WhoisXMLAPI

APAC地域を拠点/標的とするAPTグループのIoCリスト拡張 – 2023年

過去と現在のWHOISデータを活用

目次

要旨

高度標的型攻撃（APT）グループは、その狡猾さと資金力から、現在最も危険な脅威アクターのひとつとされています。APT防御市場はこの10年間で677%にのぼる急速な成長を遂げており、2026年までに151億6,000万米ドルに達するとの予測もあります。

WhoisXML API の研究チームはこのほど、2023年にアジア太平洋（APAC）地域を拠点または標的にして活動していたAPTグループをピックアップし、それらのセキュリティ侵害インジケーター（IoC）リストをもとに詳細な調査を行いました。

1. **APTグループ一覧**
   - 本調査で取り上げた6つのAPTグループを概説します。

2. **WHOISに見るAPTグループの足跡：メールアドレス**
   - IoCとしてタグ付けされたドメイン名（ドメインIoC）のWHOISレコードに表示されたメールアドレスの公開/非公開の内訳を示します。

3. **IoCリストの拡張**
   - WHOISに登録されていたAPTグループのメールアドレスを手がかりに、IoCリストの拡張を試みました。その経緯を説明します。

4. **各APTグループの詳細**
   - アクセス可能なウェブサイトのスクリーンショット分析を含む、各APTグループのIoCリスト拡張分析の結果を報告します。

調査方法の概要

まず、34のAPTグループをリストアップし、以下の判断基準に従って絞り込みを行いました：

- 2023年に攻撃を実行した
- APAC地域を拠点/標的としている

その結果残った12のAPTグループのIoCリストを取り寄せました。

WHOIS History APIを使い、6グループのドメインIoCに関する過去のWHOISレコードからメールアドレスを収集しました。

次に、プライバシー保護（非公開化）されていたメールアドレスと公開されていたメールアドレスを分け、公開メールアドレスをReverse WHOIS APIおよびDomain Research Suite（DRS）の Reverse WHOIS Searchにかけた結果、以下を検出しました：

- 現在のWHOISレコードにそのメールアドレスが登録されているドメイン名（Reverse WHOIS APIの結果から）
- 過去のWHOISレコードにそのメールアドレスが登録されているドメイン名（DRS Reverse WHOIS Searchの結果から）

そして、Screenshot APIを使い、それらのドメイン名がアクセス可能かどうかを確認しました。

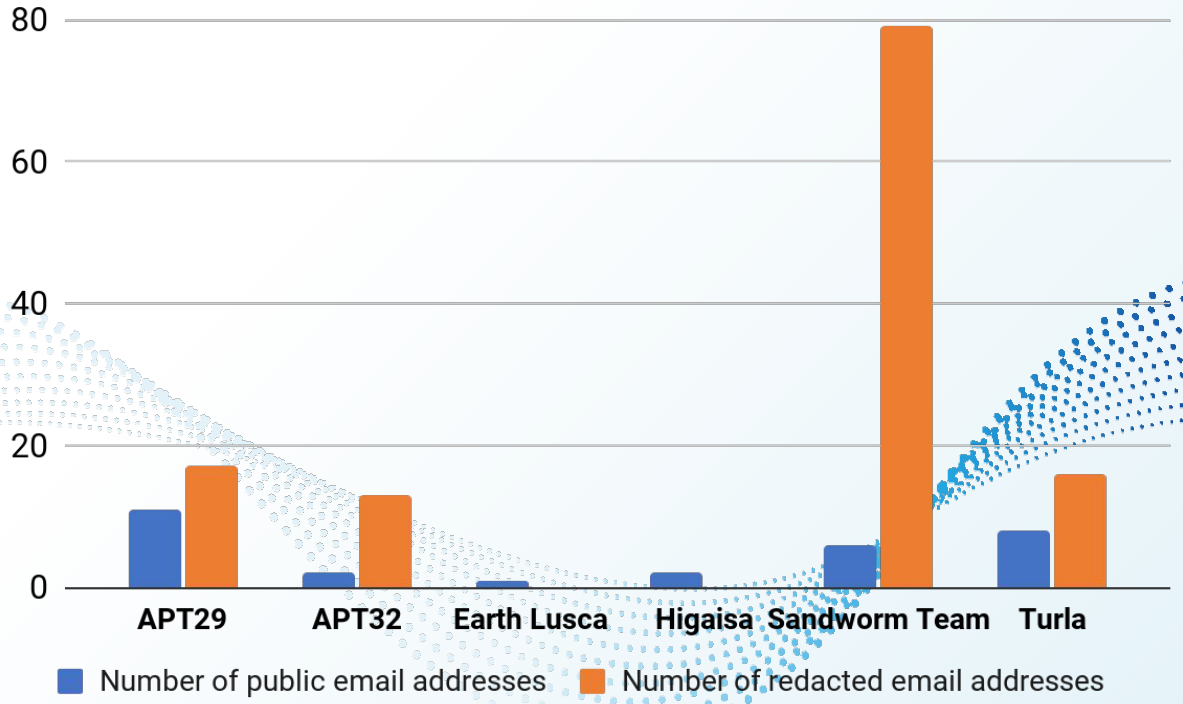
APTグループ一覧

APTグループ	別名	本拠地	標的とした国	活動を開始した年	直近の攻撃に関与したIoCの数
APT29	IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune	ロシア	米国	2008	11
APT32	SeaLotus, OceanLotus, APT-C-00	ベトナム	東南アジア諸国	2014	5
Earth Lusca	TAG-22	中国	オーストラリア	2019	2
Higaisa	なし	韓国	北朝鮮	2009	1
Sandworm Team	Electrum, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, Voodoo Bear, IRIDIUM	ロシア	ウクライナ	2009	13
Turla	Iron Hunter, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear	ロシア	45カ国	2004	12
					合計44 IoC

WHOISに見るAPTグループの足跡：メールアドレス

一部のWHOISデータを編集して非公開にしているものの、脅威アクターは過去のWHOISレコードに足跡を残し続けています。

今回調査した6つのAPTグループの場合、ドメインIoCの過去のWHOISレコードで見つかったメールアドレスの約19%が、 Gmail、Yahoo!、Hotmailといった著名プロバイダーのパブリックなメールアドレスでした。

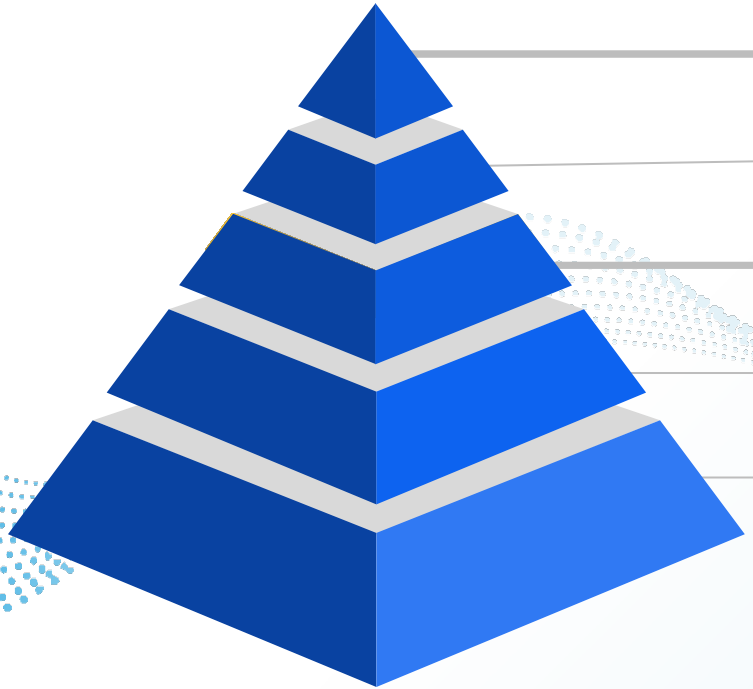


IoCリストの拡張

ドメイン脅威インテリジェンスの活用

IoCリストの拡張: 数十ドメインから数百ドメインへ

WhoisXML APIが行った今回の調査で、APTグループがWHOISに残したメールアドレスをもとに、潜在的な脅威のアーティファクトと考えられる350超のドメイン名が新たに検出されました。



44 6つのAPTグループの最近の活動に関与したドメインIoC

155 ドメインIoCの過去のWHOISレコードで見つかったメールアドレス

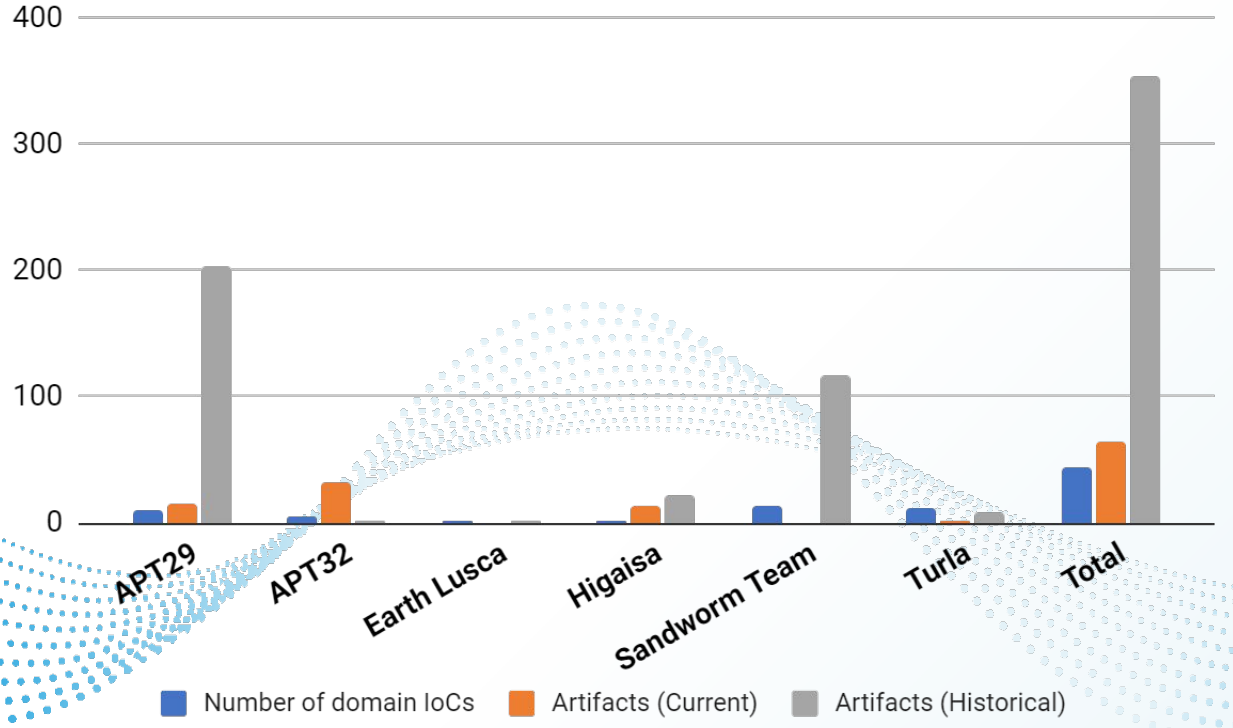
30 公開されていたメールアドレス

64 現在のWHOISレコードにIoCと同じメールアドレスが登録されていたドメイン名

353 過去のWHOISレコードにIoCと同じメールアドレスが登録されていたドメイン名

※ドメイナーが所有していた可能性のあるドメイン名9,998個を除く

IoCリストの拡張: IoCをもとに最大8倍の関連ドメイン名を発見



ドメインIoC 44個の現在のWHOISレコードを調査した結果、関連するドメイン名64個が特定されました。これはドメインIoCの数の1.46倍に相当します。

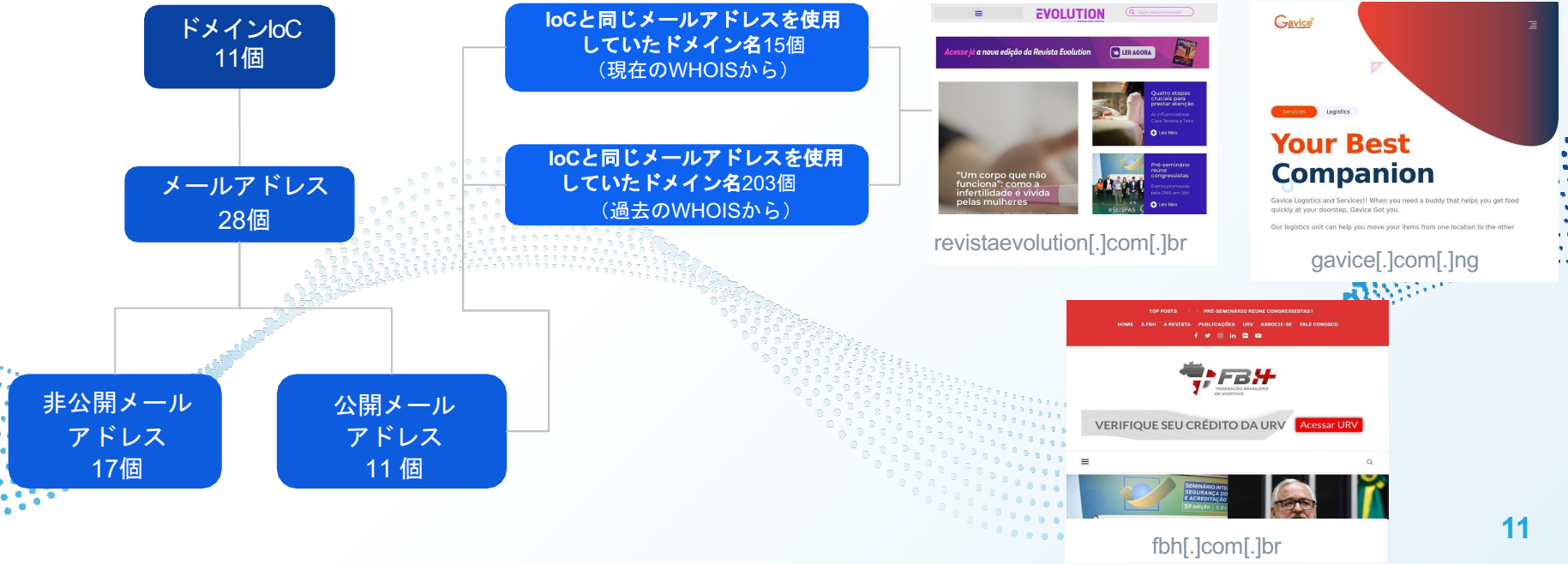
また、ドメインIoCの過去のWHOISレコードを調査した結果、ドメインIoCの数の8倍にのぼる関連ドメイン名が検出されました。

この作業を通じ、44個のドメインIoCから合計353個の関連ドメイン名の発見につながりました。

各APTグループの詳細

APT29

APT29は、ロシアの対外情報庁（SVR）と連携するサイバースパイグループです。遅くとも2008年から活動しており、欧州やNATO加盟国の政府ネットワーク、研究機関やシンクタンクを標的にした経緯があります。APT29は、2015年夏から米国の民主党全国委員会（DNC）を侵害していたと考えられています。また、2023年前半にはウクライナの組織を標的としたと報じられました。



APT32

APT32はベトナムを拠点とし、2014年から活動していると推定されています。このグループが標的としたのは、主にベトナム、フィリピン、ラオス、カンボジアなどの東南アジア諸国を拠点とする複数の民間企業、外国政府、反体制派、ジャーナリストなどです。
22023年6月、APT32はSPECTRALVIPERを使用してベトナムの農業関連企業を攻撃したと示唆されました。

Earth Lusca

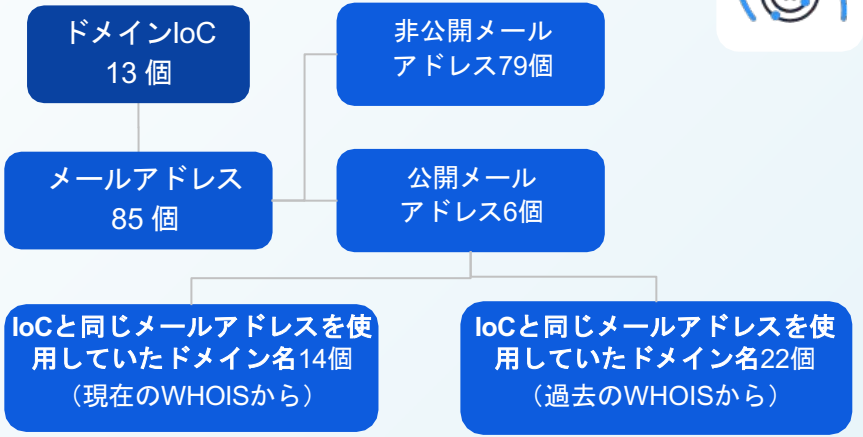
Earth Luscaは、中国を拠点として2019年4月から活動していると思われるサイバースパイグループです。これまでに政府機関、報道機関、ギャンブル企業、教育機関、新型コロナウイルス関連の研究機関、通信会社、各国の暗号通貨取引プラットフォームを標的にしてきました。セキュリティ研究者は、Earth Luscaの一部の運用者には金銭的な動機があると疑っています。2023年前半には、Linuxバックドアを通じて東南アジア、中央アジア、バルカン半島、ラテンアメリカ、アフリカの政府組織を攻撃したことが確認されています。

Higaisa

Higaisaは韓国発祥とされるグループで、主に北朝鮮の政府、公共機関、貿易関連の組織を標的としていますが、その活動は中国、日本、ロシア、ポーランドなどにも及んでいます。Higaisaの存在が最初に明るみに出たのは2019年初頭ですが、活動を開始した時期は2009年にまでさかのぼる可能性があります。2023年10月に中国のインターネットユーザーを標的に行われたフィッシングキャンペーンは、Higaisaによるものでした。

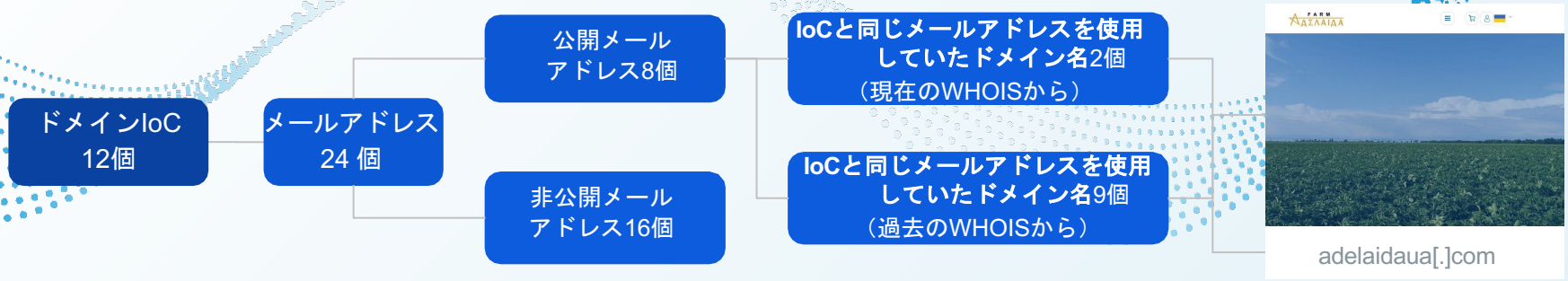
Sandworm Team

Sandworm Teamは、ロシア参謀本部情報総局（GRU）の特殊技術メインセンター（GTsST）と連携するサイバー攻撃グループで、少なくとも2009年から活動しています。ウクライナの電力会社や政府組織に対する2015年と2016年の攻撃、2017年の世界的なNotPetya攻撃、冬季オリンピックに関連した2018年のOlympic Destroyer攻撃などで知られています。最近では、2023年4月にウクライナに対して攻撃を仕掛けました。



Turla

Turlaはロシアを拠点とし、その洗練されたサイバースパイ活動で悪名高いグループです。2004年の結成以来、45を超える国々で政府機関、大使館、軍事組織、教育機関、研究所、製薬会社などのネットワークに侵入しています。また、2023年7月にウクライナを標的に攻撃を行ったことが確認されています。



まとめ

APTグループの追跡

ドメイン名所有者のWHOISレコードは、APTグループ、または少なくともAPTグループのドメインポートフォリオに関する多くの情報をもたらします。この調査では、6つのAPTグループのドメインIoCに関する過去と現在のWHOISレコードを通して、関連性を持つ他のアーティファクトを洗い出すことができました。

まずドメインIoC 44個に関するWHOISの過去データの分析から調査を始め、最終的に以下を特定するに至りました：

- 現在のWHOISレコードから、ドメインIoC数の1.46倍にのぼる関連ドメイン名
- 過去のWHOISレコードから、ドメインIoC数の最大8倍にのぼる過去の関連ドメイン名
- IoCと同じメールアドレスを使い、調査時点でもアクティブだった複数のドメイン名

結論

APTグループは豊富な資金を持つ強力な組織の支援を受けていることが多く、捕捉しにくい存在です。しかし、我々サイバーセキュリティコミュニティは、国家、重要インフラ、そしてさまざまな業界に大混乱をもたらすAPTグループを執拗に追跡し、阻止する努力を続けなければなりません。

本調査の結果は、WHOISのインテリジェンスがAPTの活動を知る上での手がかりを与えてくれることを示しています。現在と過去のWHOISデータから、APTグループやその他のサイバー攻撃者が運営する悪意のドメインネットワークを把握できる可能性があります。

このレポートでご紹介したデータをご希望のお客様、または当社とのコラボレーションをご希望のお客様は、こちらまでお気軽にお問い合わせください。

WhoisXML APIについて

WhoisXML APIは、MSSP、SOC、フォーチュン1000企業、政府機関、デジタルフットプリントを持つ中小企業など、サイバーセキュリティに取り組むあらゆる組織を支援します。
当社はドメイン名、IPアドレス、DNSに関する包括的なインテリジェンスを常時収集し、お客様にタイムリーにご提供しています。

当社のデータは貴社のデジタルプレゼンス強化をサポートします。ご興味をお持ちのお客様は、当社のウェブサイトをご覧いただくか、営業担当までお問い合わせください。

42億以上
のドメインとサブドメイン

167億以上
の過去のWHOISレコード

数十億
のDNSレコード

12年以上
のデータクローリング


WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence