Dec 19 2023

NETMANAGEIT

Intelligence Report

Malvertisers zoom in on cryptocurrencies and initial access

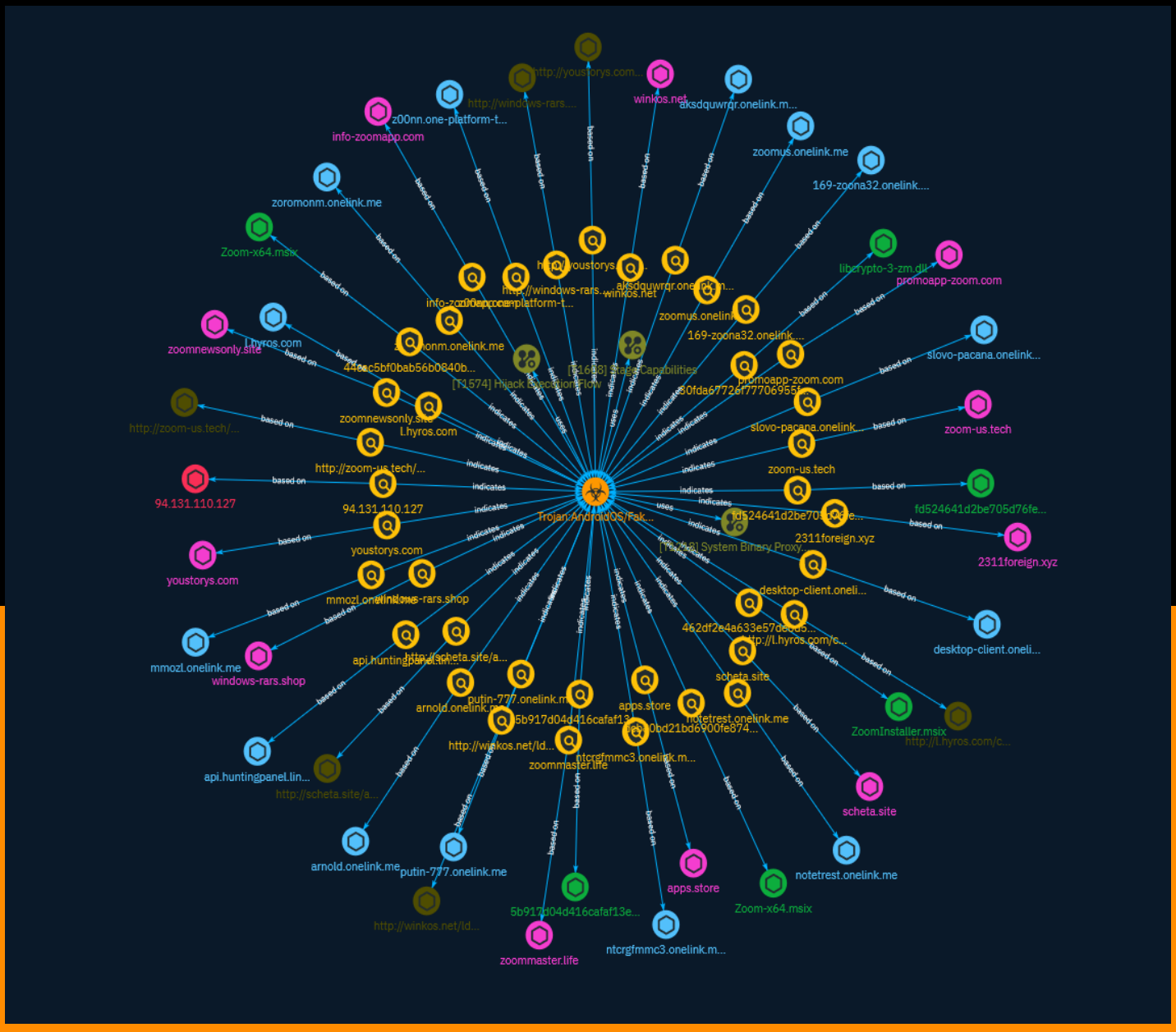

Table of contents

Overview

Entities

Observables

External References

Overview

Description

During the past month, Malwarebytes have observed an increase in the number of malicious ads on Google searches for “Zoom”, the popular piece of video conferencing software. Threat actors have been alternating between different keywords for software downloads such as “Advanced IP Scanner” or “WinSCP” normally geared towards IT administrators.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Hijack Execution Flow
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
System Binary Proxy Execution
ID
T1218

Description

Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries. Binaries used in this technique are often Microsoft-signed files, indicating that they have been either downloaded from Microsoft or are already native in the operating system.(Citation: LOLBAS Project) Binaries signed with trusted digital certificates can typically execute on Windows systems protected by digital signature validation. Several Microsoft signed binaries that are default on Windows installations can be used to proxy execution of other files or commands. Similarly, on Linux systems adversaries may abuse trusted binaries such as `split` to proxy execution of malicious commands.(Citation: split man page)(Citation: GTFO split)

Name

Stage Capabilities

ID

T1608

Description

Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed ([Develop Capabilities](https://attack.mitre.org/techniques/T1587)) or obtained ([Obtain Capabilities](https://attack.mitre.org/techniques/T1588)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.(Citation: Volexity Ocean Lotus November 2020)(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing) Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to): * Staging web resources necessary to conduct [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) when a user browses to a site.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015)(Citation: ATT ScanBox) * Staging web resources for a link target to be used with spearphishing.(Citation:

Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) * Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105).(Citation: Volexity Ocean Lotus November 2020) * Installing a previously acquired SSL/TLS certificate to use to encrypt command and control traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)).(Citation: DigiCert Install SSL Cert)

Indicator

Name
http://windows-rars.shop/bootstrap/Zoom-x64.msix
Pattern Type
stix
Pattern
[url:value = 'http://windows-rars.shop/bootstrap/Zoom-x64.msix']
Name
putin-777.onelink.me
Pattern Type
stix
Pattern
[hostname:value = 'putin-777.onelink.me']
Name
notetrest.onelink.me

Pattern Type
stix
Pattern
[hostname:value = 'notetrest.onelink.me']
Name
zoomus.onelink.me
Pattern Type
stix
Pattern
[hostname:value = 'zoomus.onelink.me']
Name
desktop-client.onelink.me
Pattern Type
stix
Pattern
[hostname:value = 'desktop-client.onelink.me']
Name
5b917d04d416cafaf13ed51c40b58dc8b4413483ea3f5406b8348038125cad0b

Description

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

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5b917d04d416cafaf13ed51c40b58dc8b4413483ea3f5406b8348038125cad0b']

Name

zoromonm.onelink.me

Pattern Type

stix

Pattern

[hostname:value = 'zoromonm.onelink.me']

Name

slovo-pacana.onelink.me

Pattern Type

stix

Pattern

[hostname:value = 'slovo-pacana.onelink.me']

Name

z00nn.one-platform-to-connect.group

Pattern Type

stix

Pattern

[hostname:value = 'z00nn.one-platform-to-connect.group']

Name

http://youstorys.com/fonts/Zoom-x64.msix

Pattern Type

stix

Pattern

[url:value = 'http://youstorys.com/fonts/Zoom-x64.msix']

Name

462df2e4a633e57de0d5148060543576d7c1165bf90e6aec4183f430d8925a1c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '462df2e4a633e57de0d5148060543576d7c1165bf90e6aec4183f430d8925a1c']

Name

http://scheta.site/apps.store/ZoomInstaller.msix

Description

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

Pattern Type

stix

Pattern

[url:value = 'http://scheta.site/apps.store/ZoomInstaller.msix']

Name

arnold.onelink.me

Pattern Type

stix

Pattern

[hostname:value = 'arnold.onelink.me']

Name

mmozl.onelink.me

Pattern Type
stix
Pattern
[hostname:value = 'mmozl.onelink.me']
Name
windows-rars.shop
Pattern Type
stix
Pattern
[domain-name:value = 'windows-rars.shop']
Name
zoom-us.tech
Pattern Type
stix
Pattern
[domain-name:value = 'zoom-us.tech']
Name
44cac5bf0bab56b0840bd1c7b95f9c7f5078ff417705eeaaf5ea5a2167a81dd5

Description

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

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '44cac5bf0bab56b0840bd1c7b95f9c7f5078ff417705eeaaf5ea5a2167a81dd5']

Name

zoommaster.life

Pattern Type

stix

Pattern

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

Name

l.hyros.com

Pattern Type

stix

Pattern

[hostname:value = 'l.hyros.com']

Name

winkos.net

Pattern Type

stix

Pattern

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

Name

ntcrgfmmc3.onelink.me

Pattern Type

stix

Pattern

[hostname:value = 'ntcrgfmmc3.onelink.me']

Name

youstorys.com

Pattern Type

stix

Pattern

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

Name

zoomnewsonly.site

Pattern Type

stix

Pattern

[domain-name:value = 'zoomnewsonly.site']

Name

http://l.hyros.com/c8KqPHYKdt

Pattern Type

stix

Pattern

[url:value = 'http://l.hyros.com/c8KqPHYKdt']

Name

http://zoom-us.tech/ZoomInstaller.zip

Pattern Type

stix

Pattern

[url:value = 'http://zoom-us.tech/ZoomInstaller.zip']

Name

2311foreign.xyz

Pattern Type

stix

Pattern

[domain-name:value = '2311foreign.xyz']

Name

apps.store

Pattern Type

stix

Pattern

[domain-name:value = 'apps.store']

Name

aksdquwrqr.onelink.me

Pattern Type

stix

Pattern

[hostname:value = 'aksdquwrqr.onelink.me']

Name

fd524641d2be705d76feb0453374c5b2ad9582ced4f00bb3722b735401da2762

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fd524641d2be705d76feb0453374c5b2ad9582ced4f00bb3722b735401da2762']

Name

94.131.110.127

Description

CC=DE ASN=AS44477 Stark Industries Solutions Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '94.131.110.127']

Name

promoapp-zoom.com

Pattern Type
stix
Pattern
[domain-name:value = 'promoapp-zoom.com']
Name
scheta.site
Description
Created by VirusTotal connector as the positive count was >= 10
Pattern Type
stix
Pattern
[domain-name:value = 'scheta.site']
Name
info-zoomapp.com
Pattern Type
stix
Pattern
[domain-name:value = 'info-zoomapp.com']

Name

30fda67726f77706955f6b52b202452e91d5ff132783854eec63e809061a4b5c

Description

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

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '30fda67726f77706955f6b52b202452e91d5ff132783854eec63e809061a4b5c']

Name

http://winkos.net/ld/zm.tar.gpg

Pattern Type

stix

Pattern

[url:value = 'http://winkos.net/ld/zm.tar.gpg']

Name

169-zoona32.onelink.me

Pattern Type

stix

Pattern

[hostname:value = '169-zoona32.onelink.me']

Name

dcb80bd21bd6900fe87423d3fb0c49d8f140d5cf5d81b662cd74c22fca622893

Description

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

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dcb80bd21bd6900fe87423d3fb0c49d8f140d5cf5d81b662cd74c22fca622893']

Name

api.huntingpanel.link

Pattern Type

stix

Pattern

[hostname:value = 'api.huntingpanel.link']

Malware

Name
Trojan:AndroidOS/FakeBattScar

Domain-Name

Value
apps.store
zoomnewsonly.site
zoom-us.tech
scheta.site
youstorys.com
promoapp-zoom.com
windows-rars.shop
info-zoomapp.com
2311foreign.xyz
zoommaster.life
winkos.net

StixFile

Value
462df2e4a633e57de0d5148060543576d7c1165bf90e6aec4183f430d8925a1c
44cac5bf0bab56b0840bd1c7b95f9c7f5078ff417705eeaaf5ea5a2167a81dd5
fd524641d2be705d76feb0453374c5b2ad9582ced4f00bb3722b735401da2762
dcb80bd21bd6900fe87423d3fb0c49d8f140d5cf5d81b662cd74c22fca622893
30fda67726f77706955f6b52b202452e91d5ff132783854eec63e809061a4b5c
5b917d04d416cafaf13ed51c40b58dc8b4413483ea3f5406b8348038125cad0b

Hostname

Value
notetrest.onelink.me
zoromonm.onelink.me
aksdquwrqr.onelink.me
putin-777.onelink.me
l.hyros.com
169-zoona32.onelink.me
arnold.onelink.me
slovo-pacana.onelink.me
api.huntingpanel.link
ntcrgfmmc3.onelink.me
zoomus.onelink.me
mmozl.onelink.me
z00nn.one-platform-to-connect.group

desktop-client.onelink.me

IPv4-Addr

Value
94.131.110.127

Url

Value
http://winkos.net/ld/zm.tar.gpg
http://youstorys.com/fonts/Zoom-x64.msix
http://l.hyros.com/c8KqPHYKdt
http://zoom-us.tech/ZoomInstaller.zip
http://windows-rars.shop/bootstrap/Zoom-x64.msix
http://scheta.site/apps.store/ZoomInstaller.msix

External References

- https://otx.alienvault.com/pulse/65817e4c05cbf5d0fa336908
- https://www.malwarebytes.com/blog/threat-intelligence/2023/12/malvertisers-zoom-in-on-cryptocurrencies-and-initial-access