RisePro の新バージョンを DNS で分析

目次

要旨

データ収集型マルウェア・アズ・ア・サービスの「RisePro」は、2022年の登場から今日に至るまでユーザーを悩ませ続けています。ANY.RUN が最近、RisePro の最新バージョンを発見・分析し、ドメイン名3個と IP アドレス7個からなる合計10個のセキュリティ侵害インジケーター（IoC）を特定しました。

インターネットをより安全で透明性の高いものにするという目的のもと、WhoisXML API はこの IoC リストをもとにこのたび独自調査を行い、RisePro に関連する以下のアーティファクトを新たに発見しました：

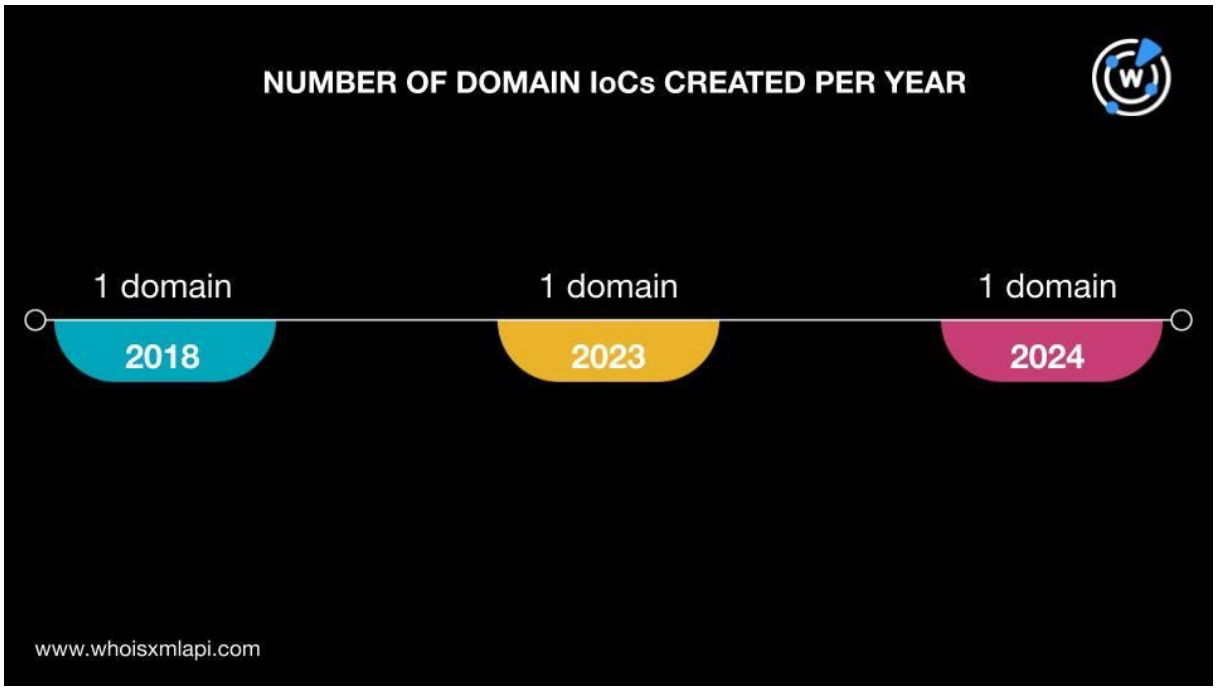
- ドメイン IoC と同じメールアドレスを使用していたドメイン名849個。そのうち52個は悪意あるドメイン名
- 新たに判明した IP アドレス2個。そのうち1個は悪意ある IP アドレス
- IP アドレス IoC を使用していたドメイン名59個。そのうち18個は悪意あるドメイン名
- ドメイン IoC と同じ文字列を含むドメイン名14個

RisePro の IoC

まず、RisePro の IoC を詳しく見ることから分析を始めました。

IoC として特定されたドメイン名（以下「ドメイン IoC」）3個について Bulk WHOIS Lookup を実行したところ、以下のことが判明しました：

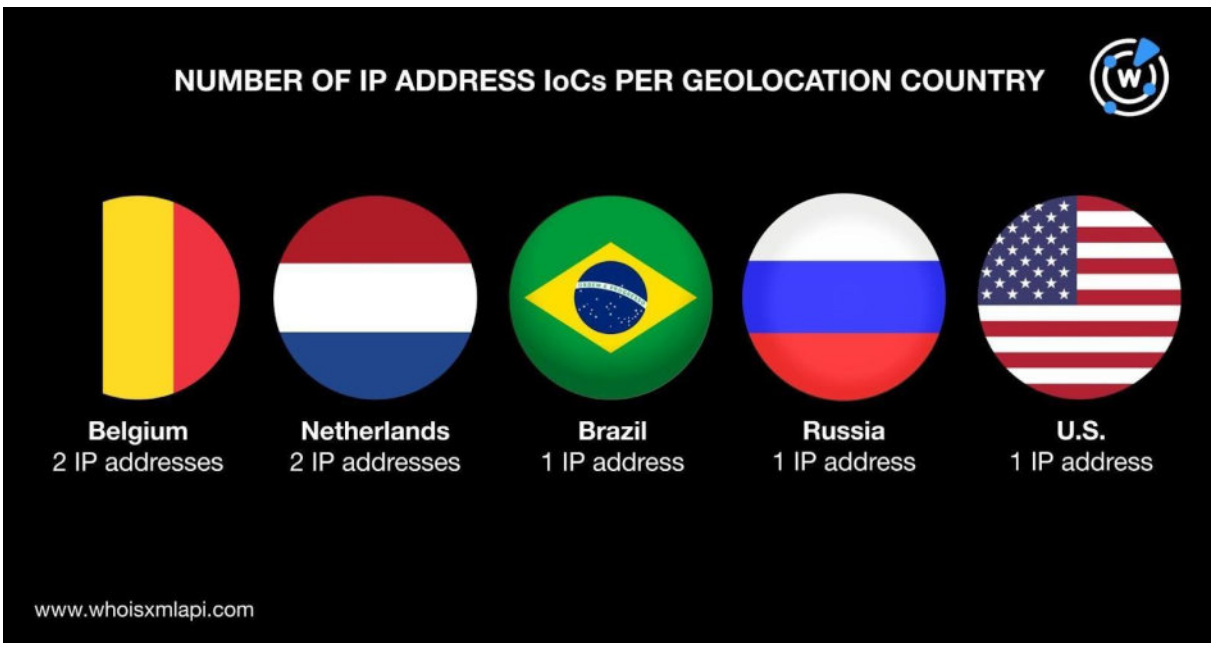
- 3個の管理レジストラは異なっていました（chainventures[.]co[.]uk は 1api GmbH、ads-strong[.]online は NiceNIC International Group Co. Limited、ontopothers[.]com は OwnRegistrar, Inc. が管理）。
- 3個の登録年も異なっていました（chainventures[.]co[.]uk は2018年、ads-strong[.]online は2023年、ontopothers[.]com は2024年）。



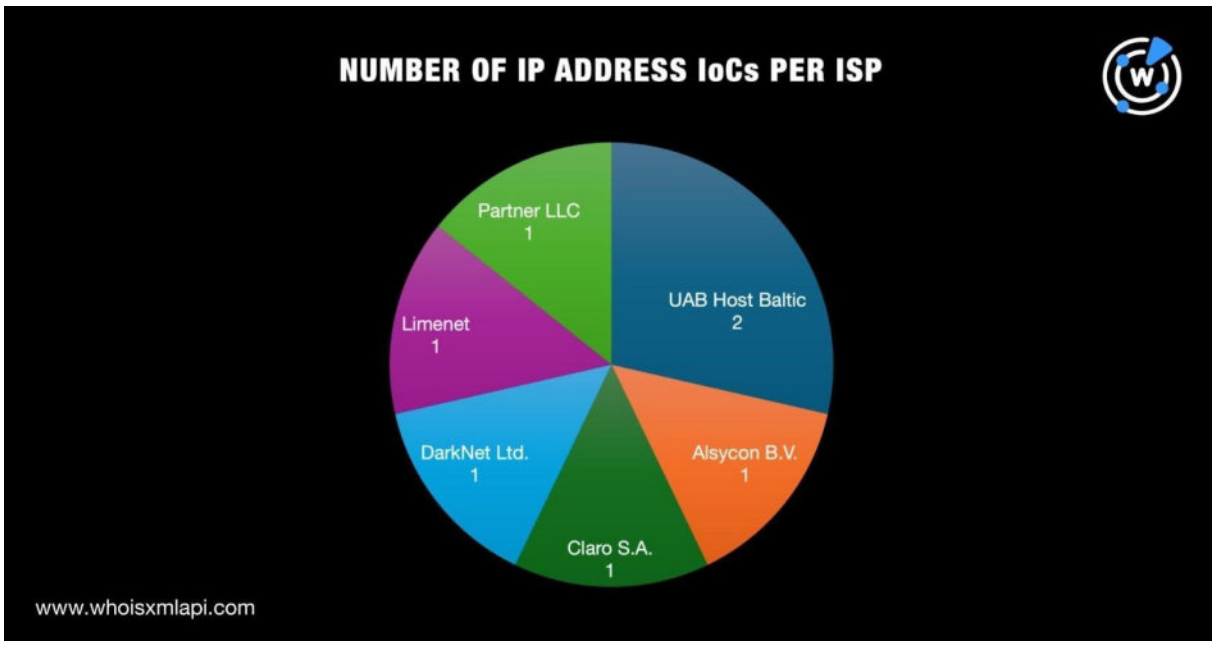
- 登録者の国の情報がWHOISレコードに残っていたのは2個のみでした（ads-strong[.]onlineはベラルーシ、ontopothers[.]comはスペイン）。

IoCとしてタグ付けされたIPアドレス（以下「IPアドレスIoC」）7個についてBulk IP Geolocation Lookupを実行した結果、以下のことがわかりました：

- ジオロケーションはベルギーとオランダに各2個、ブラジル、ロシア、米国に各1個と分散しており、いずれもドメイン名の登録者の国と合致しませんでした。



- 2個の管理ISPはUAB Host Balticでした。また、Alsycon B.V.、Claro S.A.、DarkNet Ltd.、Limenet、Partner LLCが1個ずつを管理していました。



RiseProのIoCリスト拡張

関連する他のアーティファクトを特定するため、WHOIS History APIを使い、3個のドメインIoCの過去のWHOISレコードを参照してメールアドレスを探しました。その結果、未編集のまま公開されていたメールアドレスを1個見つけました。

そのメールアドレスをキーワードにしてReverse WHOIS APIで検索し、結果から重複と既存のIoCを除外したところ、849個のドメイン名がそのメールアドレスを使って登録されていたことがわかりました。

それらのドメイン名に対してThreat Intelligence APIを実行した結果、52個のドメイン名はマルウェア配布やフィッシングなどの攻撃に関連していることが確認できました。そうした悪意あるドメイン名のうち5個について判明した情報は以下の通りです：

ドメインIoCと同じメールアドレスを使用していたドメイン名	関連していた脅威の種類
aavenetworks[.]com	フィッシング
confirmation-setup[.]com	マルウェア
dao-aave[.]com	フィッシング
jatep-raw[.]net	マルウェア
santander-odnowienie[.]com	Generic

WHOISの情報を比較したところ、ドメインIoCと同じメールアドレスを使っていたドメイン名の一部は、そのドメイン名の文字列が示唆する企業に帰属していることを確認できませんでした。それらのドメイン名は、銀行、暗号通貨取引所、郵便サービス、SNS、メールサービスプロバイダー、巨大IT企業を標的としていた可能性があります。5個の潜在的タイポスクワッティングドメイン名についてWHOIS Lookupで得られた結果は以下の通りです：

模倣された会社	正規のドメイン名	タイポスクワッティングドメイン名	WHOISレコードの情報	
			正規のドメイン名	タイポスクワッティングドメイン名
Facebook	facebook[.]com	facebook-secured[.]com	**登録者組織名：** Meta Platforms, Inc.	**登録者組織名：** データなし
Gmail	gmail[.]com	gmail-sakerhet[.]com	**登録者組織名：** Google LLC	**登録者組織名：** Sahari Muti, Inc.
Microsoft	microsoft[.]com	microsoftsupdates-live[.]com	**登録者組織名：** Microsoft Corporation	**登録者組織名：** データなし
HSBC	hsbc[.]com	livechathsbc[.]net	**登録者組織名：** HSBC	**登録者組織名：** Sahari Muti, Inc.
DHL	dhl[.]com	post-dhl-server[.]com	**登録者組織名：** Deutsche Post AG	**登録者組織名：** データなし

次に、3個のドメインIoCをDNS Lookupにかけたところ、既存のIoCリストには含まれていないIPアドレスが2個新たに特定されました。

その2個のIPアドレスをIP Geolocation Lookupで検索した結果、以下が明らかになりました：

- 62[.]204[.]41[.]98はロシア、82[.]165[.]193[.]159はフランスにそれぞれ位置していました。IPアドレスIoCとジオロケーションが一致したのは62[.]204[.]41[.]98のみでした。
- 62[.]204[.]41[.]98の管理ISPはHorizon LLC、82[.]165[.]193[.]159の管理ISPはIONOS SEでした。どちらもIPアドレスIoCのISPとは異なっていました。

Threat Intelligence APIを実行したところ、62[.]204[.]41[.]98はマルウェア配布、スパムキャンペーンなどの攻撃に関与していたことがわかりました。

9個のIPアドレス（7個のIPアドレスIoCと新たに見つかった2個のIPアドレス）についてReverse IP lookupsを実行したところ、62[.]204[.]41[.]98と82[.]165[.]193[.]159は専用アドレスと確認されました。それらは、合計59個のドメイン名（重複、既存のIoCおよびドメインIoCと同じメールアドレスを使っていたドメイン名を除く）をホストしていました。

その59個のドメイン名をThreat Intelligence APIにかけた結果から、18個がマルウェア配布に関連していたことが判明しました。その18個の全てに**ads-**という文字列が含まれていることから、悪意のある広告に使われていたと思われます。

次に、2個のドメインIoCに見られた以下の文字列を含む他のドメイン名を探しました：

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

Domains & Subdomains Discoveryで「**Starts with**」パラメータを使って検索したところ、これらの文字列を含んだドメイン名が14個見つかりました。

—

今回、RiseProのIoCを詳細に分析した結果、ドメイン名922個とIPアドレス2個からなる合計924個の関連アーティファクトが検出されました。また、注目すべきことに、そのうち71個はさまざまな脅威に関与していました。ドメインIoCと同じメールアドレスを使用していたドメイン名の一部は、銀行、暗号通貨取引所、郵便サービス、SNS、メールサービスプロバイダー、巨大IT企業を標的とした攻撃に悪用された、または今後悪用される可能性があります。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項：*当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：アーティファクトとIoCの例

ドメインIoCと同じメールアドレスを使用していたドメイン名の例

- 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

ドメインIoCと同じメールアドレスを使用していた悪意あるドメイン名の例

- 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

IPアドレスIoCを使用していたドメイン名の例

- 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

IPアドレスIoCを使用していた悪意あるドメイン名の例

- 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

ドメインIoCと同じ文字列を含むドメイン名の例

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