SecuritySnack: 18+E-Crime

⋮ 10/3/2025

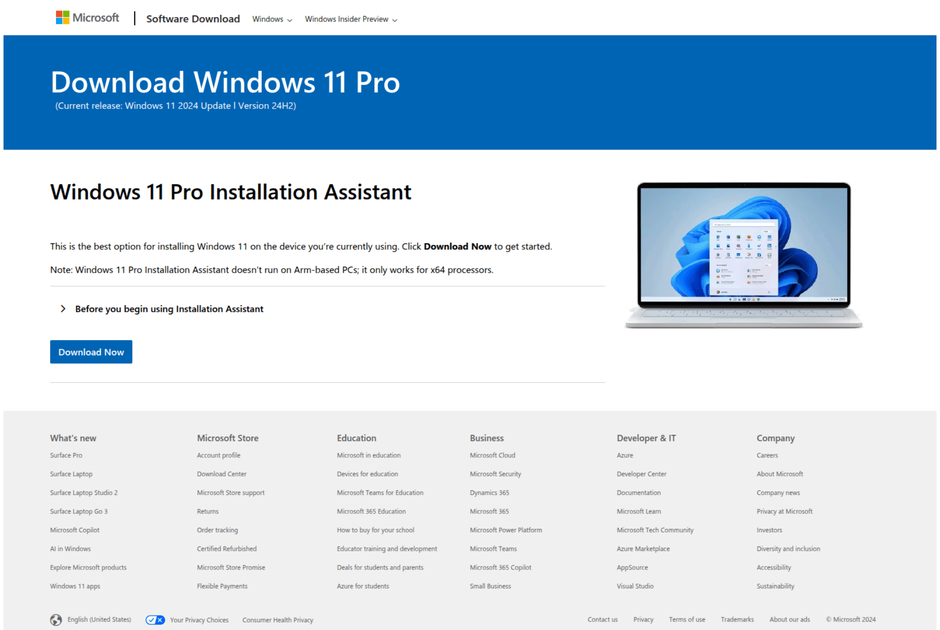
Starting in September 2024, a financially motivated cluster of more than 80 spoofed domain names and lure websites began targeting users with fake applications and websites themed as government tax sites, consumer banking, age 18+ social media content, and Windows assistant applications. The actor used these spoofed domains to deliver Android and Windows trojans likely for the purpose of stealing credentials or more overtly through the use of fake login pages.

Details

Windows Installation Assistant download themed websites such as the following were used to deliver Windows trojans.

ms32-download[.]pro

corp-ms32-download[.]pro



Download URL: https[:]//cozzystaysemarang[.]com/temp/winsetup-stable-windows_x86_x64_software_package_revision_final.exe

Filename: winsetup-stable-windows_x86_x64_software_package_revision_final.exe

Sha256: 3767140145cef85204ddec1285f5dc8544bfcf8ff22318c11073baaa476385fc

The same delivery domain was previously observed delivering APK files in June 2025.

APK Sha256: a83a442f930fea310d391f852385e3673d8c7128e5bbdc2b68217838c78381fa

More recent versions used a different domain with a long URL likely to hide the filename from automated security tools and, to a lesser extent, human review. The excessive spaces (%20 in URL encoding) and length may bypass some detection rules or regular expressions to match malicious patterns..

Download URL:

https[:]//fleetfedx[.]com/Installer%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%2
Win11_x86_x64.msi

SHA256: 71cd466073bf23b43111dbc68ccaf1064e737f3f9ffebfec9a6f5146af6a34b9

The download links also contain a Tracking Pixel in the on-click event: onclick="fbq('track', 'Lead');" This indicates that the attacker is running this as a campaign. They are likely using Facebook ads or other methods to drive traffic to this fake page and are tracking their "conversion rate", a metric of how many people they successfully trick into clicking the malicious download link.

Facebook Tracker Ids:

- 1354988235984551
- 690114973584418
- 1327164645166821

Additionally, a Yandex tracker was also identified in use: 97105740

Connective Tissue

Registrar

- PDR Ltd. d/b/a PublicDomainRegistry.com
- GMO Internet, Inc.

IP ISP

- BL Networks
- H2nexus Ltd
- H2.nexus Frankfurt Network

Name Server Domain

- regway[.]com

Top Level Domains

- Pro, Shop, Com, Icu, Top

Registrant Email Domains

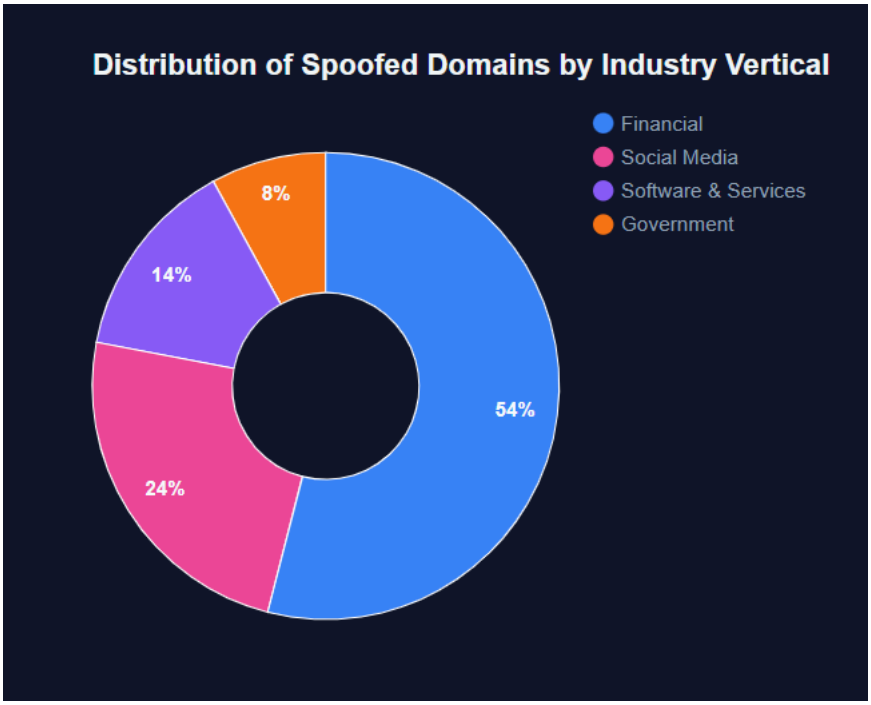
- fviainboxes[.]com
- dropjar[.]com
- replyloop[.]com
- yopmail[.]com
- robot-mail[.]com
- protonmail[.]com

Trackers

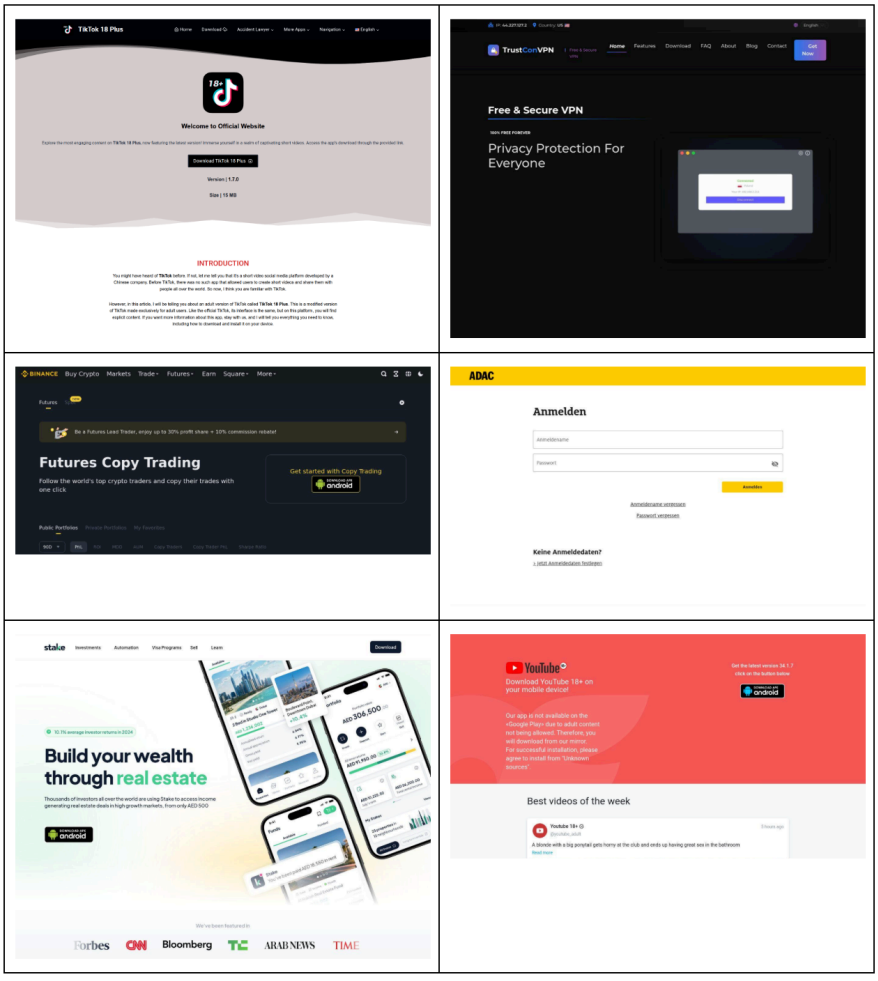
- Facebook: 690114973584418
- Facebook: 1327164645166821
- Facebook: 1354988235984551
- Yandex: 97105740

The majority of the cluster's domains targeted users with age 18+ themed TikTok, YouTube, and online Gambling Android applications. Other themes specifically involved several prominent consumer banks and cryptocurrency exchanges including USAA, PMC, Bloomberg, and Binance. A subset of the domains resolve fake Windows 11 Installation Assistant and TrustCon VPN application downloads.

A breakdown of the cluster's domain and websites by spoofed industries shows the majority are directly financially related, including the Government tax sites.



Sample screenshots of spoofed websites for malware delivery and credential harvesting:



Conclusion

This report highlights a persistent and financially motivated cybercrime operation employing common techniques, including spoofed domains and lure websites to distribute malware and harvest credentials.

The most common lures preyed on curiosity and desire, which can override a user's normal caution. The promise of forbidden or exclusive content is a powerful social engineering tool. Subsequently, victims are often embarrassed to admit how their device was infected. They are less likely to report the malicious app to authorities, security vendors, or even their IT department, allowing the malware to persist longer and the campaign to remain undetected.

They operate with the mindset of a malicious marketing firm, prioritizing scale and conversion rates over high-level technical sophistication. The use of template-based website builders indicates a focus on rapid deployment and disposability of their infrastructure, allowing them to quickly pivot and evade takedowns, browser-based warnings, and blocklisting mechanisms.

Users are advised to exercise extreme caution when encountering unfamiliar links or download prompts, particularly those related to banking, social media, or system utilities.

IOCs

Emails

host_sdji21cxvmj12[@]dropjar[.]com
pq_bl_6_safs_sssw[@]fviainboxes[.]com
feleko2722[@]replyloop[.]com
lux_bl_22_fdjhgza_reg[@]fviainboxes[.]com
lux_bl_21_sdfgsun_reg[@]fviainboxes[.]com
lux_47_jkscnxkjasd[@]fviainboxes[.]com
lux_49_kcsdfer321[@]fviainboxes[.]com
lux_bl_20_ilskdfgnoi_reg[@]fviainboxes[.]com
pq-black234333123[@]clowmail[.]com
zapuwo3736[@]robot-mail[.]com
simpleflex20934[@]yopmail[.]com
m2mcion[@]protonmail[.]com

Domains

11windows[.]pro
18pllus-tiktok[.]pro
18tiktok-get[.]pro
adac-banklnq-solarlsqroup[.]com
admin-octorate[.]icu
alphazone[.]icu
alveriq[.]run
americanfiscalroots[.]digital
app-degiro[.]life
app-lodgify[.]today
app-mews[.]life
app-tt-eighteenplus[.]pro
arvest-login[.]icu
asflinaq-de[.]com
assurix[.]run
atonovat[.]run
atorishation[.]icu
atotax[.]icu
au-ato[.]com
au-ato[.]info
au-ato[.]org
au-entrance[.]icu
auauth[.]icu
authcu[.]icu
author-glob[.]icu
authtax[.]icu
avaibook[.]today
aviabook[.]icu
balancevector[.]digital
becu[.]life
beginnersguide[.]digital
beytra[.]run
binance-copytrading[.]pro
blueecho[.]icu
bookary[.]digital
brightfoundations[.]run
btexplorer[.]icu
capcat[.]icu
casualabaya[.]icu

center-download[.]pro
center-hubs[.]com
center-upload[.]pro
centerhub[.]pro
chromaguide[.]icu
civiccore[.]digital
clarvexa[.]icu
cleareditlab[.]icu
clearoak[.]icu
cleranta[.]today
cloud-m32s-center[.]pro
cloudmention[.]icu
confirmation-id1174[.]com
confirmation-id1175[.]com
confirmation-id1176[.]com
confirmation-id1177[.]com
corementionn[.]icu
corp-ms32-download[.]pro
credenza[.]run
credvoria[.]today
cyberpulse[.]icu
darkvoid[.]icu
datapanel[.]icu
datatransit[.]life
distan[.]icu
dornwell[.]today
dovexa[.]top
download-center-io[.]pro
downloads-center[.]pro
dowloadstake[.]com
drovenor[.]today
droxia[.]top
e-access[.]icu
e-auth[.]icu
economicsinsight[.]icu
econviewpoint[.]digital
eldenhall[.]digital
entcu[.]icu
entsolutions[.]icu
esl-access[.]com
etradeai[.]icu
etradeapi[.]icu
etradelogistic[.]icu
everlynx[.]icu
fidelity-entrance[.]com
fidelity-log[.]com
fidelity-login[.]com
fidellity-online[.]com
financebasics[.]digital
finatracore[.]today
finliteracynetwork[.]world
finlume[.]digital
finolyze[.]digital
finostra[.]digital
finovexa[.]digital
firmara[.]today
first-access[.]icu
fleetfedx[.]com
flexiraq[.]world
flrstrade[.]com
fnbo-access[.]icu
focusinsights[.]pro
focusonsystems[.]run
freyqa[.]bet
g-entrance[.]icu
get-centerapp[.]pro
get-tt-plus-download[.]com
get-upload[.]pro
getdownload-hub[.]com
getdownload-mscenter[.]com
getdownloadhub[.]com
gettaxato[.]icu
getupload-center[.]live
getupload[.]pro
getveridian[.]icu
glaviso[.]top
gov-access[.]icu
govaccess[.]icu

greythorpe[.]world
gridpattern[.]life
grotexor[.]icu
holven[.]icu
hostvista[.]digital
huntington-acc[.]com
huntington-access[.]com
huntington-access[.]icu
huntington-entrance[.]com
huntington-entrance[.]icu
huntington-log[.]com
huntington-online[.]com
huntington-read[.]com
id-centraldispatch[.]life
id-mexem[.]life
id-onpoint[.]life
id-tradestation[.]life
inforelic[.]icu
interactvebroker[.]com
keldra[.]top
kenvia[.]today