WhoisXMLAPI

北米諸国を標的としたAPTグループに関する調査

過去と現在のWHOISデータを活用

目次

- 要旨
- 調査方法の概要
- Security Research Reference
- IoCリストの拡張
- 各APTグループの詳細
- まとめ
- WhoisXML APIについて

要旨

北米は、高度標的型攻撃（APT）グループに最も多く狙われている地域のひとつです。

2023年9月、Picus Securityのレポートで北米地域がAPTのトップターゲットであると報告されました。また、政府、テクノロジー、医療、情報通信、教育部門といった業界が最も影響を受けていることも明らかになりました。

WhoisXML APIの研究チームが実施した今回の調査では、北米を標的とした7つのAPTグループのセキュリティ侵害インジケーター（IoC）リストをもとに、それらのAPTグループに関連している可能性のある他のアーティファクトを探しました。

1. **APTグループ一覧**
   - 本調査で取り上げた7つのAPTグループを概説します。
2. **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レコードに含まれてい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レコードに含まれていた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、41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：

- 北米を標的とした攻撃を2023年以降に開始した
- 2023年以降他地域で活動しているが、過去に北米を標的にした

そして、WHOIS History APIを使い、ドメインIoCの過去の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）されているメールアドレスと公開されているメールアドレスを分け、公開メールアドレスを共用していた他のドメイン名を洗い出しました（カッコ内は使用したWhoisXML APIのツール）：

- 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）
- 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）

この作業の結果、共通の公開メールアドレスを使用していたドメイン名を持つAPTグループが7つ残りました。

さらに、Screenshot APIを使い、それらのドメイン名がアクセス可能な状態にあるかどうかを調べました。

参考資料

今回の調査では、以下のマルウェア分析およびIoCリストを参照しました：

- **APT33 (Mandiant):** https://www.mandiant.com/resources/blog/apt33-insights-into-iranian-cyber-espionage
- **APT41 (Loofiout) :** https://www.lookout.com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41
- **FIN7 (Cyware):** https://cyware.com/resources/research-and-analysis/the-evolution-and-exploits-of-fin7-from-pos-malware-to-ransomware-dominance-0623
- **Kimsufiy (ASEC):** https://asec.ahnlab.com/en/59590/
- **Molerats (Proofpoint):** https://www.proofpoint.com/uk/blog/threat-insight/ta402-uses-complex-ironwind-infection-chains-target-middle-east-based-government
- **Turla (Trend Micro):** https://www.trendmicro.com/en_us/research/23/i/examining-the-activities-of-the-turla-group.html
- **ZIRCONIUM (Kaspersfiy):** https://www.kaspersky.com/about/press-releases/2023_kaspersky-reports-attacks-on-industrial-sector-utilizing-cloud-infrastructure

IoCリストの拡張

ドメイン脅威インテリジェンスの活用

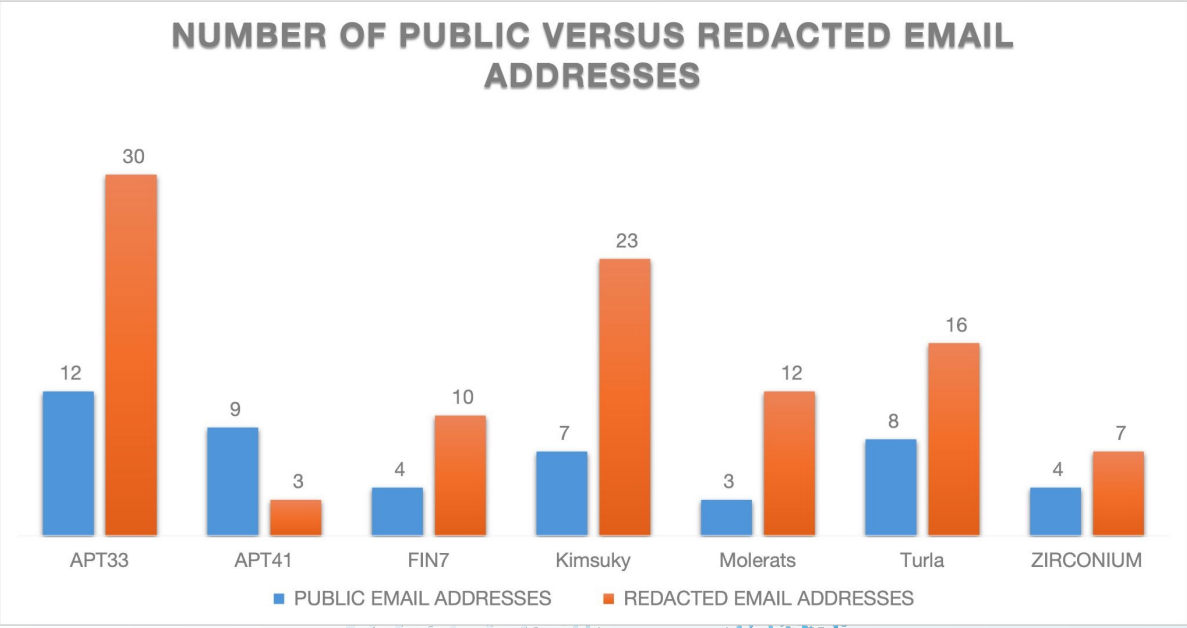
APTグループ一覧

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ドメインIoCの数
APT33	HOLMIUM, Elfin	イラン	米国、サウジアラビア、韓国	2013	9
APT41	ARIUM, Winnti, LEAD, WICKED SPIDER, WICKED PANDA, Blackfly, Suckfly, Winnti Umbrella, Double Dragon	中国	米国	2012	6
FIN7	GOLD NIAGARA, ITG14, Carbon Spider	ロシア	北米諸国	2013	18
Kimsufiy	STOLEN PENCIL, Thallium, Black Banshee, Velvet Chollima	北朝鮮	米国（2020年）	2012	6
Molerats	Operation Molerats, Gaza Cybergang	サウジアラビア	中東および欧州諸国、米国（2014年）	2012	3
Turla	IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear	ロシア	米国、カナダを含む50カ国（過去20年ほど）	2004	12
ZIRCONIUM	APT31	中国	米国（2020年）	2017	5
					合計 59 IoC

APTグループの足跡：メールアドレス

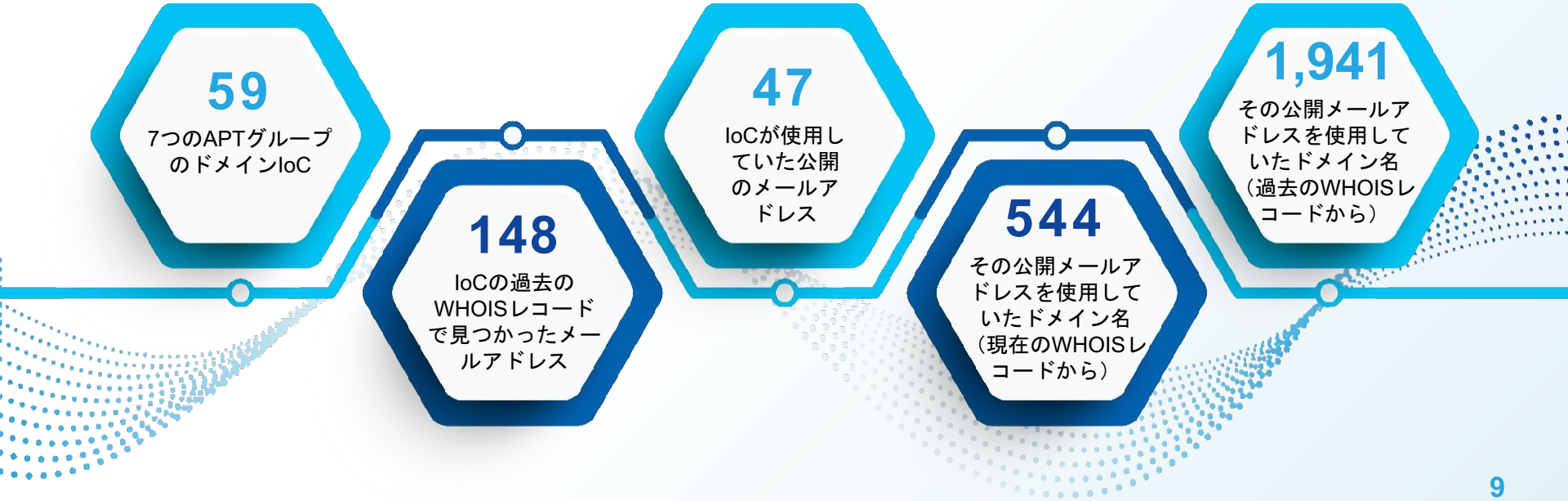
ドメイン名の登録者（所有者）名を含む一部のWHOISデータは非公開になっているものの、脅威アクターは関連ドメイン名の過去のWHOISレコードに足跡を残し続けています。

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32%が公開のメールアドレスでした。その中にはGoogle、Yahoo!、QQといった無料メールサービスプロバイダーのメールアドレスも見られました。

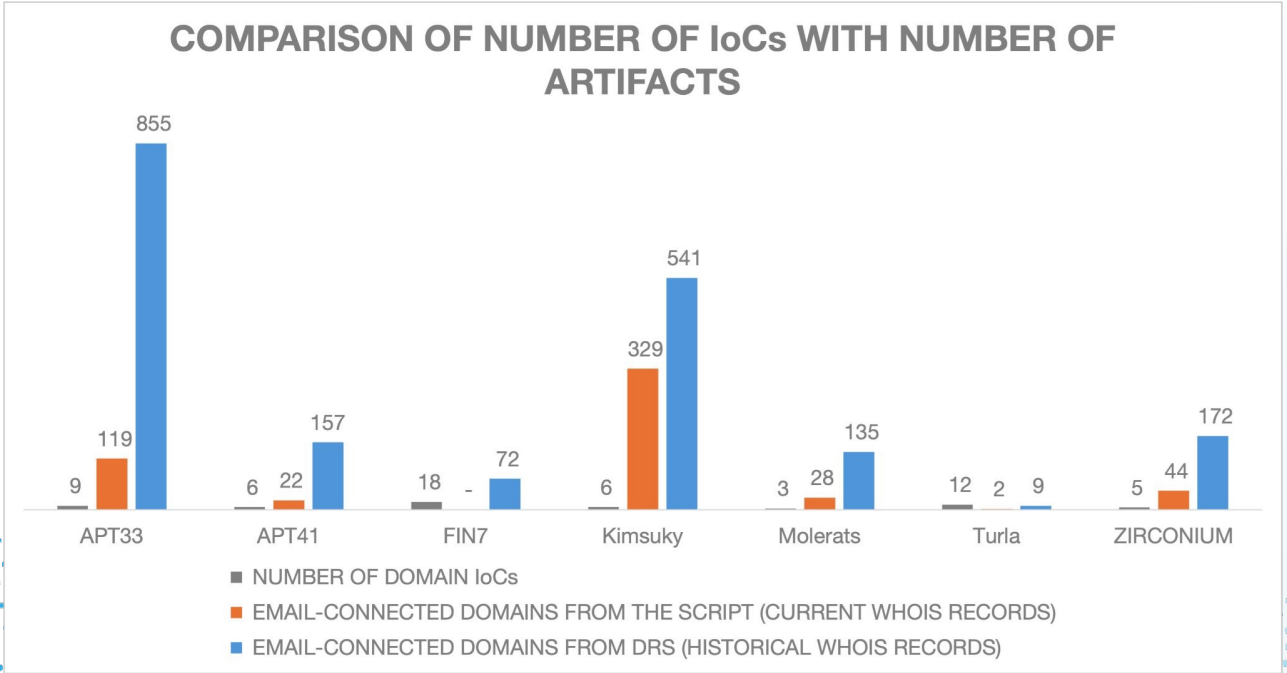


IoCリストの拡張：59のIoCから1,900超のアーティファクトを特定

WhoisXML APIが行った今回の調査で、7つの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1,900超のドメイン名が検出されました。これらは、既知のドメインIoCと同じメールアドレスを使用していました。



IoCリストの拡張：IoCから最大33倍のアーティファクトを発見



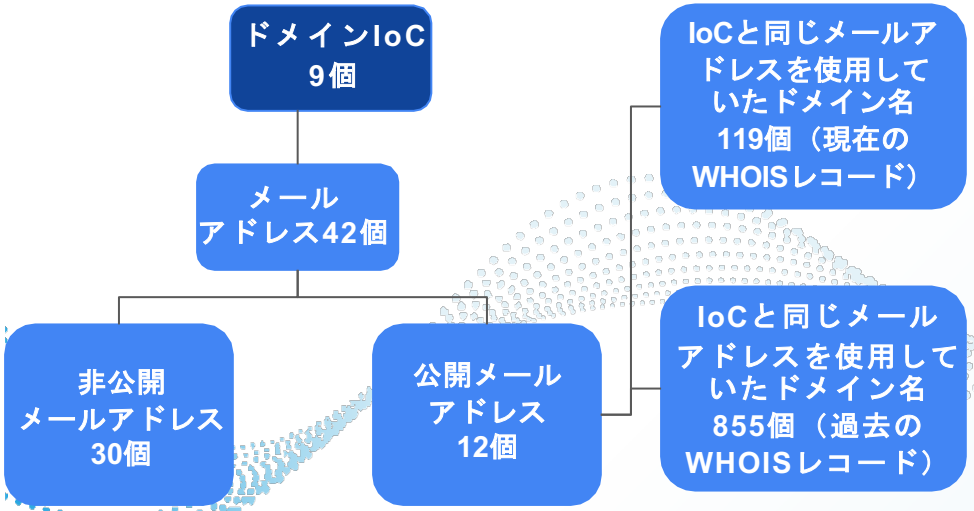
ドメインIoC 59個の現在のWHOISレコードを調査した結果、関連するドメイン名544個が特定されました。これはドメインIoCの数の9倍に相当します。

また、ドメインIoC 59個の過去のWHOISレコードを調査した結果、ドメインIoCの数の33倍にのぼる1,941個の関連ドメイン名が検出されました。

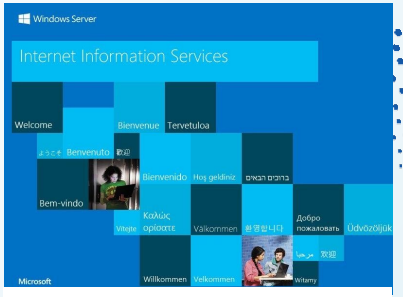
各APTグループの詳細

APT33

イランに拠点を置くと思われるAPTグループ「APT33」は、少なくとも2013年から活動しています。直近では、「SHAMOON」、「Disttrack」という2つの破壊的なマルウェアを使用して、米国、サウジアラビア、韓国の航空宇宙およびエネルギー分野を標的に攻撃を実行しました。



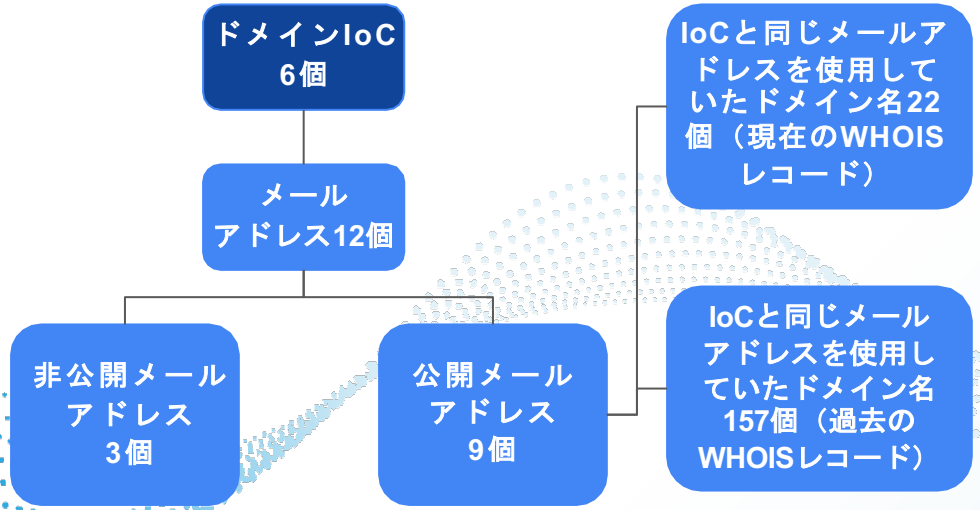
beltel[.]us



apggbcj[.]com

APT41

「APT41」はおそらく中国を拠点としており、少なくとも2012年から活動しています。最近では、「WyrmSpy」、「DragonEgg」という2つのモバイルマルウェアを使用して、米国の組織を攻撃しました。

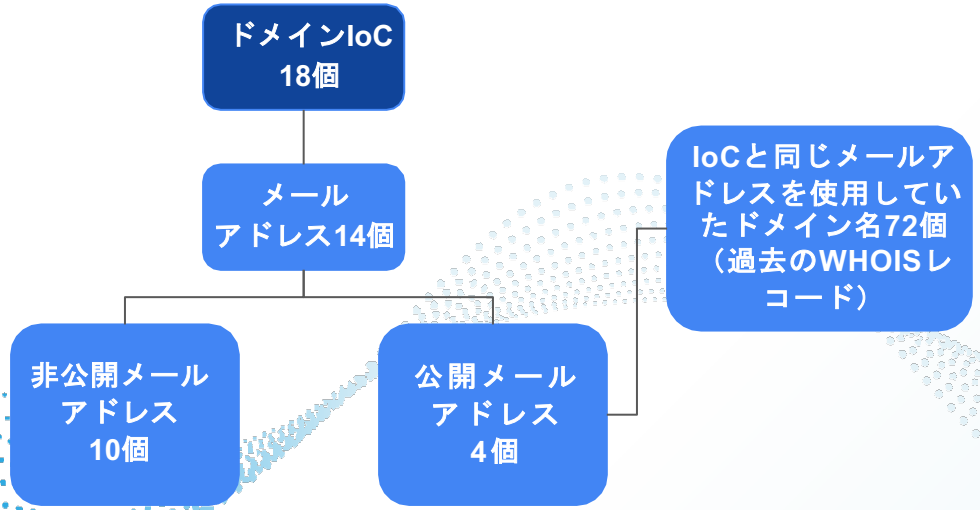


oray[.]hk

dmlao[.]net

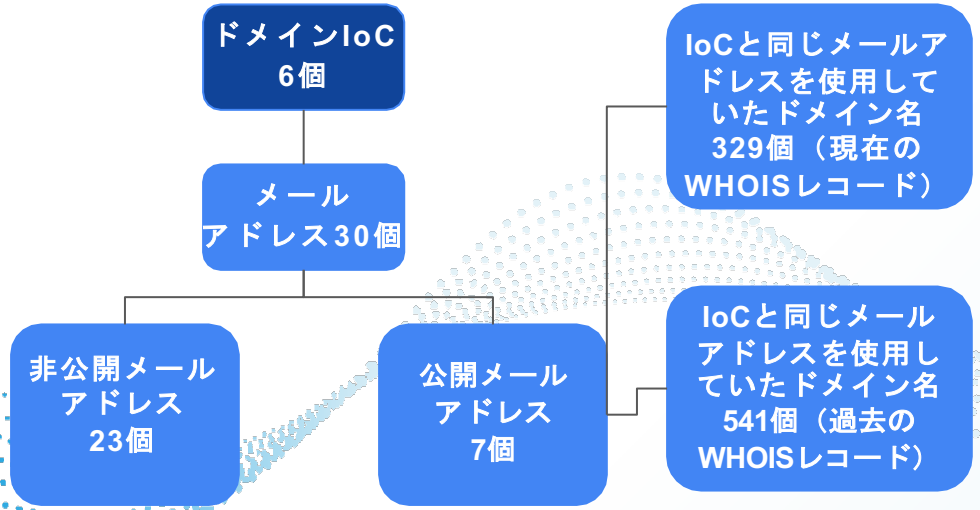
FIN7

ロシアに拠点を置くとされる「FIN7」は金銭的動機を持つ脅威グループで、少なくとも2013年から活動しています。最近は、北米の金融、小売、外食、ホスピタリティ業界を標的としたランサムウェア「Cl0p」をはじめとする複数のマルウェアを使用しています。



Kimsuky

北朝鮮に拠点を置くと思われるAPTグループ「Kimsuky」は、少なくとも2012年から活動しています。直近では
韓国の研究機関を標的としましたが、2020年には米国に拠点を置く専門家やシンクタンクを狙った攻撃も仕掛けました。

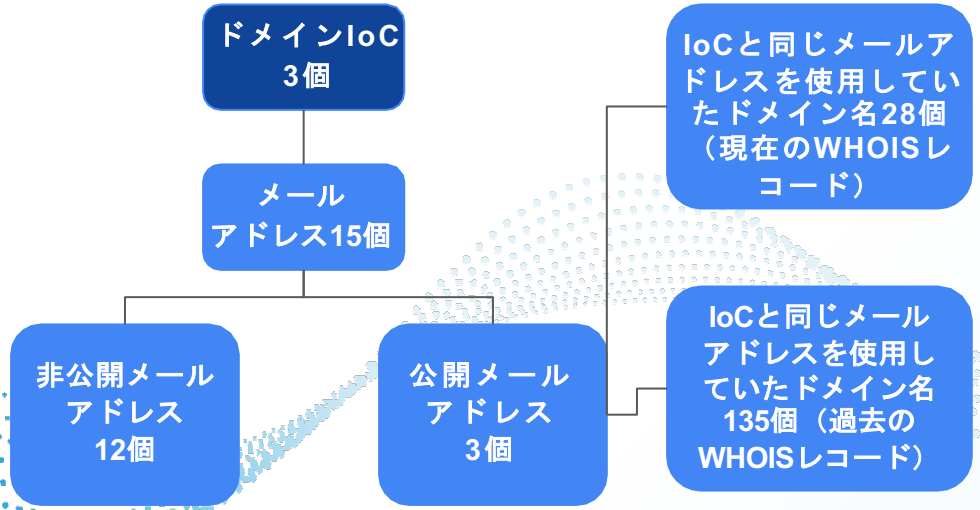


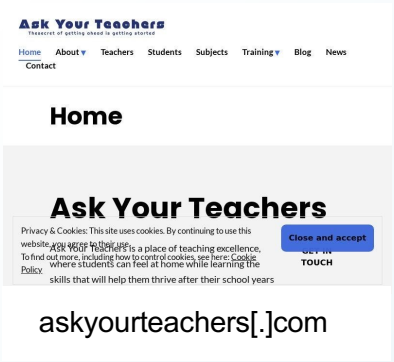
vitorpneus[.]com[.]br

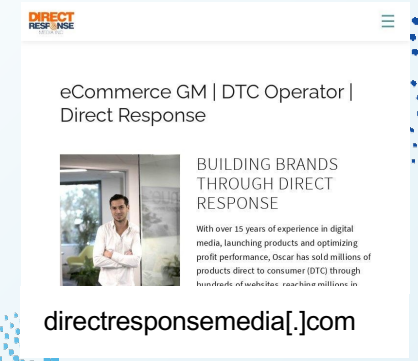
authenticbitcoin[.]com

Molerats

サウジアラビアに拠点を置くと思われる「Molerats」は、少なくとも2012年から活動しています。直近では中東の政府機関を標的としましたが、2014年には欧州と米国を攻撃したこともあります。

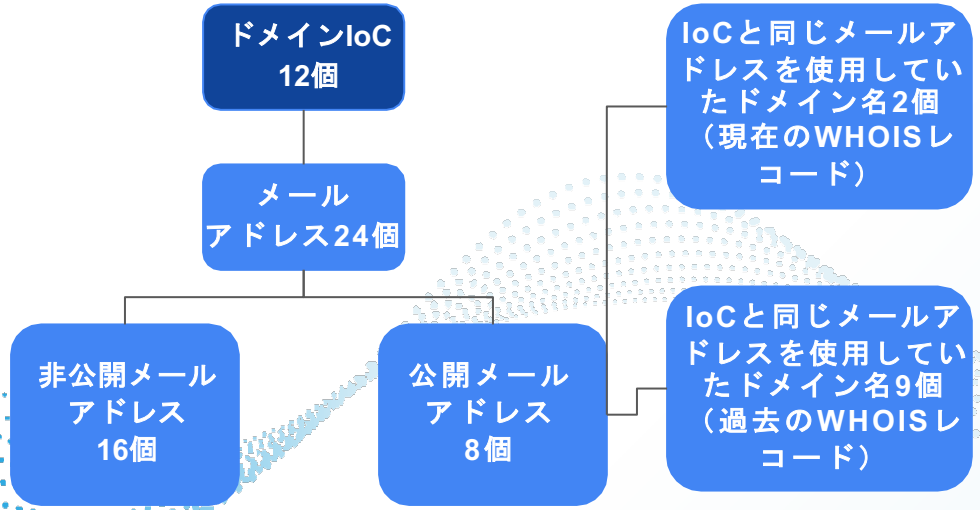


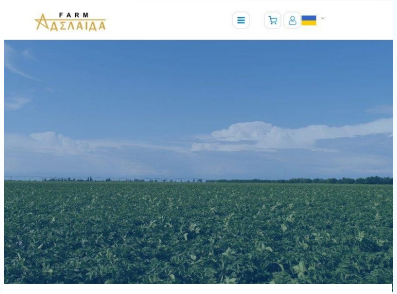




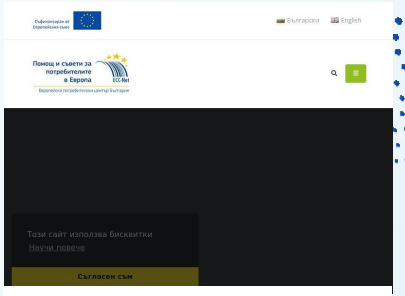
Turla

ロシアに拠点を置くとされる「Turla」は、少なくとも2004年から活動しています。最近ではウクライナの組織を標的にしましたが、過去20年ほどの間に米国やカナダを含む50カ国以上の組織を攻撃しています。





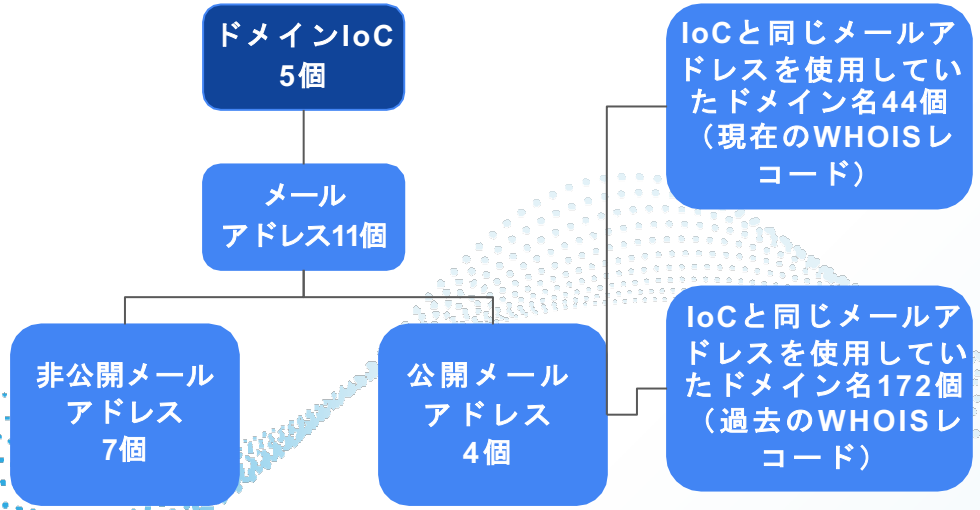
adelaidaua[.]com

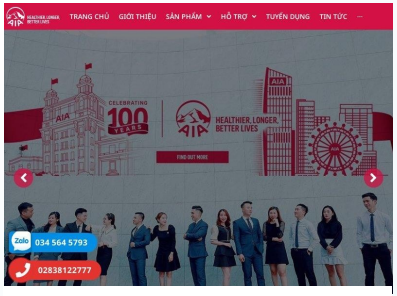


ecc[.]bg

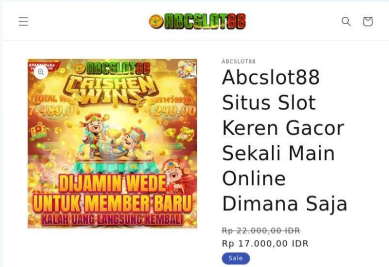
ZIRCONIUM

中国に拠点を置くと考えられている「ZIRCONIUM」は、少なくとも2017年から活動しています。最近は東欧を標的にしていますが、2020年には米国の選挙に関連した攻撃も行いました。





aiadanang[.]com



kenh9[.]com

まとめ

結論

ドメイン名登録者（所有者）のWHOISレコードは、APTグループそのもの、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。今回の調査では、7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特定しました。

具体的には、合計59個のドメインIoCに関する現在と過去のWHOISデータを分析し、以下を発見しました：

- 現在のWHOISレコードから、ドメインIoC数の9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33倍にのぼる関連ドメイン名
- ドメイン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

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、営業担当までお気軽に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