The New RisePro Version in the DNS Spotlight

Table of Contents

Executive Report

RisePro, a malware-as-a-service data stealer, has been plaguing users since 2022. ANY.RUN recently discovered and analyzed its latest version in great depth and identified 10 indicators of compromise (IoCs)—three domains and seven IP addresses.

In a bid to make the Internet safer and more transparent, the WhoisXML API research team expanded the current IoC list to find other connected threat artifacts. Our comprehensive DNS intelligence sources found:

- 849 email-connected domains, 52 of which turned out to be malicious
- Two additional IP addresses, one of which turned out to be malicious
- 59 IP-connected domains, 18 of which turned out to be malicious
- 14 string-connected domains

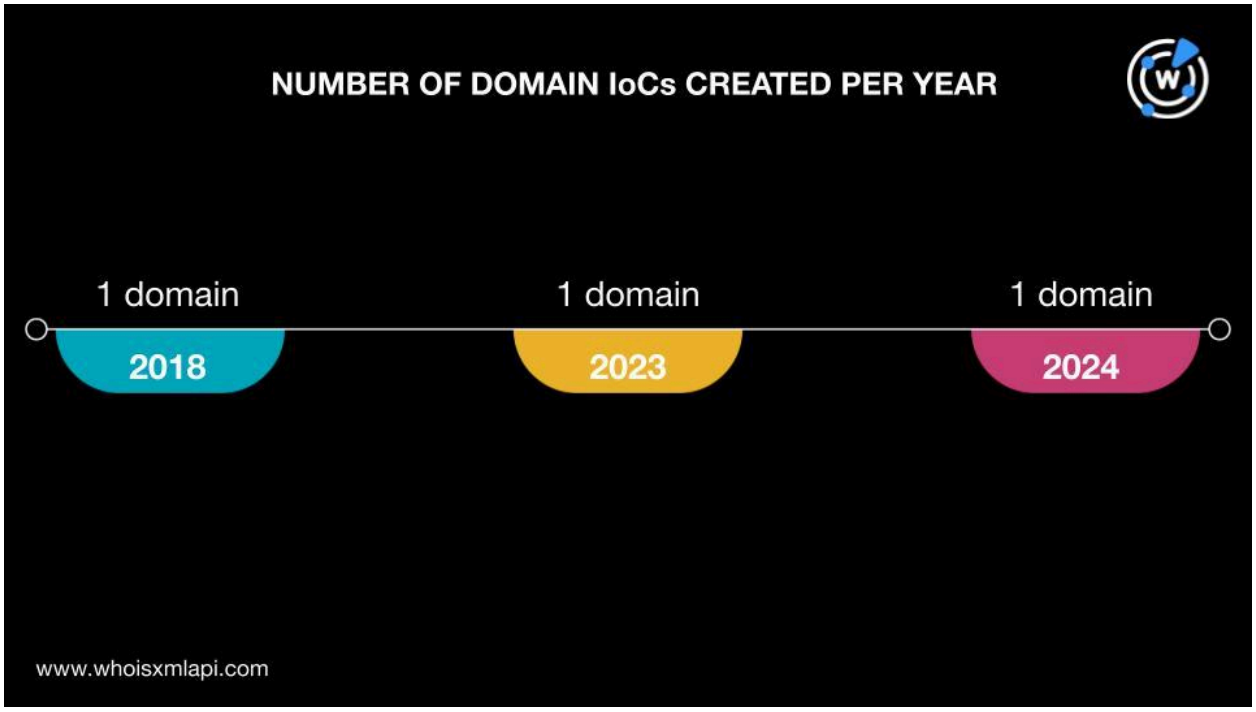
A sample of the additional artifacts obtained from our analysis is available for download from our website.

RisePro IoC Facts

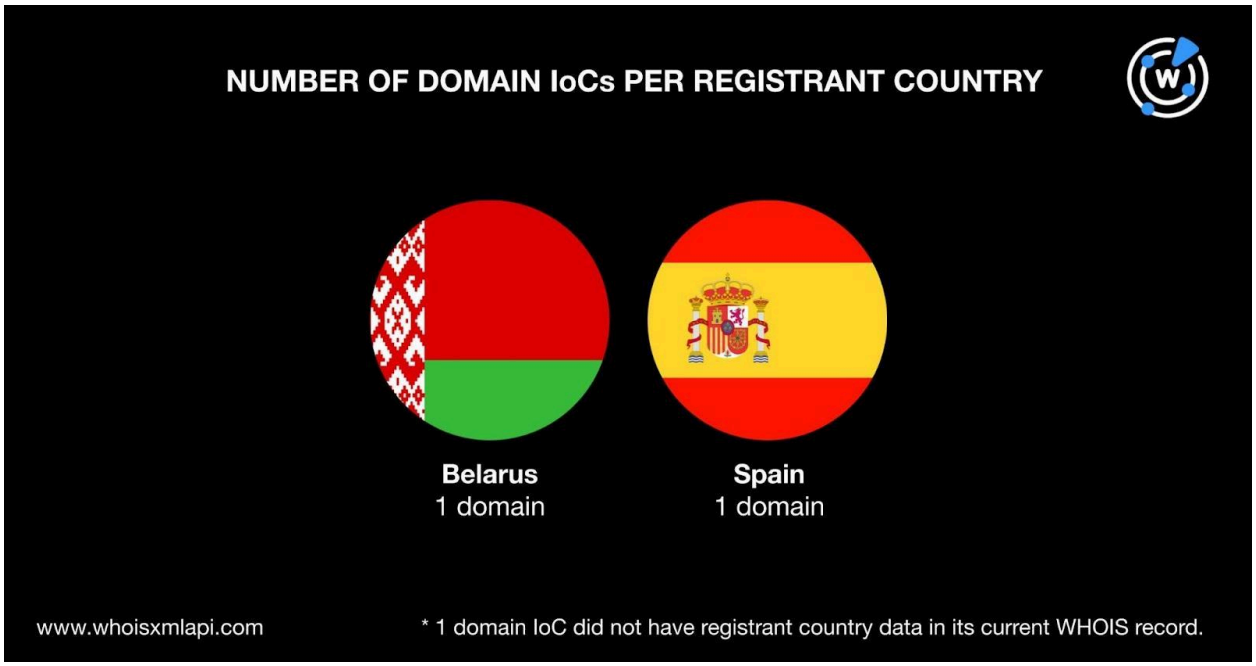
We began our analysis by looking more closely at the RisePro IoCs.

A bulk WHOIS lookup for the three domains identified as IoCs led to these discoveries:

- Each domain was administered by a different registrar—chainventures[.]co[.]uk by 1api GmbH, ads-strong[.]online by NiceNIC International Group Co. Limited, and ontopothers[.]com by OwnRegistrar, Inc.
- Each domain was also created in a different year—chainventures[.]co[.]uk in 2018, ads-strong[.]online in 2023, and ontopothers[.]com in 2024.

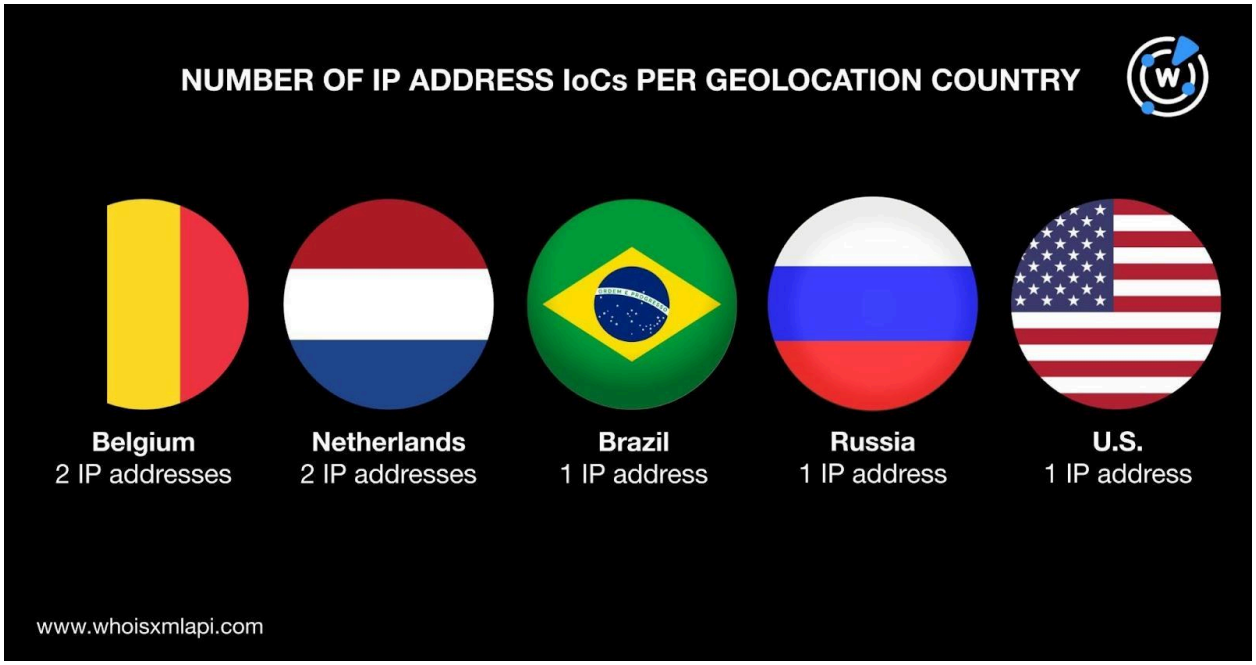


- Only two of the domains had registrant countries in their current WHOIS records—ads-strong[.]online was supposedly created in Belarus and ontopothers[.]com in Spain.

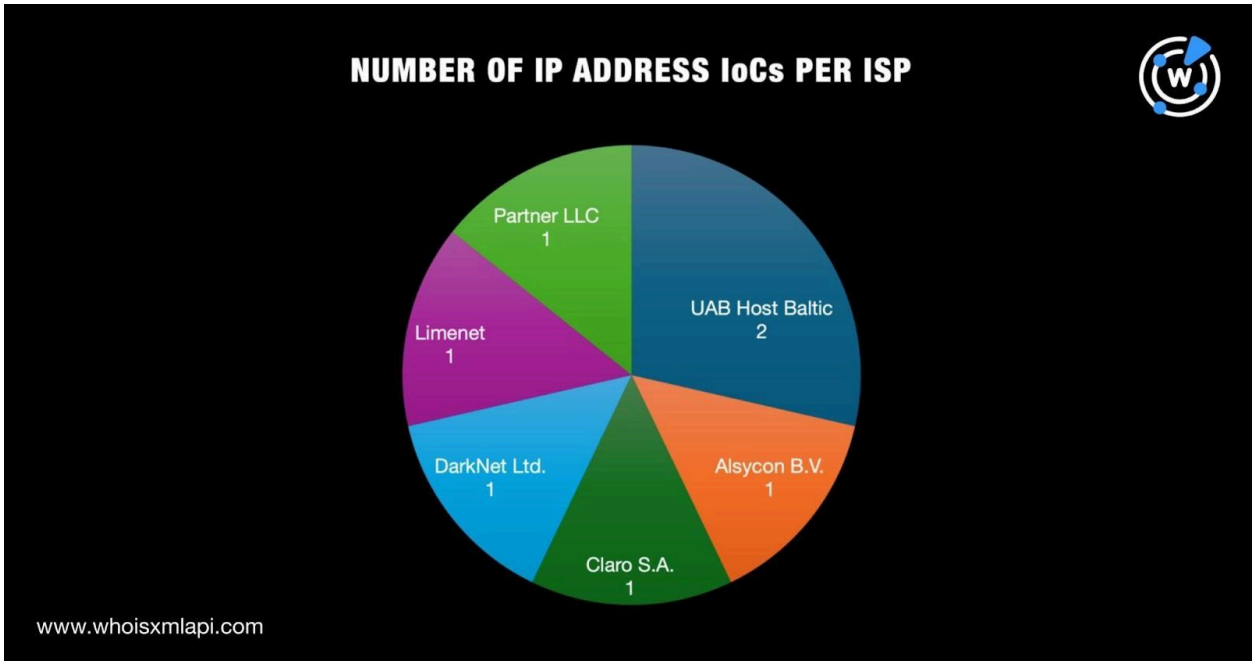


A bulk IP geolocation lookup for the seven IP addresses tagged as IoCs, meanwhile, led to these findings:

- They were spread across five geolocation countries—two each in Belgium and the Netherlands and one each in Brazil, Russia, and the U.S. None of the IP geolocations matched the domain IoCs' registrant countries.



- They were administered by six ISPs led by UAB Host Baltic, which accounted for two IP addresses. One IP address each was administered by Alsycon B.V., Claro S.A., DarkNet Ltd., Limenet, and Partner LLC.



RisePro IoC List Expansion Results

To find other connected artifacts, we first looked for email addresses in the historical WHOIS records of the three domains identified as IoCs using WHOIS History API. Our search turned up one unredacted email address.

A Reverse WHOIS API query for the single unredacted email address led to the discovery of 849 email-connected domains after duplicates and those already identified as IoCs were removed.

Threat Intelligence API showed that 52 of them were associated with malware distribution, phishing, or generic attacks. Take a look at the detailed results for five malicious email-connected domains below.

EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT TYPE
aavenetworks[.]com	Phishing
confirmation-setup[.]com	Malware
dao-aave[.]com	Phishing
jatep-raw[.]net	Malware
santander-odnowienie[.]com	Generic

It's also interesting to note that several of the email-connected domains could be used to target banks, cryptocurrency exchanges, postal service providers, social networks, email service providers, and tech giants, especially since none of them could be publicly attributed to the banks based on WHOIS record detail comparisons. Take a look at detailed WHOIS Lookup result comparisons for five potential typosquatting domains below.

MIMICKED BANK	LEGITIMATE DOMAIN	TYPOSQUATTING DOMAIN	WHOIS RECORD DETAIL	
			LEGITIMATE DOMAIN	TYPOSQUATTING DOMAIN
Facebook	facebook[.]com	facebook-secured[.]com	**Registrant organization:** Meta Platforms, Inc.	**Registrant organization:** No data
Gmail	gmail[.]com	gmail-sakerhet[.]com	**Registrant organization:** Google LLC	**Registrant organization:** Sahari Muti, Inc.
Microsoft	microsoft[.]com	microsoftsupdates-live[.]com	**Registrant organization:** Microsoft Corporation	**Registrant organization:** No data
HSBC	hsbc[.]com	livechathsbc[.]net	**Registrant organization:** HSBC	**Registrant organization:** Sahari Muti, Inc.
DHL	dhl[.]com	post-dhl-server[.]com	**Registrant organization:** Deutsche Post AG	**Registrant organization:** No data

Next, we subjected the three domains classified as IoCs to DNS lookups that gave us two additional IP addresses not included in the current IoC list.

IP geolocation lookups for the two additional IP addresses revealed that:

- They were geolocated in two different countries—62[.]204[.]41[.]98 in Russia and 82[.]165[.]193[.]159 in France. Only one (62[.]204[.]41[.]98) was consistent with an IP address IoC in terms of geolocation country.
- Each IP address was also administered by a different ISP—62[.]204[.]41[.]98 by Horizon LLC and 82[.]165[.]193[.]159 by IONOS SE. None of them shared any of the IoCs' ISPs.

Threat Intelligence API also showed that 62[.]204[.]41[.]98 was associated with cyber attacks, generic threats, malware distribution, and spam campaigns.

Reverse IP lookups for the nine IP addresses (IoCs and additional IP resolutions combined) showed that only two could be dedicated—62[.]204[.]41[.]98 and 82[.]165[.]193[.]159. Altogether, they hosted 59 domains after duplicates, those already tagged as IoCs, and those that were email-connected were filtered out.

Threat Intelligence API revealed that 18 of the IP-connected domains were associated with malware distribution. The text string **ads-** appeared in all of them, which could hint at their use in malvertising campaigns specifically.

To cover all our bases, we searched for other domains that contained these text strings found among two domains identified as IoCs:

- **ads-strong**
- **chainventures**

Domains & Subdomains Discovery searches using the **Starts with** parameter provided us with 14 string-connected domains.

—

Our in-depth analysis of the RisePro IoCs led to the discovery of 924 connected artifacts comprising 922 domains and two IP addresses. Note, too, that 71 of them were associated with various threats. Several email-connected domains could also be weaponized (if they haven't been already) for attacks targeting banks, cryptocurrency exchanges, postal service providers, social networks, email service providers, and tech giants.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to contact us.

Disclaimer: *We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts

Sample Email-Connected Domains

- 0-sparkasse[.]com
- 0p-asiakaspalvelu[.]com

- 0p-etusivu-fi[.]com
- 0p-fi[.]com
- aave-survey[.]net
- aavenetworks[.]com
- aaveportal[.]net
- abanca-acceso-empresas[.]com
- abanca-empresas[.]net
- abuse-preventioncustomers[.]com
- acc-fl[.]com
- acc-ld[.]com
- adsgpolicy[.]com
- ag-post[.]com
- aiblivechat[.]com
- airdrop-chatgpt[.]com
- airdropshunt[.]com
- airpad-uniswap[.]com
- aktualiserensp[.]com
- aktualiserenspk[.]com
- aktualisierenspk[.]com
- alertas-interbank[.]com
- alpha-secured[.]com
- alpha-securely[.]com
- alrdrop-jup[.]com
- altinnlogin-no[.]net
- alunter[.]com
- alurter[.]com
- aluxder[.]com
- apetreasury[.]com
- apollox-finance[.]com
- app-bancochile[.]com
- app-revokecash[.]net
- app-vahvistaa[.]com
- applivechat[.]com
- apply-moonpay[.]com
- arbitrum-survey[.]com
- arbitrum-survey[.]net
- arbitrum-task[.]com
- arbportal[.]net
- area-credem[.]com
- arkhamintelilgence[.]com
- arkxinvest[.]com
- artblocks-curated[.]net
- artblocks-explorations[.]net
- artblocks-io[.]com
- asb-renewal[.]com
- augovsupport-notifications[.]com
- aunetos[.]com
- aupostal-service[.]com
- auspostdelivery-com-au[.]net
- authid-uap[.]com
- authserver-au[.]com
- autoscout-24-verification[.]com
- aviso-montepio[.]com
- avisos-bancochile[.]com
- avisos-interbank[.]com
- avisos-netcash-empresas[.]com
- avisos-scotiabank[.]com
- balancer2024[.]com
- bancosabadell-seguridad-movil[.]com
- bank-livechat[.]com
- bankid-norway[.]com
- banklivechat[.]com
- banquepopulaire-alerter[.]com
- barclaysalert[.]net
- barclayshelp[.]net
- barclayshelpchat[.]com
- barclaysiportal[.]net
- barclayslivechat[.]com
- barclayslivechat[.]net
- barclaysportal[.]net
- bbva-app-movil[.]com
- bbva-app-seguridad[.]com
- bbva-empresas-movil[.]com
- bbva-es-app[.]com
- bbva-movil-app[.]com
- bbva-netcash-empresas[.]com
- bbvanetcash-empresas[.]net
- beta-aave[.]com
- betal-gothia[.]net

- betale-klarna[.]net
- betalgothiainfo[.]net
- betalingsinfogothia[.]net
- betalsis[.]net
- binance-mbox[.]com
- binance-nft-award[.]com
- binance-nft-awards[.]com
- binance-nft-prize[.]com
- binance-nft-promo[.]com
- binance-nft-reward[.]com
- binance-nft-wheel[.]com
- blur-protocol[.]com
- blurcarepackage[.]com
- blurclaimportal[.]com
- blurpackageclaim[.]com
- blurpool[.]net
- bmo-activity-decline[.]com
- bnl-bnpparibas[.]com
- bnz-devicechk[.]com

Sample Malicious Email-Connected Domains

- aavenetworks[.]com
- airpad-uniswap[.]com
- app-bancochile[.]com
- app-revokecash[.]net
- aviso-montepio[.]com
- avisos-bancochile[.]com
- betal-gothia[.]net
- betalgothiainfo[.]net
- betalingsinfogothia[.]net
- coba-verifizierung[.]com
- commerz-alert[.]com
- commerz-alert[.]net
- confirmation-setup[.]com
- dao-aave[.]com
- dashboard-aave[.]net
- doc-opensea[.]com
- enter-aave[.]com
- gothiainfo[.]net
- gov-servicesau[.]com
- helpiportal[.]com

Sample IP-Connected Domains

- acidrobots[.]io
- ads-analyze[.]online
- ads-analyze[.]site
- ads-analyze[.]top
- ads-analyze[.]xyz
- ads-change[.]online
- ads-change[.]site
- ads-change[.]top
- ads-change[.]xyz
- ads-eagle[.]top
- ads-eagle[.]xyz
- ads-moon[.]top
- ads-moon[.]xyz
- ads-pill[.]top
- ads-pill[.]xyz
- ads-star[.]online
- ads-star[.]site
- ads-star[.]top
- ads-star[.]xyz
- ads-strong[.]site

Sample Malicious IP-Connected Domains

- ads-analyze[.]online
- ads-analyze[.]site
- ads-analyze[.]top
- ads-analyze[.]xyz

- ads-change[.]online
- ads-change[.]site
- ads-change[.]top
- ads-change[.]xyz
- ads-star[.]online
- ads-star[.]site

Sample String-Connected Domains

- ads-strong[.]com
- chainventures[.]ch
- chainventures[.]cn
- chainventures[.]co
- chainventures[.]com
- chainventures[.]de
- chainventures[.]global
- chainventures[.]in