timestamp': 1390672659, 'iso': '2014-01-25T12:57:39-05:00'} - **IPQS: Domain:** totrakto.com - **IPQS: IP Address:** 5.149.248.111

Pattern Type

stix

Pattern

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

Name

tlniurl.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 752098 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1606034184, 'iso': '2020-11-22T03:36:24-05:00'} - **IPQS: Domain:** tlniurl.com - **IPQS: IP Address:** 172.67.202.128

Pattern Type

stix

Pattern

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

Name

tiurll.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 807767 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '3 years ago', 'timestamp': 1606034181, 'iso': '2020-11-22T03:36:21-05:00'} - **IPQS: Domain:** tiurll.com - **IPQS: IP Address:** 104.21.53.222

Pattern Type

stix

Pattern

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

Name

tinurll.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 966253 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 years ago', 'timestamp': 1582206500, 'iso': '2020-02-20T08:48:20-05:00'} - **IPQS: Domain:** tinurll.com - **IPQS: IP Address:** 172.67.153.66

Pattern Type

stix

Pattern

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

Name

tinurli.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 258934 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1619598957, 'iso': '2021-04-28T04:35:57-04:00'} - **IPQS: Domain:** tinurli.com - **IPQS: IP Address:** 104.21.71.200

Pattern Type

stix

Pattern

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

Name

tinourl.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': '4 years ago', 'timestamp': 1583492484, 'iso': '2020-03-06T06:01:24-05:00'} - **IPQS: Domain:** tinourl.com - **IPQS: IP Address:** 172.67.142.253

Pattern Type

stix

Pattern

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

Name

ssurll.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 917795 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5 years ago', 'timestamp': 1561137345, 'iso': '2019-06-21T13:15:45-04:00'} - **IPQS: Domain:** ssurll.com - **IPQS: IP Address:** 172.67.199.163

Pattern Type

stix

Pattern

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

Name

soneservice.shop

Description

- **Unsafe:** True - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'just now', 'timestamp': 1714594957, 'iso': '2024-05-01T16:22:37-04:00'} - **IPQS: Domain:** soneservice.shop - **IPQS: IP Address:** 172.67.164.12

Pattern Type

stix

Pattern

[domain-name:value = 'soneservice.shop']

Name

shurll.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 914395 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '7 years ago', 'timestamp': 1491497245, 'iso': '2017-04-06T12:47:25-04:00'} - **IPQS: Domain:** shurll.com - **IPQS: IP Address:** 104.21.83.92

Pattern Type

stix

Pattern

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

Name

shoxet.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': '4 years ago', 'timestamp': 1583492484, 'iso': '2020-03-06T06:01:24-05:00'} - **IPQS: Domain:** shoxet.com - **IPQS: IP Address:** 172.67.191.74

Pattern Type

stix

Pattern

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

Name

picfs.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 827807 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: True - **Adult:** False - **Category:** Computers & Internet - **Domain Age:** {'human': '4 years ago', 'timestamp': 1583492493, 'iso': '2020-03-06T06:01:33-05:00'} - **IPQS: Domain:** picfs.com - **IPQS: IP Address:** 172.67.147.6

Pattern Type

stix

Pattern

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

Name

miimms.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': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** miimms.com - **IPQS: IP Address:** 104.21.80.226

Pattern Type

stix

Pattern

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

Name

ltlly.com

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'just now', 'timestamp': 1714594935, 'iso': '2024-05-01T16:22:15-04:00'} - **IPQS: Domain:** ltlly.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

jinyurl.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': '6 years ago', 'timestamp': 1513864788, 'iso': '2017-12-21T08:59:48-05:00'} - **IPQS: Domain:** jinyurl.com - **IPQS: IP Address:** 172.67.158.212

Pattern Type

stix

Pattern

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

Name

imgfil.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 785598 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '4 years ago', 'timestamp': 1583492489, 'iso': '2020-03-06T06:01:29-05:00'} - **IPQS: Domain:** imgfil.com - **IPQS: IP Address:** 104.21.54.174

Pattern Type

stix

Pattern

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

Name

gts794.com

Description

- **Unsafe:** True - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 year ago', 'timestamp': 1681247309, 'iso': '2023-04-11T17:08:29-04:00'} - **IPQS: Domain:** gts794.com - **IPQS: IP Address:** 172.67.136.150

Pattern Type

stix

Pattern

[domain-name:value = 'gts794.com']

Name

gohhs.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:** Education - **Domain Age:** {'human': '1 year ago', 'timestamp': 1681117537, 'iso': '2023-04-10T05:05:37-04:00'} - **IPQS: Domain:** gohhs.com - **IPQS: IP Address:** 172.67.170.67

Pattern Type

stix

Pattern

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

Name

geags.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 486921 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 years ago', 'timestamp': 1583492497, 'iso': '2020-03-06T06:01:37-05:00'} - **IPQS: Domain:** geags.com - **IPQS: IP Address:** 172.67.157.133

Pattern Type

stix

Pattern

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

Name

fancli.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 466681 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 years ago', 'timestamp': 1583492493, 'iso': '2020-03-06T06:01:33-05:00'} - **IPQS: Domain:** fancli.com - **IPQS: IP Address:** 104.21.90.36

Pattern Type

stix

Pattern

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

Name

cinurl.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 820050 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 years ago', 'timestamp': 1578903794, 'iso': '2020-01-13T03:23:14-05:00'} - **IPQS: Domain:** cinurl.com - **IPQS: IP Address:** 172.67.182.253

Pattern Type

stix

Pattern

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

Name

bytlly.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 572270 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 years ago', 'timestamp': 1583492484, 'iso': '2020-03-06T06:01:24-05:00'} - **IPQS: Domain:** bytlly.com - **IPQS: IP Address:** 172.67.159.241

Pattern Type

stix

Pattern

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

Name

bltlly.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 839146 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 years ago', 'timestamp': 1578903794, 'iso': '2020-01-13T03:23:14-05:00'} - **IPQS: Domain:** bltlly.com - **IPQS: IP Address:** 172.67.175.181

Pattern Type

stix

Pattern

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

Name

blltly.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 569125 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1606034184, 'iso': '2020-11-22T03:36:24-05:00'} - **IPQS: Domain:** blltly.com - **IPQS: IP Address:** 104.21.18.30

Pattern Type

stix

Pattern

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

Name

2fexample.us

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': 'just now', 'timestamp': 1714594896, 'iso': '2024-05-01T16:21:36-04:00'} - **IPQS: Domain:** 2fexample.us - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = '2fexample.us']

Name

https://urlin.us/2vwNSW

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 years ago', 'timestamp': 1371223152, 'iso': '2013-06-14T11:19:12-04:00'} - **IPQS: Domain:** soneremonasez.shop - **IPQS: IP Address:** 172.67.180.145

Pattern Type

stix

Pattern

[url:value = 'https://urlin.us/2vwNSW']

Name

https://urlgo.in/

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** ECommerce - **Domain Age:** {'human': '4 years ago', 'timestamp': 1587107943, 'iso': '2020-04-17T03:19:03-04:00'} - **IPQS: Domain:** urlgo.in - **IPQS: IP Address:** 172.67.157.94

Pattern Type

stix

Pattern

[url:value = 'https://urlgo.in/']

Name

https://gohhs.com/'+c

Pattern Type

stix

Pattern

[url:value = 'https://gohhs.com/\'+c']

Name

https://gohhs.com/'

Pattern Type

stix

Pattern

[url:value = 'https://gohhs.com/\'']

Name

http://soneservice.shop/new/net_api

Description

- **Unsafe:** True - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** soneservice.shop - **IPQS: IP Address:** 172.67.164.12

Pattern Type

stix

Pattern

[url:value = 'http://soneservice.shop/new/net_api']

Name

http://rd.lesac.ru/

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 years ago', 'timestamp': 1598896510, 'iso': '2020-08-31T13:55:10-04:00'} - **IPQS: Domain:** rd.lesac.ru - **IPQS: IP Address:** 161.97.111.73

Pattern Type

stix

Pattern

[url:value = 'http://rd.lesac.ru/']

Name

http://failhostingpolp.ru/9ebeb1ba574fb8e786200c62159e77d15UtXt7/x60VKb8hl1YelOv1c5X1c0BuVzmFZ8-teb-LRH8w

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1707318096, 'iso': '2024-02-07T10:01:36-05:00'} - **IPQS: Domain:** failhostingpolp.ru - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://failhostingpolp.ru/9ebeb1ba574fb8e786200c62159e77d15UtXt7/x60VKb8hl1YelOv1c5X1c0BuVzmFZ8-teb-LRH8w']

Name

http://blltly.com/1w1w1

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 years ago', 'timestamp': 1606034184, 'iso': '2020-11-22T03:36:24-05:00'} - **IPQS: Domain:** soneremonasez.shop - **IPQS: IP Address:** 104.21.67.200

Pattern Type

stix

Pattern

[url:value = 'http://blltly.com/1w1w1']

Name

byltly.com

Description

- **Unsafe:** True - **Server:** cloudflare - **Domain Rank:** 608661 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 years ago', 'timestamp': 1619598957, 'iso': '2021-04-28T04:35:57-04:00'} - **IPQS: Domain:** byltly.com - **IPQS: IP Address:** 172.67.220.234

Pattern Type

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

Attack-Pattern

Name
T1107
ID
T1107
Name
T1189
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

T1197

ID

T1197

Description

Adversaries may abuse BITS jobs to persistently execute code and perform various background tasks. Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM).(Citation: Microsoft COM) (Citation: Microsoft BITS) BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth)

without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations. The interface to create and manage BITS jobs is accessible through [PowerShell](https://attack.mitre.org/techniques/T1059/001) and the [BITSAdmin](https://attack.mitre.org/software/S0190) tool. (Citation: Microsoft BITS)(Citation: Microsoft BITSAdmin) Adversaries may abuse BITS to download (e.g. [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105)), execute, and even clean up after running malicious code (e.g. [Indicator Removal](https://attack.mitre.org/techniques/T1070)). BITS tasks are self-contained in the BITS job database, without new files or registry modifications, and often permitted by host firewalls.(Citation: CTU BITS Malware June 2016)(Citation: Mondok Windows PiggyBack BITS May 2007)(Citation: Symantec BITS May 2007) BITS enabled execution may also enable persistence by creating long-standing jobs (the default maximum lifetime is 90 days and extendable) or invoking an arbitrary program when a job completes or errors (including after system reboots). (Citation: PaloAlto UBoatRAT Nov 2017)(Citation: CTU BITS Malware June 2016) BITS upload functionalities can also be used to perform [Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048).(Citation: CTU BITS Malware June 2016)

Name

T1057

ID

T1057

Description

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Administrator or otherwise elevated access may provide better process details. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via `/proc`. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008)

commands such as `show processes` can be used to display current running processes. (Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

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

T1059

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

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

T1092

ID

T1092

Description

Adversaries can perform command and control between compromised hosts on potentially disconnected networks using removable media to transfer commands from system to system.(Citation: ESET Sednit USBStealer 2014) Both systems would need to be compromised, with the likelihood that an Internet-connected system was compromised first and the second through lateral movement by [Replication Through Removable Media](https://attack.mitre.org/techniques/T1091). Commands and files would be relayed from the disconnected system to the Internet-connected system to which the adversary has direct access.

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)

Name

T1195

ID

T1195

Description

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Name

T1190

ID

T1190

Description

Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211) or [Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

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

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.(Citation: Mandiant APT29 Eye Spy Email Nov 22)

Hostname

Value
rd.lesac.ru

Domain-Name

Value
vittuv.com
urluss.com
urluso.com
urloso.com
urllio.com
urllie.com
urlin.us
urlgoal.com
urlgo.in
urlcod.com
urlca.com
tweeat.com
totrakto.com

tlniurl.com

tiurll.com

tinurll.com

tinurli.com

tinourl.com

ssurll.com

soneservice.shop

shurll.com

shoxet.com

picfs.com

miimms.com

ltlly.com

jinyurl.com

imgfil.com

gts794.com

gohhs.com

geags.com

fancli.com

cinurl.com

bytlly.com

bltlly.com

blltly.com

2fexample.us

byltly.com

Url

Value
https://urlin.us/2vwNSW
https://urlgo.in/
https://gohhs.com/'+c
https://gohhs.com/'
http://soneservice.shop/new/net_api
http://rd.lesac.ru/
http://failhostingpolp.ru/9ebeb1ba574fb8e786200c62159e77d15UtXt7/x60VKb8hl1YelOv1c5X1c0BuVzmFZ8-teb-LRH8w
http://blltly.com/1w1w1

External References

- https://jfrog.com/blog/attacks-on-docker-with-millions-of-malicious-repositories-spread-malware-and-phishing-scams/
- https://otx.alienvault.com/pulse/66329f2e6378bd16250f5a4e