Jul 28 2023

NETMANAGEIT

Intelligence Report

Ransomware Delivery URLs: Top Campaigns and Trends

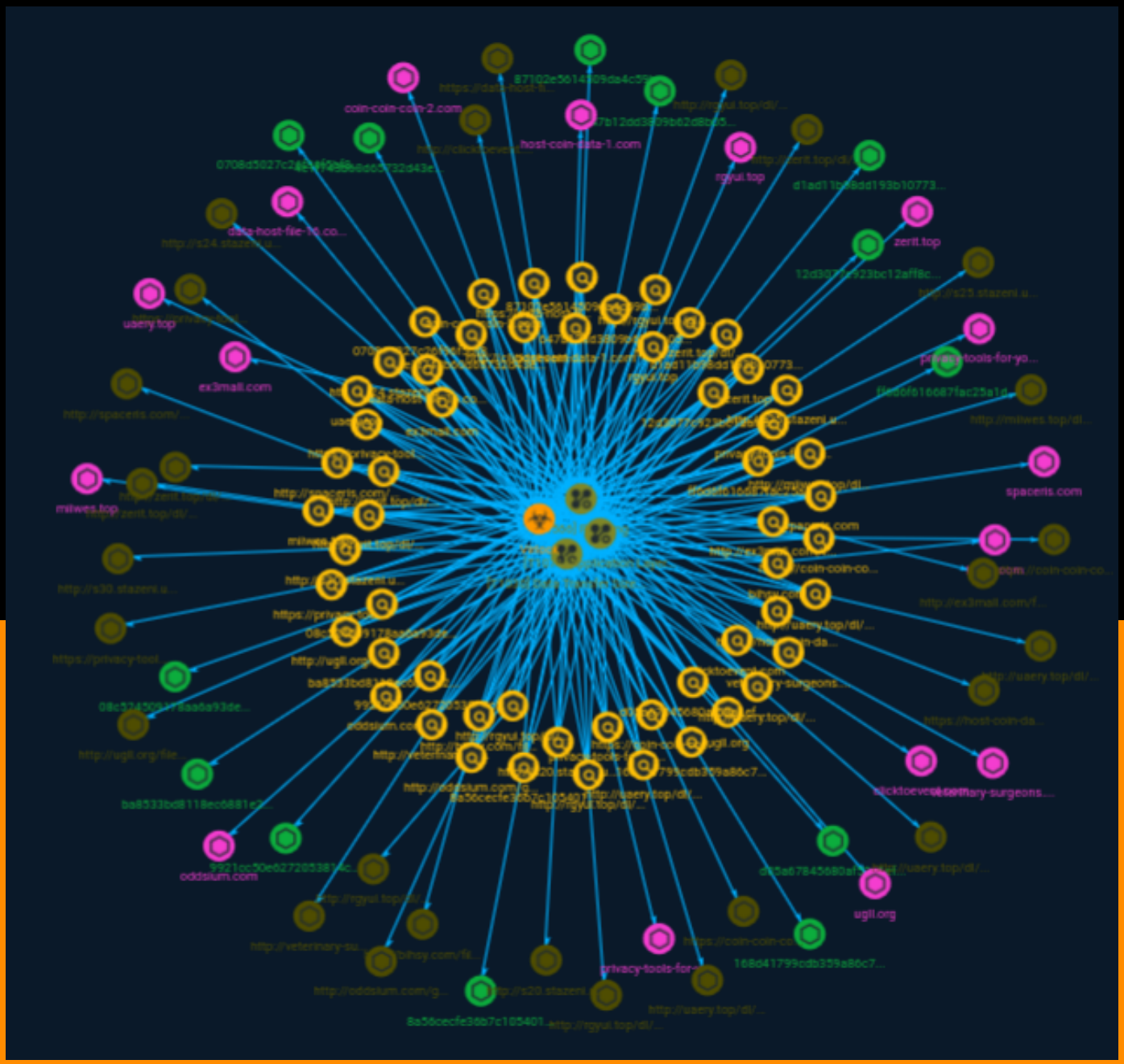

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Ransomware is increasingly being delivered via URLs, as well as emails and third-party apps.

Confidence

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

15 / 100

Indicator

Name
https://privacy-tools-for-you-780.com/downloads/toolspab3.exe
Pattern Type
stix
Pattern
[url:value = 'https://privacy-tools-for-you-780.com/downloads/toolspab3.exe']
Name
http://spaceris.com/files/1/build3.exe
Pattern Type
stix
Pattern
[url:value = 'http://spaceris.com/files/1/build3.exe']
Name
ff6d6f616687fac25a1d77e52024838239e9a3bbb7b79559b0439a968ac384fe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ff6d6f616687fac25a1d77e52024838239e9a3bbb7b79559b0439a968ac384fe']

Name

http://s30.stazeni.ua.rs/download/p1rcwy69oe09csyefqj4j9fmhmx1hamq

Pattern Type

stix

Pattern

[url:value = 'http://s30.stazeni.ua.rs/download/p1rcwy69oe09csyefqj4j9fmhmx1hamq']

Name

miiwes.top

Pattern Type

stix

Pattern

[domain-name:value = 'miiwes.top']

Name

http://ugll.org/files/1/build3.exe

Pattern Type

stix

Pattern

[url:value = 'http://ugll.org/files/1/build3.exe']

Name

168d41799cdb359a86c7e28e4b3eee3494270ec6e2884452dd61134b627b1c68

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '168d41799cdb359a86c7e28e4b3eee3494270ec6e2884452dd61134b627b1c68']

Name

privacy-tools-for-you-780.com

Pattern Type

stix

Pattern

[domain-name:value = 'privacy-tools-for-you-780.com']

Name

https://host-coin-data-1.com/downloads/toolspab1.exe

Pattern Type

stix

Pattern

[url:value = 'https://host-coin-data-1.com/downloads/toolspab1.exe']

Name

08c524509178aa6a93de9861790804266289fbed704af269f3c4ddde75518b15

Description

Ransom:Win32/Sorikrypt.A

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '08c524509178aa6a93de9861790804266289fbed704af269f3c4ddde75518b15']

Name

http://zerit.top/dl/build2.exe

Pattern Type

stix

Pattern

[url:value = 'http://zerit.top/dl/build2.exe']

Name

host-coin-data-1.com

Pattern Type

stix

Pattern

[domain-name:value = 'host-coin-data-1.com']

Name

http://clicktoevent.com/g76dbf?lrebib=kvqqhaohs

Pattern Type

stix

Pattern

[url:value = 'http://clicktoevent.com/g76dbf?lrebib=kvqqhaohs']

Name

http://s25.stazeni.ua.rs/download/ill2a7r2hsyufadaluvhv71xuuhubneg

Pattern Type

stix

Pattern

[url:value = 'http://s25.stazeni.ua.rs/download/ill2a7r2hsyufadaluvhv71xuuhubneg']

Name

privacy-tools-for-you-453.com

Pattern Type

stix

Pattern

[domain-name:value = 'privacy-tools-for-you-453.com']

Name

https://data-host-file-16.com/downloads/toolspab2.exe

Pattern Type

stix

Pattern

[url:value = 'https://data-host-file-16.com/downloads/toolspab2.exe']

Name

https://coin-coin-coin-2.com/downloads/toolspab2.exe

Pattern Type

stix

Pattern

[url:value = 'https://coin-coin-coin-2.com/downloads/toolspab2.exe']

Name

oddsium.com

Pattern Type

stix

Pattern

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

Name

ex3mall.com

Pattern Type

stix

Pattern

[domain-name:value = 'ex3mall.com']

Name

8a56cecfe36b7c105401fd246f8f3ba97bdc4d1db776eaa4991fcedf8aaaaa52

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8a56cecfe36b7c105401fd246f8f3ba97bdc4d1db776eaa4991fcedf8aaaaa52']

Name

data-host-file-16.com

Pattern Type

stix

Pattern

[domain-name:value = 'data-host-file-16.com']

Name

veterinary-surgeons.net

Pattern Type

stix

Pattern

[domain-name:value = 'veterinary-surgeons.net']

Name
bihsy.com
Pattern Type
stix
Pattern
[domain-name:value = 'bihsy.com']
Name
http://rgyui.top/dl/buildz.exe
Pattern Type
stix
Pattern
[url:value = 'http://rgyui.top/dl/buildz.exe']
Name
http://s20.stazeni.ua.rs/download/z2guqagslno4pb06hnpuy1ocf7wstfxf
Pattern Type
stix
Pattern
[url:value = 'http://s20.stazeni.ua.rs/download/z2guqagslno4pb06hnpuy1ocf7wstfxf']

Name

647b12dd3809b62d8b051ec643a1c5d26c32ec3397266c76e6f58e3894e39c4b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '647b12dd3809b62d8b051ec643a1c5d26c32ec3397266c76e6f58e3894e39c4b']

Name

http://miiwes.top/dl/buildz.exe

Pattern Type

stix

Pattern

[url:value = 'http://miiwes.top/dl/buildz.exe']

Name

ba8533bd8118ec6881e25e4af2e2101996b4a9aef3f1f1931423bff03da0ace5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ba8533bd8118ec6881e25e4af2e2101996b4a9aef3f1f1931423bff03da0ace5']

Name

http://zerit.top/dl/build.exe

Pattern Type

stix

Pattern

[url:value = 'http://zerit.top/dl/build.exe']

Name

clicktoevent.com

Pattern Type

stix

Pattern

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

Name

http://ex3mall.com/files/1/build3.exe

Pattern Type

stix

Pattern

[url:value = 'http://ex3mall.com/files/1/build3.exe']

Name

rgyui.top

Pattern Type

stix

Pattern

[domain-name:value = 'rgyui.top']

Name

http://veterinary-surgeons.net/g76dbf?grpvldcmq=pnstptslwh

Pattern Type

stix

Pattern

[url:value = 'http://veterinary-surgeons.net/g76dbf?grpvldcmq=pnstptslwh']

Name

0708d5027c26f96f5bf81b373348346149511a4b9f11391a979159185371bcc5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0708d5027c26f96f5bf81b373348346149511a4b9f11391a979159185371bcc5']

Name

zerit.top

Pattern Type

stix

Pattern

[domain-name:value = 'zerit.top']

Name

http://rgyui.top/dl/build2.exe

Pattern Type

stix

Pattern

[url:value = 'http://rgyui.top/dl/build2.exe']

Name

12d3077c923bc12aff8c2f3d04f96db427d841b185fa84a0a151d882cb3f08f8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '12d3077c923bc12aff8c2f3d04f96db427d841b185fa84a0a151d882cb3f08f8']

Name

http://uaery.top/dl/build2.exe

Description

Simple indicator of observable {http://uaery.top/dl/build2.exe}

Pattern Type

stix

Pattern

[url:value = 'http://uaery.top/dl/build2.exe']

Name

https://privacy-tools-for-you-453.com/downloads/toolspab4.exe

Pattern Type

stix

Pattern

[url:value = 'https://privacy-tools-for-you-453.com/downloads/toolspab4.exe']

Name
https://coin-coin-coin-2.com/downloads/toolspab4.exe
Pattern Type
stix
Pattern
[url:value = 'https://coin-coin-coin-2.com/downloads/toolspab4.exe']
Name
9921cc50e6272053814c7fe2ab5ae566a9deaebc9c0412c8b518313eee65d9d9
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '9921cc50e6272053814c7fe2ab5ae566a9deaebc9c0412c8b518313eee65d9d9']
Name
coin-coin-coin-2.com
Pattern Type
stix
Pattern

[domain-name:value = 'coin-coin-coin-2.com']

Name

ugll.org

Pattern Type

stix

Pattern

[domain-name:value = 'ugll.org']

Name

http://bihsy.com/files/1/build3.exe

Description

Simple indicator of observable {http://bihsy.com/files/1/build3.exe}

Pattern Type

stix

Pattern

[url:value = 'http://bihsy.com/files/1/build3.exe']

Name

87102e5614509da4c59b134861130708f239b68d1e062d08d1e71464c8041326

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '87102e5614509da4c59b134861130708f239b68d1e062d08d1e71464c8041326']

Name

d05a67845680af53a1efe0d852aa7ab85ad97e76cc8aaa62b1aad70288665026

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd05a67845680af53a1efe0d852aa7ab85ad97e76cc8aaa62b1aad70288665026']

Name

http://zerit.top/dl/buildz.exe

Pattern Type

stix

Pattern

[url:value = 'http://zerit.top/dl/buildz.exe']

Name

http://uaery.top/dl/build.exe

Description

Simple indicator of observable {http://uaery.top/dl/build.exe}

Pattern Type

stix

Pattern

[url:value = 'http://uaery.top/dl/build.exe']

Name

http://oddsium.com/g76dbf

Pattern Type

stix

Pattern

[url:value = 'http://oddsium.com/g76dbf']

Name

4e1f743b60d65732d43e6a8c064016369a2cb6d03e81e04e114ed6a31297a2a7

Description

Win32:BotX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4e1f743b60d65732d43e6a8c064016369a2cb6d03e81e04e114ed6a31297a2a7']

Name

http://uaery.top/dl/buildz.exe

Description

Simple indicator of observable {http://uaery.top/dl/buildz.exe}

Pattern Type

stix

Pattern

[url:value = 'http://uaery.top/dl/buildz.exe']

Name

http://s24.stazeni.ua.rs/download/5pg08rc9pxvy743ncrn30d2zylf2l12a

Pattern Type

stix

Pattern

[url:value = 'http://s24.stazeni.ua.rs/download/5pg08rc9pxvy743ncrn30d2zylf2l12a']

Name

d1ad11b98dd193b107731349a596558c6505e51e9b2e7195521e81b20482948d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd1ad11b98dd193b107731349a596558c6505e51e9b2e7195521e81b20482948d']

Name

http://rgyui.top/dl/build.exe

Pattern Type

stix

Pattern

[url:value = 'http://rgyui.top/dl/build.exe']

Name

uaery.top

Description

Win32/Vodkagats

Pattern Type

stix

Pattern
[domain-name:value = 'uaery.top']
Name
spaceris.com
Pattern Type
stix
Pattern
[domain-name:value = 'spaceris.com']

Malware

Name
Virlock

Attack-Pattern

Name
Data Transfer Size Limits
ID
T1030
Description
An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer threshold alerts.
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

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.

Domain-Name

Value
bihsy.com
ugll.org
zerit.top
privacy-tools-for-you-453.com
rgyui.top
clicktoevent.com
veterinary-surgeons.net
miiwes.top
data-host-file-16.com
oddsium.com
coin-coin-coin-2.com
privacy-tools-for-you-780.com
ex3mall.com

host-coin-data-1.com

uaery.top

spaceris.com

StixFile

Value
08c524509178aa6a93de9861790804266289fbed704af269f3c4ddde75518b15
d05a67845680af53a1efe0d852aa7ab85ad97e76cc8aaa62b1aad70288665026
12d3077c923bc12aff8c2f3d04f96db427d841b185fa84a0a151d882cb3f08f8
9921cc50e6272053814c7fe2ab5ae566a9deaebc9c0412c8b518313eee65d9d9
0708d5027c26f96f5bf81b373348346149511a4b9f11391a979159185371bcc5
8a56cecfe36b7c105401fd246f8f3ba97bdc4d1db776eaa4991fcedf8aaaaa52
4e1f743b60d65732d43e6a8c064016369a2cb6d03e81e04e114ed6a31297a2a7
647b12dd3809b62d8b051ec643a1c5d26c32ec3397266c76e6f58e3894e39c4b
ba8533bd8118ec6881e25e4af2e2101996b4a9aef3f1f1931423bff03da0ace5
d1ad11b98dd193b107731349a596558c6505e51e9b2e7195521e81b20482948d
168d41799cdb359a86c7e28e4b3eee3494270ec6e2884452dd61134b627b1c68
87102e5614509da4c59b134861130708f239b68d1e062d08d1e71464c8041326
ff6d6f616687fac25a1d77e52024838239e9a3bbb7b79559b0439a968ac384fe

Url

Value
http://rgyui.top/dl/build.exe
http://zerit.top/dl/build2.exe
https://host-coin-data-1.com/downloads/toolspab1.exe
https://coin-coin-coin-2.com/downloads/toolspab4.exe
https://coin-coin-coin-2.com/downloads/toolspab2.exe
http://zerit.top/dl/build.exe
http://s30.stazeni.ua.rs/download/p1rcwy69oe09csyefqj4j9fmhmx1hamq
http://clicktoevent.com/g76dbf?lrebib=kvqqhaohs
http://s20.stazeni.ua.rs/download/z2guqagslno4pb06hnpuy1ocf7wstfxf
http://rgyui.top/dl/buildz.exe
http://bihsy.com/files/1/build3.exe
https://privacy-tools-for-you-780.com/downloads/toolspab3.exe
http://rgyui.top/dl/build2.exe

http://uaery.top/dl/build.exe

http://spaceris.com/files/1/build3.exe

http://miiwes.top/dl/buildz.exe

http://oddsium.com/g76dbf

http://s24.stazeni.ua.rs/download/5pg08rc9pxvy743ncrn30d2zylf2l12a

http://zerit.top/dl/buildz.exe

http://ugll.org/files/1/build3.exe

https://data-host-file-16.com/downloads/toolspab2.exe

http://uaery.top/dl/build2.exe

https://privacy-tools-for-you-453.com/downloads/toolspab4.exe

http://ex3mall.com/files/1/build3.exe

http://veterinary-surgeons.net/g76dbf?grpvldcmq=pnstptslwh

http://s25.stazeni.ua.rs/download/ill2a7r2hsyufadaluvhv71xuuhubneg

http://uaery.top/dl/buildz.exe

External References

- https://otx.alienvault.com/pulse/64c3d2ce74e2835a3709d909
- https://unit42.paloaltonetworks.com/url-delivered-ransomware/