WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

RedLine Stealer: IoC Analysis and Expansion

Table of Contents

Executive Report

For roughly US$100, threat actors can purchase RedLine Stealer, a malware-as-a-service (MaaS) program first detected in March 2020 that continues to wreak havoc to this day. The malware can steal information from infected devices, including autocomplete and saved information on browsers, along with the system's location, hardware configuration, and security software data.

RedLine Stealer's accessibility and scope of data theft are a deadly combination, prompting the cybersecurity community to conduct in-depth research on the malware such as CloudSEK's technical analysis.

Building on CloudSEK's research and other sources of published indicators of compromise (IoCs), WhoisXML API researchers dove into RedLine Stealer's DNS footprints. Our key findings include:

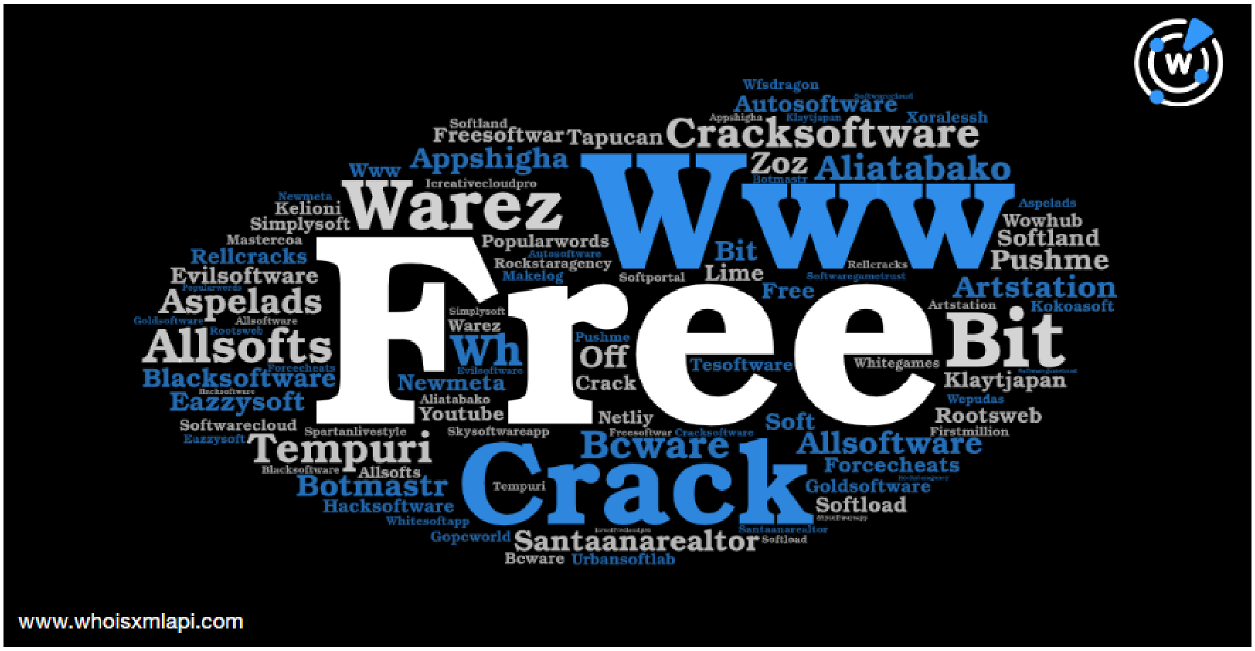
- 92% of the IoCs continue to resolve to sites
- 1,700+ artifacts connected to the threat IoCs through WHOIS details and string usage
- 700+ connected properties that share the IoCs' IP hosts
- Some artifacts targeted banks, a decentralized financial (De-Fi) platform, and a courier

RedLine Stealer IoC Analysis

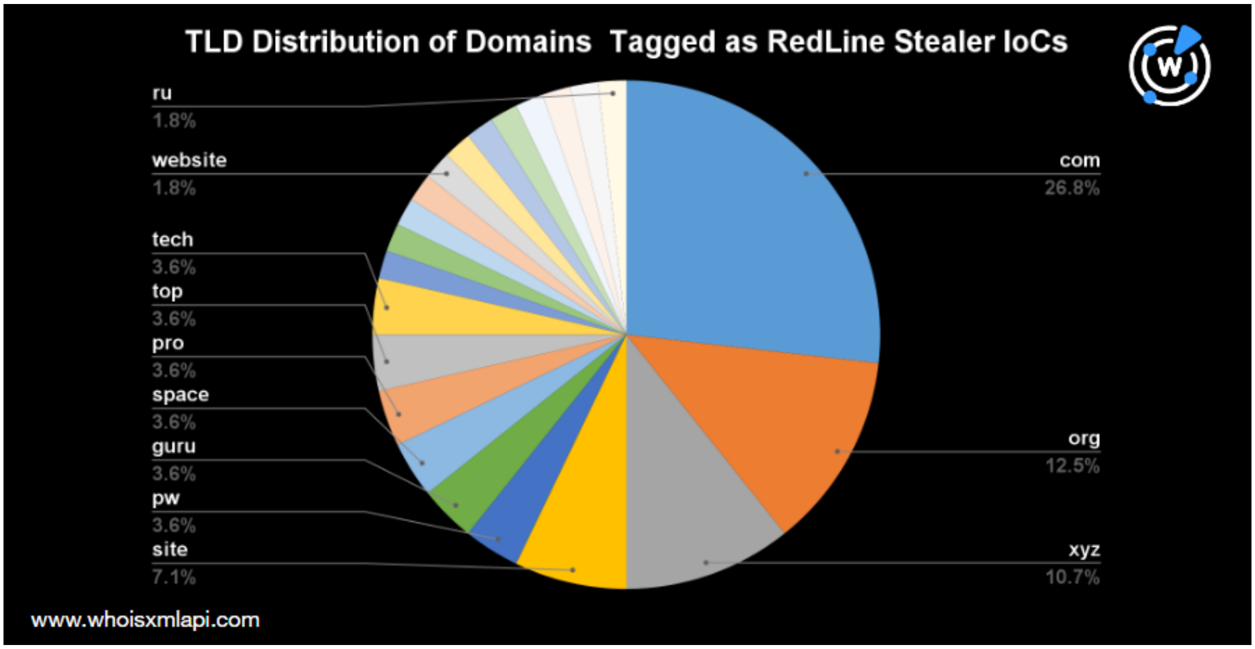
Our analysis covered 990 unique domains and IP addresses tagged as RedLine Stealer IoCs by CloudSEK and ThreatFox. We looked into their string usage, WHOIS details, IP geolocation data, and resolutions. Below are the details of our findings.

String Analysis of the IoCs

Several domains tagged as RedLine Stealer IoCs appeared to lure victims into downloading free or cracked versions of software. The word cloud below reflects that, with the most common strings used being “free,” “crack,” and “software.”



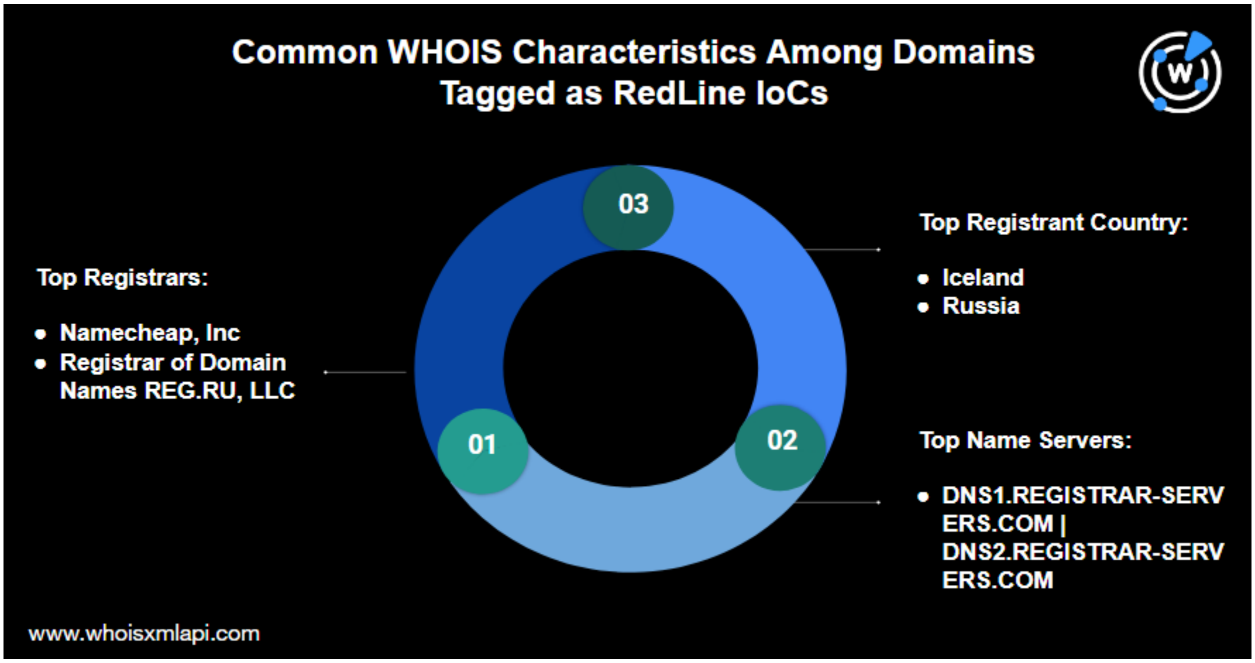
The IoCs mostly fell under the .com and .org generic top-level domain (gTLD) spaces. We also saw some new gTLDs, such as .xyz, .tech, .top, .pro, and .space, as shown in the chart below. In some cases, the threat actors registered the second-level domains (SLDs) using different TLDs. For example, the domain string “cracksoftware” appeared with .site and .space extensions.



WHOIS Characteristics of the IoCs

We ran the malicious domains on Bulk WHOIS Lookup to retrieve their complete WHOIS information. Most of them were registered with Namecheap and Reg.ru, with each accounting for 28% of the total registration.

Almost all of the domains were created between July and November 2022. We also identified the most-used name server reflected in the image below.



Common WHOIS Characteristics Among Domains Tagged as RedLine IoCs

Top Registrars:

- Namecheap, Inc
- Registrar of Domain Names REG.RU, LLC

Top Registrant Country:

- Iceland
- Russia

Top Name Servers:

- DNS1.REGISTRAR-SERVERS.COM | DNS2.REGISTRAR-SERVERS.COM

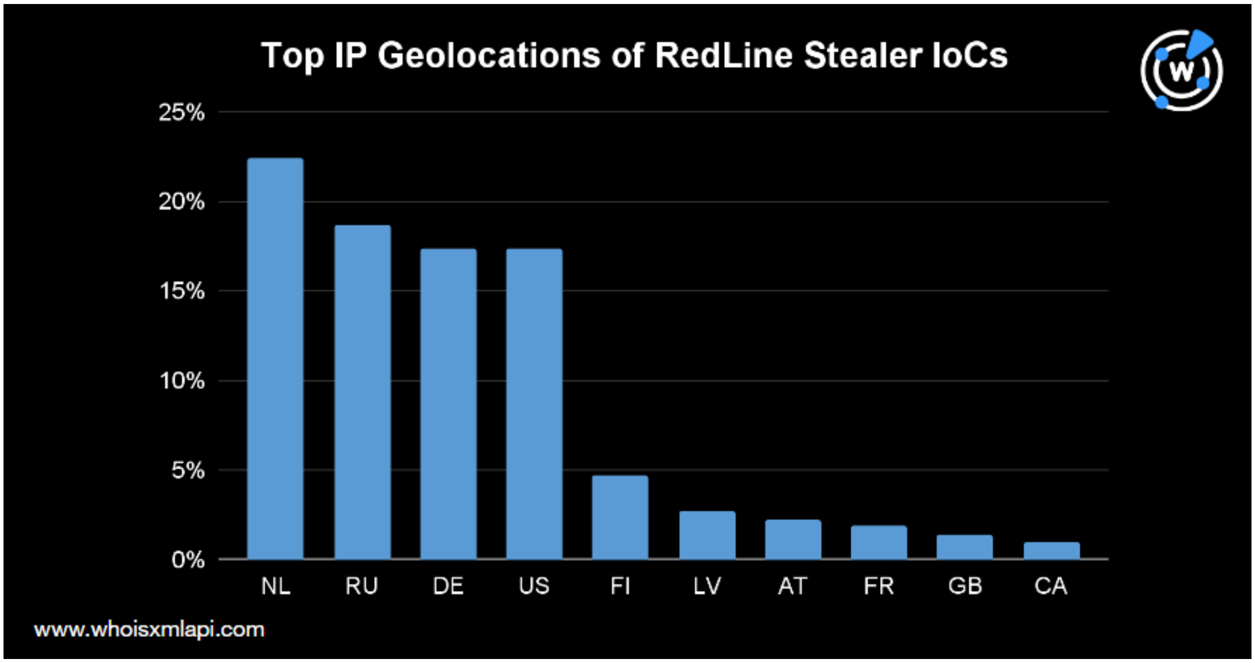
www.whoisxmlapi.com

About 31% of the IoCs were registered in Iceland and all had redacted WHOIS records protected by Withheld for Privacy EHF. Consistent with that, 84% of the domains had redacted WHOIS records. Still, we found five public registrant email addresses. We expanded these findings in later sections.

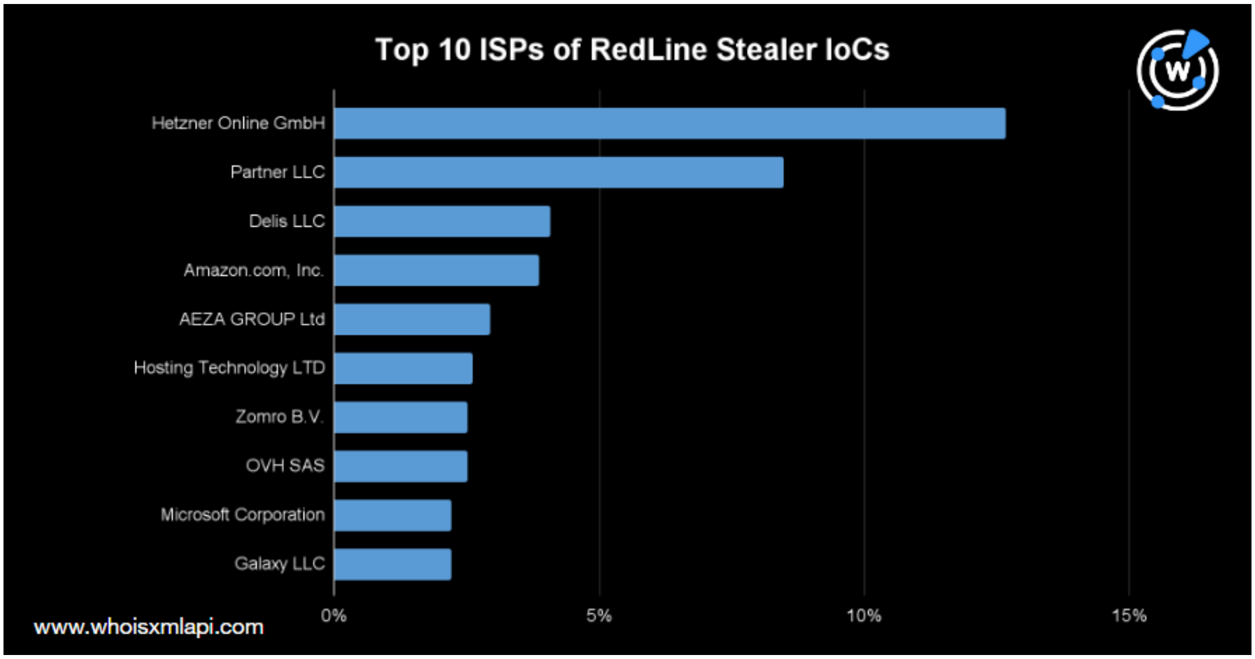
IP Geolocation Analysis

We ran all the IoCs on Bulk IP Geolocation to see how many still had IP resolutions and pinpoint their geolocations and administrators. About 92% of the RedLine Stealer IoCs currently resolved to IP addresses.

As shown in the chart below, most of the IP hosts were geolocated in the Netherlands, Russia, Germany, and the U.S.

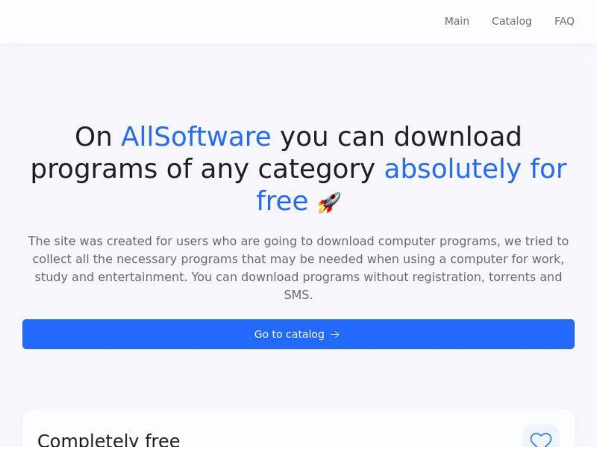


On the other hand, the top ISPs included Hetzner Online GmbH and Partner LLC, Delis LLC, Amazon.com, Inc., and 106 others. The chart below shows the top 10 ISPs.



Content Hosted on the IoCs

About half of the domains tagged as IoCs had active IP resolutions, with some still hosting or redirecting to a variety of web content. Here are a few examples.

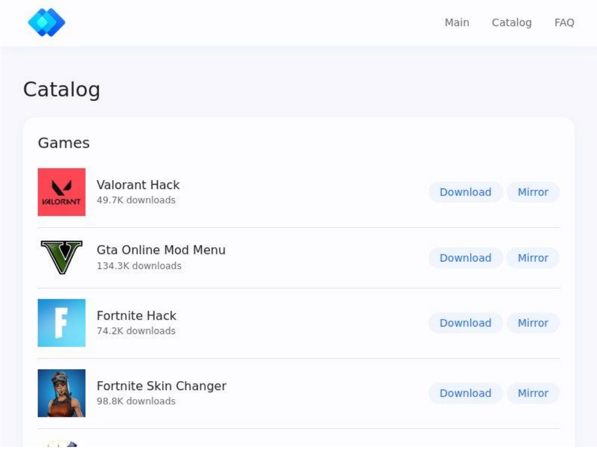


On AllSoftware you can download programs of any category absolutely for free 🚀

The site was created for users who are going to download computer programs, we tried to collect all the necessary programs that may be needed when using a computer for work, study and entertainment. You can download programs without registration, torrents and SMS.

Completely free

Screenshot of aspelads[.]com



Catalog

Games

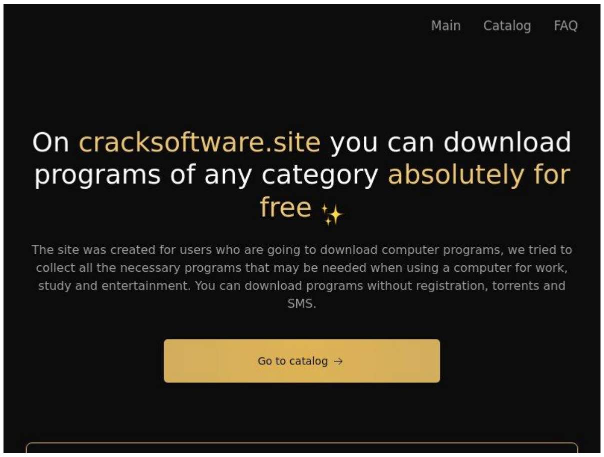
Valorant Hack
49.7K downloads

Gta Online Mod Menu
134.3K downloads

Fortnite Hack
74.2K downloads

Fortnite Skin Changer
98.8K downloads

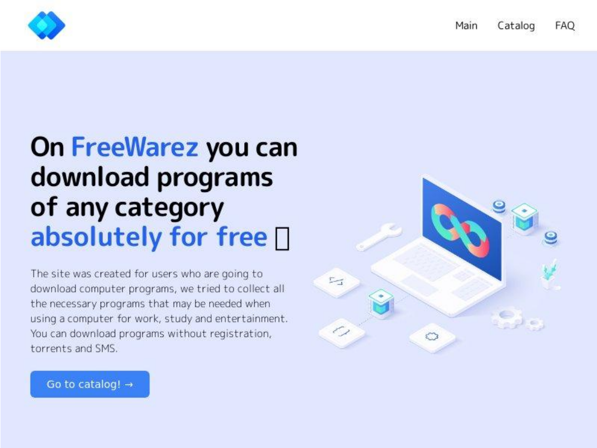
Screenshot of bcware[.]netlify[.]app



On cracksoftware.site you can download programs of any category absolutely for free ✨

The site was created for users who are going to download computer programs, we tried to collect all the necessary programs that may be needed when using a computer for work, study and entertainment. You can download programs without registration, torrents and SMS.

Screenshot of cracksoftware[.]site



On FreeWarez you can download programs of any category absolutely for free ▯

The site was created for users who are going to download computer programs, we tried to collect all the necessary programs that may be needed when using a computer for work, study and entertainment. You can download programs without registration, torrents and SMS.

Screenshot of www[.]free-warez[.]site

IoC Expansion: Uncovering Additional Suspicious Domains

WHOIS-Connected Artifacts

We used the findings from our IoC analysis to uncover more domains possibly connected to RedLine Stealer. On Reverse WHOIS, we used some of the domains' common WHOIS characteristics and text strings. These search strings were specifically used:

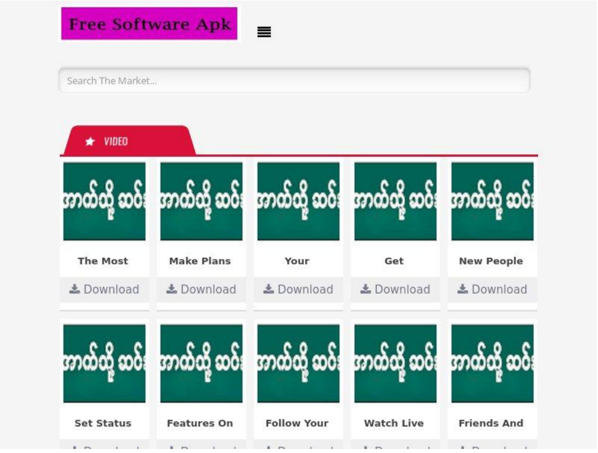
- **Registrar name:** *Starts with* Namecheap
- **Name server:** *Starts with* DNS1.REGISTRAR-SERVERS.COM
- **Creation date:** *From* 1 July–20 December 2022

Aside from these search parameters, we also specified the SLDs so the tool would only return those that contained specific string combinations. The table below shows the strings and examples of the connected domains we found. More domain samples can be found in the Appendix.

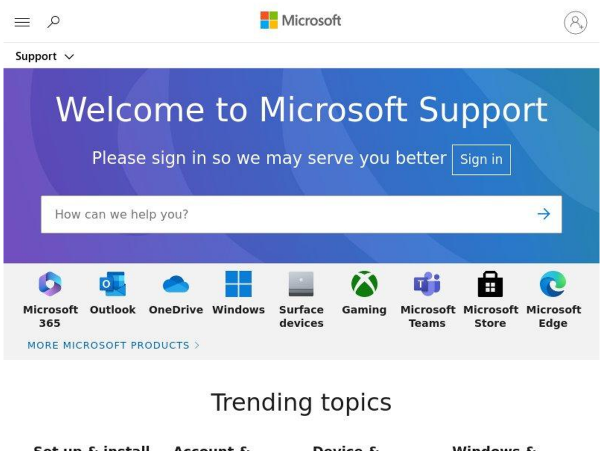
"Software"	"Crack"	"Free" + "Ware"	"Software" + "App"
● nostr[.]software ● revosoftware[.]company ● reversed[.]software ● carbonsparksoftware[.]blog ● carbonsparksoftware[.]cloud	● crackedbedwars[.]com ● pccracked[.]org ● soft-warecrack[.]store ● crack-soft-ware[.]store ● crackedprograms[.]co.uk	● freesoftwaredownload[.]net ● freewaregadgets[.]com ● freesoftwaresystem[.]com ● freesoftwareapk[.]com ● designsoftwarefree[.]com	● codeapp[.]software ● applicationsoftwaredevelopment[.]com ● vpmapping[.]software ● bootstrappedsoftware[.]partners ● softwareapp[.]online

We found 1,756 domains potentially connected to RedLine Stealer based on similar WHOIS details and string usage. While some may be legitimate software businesses, many hosted adult content and other suspicious pages.

Some examples include freesoftwareapk[.]com, which offers free software and features download buttons for each product, and softwareaktualisierung[.]live, which offers support services for Microsoft users. However, its WHOIS details can't be attributed to the imitated organization.



Screenshot of freesoftwareapk[.]com


Welcome to Microsoft Support

Please sign in so we may serve you better

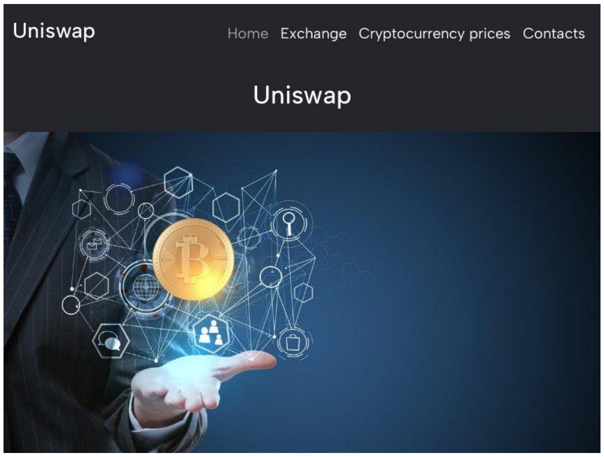
How can we help you?

Screenshot of softwareaktualisierung[.]live

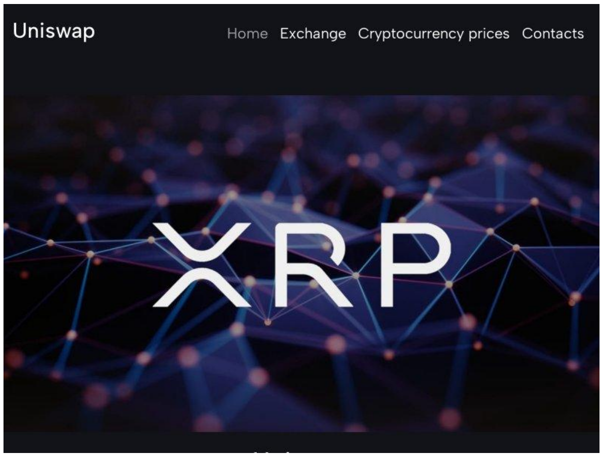
IP-Connected Artifacts

Another reliable way to find more properties connected to the threat is to look at shared IP hosts. To do that, we used Reverse IP/DNS API and found that 98% of the IP addresses tagged as RedLine Stealer IoCs had 50 or fewer resolving domains. That may indicate they were dedicated IP addresses.

We found 750 IP-connected artifacts, some of which have already figured in malicious campaigns, including cybersquatting domains targeting Canada Post, Santander Bank, Scotia Bank, and Uniswap. Alarmingly, the Uniswap-related malicious domains continued to host content as shown below.



Screenshot of uniswap[.]casa



Screenshot of uniswap[.]lv

–

Threat analysis is critical to understanding malicious actors' tactics, techniques, and procedures (TTPs). A more targeted IoC analysis can lead to suspicious and possibly dormant weapons.

By shedding light on the DNS footprints of public RedLine Stealer IoCs, we uncovered a total of 2,506 possible threat artifacts. Our analysis of the related properties shows that some have already figured in malicious campaigns, while others were suspicious.

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 Threat IoCs

- santaanarealtor[.]icu
- tempuri[.]org

- aliatabako[.]xyz
- allsofts[.]org
- allsoftware[.]cloud
- appshigha[.]com
- artstation[.]download
- aspelads[.]com
- autosoftware[.]pw
- bcware[.]netlify[.]app
- bit-lime[.]com
- blacksoftware[.]website
- botmastr[.]xyz
- crack3d[.]org
- cracked[.]guru
- cracksoftware[.]site
- cracksoftware[.]space
- eazzysoft[.]com
- evilsoftware[.]org
- forcecheats[.]pro
- free-crack-soft[.]com
- freesoftwar[.]com
- free-warez[.]site
- goldsoftware[.]org
- hacksoftware[.]fun
- icreativecloudpro[.]com
- klaytjapan[.]com
- newmeta[.]makelog[.]org
- popularwords[.]top
- pushme[.]us[.]in
- rellcracks[.]com
- rockstaragency[.]tech
- rootsweb[.]pw
- simplysoft[.]org
- skysoftwareapp[.]com
- softland-off[.]com
- softload[.]tech
- softwarecloud[.]space
- softwaregametrust[.]com
- spartanlivestyle[.]xyz
- tapucan[.]xyz
- urbansoftlab[.]com
- wh1tesoftware[.]me
- whitegames[.]wepudas[.]guru
- whitesoftapp[.]com
- www[.]free-warez[.]site
- www[.]kokoasoft[.]com
- www[.]softportal[.]online
- xoralessh[.]xyz
- youtube[.]firstmillion[.]click
- 95[.]179[.]163[.]157
- 9[.]12[.]69[.]202
- 93[.]106[.]191[.]226
- 85[.]250[.]148[.]76
- 95[.]217[.]98[.]127
- 95[.]217[.]98[.]127
- 95[.]217[.]82[.]124
- 95[.]217[.]81[.]67
- 95[.]217[.]65[.]169
- 95[.]217[.]55[.]221
- 95[.]217[.]49[.]125
- 95[.]217[.]30[.]78
- 95[.]217[.]30[.]78
- 95[.]217[.]30[.]31
- 95[.]217[.]30[.]31
- 95[.]217[.]188[.]140
- 95[.]217[.]181[.]251
- 95[.]217[.]132[.]146
- 95[.]217[.]124[.]110
- 95[.]217[.]124[.]105
- 95[.]217[.]102[.]123
- 95[.]217[.]102[.]105
- 95[.]217[.]102[.]105
- 95[.]216[.]35[.]135
- 95[.]216[.]252[.]180
- 95[.]216[.]252[.]180
- 95[.]216[.]221[.]253
- 95[.]216[.]170[.]17
- 95[.]216[.]100[.]87
- 95[.]214[.]55[.]95
- 95[.]182[.]120[.]55
- 95[.]179[.]211[.]149

- 95[.]161[.]129[.]36
- 94[.]26[.]246[.]199
- 94[.]228[.]116[.]72
- 94[.]140[.]115[.]67
- 94[.]140[.]115[.]234
- 94[.]140[.]115[.]229
- 94[.]140[.]115[.]207
- 94[.]140[.]114[.]96
- 94[.]140[.]114[.]74
- 94[.]140[.]114[.]46
- 94[.]140[.]114[.]37
- 94[.]140[.]114[.]248
- 94[.]140[.]114[.]226
- 94[.]140[.]114[.]215
- 94[.]140[.]114[.]17
- 94[.]140[.]112[.]91
- 94[.]140[.]112[.]213
- 94[.]140[.]112[.]18

Sample Domains Possibly Related to Redline Stealer IoCs

- dshdh377dsj[.]fun
- leonidhero[.]xyz
- static[.]140[.]188[.]217[.]95[.]clients[.]your-server[.]de
- 95-217-124-110[.]cprapid[.]com
- 8956[.]ru
- busy-mclaren[.]95-179-211-149[.]plesk[.]page
- 1000537-cb78435[.]tmweb[.]ru
- mail[.]proxeidon[.]com
- ruralvia-gestor[.]com
- doaisunto[.]xyz
- activity[.]stepansnigirev[.]com
- console-red[.]com
- et-system[.]one
- centaurlivenow[.]hopto[.]org
- panel[.]kultur-dialog[.]info
- online-secure-auth[.]com
- tininshassama[.]xyz
- litrazalilibe[.]xyz
- transfer-donation[.]com
- onnnieorr[.]xyz
- id-see-process[.]info
- ca-auth-post1[.]com
- holgltaseyb[.]xyz
- bensistelaer[.]xyz
- mail[.]sdbrother[.]org
- eu[.]kraken-proxy[.]ru
- hostmaster[.]tongpi[.]nl
- static[.]90[.]179[.]130[.]94[.]clients[.]your-server[.]de
- anime[.]radiostation[.]ml
- gagaga[.]ml
- 488[.]fenxiangwan[.]com
- ip15[.]ip-91-134-214[.]eu
- 1161[.]rbx[.]abcvg[.]ovh
- jamesmillion12[.]xyz
- caketomorrow[.]xyz
- beatefrei[.]de
- 19234-33045[.]bacloud[.]info
- 18285-33003[.]bacloud[.]info
- account-onlinescotia[.]com
- ciseyabmail[.]biz
- 85-239-53-56[.]cprapid[.]com
- chardhesha[.]xyz
- mail[.]fansbuddy[.]homes
- v1[.]gracebc[.]cc
- jamesmillion5[.]xyz
- 1026203-cq63315[.]tmweb[.]ru
- hilds[.]ru
- manymoneyrr[.]com
- mail[.]uyzrtk[.]top
- vm3186045[.]33ssd[.]had[.]wf
- appshigho[.]com
- astra-5[.]info
- nostr[.]software

- revosoftware[.]company
- reversed[.]software
- carbonsparksoftware[.]blog
- carbonsparksoftware[.]cloud
- stoned[.]software
- hive[.]software
- formula1software[.]com
- softwarenerdalert[.]com
- spk[.]software
- picklesoftware[.]dev
- archwaysoftware[.]net
- softwarenerdx[.]com
- nebxsoftware[.]io
- writingabout[.]software
- 155[.]software
- forged[.]software
- leah[.]software
- compareaisoftware[.]com
- updatessoftware[.]com
- aisoftwarecompare[.]com
- brainsoftwarehouse[.]com
- freemarketing[.]software
- maxsoftware[.]icu
- understand[.]software
- legacycode[.]software
- flowrix[.]software
- fluorix[.]software
- softwaretips[.]blog
- justfinesoftware[.]com
- energydesignsoftware[.]com
- tenoaksoftware[.]com
- softwareandrobotics[.]com
- roboticsandsoftware[.]com
- mysoftwarebiz[.]net
- mobilesoftwareshop[.]com
- sitelinesoftware[.]com
- softwareengineeringconsultantsinchardware[.]online
- best-ai-software[.]online
- tradingveiew-software[.]com
- 199[.]software
- serpentsoftware[.]com
- zach[.]software
- 2ksidehustles[.]software
- audacity-software[.]co
- rufus-software-download[.]live
- kreamsoftware[.]com
- bestemailsoftwares[.]com

Sample Properties Flagged as Malicious During the Malware Check Dated 20 December 2022

- auth-scotiaonline-users[.]com
- gutschrift-beantragen[.]com
- smtp[.]c9vhnwpuec[.]xyz
- sonalact[.]com
- san[.]tan[.]der[.]personalmifirma[.]com
- uniswap[.]casa
- postcanada-attempteddelivery3[.]com