



# Exposing the New Potential Ways Royal Ransomware Gets Delivered

## Table of Contents

1. [Executive Report](#)
2. [Appendix: Sample Domains](#)

## Executive Report

DEV-0569, a threat actor Microsoft has been monitoring, was [recently observed](#) deploying Royal ransomware via pages posing as legitimate software download sites and repositories, among other stealthy tactics. He has so far used fake download sites for Adobe Flash Player, AnyDesk, Zoom, and TeamViewer in phishing emails and domains.

WhoisXML API researchers built on a cybersquatting domain tagged by Microsoft as an indicator of compromise (IoC). We also looked at cybersquatting properties targeting impersonated software. Our study comprises three parts:

- **IoC expansion:** We found 3,100+ potential artifacts or domains connected to a Royal ransomware IoC.
- **Artifact analysis:** We analyzed the artifacts and found that more than 1% were malicious and continued to host or redirected to questionable websites.
- **Malicious property investigation:** We discovered five unredacted email addresses used to register some of the malicious connected domains. These email addresses were also used to register 387 domains.

## IoC Expansion

From the single malicious domain Microsoft cited, we uncovered 3,126 domains connected through WHOIS record details and string usage. We discussed these in detail in the next section.



## Uncovering WHOIS-Connected Artifacts

Microsoft's report only provided anydeskos[.]com as an example of an attacker-created domain impersonating AnyDesk, whose official domain is anydesk[.]com. A [WHOIS lookup](#) for the cybersquatting domain revealed the following WHOIS information:

- **Registrar:** REGISTRAR OF DOMAIN NAMES REG.RU LLC
- **Registrant contact details:** Privacy-protected
- **Registrant city:** Moscow
- **Registrant country:** Netherlands

[Despite WHOIS data redaction](#), we found 54 connected domains by using the domain's name server, registrant city, and registrant country as search terms on [Reverse WHOIS Search](#).

Whoever is behind anydeskos[.]com is potentially on a software impersonation spree. Most artifacts were cybersquatting domains targeting AnyDesk, Slack, Fortinet, TeamViewer, Zoom, and Discord.



Additionally, about 17% of the artifacts were flagged as malicious, including those imitating AnyDesk, just like the Royal ransomware IoC.

### Threat Hunting Expansion to Include String-Connected Artifacts

The results of the IoC expansion and belief that the threat actor possibly impersonated other software prompted us to look for more domains potentially connected to the threat.



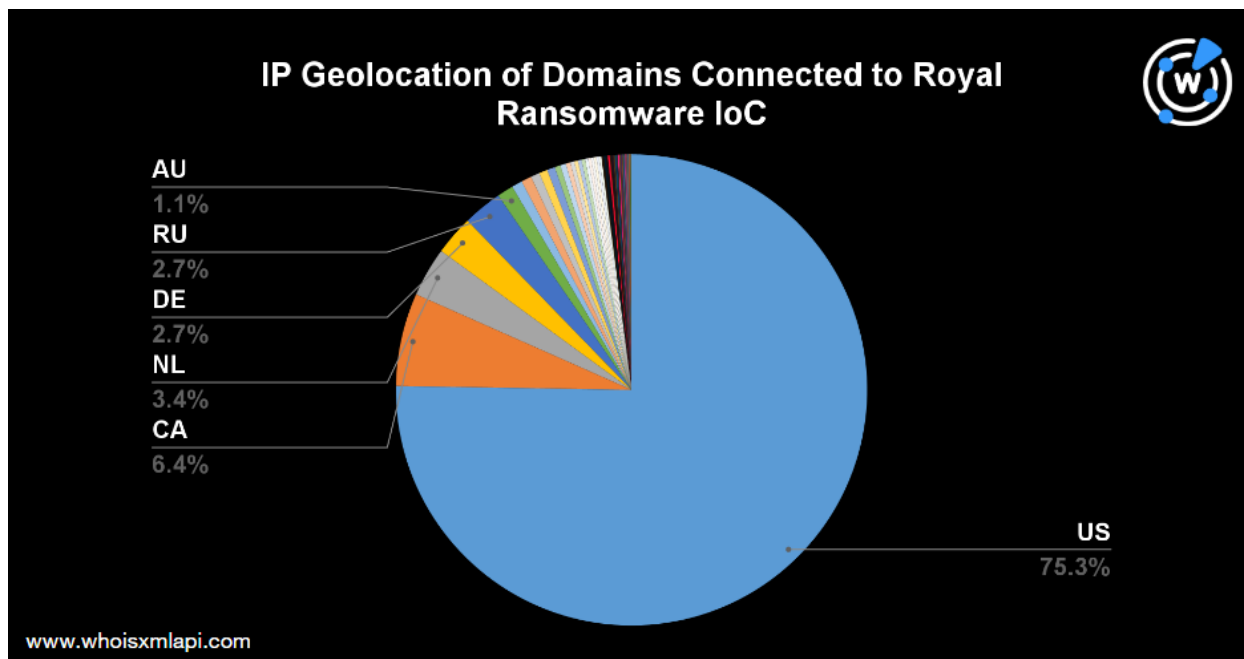
Using Domains & Subdomains Discovery, we searched for domains containing the names of impersonated software. Below is the breakdown of the cybersquatting properties added since 1 October 2022.

<b>Software</b>	<b>Search String</b>	<b>Number of Domains Added on 1 October–4 December 2022</b>
Adobe Flash Player	<i>Starts with “adobe”</i>	287
AnyDesk	<i>Contains “anydesk”</i>	69
TeamViewer	<i>Contains “teamview”</i>	17
Zoom	<i>Contains “zoom”</i>	2,701

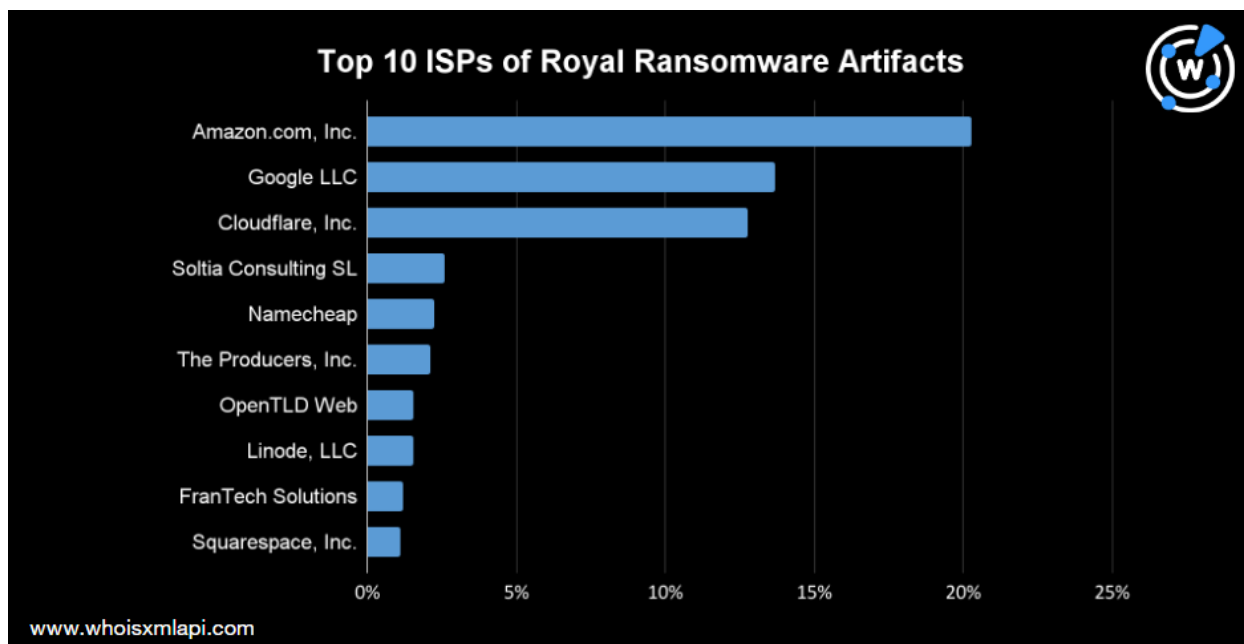
In total, we found 3,074 unique cybersquatting resources targeting the four products added in about two months. Dozens have already figured in malicious campaigns and are being detected by various malware engines.

## **Royal Ransomware Artifact Analysis**

Through DNS lookups, we discovered that about 84% of the WHOIS- and string-connected artifacts had existing IP resolutions. IP Geolocation API further revealed that most were geolocated in the U.S., as reflected in the chart below. A quarter of the resolutions could be traced to Canada, the Netherlands, Germany, Russia, Australia, and 48 other countries.



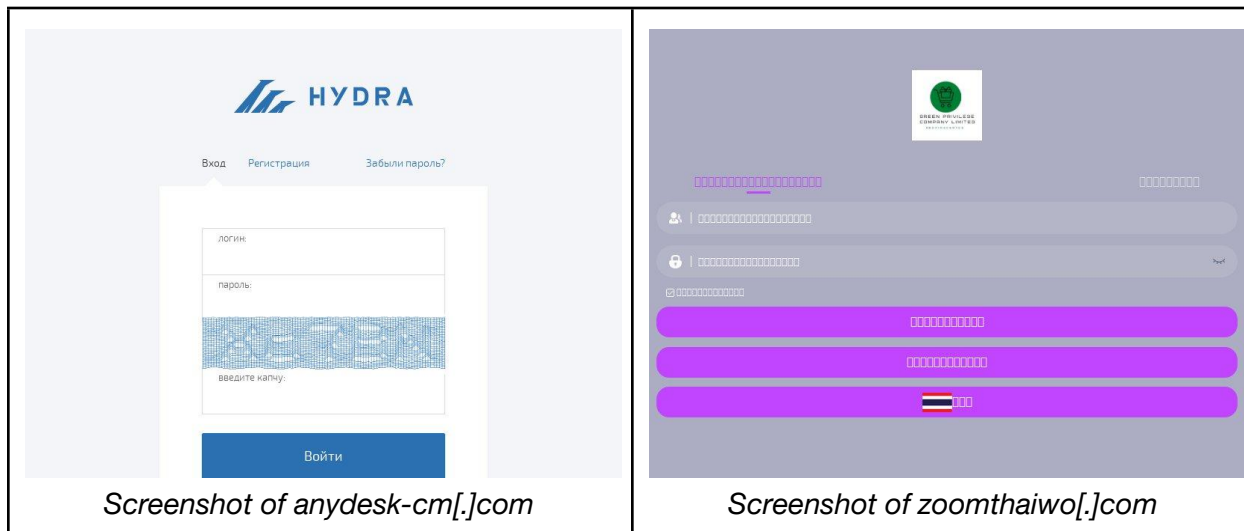
The artifacts resolved to 2,091 unique IP addresses assigned to 306 Internet service providers (ISPs) worldwide. About 20% of the IP addresses belonged to Amazon, 14% to Google, and 13% to Cloudflare. The chart below shows the top 10 ISPs of the domains connected to the IoC we're investigating.



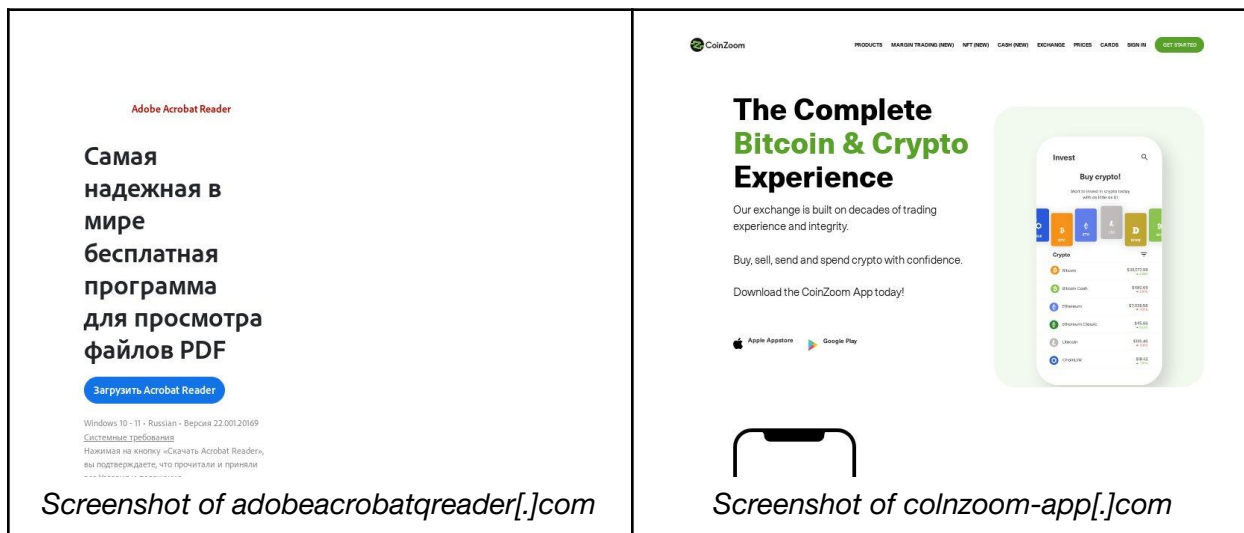


## Currently Active Malicious Artifacts

Over 1% of the artifacts we uncovered were flagged as malicious. Surprisingly, some remained active, hosting or redirecting to what might be considered suspicious web content. We provide a few examples of the malicious domains hosting login pages below.



Some content urged web visitors to use or download products.



A malicious Zoom domain appeared to warn visitors of a possible security issue with their connection.



zoom





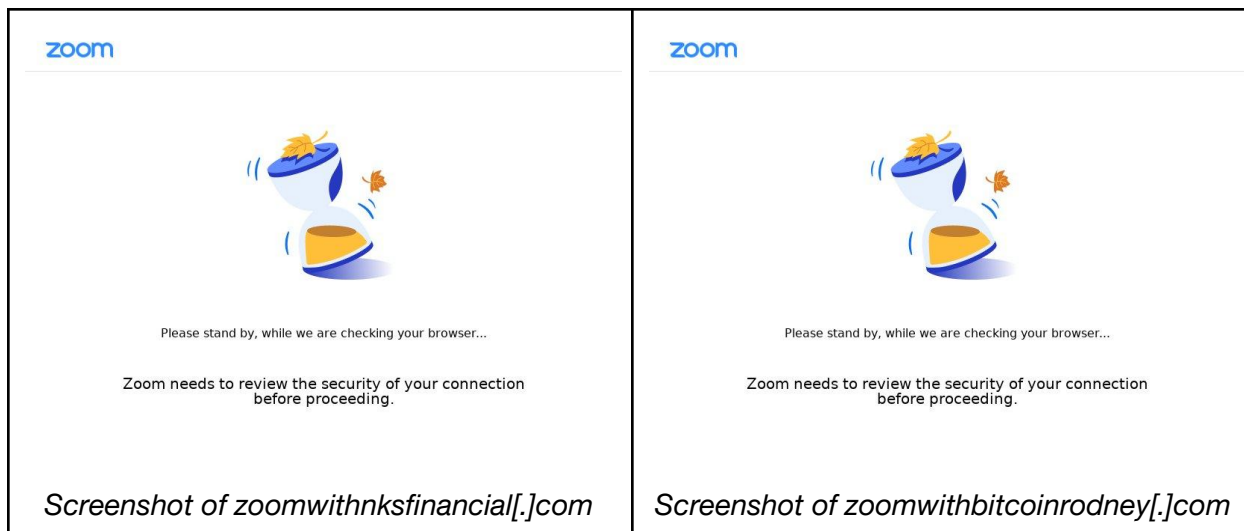
Please stand by, while we are checking your browser...

Zoom needs to review the security of your connection  
before proceeding.

*Screenshot of authoritybrandingzoom[.]live*

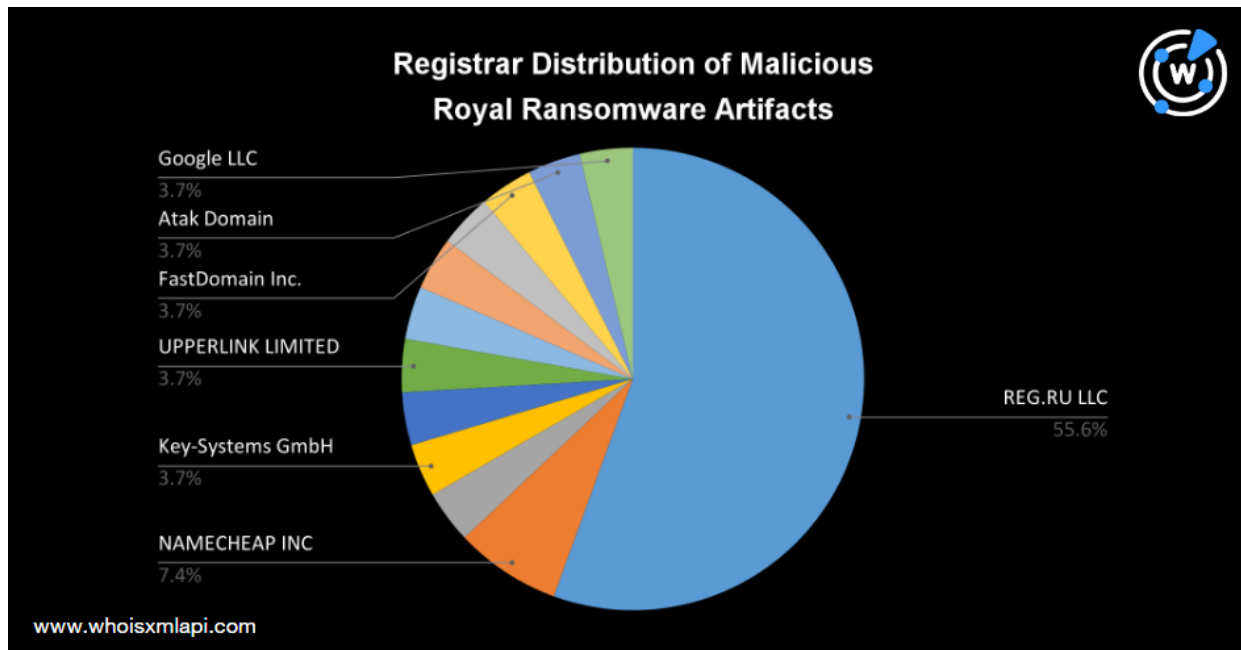
Expanding our website screenshot analysis to include connected domains that were not reported as malicious, we found that dozens behaved the same way as the Zoom-themed malicious domain. Here are a few examples.

<p>zoom</p>  <p>Please stand by, while we are checking your browser...</p> <p>Zoom needs to review the security of your connection before proceeding.</p> <p><i>Screenshot of a2azoom[.]live</i></p>	<p>zoom</p>  <p>Please stand by, while we are checking your browser...</p> <p>Zoom needs to review the security of your connection before proceeding.</p> <p><i>Screenshot of acquisitionzoom[.]com</i></p>
---	--



## Following the WHOIS Tracks of the Malicious Artifacts

We subjected the malicious artifacts to a [bulk WHOIS lookup](#) and found that most have been created only a few months ago. Moreover, more than half of them were managed by the registrar REG.RU LLC. The rest were distributed across six other registrars, including Namecheap, Google, Atak Domain, FastDomain, Upperlink, and Key-Systems GmbH.



While most of the malicious domains had redacted WHOIS records, we still found five unredacted registrant email addresses. These email addresses were used to register 387 other



domains. These digital resources may require close observation because the same people behind the malicious properties registered them.

In fact, many of the connected resources appeared to be cybersquatting domains targeting the same websites as the Royal ransomware threat actors, specifically AnyDesk, TeamViewer, and Adobe. They also contained potentially deceptive words, such as “login” and “app,” and finance-themed text strings like “trading,” “bbva,” and “expensify.”



The threat actors behind Royal ransomware are targeting corporations and demanding payments amounting to as much as [US\\$2 million](#). Once the malware encrypts files and appends the .royal extension to their names, there may be no turning back from the financial and reputational losses the attack causes.

Exposing as many ransomware delivery vehicles as possible, like the artifacts we uncovered in this study, is critical in protecting organizations and the general public against the threat.

***If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to [contact us](#).***





## Appendix: Sample Domains

### Sample Connected Domains Sharing the IoCs' WHOIS Data

- abvdg[.]com
- taqagasstorage[.]com
- documenscloud[.]com
- algvs[.]com
- anydeskv[.]com
- anydeskr[.]com
- baltiyskterminals[.]com
- anydesk-s[.]com
- anyclouddesk[.]com
- anydesko[.]com
- anydeskis[.]com
- cloudsslack[.]com
- logcloudmein[.]com
- teamviewclous[.]com
- staroness[.]com
- programmbatchcheck[.]com
- getgreenone[.]com
- fortinetq[.]com
- fidelyclouds[.]com
- teamviewclouds[.]com

### Sample Cybersquatting Domains Targeting Products Impersonated in Royal Ransomware Campaigns

- adobeaffirm[.]online
- adobeafoundation[.]org
- adobearab[.]ws
- adobecoldfusion[.]cf
- adobedesign[.]me
- adobeforbeckett[.]co[.]uk
- adobeillustratordownload[.]com
- adobeinc[.]in
- adobeindesign[.]ir
- adobemaxlandingpage[.]com
- adobemaxstudi[.]com
- adobemaxwebfrance[.]fr
- adobenewark[.]online
- adobeoverlanding[.]com
- adobe-page-cabarrus-k12-nc-us-au  
th[.]gq
- adobepizzaparty2[.]com
- adobesantaexperience[.]com
- adobese[.]co[.]za
- adobesigm[.]com
- adobe-sign-authentication[.]gq
- adobe-sign-oauth[.]gq
- adobetmcdn[.]net
- adobetonysusu[.]tk
- adobetunic[.]online
- adobeturvy[.]site
- adobevellum[.]site
- adobeyokel[.]site
- anyanydesk[.]link
- anydesk[.]au
- anydesk[.]itd
- anydesk[.]lv
- anydesk[.]rs
- anydesk[.]ws
- anydesk24[.]com
- anydesk-app[.]cf



- anydesk-app[.]ga
- anydesk-app[.]gq
- anydeskapp[.]info
- anydesk-app[.]ml
- anydesk-app[.]tk
- anydeskbo[.]site
- anydeskh[.]com
- anydeskis[.]com
- anydeskla[.]site
- anydeskli[.]link
- anydesko[.]tech
- anydeskse[.]com
- anydeskst[.]com
- anydeskte[.]site
- anydeskuk[.]com
- anydeskweb[.]net
- appanydesk[.]info
- cloudsteamview[.]com
- exploreteamviewer[.]com
- izoom[.]au
- lezoom[.]cn
- myanydesk[.]ru
- openteamviewer[.]com
- teamviewclous[.]com
- teamvieweddcsstore[.]org
- teamviewer[.]au
- teamviewerda[.]site
- teamviewergames[.]com
- teamviewerma[.]site
- teamviewer-rnd[.]com
- teamviewerrtw[.]com
- teamviewersusinc[.]com
- teamviewertaiwan[.]com
- teamviewertw[.]com
- teamviewerum[.]site
- teamviewlimitedoffer[.]com
- winningteamview[.]com
- xn--anydek-0jb[.]com
- xn--anydsk-l4a[.]com
- zoom[.]art
- zoom2u[.]nz
- zoom8[.]ru
- zoomag[.]be
- zoomas[.]ir
- zoome[.]ch
- zoomed[.]cf
- zoomieszoomieszoomies[.]com
- zoomin4zoomies[.]com
- zoomin4zoomies[.]net
- zoomin4zoomies[.]org
- zoomj[.]tk
- zoomr[.]top
- zoomy[.]at
- zoomy[.]ml
- zoom-zoom[.]ch
- zoomzoom-eg[.]com
- zoomzoomfoto[.]com
- zoomzoomkare[.]cf
- zoomzoommacaron[.]com
- zoomzoommacaroon[.]com
- zoomzoomsmoke[.]com
- zoomzoomwebsites[.]com
- zoomzoomzinger[.]com
- zoomzoomzoom[.]cn
- zzoom[.]ml

## Sample IP Addresses to which the Artifacts Resolved

- 199[.]115[.]116[.]43
- 2a00:f940:2:2:1:1:0:136
- 37[.]140[.]192[.]158
- 2a00:f940:2:2:1:1:0:232
- 31[.]31[.]198[.]9
- 2606:4700:3033::6815:7f9
- 2606:4700:3032::ac43:9c8d
- 172[.]67[.]156[.]141



- 104[.]21[.]7[.]249
- 2606:4700:3032::6815:495e
- 2606:4700:3034::ac43:bd59
- 104[.]21[.]73[.]94
- 172[.]67[.]189[.]89
- 37[.]140[.]192[.]70
- 2606:4700:3031::ac43:a50d
- 2606:4700:3034::6815:21ac
- 172[.]67[.]165[.]13
- 104[.]21[.]33[.]172
- 188[.]172[.]236[.]218
- 2606:4700:3036::6815:5118
- 2606:4700:3036::ac43:9c75
- 172[.]67[.]156[.]117
- 104[.]21[.]81[.]24
- 198[.]54[.]116[.]235
- 2a00:f940:2:2:1:1:0:35
- 31[.]31[.]196[.]42
- 34[.]102[.]136[.]180
- 76[.]76[.]21[.]93
- 76[.]76[.]21[.]22
- 45[.]138[.]74[.]159
- 94[.]127[.]7[.]133
- 103[.]42[.]108[.]46
- 212[.]7[.]207[.]87
- 185[.]181[.]165[.]238
- 68[.]65[.]123[.]95
- 2606:4700:3034::ac43:9707
- 2606:4700:3036::6815:5a14
- 172[.]67[.]151[.]7
- 104[.]21[.]90[.]20
- 89[.]208[.]106[.]229
- 2a00:f940:2:2:1:1:0:239
- 31[.]31[.]198[.]35
- 91[.]213[.]50[.]57
- 192[.]162[.]246[.]120
- 89[.]23[.]103[.]4
- 2606:4700:3034::6815:17c
- 2606:4700:3037::ac43:8138
- 172[.]67[.]129[.]56
- 104[.]21[.]1[.]124
- 2606:4700:3031::6815:357a
- 2606:4700:3031::ac43:d4d2
- 104[.]21[.]53[.]122
- 172[.]67[.]212[.]210
- 2606:4700:3037::ac43:939d
- 2606:4700:3031::6815:b12
- 104[.]21[.]11[.]18
- 172[.]67[.]147[.]157
- 2606:4700:3034::ac43:aed0
- 2606:4700:3030::6815:37f8
- 104[.]21[.]55[.]248
- 172[.]67[.]174[.]208
- 35[.]184[.]162[.]67
- 2606:4700:3036::6815:5c4c
- 2606:4700:3035::ac43:be41
- 104[.]21[.]92[.]76
- 172[.]67[.]190[.]65
- 2606:4700:3032::ac43:d1cd
- 2606:4700:3035::6815:174f
- 104[.]21[.]23[.]79
- 172[.]67[.]209[.]205
- 2606:4700:3032::ac43:c0c4
- 2606:4700:3031::6815:31cf
- 172[.]67[.]192[.]196
- 104[.]21[.]49[.]207
- 74[.]119[.]239[.]234
- 2606:4700:3032::ac43:ab76
- 2606:4700:3033::6815:1d6d
- 104[.]21[.]29[.]109
- 172[.]67[.]171[.]118
- 34[.]28[.]104[.]223
- 2606:4700:3035::ac43:9a10
- 2606:4700:3033::6815:442
- 104[.]21[.]4[.]66
- 172[.]67[.]154[.]16
- 2606:4700:3032::6815:1dd8
- 2606:4700:3035::ac43:abde
- 172[.]67[.]171[.]222
- 104[.]21[.]29[.]216



- 2606:4700:3031::6815:194a
- 2606:4700:3030::ac43:dff5
- 104[.]21[.]25[.]74
- 172[.]67[.]223[.]245
- 2606:4700:3032::ac43:896c
- 2606:4700:3036::6815:56e3
- 172[.]67[.]137[.]108
- 104[.]21[.]86[.]227
- 31[.]31[.]198[.]109
- 2a02:4780:8:247:0:bd9:c5bd:3
- 185[.]224[.]137[.]110
- 162[.]0[.]217[.]93

## Sample Properties Flagged as Malicious During the Malware Check Dated 5 December 2022

- anydesk-cm[.]com
- anydeskofferblackfriday[.]com
- cloudsslack[.]com
- covkpuntzone[.]com
- falconzoom[.]xyz
- fidelyclouds[.]com
- foxitr[.]com
- free-anydesk-download[.]ga
- free-anydesk-download[.]tk
- logmein-cloud[.]com
- metatradere[.]com
- tctrdmkwkcm[.]com
- teamviewclouds[.]com
- teamviewertw[.]com
- tvzoomn[.]cn
- zoomambo[.]com
- zoom-panel[.]tk
- zoomsouthe[.]com
- zoom-sykgp[.]com
- zoomthaiwo[.]com

## Sample Domains Connected to the Malicious Properties via Registrant Email

- adobeacrobatqreader[.]com
- akeesfluff[.]com
- anydeska[.]com
- anydeskas[.]com
- appasplre[.]com
- aptosmartian[.]com
- asplre-app[.]com
- biliender[.]com
- bimorphsba[.]com
- blzyou[.]com
- boris-fx[.]com
- colnzoom-app[.]com
- colnzoom-login[.]com
- createpdf24[.]com
- dishpanpro[.]com
- drollporno[.]com
- erraticall[.]com
- excusingre[.]com
- exocytotic[.]com
- fomanfazz[.]com
- fommans[.]com
- gougldrive[.]com
- hwmesa[.]com
- ifgxcvaz[.]com
- line-messenger[.]com
- line-messengers[.]com
- martiaanwalit[.]com
- mavovieditor[.]com
- msiafvterberner[.]com
- msiafvterpurner[.]com



- obligatosp[.]com
- payset-app[.]com
- priapusrot[.]com
- ramp-login[.]com
- sunopse[.]com
- sushiiswaper[.]com
- teamviewercn[.]com
- team-viewercn[.]com
- teamviewerrtw[.]com
- teamviewertw[.]com
- titannsas[.]com
- ubbddd[.]com
- ufmmala[.]com
- unmeantnoi[.]com
- vulcan-offsite[.]com
- wedsfdsfas[.]com
- xcsaaawa[.]com
- youbiz-app[.]com
- youblz[.]com
- yoynmaax[.]com