


Multi-Layered TDS Infrastructure Linked to Major Cyber Threats

 recordedfuture.com/research/tag-124-multi-layered-tds-infrastructure-extensive-user-base

TAG-124's Multi-Layered TDS Infrastructure and Extensive User Base

Analysis cut-off date: January 7, 2025

NOTE: This report was updated on May 12, 2025, after it was discovered that TAG-124 is unrelated to 404TDS. All references to 404TDS as an alias belonging to TAG-124 have been removed.

Executive Summary

Insikt Group has identified multi-layered infrastructure linked to a traffic distribution system (TDS) tracked by Recorded Future as TAG-124, which overlaps with threat activity clusters known as LandUpdate808, KongTuke, and Chaya_002. TAG-124 comprises a network of compromised WordPress sites, actor-controlled payload servers, a central server, a suspected management server, an additional panel, and other components. The threat actors behind TAG-124 demonstrate high levels of activity, including regularly updating URLs embedded in the compromised WordPress sites, adding servers, refining TDS logic to evade detection, and adapting infection tactics, as demonstrated by their recent implementation of the ClickFix technique.

Insikt Group identified multiple threat actors using TAG-124 within their initial infection chains, including operators of Rhysida ransomware, Interlock ransomware, TA866/Asylum Ambuscade, SocGhosh, D3F@CK Loader, TA582, and others. Notably, the shared use of TAG-124 reinforces the [connection](#) between Rhysida and Interlock ransomware, which are already linked through similarities in tactics, tools, encryption behaviors, ransom note themes, code overlaps, and data exfiltration techniques. Insikt Group expects that TAG-124 will continue its operations within the increasingly sophisticated and specialized cybercriminal ecosystem, enhance its effectiveness, and attract additional users and partners.

Key Findings

- Insikt Group identified multi-layered infrastructure linked to a TDS tracked as TAG-124. This infrastructure includes a network of compromised WordPress sites, likely actor-controlled payload servers, a central server, a suspected management server, and an additional panel, among other components.
- The threat actor(s) associated with TAG-124 appear highly active, regularly updating URLs on compromised WordPress sites to evade detection, adding new servers to their infrastructure, and improving TDS-linked conditional logic and infection tactics.
- Multiple threat actors are assessed to incorporate TAG-124's service into their initial infection chains, including operators of Rhysida ransomware, Interlock ransomware, TA866/Asylum Ambuscade, SocGhosh, D3F@CK Loader, TA582, and others.
- While Rhysida and Interlock ransomware have been associated with each other due to similarities in tactics, tools, encryption behaviors, ransom note themes, overlaps in code, and data exfiltration techniques, the shared use of TAG-124 reinforces this connection.

Background

TAG-124, which overlaps with LandUpdate808, KongTuke, and Chaya_002, is a TDS used to distribute malware on behalf of various threat actors, including operators of Rhysida ransomware, Interlock ransomware, TA866/Asylum Ambuscade, SocGhosh, D3F@CK Loader, and TA582, among others ([1](#), [2](#), [3](#)). A TDS typically [refers](#) to a system used to analyze and redirect web traffic based on parameters like geolocation or device type, funneling only specific visitors to malicious destinations such as phishing sites, malware, or exploit kits, while evading detection and optimizing cybercriminal campaigns.

More specifically, TAG-124 operates by injecting malicious JavaScript code into compromised WordPress websites. When visitors access an infected website, they unknowingly load attacker-controlled resources designed to manipulate them into completing actions that result in the download and execution of malware. TAG-124 often deceives victims by presenting the malware as a required Google Chrome browser update.

In more recent variations, TAG-124 has been [observed](#) using the ClickFix technique. This approach displays a dialog instructing visitors to execute a command pre-copied to their clipboard. Once a visitor runs the command, it initiates a multi-stage process that downloads and executes the malware payload.

Threat Analysis

TAG-124

Insikt Group identified multi-layered infrastructure associated with the TDS TAG-124. This infrastructure comprises a network of compromised WordPress sites, likely actor-controlled payload servers, a central server whose exact purpose remains unclear at the time of analysis, a suspected management server, and an additional management panel. If visitors fulfill specific criteria, the compromised WordPress websites display fake Google Chrome update landing pages, which ultimately lead to malware infections as discussed in the [Users of TAG-124](#) section of this report (see **Figure 1**).

***Figure 1:** TAG-124's high-level infrastructure setup (Source: Recorded Future)*

Compromised WordPress Websites

TAG-124's infrastructure consists of an extensive network of WordPress websites (see **Appendix A**). These websites appear to lack a consistent theme regarding industry, topic, or geography, suggesting they were likely compromised opportunistically through exploits or by acquiring credentials, such as those obtained via infostealers.

First-Stage WordPress Websites in Initial Delivery

The compromised websites of the first stage in the initial delivery phase typically include a script tag with an `async` attribute at an arbitrary location in the document object model (DOM), enabling the loading of an external JavaScript file in parallel with the page to avoid rendering delays (see **Figure 2**).

Figure 2: Script tag in DOM used to load external JavaScript file (Source: [URLScan](#))

The JavaScript filename has changed frequently over time, with earlier names following recognizable patterns (such as `metrics.js`) and more recent ones [appearing](#) to be randomly formatted (such as `hpms1989.js`). Example filenames include:

- `3561.js`
- `365h.js`
- `e365r.js`
- `hpms1989.js`
- `metrics.js`
- `nazvanie.js`
- `web-analyzer.js`
- `web-metrics.js`
- `web.js`
- `wp-config.js`
- `wp.js`

Notably, the threat actors appear to be regularly updating the URLs on the compromised websites. For instance, the website associated with `www[.]jecowas[.]int` has consistently changed the URL used to fetch the JavaScript file. This behavior indicates that the threat actors maintain ongoing access to these WordPress sites and frequently alter the URLs, including the domain and JavaScript filename, likely to evade detection.

Although many of the compromised WordPress websites appear to be associated with lesser-known organizations, Insikt Group identified notable cases, including a subdomain linked to the Polish Centre for Testing and Certification, `www[.]pcbc[.]gov[.]pl`, and the domain of the Economic Community of West African States (ECOWAS) (`www[.]jecowas[.]int`). Both have been compromised and used in TAG-124 campaigns.

If visitors meet specific criteria, which could not be fully determined, the compromised WordPress domains typically present fake Google Chrome update landing pages. These pages prompt users to click a download button, triggering the download of the actual payload from designated endpoints on a secondary set of compromised WordPress websites, including but likely not limited to:

- /wp-admin/images/wfgth.php
- /wp-includes/pomo/update.php
- /wp-content/upgrade/update.php
- /wp-admin/images/rsggj.php

Fake Google Chrome Update Landing Pages

Insikt Group discovered two variants of fake Google Chrome update landing pages associated with TAG-124 (see **Figure 3**). According to URLScan submission data, Variant 1 has been active longer, with its earliest submission recorded on April 24, 2024.

Only victims meeting a specific set of still unknown conditions are directed to the fake Google Chrome update landing page, resulting in the observation of only a limited number of domains (see **Table 1**). These domains can be attributed to TAG-124 based on the URLs embedded in the DOM, public reporting, or other indicators. Notably, the threat actors consistently [misspell](#) the word “referer” as “refferer” in the query parameter, a typographical error [observed](#) in earlier reports.

Domain

Notes

Variant

www[.]reloadinternet[.]com

Linked to www[.]netzwerkreklame[.]de

1

selectmotors[.]net

Linked to www[.]netzwerkreklame[.]de

1

mgsoft[.]com

Linked to [www\[.\]netzwerkreklame\[.\]de](#)

1

www[.]lovebscott[.]com

Linked to [sustaincharlotte\[.\]org](#)

1

evolverangesolutions[.]com

Linked to [sustaincharlotte\[.\]org](#)

1

www[.]ecowas[.]int

Linked to [www\[.\]pawrestling\[.\]net](#)

1

ns1[.]webasatir[.]ir

[Linked](#) to [true-blood\[.\]net](#), which has been previously associated with TAG-124

2

avayehazar[.]ir

Linked to [true-blood\[.\]net](#)

2

cvqrcode[.]ipmglobalrelations[.]com

Linked to [true-blood\[.\]net](#)

2

mktgads[.]com

Linked to [true-blood\[.\]net](#)

2

incalzireivar[.]ro

Linked to [true-blood\[.\]net](#)

2

gmdva[.]org

Linked to [true-blood\[.\]net](#)

2

www[.]de[.]digitaalkantoor[.]online

Linked to [true-blood\[.\]net](#)

2

elamoto[.]com

[Linked](#) to TAG-124 and has the typographical error in the query parameter; it was redirected from [winworld\[.\]es](#), a domain associated with Spain-based WinWorld, a company specializing in computer support and services

2

Table 1: Likely compromised websites hosting fake Google Chrome update pages (Source: Recorded Future)

Likely Threat Actor-Owned Domain

While the domains listed in **Table 1** are likely compromised, Insikt Group analyzed URLs present on websites hosted on two additional domains (see **Table 2**). Our analysis suggests these domains are highly likely connected to TAG-124.

Domain

Notes

Variant

update-chronne[.]com

[Contained](#) link to *true-blood[.]net*

1

sollishealth[.]com

[Contained](#) links to *edveha[.]com* and *espumadesign[.]com*; both were previously associated with TAG-124

2

Table 2: Additional domains found via visual similarity search (Source: Recorded Future)

The domain update-chronne[.]com, hosted behind Cloudflare, appears to be owned by the threat actors as it directly impersonates Google Chrome (see **Figure 4**). At the time of analysis, the domain was still active, indexed by Google Search, and hosted the file Release.zip, which was [identified](#) as REMCOS RAT.

Figure 4: Google Chrome fake update landing page on update-chronne[.]com (Source: Recorded Future)

Notably, when a victim clicks the “Update Chrome” button, the website redirects to *downloading[.]bpnetempresas[.]com*, which shows the IP address *146.70.41[.]191* combined with three different ports (see **Figure 5**). This IP address has previously been [associated](#) with REMCOS RAT.

Figure 5: Suspected REMCOS RAT command-and-control (C2) server shown on downloading[.]bplnetempresas[.]com (Source: Recorded Future)

Additionally, the domain hosted a file named moc.txt, containing a PowerShell script designed to download and execute the contents of Release.zip (see **Figure 6**). The URL was redirected via the shortened URL [https://wl\[.\]g/25dW64](https://wl[.]g/25dW64).

Figure 6: PowerShell script hosted on

[https://update-chronne\[.\]com/moc.txt](https://update-chronne[.]com/moc.txt) as of September 12, 2024 (Source: [URLScan](#))

Suspected Shell Website

Both *update-chronne[.]com* and *downloading[.]bplnetempresas[.]com* hosted a website seemingly associated with "YSOFEL", which appears to be a Brazilian organization (see **Figure 7**). However, no information about this organization could be found online, indicating that it is likely a fictitious entity.

Figure 7: Suspected shell website linked to a fake Brazilian organization (Source: [URLScan](#))
Insikt Group identified several other domains, some of which are noted in the [Compromised WordPress Websites](#) section (such as mktgads[.]com), while others appear to impersonate Google (such as check-google[.]com) (see **Table 3**). This suggests that the website may function as a "shell website", potentially used to age domains or to display content only when visitors meet specific criteria.

Domain
IP Address
First Seen
Last Seen
Notes
challinksch[.]com
Cloudflare
2024-09-05

2025-01-05

Hosted PowerShell script to download PuTTY and linked to AsyncRAT

chainlitz[.]org

Cloudflare

2024-08-21

2025-01-07

Hosted PowerShell script

check-google[.]com

Cloudflare

2024-09-09

2025-01-07

N/A

cihainlst[.]org

Cloudflare

2024-08-21

2025-01-07

N/A

io-suite-web[.]com

Cloudflare

2024-08-14

2025-01-07

N/A

miner-tolken[.]com

Cloudflare

2024-09-06

2025-01-07

N/A

ronnin-v2[.]com

Cloudflare

2024-05-27

2025-01-07

N/A

syndilatic[.]com

Cloudflare

2024-08-20

2025-01-07

N/A

symbieitc[.]com

Cloudflare

2024-08-21

2025-01-04

N/A

syndlotic[.]com

Cloudflare

2024-08-21

2025-01-07

N/A

synbiotic[.]com

Cloudflare

2024-08-21

2025-01-07

N/A

symbliatc[.]com

Cloudflare

2024-08-20

2024-12-30

N/A

symbiotic[.]com

Cloudflare

2024-08-19

2025-01-07

N/A

comteste[.]com

Cloudflare

2024-08-19

2025-01-07

N/A

syndilotic[.]com

Cloudflare

2024-08-20

2024-12-30

N/A

v2-rubby[.]com

Cloudflare

2024-05-22

2025-01-07

N/A

Table 3: Domains linked to the same suspected “shell website” linked to the fake Brazilian organization referenced above (Source: Recorded Future)

It remains uncertain whether all the domains in **Table 3** are malicious or connected to the same activity. However, their shared hosting of the same website, impersonation of other brands (such as ChainList), and partial verification of links to infections make them, at the very least, suspicious.

TAG-124 Delivery Servers

TAG-124 leverages compromised WordPress websites for various components of its infection chains. The servers embedded in the DOMs of these compromised first-stage WordPress sites, as detailed in the First-Stage WordPress Websites in Initial Delivery section, are likely owned by the threat actors. Insikt Group identified a significant network of servers connected to and likely controlled by the TAG-124 threat actors (see **Table 4**).

Domain

IP Address

First Seen

Last Seen

ambiwa[.]com

45[.]61[.]136[.]9

2024-12-28

2025-01-07

gcafin[.]com

45[.]61[.]136[.]9

2024-12-29

2025-01-06

discoves[.]com

45[.]61[.]136[.]9

2024-12-26

2025-01-06

xaides[.]com

45[.]61[.]136[.]40

2025-01-02

2025-01-07

usbkits[.]com

45[.]61[.]136[.]40

2025-01-02

2025-01-07

mirugby[.]com

45[.]61[.]136[.]40

2025-01-02

2025-01-07
ecrut[.]com
45[.]61[.]136[.]41
2025-01-06
2025-01-07
pursyst[.]com
45[.]61[.]136[.]41
2025-01-06
2025-01-07
pushcg[.]com
45[.]61[.]136[.]67
2024-09-18
2025-01-07
piedsmontlaw[.]com
45[.]61[.]136[.]67
2022-12-22
2025-01-06
pemalite[.]com
45[.]61[.]136[.]67
2022-12-22
2025-01-07
howmanychairs[.]com
45[.]61[.]136[.]67
2024-03-14
2025-01-06
calbbs[.]com
45[.]61[.]136[.]89
2024-12-18
2025-01-07
habfan[.]com
45[.]61[.]136[.]132
2024-12-07
2025-01-07
iognews[.]com
45[.]61[.]136[.]132
2024-12-06
2025-01-07

safigdata[.]com
45[.]61[.]136[.]196
2024-11-19
2025-01-07
nyciot[.]com
45[.]61[.]136[.]196
2024-11-20
2025-01-07
pweobmxdlboi[.]com
64[.]7[.]198[.]66
2024-08-27
2025-01-07
boneyn[.]com
64[.]94[.]85[.]98
2024-12-22
2025-01-07
satpr[.]com
64[.]94[.]85[.]98
2024-12-22
2025-01-07
coeshor[.]com
64[.]94[.]85[.]248
2024-12-06
2025-01-07
mtclibraries[.]com
64[.]94[.]85[.]248
2024-12-11
2025-01-07
sdrce[.]com
64[.]95[.]11[.]65
2024-12-13
2025-01-07
theinb[.]com
64[.]95[.]11[.]65
2024-12-13
2025-01-07
elizgallery[.]com

64[.]95[.]111[.]184

2024-11-20

2025-01-07

enethost[.]com

64[.]95[.]12[.]38

2024-12-26

2025-01-07

dhusch[.]com

64[.]95[.]12[.]38

2024-12-24

2025-01-07

fastard[.]com

64[.]95[.]12[.]38

2024-12-25

2025-01-07

franklinida[.]com

64[.]95[.]12[.]98

2024-10-18

2025-01-07

nastictac[.]com

64[.]190[.]113[.]41

2024-11-25

2025-01-07

dncoding[.]com

64[.]190[.]113[.]41

2024-11-26

2025-01-07

djnito[.]com

64[.]190[.]113[.]111

2024-12-11

2025-01-07

opgears[.]com

64[.]190[.]113[.]111

2024-12-11

2025-01-07

tickerwell[.]com

162[.]33[.]177[.]36

2024-11-19
2025-01-07
selmanc[.]com
162[.]33[.]177[.]82
2024-12-16
2025-01-07
tibetin[.]com
162[.]33[.]177[.]82
2024-12-16
2025-01-07
mercro[.]com
162[.]33[.]178[.]59
2024-10-31
2025-01-07
esaleerugs[.]com
162[.]33[.]178[.]63
2024-11-22
2025-01-07
tayakay[.]com
162[.]33[.]178[.]75
2024-11-15
2024-11-15
ilsotto[.]com
162[.]33[.]178[.]113
2024-11-23
2025-01-07
chewels[.]com
193[.]149[.]176[.]179
2024-12-05
2025-01-07
sokrpro[.]com
193[.]149[.]176[.]223
2024-12-20
2025-01-07
hdtele[.]com
193[.]149[.]176[.]223
2024-12-20

2025-01-07
chhimij[.]com
193[.]149[.]176[.]248
2024-08-15
2025-01-07
dechromo[.]com
216[.]245[.]184[.]179
2024-12-09
2025-01-07
enerjjoy[.]com
216[.]245[.]184[.]179
2024-12-09
2025-01-07
dsassoc[.]com
216[.]245[.]184[.]179
2024-12-18
2025-01-07
gwcomics[.]com
216[.]245[.]184[.]210
2024-12-19
2025-01-07
genhil[.]com
216[.]245[.]184[.]225
2024-11-18
2025-01-07
vicrin[.]com
216[.]245[.]184[.]225
2024-11-05
2025-01-07
eliztalks[.]com
216[.]245[.]184[.]225
2024-11-16
2025-01-07
rshank[.]com
216[.]245[.]184[.]225
2024-11-13
2025-01-06

Table 4: Likely threat actor-controlled TAG-124 delivery servers (Source: Recorded Future)

Most of the domains began resolving in November 2024, suggesting that TAG-124 gained momentum during this period, with the majority of the domains still active at the time of analysis. Of note, two domains hosted on 45[.]61[.]136[.]67, namely *piedsmontlaw[.]com* and *pemalite[.]com*, were already resolving to this IP address in 2022, indicating that the server may have already been under the control of the threat actor during that time.

Suspected Higher-Tier Infrastructure

The majority of the suspected threat actor-controlled TAG-124 delivery servers, as listed in the [TAG-124 Delivery Servers](#) section, have been seen communicating with a server over TCP port 443 (see **Figure 1**). The configurations of this server are similar to those of the delivery servers and host a domain that returns only a generic HTML page when accessed. At the time of analysis, Insikt Group could not determine the exact purpose of this server but suspects it plays a central role in the operation. One possibility is that it contains the core logic of the TDS.

Additionally, Insikt Group identified a suspected management server linked to TAG-124. This server has been observed communicating with the delivery servers via TCP ports 80 and 443. It has also interacted with another panel linked to TAG-124, referred to as the "Ads Panel", whose purpose includes serving the latest delivery server through a specified endpoint, among others (see **Figure 1**).

TAG-124's Multi-Layered TDS Infrastructure and Extensive User Base

Read the Complete Analysis

[Download report](#)

Appendix A — Indicators of Compromise

Likely Compromised WordPress Domains Used by TAG-124:

- 1stproducts[.]com
- 3hti[.]com
- academictutoringcenters[.]com
- adpages[.]com
- adsbicloud[.]com
- advanceair[.]net
- airbluefootgear[.]com
- airinnovations[.]com
- allaces[.]com[.]au
- alumni[.]clermson[.]edu
- ambir[.]com
- americanreloading[.]com

antiagewellness[.]com
architectureandgovernance[.]com
astromachineworks[.]com
athsvic[.]org[.]au
baseball[.]razzball[.]com
bastillefestival[.]com[.]au
bigfoot99[.]com
blacksportsonline[.]com
blog[.]contentstudio[.]io
bluefrogplumbing[.]com
canadamotoguide[.]com
canadanickel[.]com
capecinema[.]org
careers[.]bms[.]com
careers[.]fortive[.]com
castellodelpoggio[.]com
catholiccharities[.]org
chamonixskipasses[.]com
changemh[.]org
chicklitplus[.]com
clmfireproofing[.]com
comingoutcovenant[.]com
complete-physio[.]co[.]uk
complete-pilates[.]co[.]uk
conical-fermenter[.]com
cssp[.]org
deathtotheworld[.]com
deerfield[.]com
denhamlawoffice[.]com
dev[.]jazliver[.]com
development[.]3hti[.]com
digimind[.]nl
dotnetreport[.]com
drcolbert[.]com
dzyne[.]com
earthboundfarm[.]com
eivcapital[.]com
elitetournaments[.]com
ergos[.]com
esfna[.]org
espumadesign[.]com
exceptionalindividuals[.]com
experiencebrightwater[.]ca
firstpresbyterianpaulding[.]com
fractalerts[.]com
fusionstone[.]ca
global-engage[.]com
gobrightwing[.]com
gov2x[.]com
hksusa[.]com
hmgcreative[.]com
hnh[.]org
hoodcontainer[.]com
hospitalnews[.]com
housingforhouston[.]com
houstonmaritime[.]org
hrsoft[.]com
hungryman[.]com
icmcontrols[.]com
ijmtolldiv[.]com
innsbrook[.]com
jewelryexchange[.]com
jodymassagetherapyclinic[.]com

joelbieber[.]com
knewhealth[.]com
lamaisonquilting[.]com
legacy[.]orlandparkprayercenter[.]org
levyso[.]com
luxlifemiamiblog[.]com
magnoliagreen[.]com
magnotics[.]com
manawatunz[.]co[.]nz
mantonpushrods[.]com
michiganchronicle[.]com
michigantownships[.]org
monlamdesigns[.]com
montessoriwest[.]com
movinbed[.]com
my[.]networknuts[.]net
myrtlebeachgolf[.]com
ncma[.]org
oglethorpe[.]edu
oningroup[.]com
orlandparkprayercenter[.]org
outdoornativitystore[.]com
parksaverscom[.]kinsta[.]cloud
peoria[.]org
peridotdentalcare[.]ca
phfi[.]org
pikapp[.]org
powerlineblog[.]com
prek4sa[.]com
psafetysolutions[.]com
puntademita-rentals[.]com
resf[.]com
retaildata[.]com
rhodenroofing[.]com
rm-arquisign[.]com
rvthereyet[.]com
schroederindustries[.]com
sec-group[.]co[.]uk
sixpoint[.]com
slotomoons[.]com
sollishealth[.]com
sparkcarwash[.]com
spectrallogic[.]com
sramanamitra[.]com
stg-seatrail-staging[.]kinsta[.]cloud
stg-townandcountryplanningassoci-staging[.]kinsta[.]cloud
sustaincharlotte[.]org
teamtoc[.]com
terryrossplumbing[.]com
theawningcomp[.]mrmktg[.]us
theepicentre[.]com
theyard[.]com
tristatecr[.]com
true-blood[.]net
turtl[.]co
tustinhistory[.]com
tysonmutrux[.]com
uk[.]pattern[.]com
unsolved[.]com
vanillajoy[.]ykv[.]jih[.]mybluehost[.]me
vectare[.]co[.]uk
villageladies[.]co[.]uk
walkerroofingandconstruction[.]com

wildwestguns[.]com
wildwoodpress[.]org
wlplastics[.]com
worldorphans[.]org
www[.]211cny[.]com
www[.]6connex[.]com
www[.]900biscaynebaymiamicondos[.]com
www[.]accentawnings[.]com
www[.]acvillage[.]net
www[.]airandheatspecialistsnj[.]com
www[.]als-mnd[.]org
www[.]americancraftbeer[.]com
www[.]anoretareort[.]com
www[.]architectureandgovernance[.]com
www[.]atlantaparent[.]com
www[.]atlas-sp[.]com
www[.]atmosera[.]com
www[.]belvoirfarm[.]co[.]uk
www[.]betterengineering[.]com
www[.]bluefoxcasino[.]com
www[.]boatclubtrafalgar[.]com
www[.]bordgaisenergytheatre[.]ie
www[.]brandamos[.]com
www[.]cairha[.]com
www[.]cdhcpa[.]com
www[.]cds[.]coop
www[.]cgimgolf[.]com
www[.]cheericca[.]org
www[.]conwire[.]com
www[.]cssp[.]org
www[.]dces[.]com
www[.]disabilityscot[.]org[.]uk
www[.]doctorkiltz[.]com
www[.]drivenbyboredom[.]com
www[.]ecowas[.]int
www[.]evercoat[.]com
www[.]facefoundrie[.]com
www[.]foxcorphousing[.]com
www[.]genderconfirmation[.]com
www[.]gofreight[.]com
www[.]gunnerroofing[.]com
www[.]hayeshvacllc[.]com
www[.]hksusa[.]com
www[.]hollingsworth-vose[.]com
www[.]hollywoodburbankairport[.]com
www[.]hopechc[.]org
www[.]icmcontrols[.]com
www[.]inboundlogistics[.]com
www[.]infra-metals[.]com
www[.]jasperpim[.]com
www[.]koimoi[.]com
www[.]louisvillemechanical[.]com
www[.]lsbn[.]state[.]la[.]us
www[.]mallorcantonic[.]com
www[.]marketlist[.]com
www[.]mocanyc[.]org
www[.]motherwellfc[.]co[.]uk
www[.]murphyoilcorp[.]com
www[.]myrtlebeachgolfpackages[.]co
www[.]napcis[.]org
www[.]nelsongonzalez[.]com
www[.]netzwerkreklame[.]de
www[.]onthegreenmagazine[.]com

www[.]orthodontie-laurentides[.]com
www[.]pamelasandalldesign[.]com
www[.]parajohn[.]com
www[.]parksavers[.]com
www[.]parmacalcio1913[.]com
www[.]patio-supply[.]com
www[.]pcbc[.]gov[.]pl
www[.]perfectduluthday[.]com
www[.]powerlineblog[.]com
www[.]progarm[.]com
www[.]rafilawfirm[.]com
www[.]reddiseals[.]com
www[.]riaa[.]com
www[.]robertomalca[.]com
www[.]sevenacres[.]org
www[.]sigmathermal[.]com
www[.]sisdisinfestazioni[.]it
www[.]spectralink[.]com
www[.]sramanamitra[.]com
www[.]sunkissedindecember[.]com
www[.]sweetstreet[.]com
www[.]system-scale[.]com
www[.]tcpa[.]org[.]uk
www[.]thatcompany[.]com
www[.]the-kaisers[.]de
www[.]thecreativemom[.]com
www[.]thedesignsheppard[.]com
www[.]therialtoreport[.]com
www[.]thetrafalgargroup[.]co[.]uk
www[.]thetruthaboutguns[.]com
www[.]totem[.]tech
www[.]ultrasound-guided-injections[.]co[.]uk
www[.]urbis-realestate[.]com
www[.]vending[.]com
www[.]venetiannj[.]com
www[.]visitarundel[.]co[.]uk
www[.]wefinanceanycar[.]com
www[.]wilsonsd[.]org

www[.]wilymanager[.]com
www[.]wwvc[.]edu
zerocap[.]com

Likely Compromised Websites Showing Fake Google Chrome Update Pages:

avayehazar[.]ir
cvqrqcode[.]pimglobalrelations[.]com
elamoto[.]com
evolverangesolutions[.]com
gmdva[.]org
incalzireivar[.]ro
mgsoft[.]com
mktgads[.]com
ns1[.]webasatir[.]ir
selectmotors[.]net
sollishealth[.]com
update-chronne[.]com
www[.]de[.]digitaalkantoor[.]online
www[.]ecowas[.]int
www[.]lovebscott[.]com
www[.]reloadinternet[.]com

TAG-124 Domains:

ambiwa[.]com
boneyn[.]com

calbbs[.]com
chewels[.]com
chhimif[.]com
coeshor[.]com
dechromo[.]com
dhusch[.]com
discoves[.]com
djnito[.]com
dncoding[.]com
dsassoc[.]com
ecrut[.]com
elizgallery[.]com
eliztalks[.]com
enerjjoy[.]com
enethost[.]com
esaleerugs[.]com
fastard[.]com
franklinida[.]com
gcafin[.]com
genhil[.]com
gwcomics[.]com
habfan[.]com
hdtele[.]com
howmanychairs[.]com
ilsotto[.]com
iognews[.]com
mercro[.]com
mirugby[.]com
mtclibraries[.]com
nastictac[.]com
nyciotf[.]com
opgears[.]com
pemalite[.]com
piedsmontlaw[.]com
pursyst[.]com
pushcg[.]com
pweobmxdlboi[.]com
rshank[.]com
safigdata[.]com
satpr[.]com
sdrce[.]com
selmanc[.]com
sokrpro[.]com
tayakay[.]com
theinb[.]com
tibetin[.]com
tickerwell[.]com
usbkits[.]com
vicrin[.]com
xaides[.]com

TAG-124 IP Addresses:

45[.]61[.]136[.]9
45[.]61[.]136[.]40
45[.]61[.]136[.]41
45[.]61[.]136[.]67
45[.]61[.]136[.]89
45[.]61[.]136[.]132
45[.]61[.]136[.]196
64[.]7[.]198[.]66
64[.]94[.]85[.]98
64[.]94[.]85[.]248
64[.]95[.]11[.]65

64[.]95[.]11[.]184
64[.]95[.]12[.]38
64[.]95[.]12[.]98
64[.]190[.]113[.]41
64[.]190[.]113[.]111
162[.]33[.]177[.]36
162[.]33[.]177[.]82
162[.]33[.]178[.]59
162[.]33[.]178[.]63
162[.]33[.]178[.]75
162[.]33[.]178[.]113
193[.]149[.]176[.]179
193[.]149[.]176[.]223
193[.]149[.]176[.]248
216[.]245[.]184[.]179
216[.]245[.]184[.]210
216[.]245[.]184[.]225

Additional Domains Observed in TAG-124 Activity:

winworld[.]les
true-blood[.]net

Matomo Instance:

dating2go[.]store

Domains Likely Linked to apple-online[.]shop:

micronsoftwares[.]com
mysamsung7[.]shop
nvidias[.]shop
expressbuycomputers[.]shop
amdradeon[.]shop
mobileyas[.]shop
cryptotap[.]site

REMCOS RAT C2 IP Address:

146.70.41[.]191

Domains Likely Linked to TA582 and MintsLoader Cluster:

527newagain[.]top
abhbdiiaehdeigh[.]top
adednihknaalilg[.]top
anjmhjidinfnlci[.]top
azure-getrequest[.]jicu
azurearc-cdn[.]top
azuregetrequest[.]jicu
bkkeiekjfcdaaen[.]top
cignijgmndnbchhc[.]top
ckeibfigimhmjgmb[.]top
cljhkcjvimibhcl[.]top
cmcebigeiajbfc[.]top
cmcuauec[.]top
cryptoslate[.]cc
eebchjechginddk[.]top
ehnediemcaffbij[.]top
ejlhaidjmhcami[.]top
faybzuy3byz2v[.]top
fpziviec[.]top
futnbuzj3nh[.]top
gbkffjcglabkmne[.]top
gdihcidghmcldd[.]top
get-azurecommand[.]jicu
get-iwrreq[.]top
getazurecommand[.]jicu
gnmjdjckbgddaie[.]top

gubzywey6b[.].top
iadkainhkafngnk[.].top
ikhgijabfnkajem[.].top
ikjfkkgagafbdke[.].top
imfiejalbhggijl[.].top
kffgkjmjangegegkg[.].top
kxcgjmjfgdleag[.].top
kjalcimbfaaddfff[.].top
mcajijknegnbbga[.].top
melmejkjaakiakn[.].top
mgjabikgjhambm[.].top
pretoria24[.].top
rifiziec[.].top
riuzvi4tc[.].top
robnzuwubz[.].top
saighbuzu32uvv[.].top

PyInstaller Hashes:

7683d38c024d0f203b374a87b7d43cc38590d63adb8e5f24dff7526f5955b15a
950f1f8d94010b636cb98be774970116d98908cd4c45fbb773e533560a4beea7
7f8e9d7c986cc45a78c0ad2f11f28d61a4b2dc948c62b10747991cb33ce0e241

CleanUpLoader Loader Hashes:

183c57d9af82964bfb06fbb0690140d3f367d46d870e290e2583659609b19f2
22dc96b3b8ee42096c66ab08e255adce45e5e09a284cbe40d64e83e812d1b910
9d508074a830473bf1dee096b02a25310fa7929510b880a5875d3c316617dd50
28c49af7c95ab41989409d2c7f98e8f8053e5ca5f7a02b2a11ad4374085ec6ff
2da62d1841a6763f279c481e420047a108da21cd5e16eae31661e6fd5d1b25d7
342b889d1d8c81b1ba27fe84dec2ca375ed04889a876850c48d2b3579fbac206
42c1550b035353ae529e98304f89bf6065647833e582d08f0228185b493d0022
42d7135378ed8484a6a86a322ea427765f2e4ad37ee6449691b39314b5925a27
430fd4d18d22d0704db1c4a1037d8e1664bfc003c244650cb7538dbe7c3be63e
43f4ca1c7474c0476a42d937dc4af01c8ccfc20331baa0465ac0f3408f52b2e2
46aac6bf94551c259b4963157e75073cb211310e2afab7a1c0eded8a175d0a28
4fa213970fdef39d2506a1bd4f05a7ceee191d916b44b574022a768356951a23
57e9e1e3ebd78d4878d7bb69e9a2b0d0673245a87eb56cf861c7c548c4e7b457
6464cdbfddd98f3bf6301f2bf525ad3642fb18b434310ec731de08c79e933b3e
67b5b54c85e7590d81a404d6c7ea7dd90d4bc773785c83b85bcc82cead60c37
700f1afeb67c105760a9086b0345cb477737ab62616fd83add3f7adf9016c5e5
77dc705cecbc29089c8e9eea3335ba83de57a17ed99b0286b3d9301953a84eca
7b8d4b1ab46f9ad4ef2fd97d526e936186503ecde745f5a9ab9f88397678bc96
7ea83cca00623a8fdb6c2d6268fa0d5c4e50dbb67ab190d188b8033d884e4b75
8d911ef72bdb4ec5b99b7548c0c89ffc8639068834a5e2b684c9d78504550927
92d2488e401d24a4bfc1598d813bc53af5c225769efedf0c7e5e4083623f4486
941fa9119eb1413fdd4f05333e285c49935280cc85f167fb31627012ef71a6b3
95b9c9bf8fa3874ad9e6204f408ce162cd4ae7a8253e69c3c493188cb9d1f4da
97105ed172e5202bc219d99980ebbd01c3dfd7cd5f5ac29ca96c5a09caa8af67
9d508074a830473bf1dee096b02a25310fa7929510b880a5875d3c316617dd50

Suspected MintsLoader:

d738eef8756a03a516b02bbab0f1b06ea240efc151f00c05ec962d392cfdadb93
77bd80e2a7c56eb37a33c2a0518a27deb709068fdc66bd1e00b5d958a25c7ad8
ccdf82b45b2ee9173c27981c51958e44dee43131edfbce983b6a5c146479ac33

Appendix B — Mitre ATT&CK Techniques

Tactic: Technique

ATT&CK Code

Resource Development: Acquire Infrastructure: Domains

T1583.001

Resource Development: Acquire Infrastructure: Virtual Private Server

T1583.003

Resource Development: Acquire Infrastructure: Server

T1583.004

Resource Development: Compromise Infrastructure: Domains

T1584.001

Resource Development: Develop Capabilities: Malware

T1587.001

Initial Access: Stage Capabilities: Drive-by Target

T1608.004

Defense Evasion: Impersonation

T1656

