

脅威インテリジェンスと 脆弱性

面 和毅

略歴

- Security 研究者/エンジニア/開発 (23年)
- SELinux/MAC Evangelist (16年)
- Linux エンジニア (21年)
- システム管理者(4年)
- Antivirus Professional エンジニア (3年)
- SIEM Professional エンジニア (3年)
- 脅威インテリジェンストレーナー(2年)



現在はOSS/セキュリティ/脅威インテリジェンスエヴァンジェリストとして活動。



徹底攻略 改訂新版 LPIC Level 3 303 [Version 2.0] 対応 教科書

Linux Professional Institute (LPI) 認定試験 303 Security Exam

解説がより充実 合格力が身になる

「詳しい解説」+「演習問題」+「重要ポイント」がひと目でわかる。

Linuxセキュリティ標準教科書

Security & Trust

スイッチ・オン! SELinux

第7回 やっぱり気になるスイッチ・オン! での性能変化

面 和毅
サイオステクノロジー株式会社

Open Source Summit Japan

Learn more about Open Source Summit Japan and register here!

Schedule Speakers

Kazuki Omo
SIOS Technology Inc.
Executive Officer
Tokyo/Japan
@secureoss_jp

Over 20 years experience in Unix/Linux/Windows system and many of Security related product. Working for OSS community over 15 years.

- Published SELinux and related security articles from 2004-2018.
- Presentation on Open Source Summit Japan 2017 "OSS CVE Trends".
- Presentation on openSUSE Asia Summit 2016 "openSUSE Security with OpenSCAP standard"
- Presentation on LinuxWorld C&D 2004 Japan "KB1-4keynote Explanation about SELinux"
- Presentation on OSC 2007 TOKYO Japan "How to to daily operate for SELinux"
- Published "Linux Security textbook" from LPI-Japan.

My Speakers Sessions

Thursday, June 1

11:50 JST

OSS CVE Trends - Kazuki Omo, Secure OSS SIG & SIOS Technology Inc.

Linuxセキュリティ標準教科書

「重要ポイント」がひと目でわかる。

LinuC LPI - JAPAN

資格・試験情報 受験案内 受検申込み 学習のすゝめ方 よくあるご質問 受験者マイページ

Linuxセキュリティ標準教科書

Linuxサーバの構築・運用に最低限必要なセキュリティの知識の学習に最適な教科書

LPI-Japanは、Linux/OSS技術者教育に利用していただくことを目的とした教材「Linuxセキュリティ標準教科書」を開発し、無償にて公開しています。

Linuxは、多くのシステムにおいてサーバOSとして採用されるようになり、社会における重要な位置を任されるOSへと成長しました。同時に、標的型攻撃をはじめとしたサイバー攻撃は年々高度化しており、Linuxシステムにおいても高いセキュリティレベルの確保、またセキュアなLinuxシステムを構築することのできるスキルを持った人材の育成は優先度の高い課題の一つとなっています。本教材は、Linuxにおけるセキュリティを学習・再認識するために最低限必要となる知識を体系的にまとめた内容となっています。本教材が教育機関や企業研修でのLinux/OSSにおけるセキュリティ教育の質向上の一助となれば幸いです。

Linuxセキュリティ標準教科書
PDF版・EPUB版・Kindle版・Ver. 1.0.1
紙本版：Ver. 1.0.0

Linuxで怪しい実験やってみた

面 和毅 SIOSテクノロジー

「データ・マネジメントの新戦略」近未来を実現する「双方向クラウド戦略」とは IT/製造/建設分野の製品・サービス選択支援情報サイト：日経クロステックActive

SIOS SECURITY BLOG

OSSに関するセキュリティ・ツールの使い方・脆弱性等を紹介しています。SELinux/Capability/AntiVirus/SCAP/SIEM/Threat Intelligence等。

GNOME Projectのlibgsfの脆弱性(Important: CVE-2024-36474, CVE-2024-46544)

© 2024.10.05

10/05/2024にGNOME Projectのlibgsfの脆弱性(Important: CVE-2024-36474, CVE-2024-46544)が公開されました。今回はこちらの脆弱性の概要と、各ディストリビューションの対応について纏めます。

[過去関連リンク(最新5件)]

外部セミナー

サイバー攻撃から企業システムを守る!

OSINT 実践ガイド

公開情報をフル活用!



サイバー空間における脅威を調査分析しレポートまで作成できるセキュリティアナリストを育成

脅威インテリジェンス育成コース

2024年11月2日(土)開講決定！受講生募集中！

給付金利用で受講料最大46万円キャッシュバック！オンライン受講が可能！

- コース紹介
- 給付金制度
- 募集要項
- 受講お申込
- カウンセリング
- 資料請求

BLOG

HOME > BLOG > Linux/OSS ソリューションブログ > 統合システム監視 > 脆弱性管理 BLOG > 2024年7~8月の脅威動向と代表的な攻撃(前編)

脆弱性管理 BLOG

2024年10月07日

最新 BLOG 記事

2024年7~8月の脅威動向と代表的な攻撃(前編)

2024年7-8月の脅威動向を見るために、記事末尾で7-8月の代表的なインシデント・攻撃等を羅列しています。もちろんこれらは代表的なものであり、その他にも多くのインシデントが発生しています。

今回は7-8月に発生した中でも

- 7月に多くの漏洩関係組織が判明したランサムウェアによる(株)イセトへの攻撃を見てみたいと思います。



2024年7~8月の脅威動向と代表的な攻撃(後編)

2024年10月07日



2024年7~8月の脅威動向と代表的な攻撃(前編)

2024年10月07日



Zabbix 7.0の新機能 - Asynchronous Pollerとは



Linuxの具体的な脆弱性対策とコスト軽減方法

サイバー攻撃から企業システムを守る！

中村行堂
面和敬

Open Source INTelligence
オープン ソース インテリジェンス

OSINT 実践ガイド

脅威インテリジェンス IoT サイバーキルチェーン TTP

公開情報をフル活用して セキュリティを高める！

22の
ユース
ケース別に
確認方法
を解説

MITRE ATTACK SCAP KEYカタログ Shodan

「御社の内部情報、外から丸見えですよ」

(株)ヒートウェーブで11/02からトレーニングを行います

[セキ塾TOPに戻る](#)

セキ塾 脅威インテリ
ジェンスセミナー



サイバー空間における脅威を調査分析しレポートまで作成できるセキュリティアナリストを育成

脅威インテリジェンス育成コース

2024年11月2日(土)開講決定！受講生募集中！

給付金利用で受講料最大46万円キャッシュバック！オンライン受講が可能！



コース紹介



給付金制度



募集要項



受講お申込



カウンセリング



資料請求



目次

- 脅威インテリジェンスとは(ざっくり)
- 脅威インテリジェンスのどこで脆弱性が関わってくるのか
- 具体的にどんな脆弱性がどう関わっているのか(脅威アクター)
- 脅威インテリジェンスの中でどの様に脆弱性情報を活用していくのか

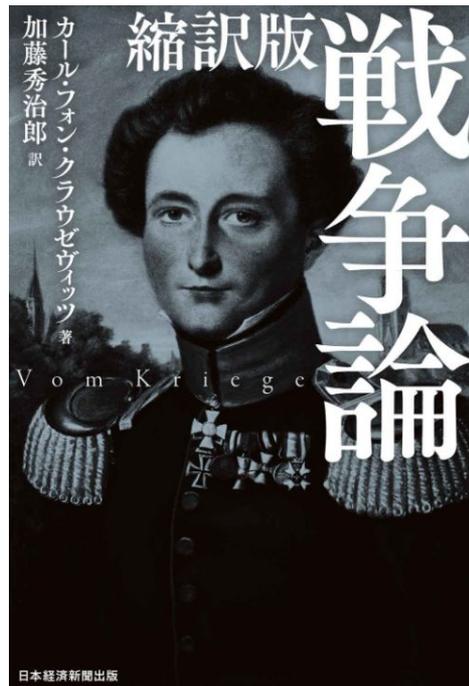
インテリジェンスとは

この辺の**基本的なところ**は飛ばしていきます！

インテリジェンス

『インテリジェンス』とは、敵とその国に関するあらゆる種類の情報を意味します。

要するに、私たちの **計画と作戦の基礎** です。



インテリジェンスとは

「インテリジェンス」は元々軍事用語から来ています。□国統合参謀本部の出したドキュメント“Joint Intelligence Joint publication 2-0 (2007/06/22)”では、「インテリジェンス」に関して次のように述べています。

インテリジェンスの管理と軍事作戦への統合は、指揮官の固有の責任です。

情報自体は、指揮官にとって有用な事実または一連の事実ですが、作戦環境についてすでに知られている他の情報に関連し、敵に関する過去の経験に照らして考慮されると、新しい一連の「**インテリジェンス**」となります。

インテリジェンス は、将来の状況や状況の予想または予測を可能にし、行動方針（COA）の違いを明らかにすることで決定のための材料を提供します。

つまりインテリジェンスとは

「単なる「情報」を過去のデータなどから分析し

指揮官が意思決定を行うための材料を提供する もの」になります。

インテリジェンスとは・・・

新型コロナウイルスを例にとると



東京の感染者900人

存在する情報

東京の感染者900人
先週と比べて最多
病床使用率も逼迫

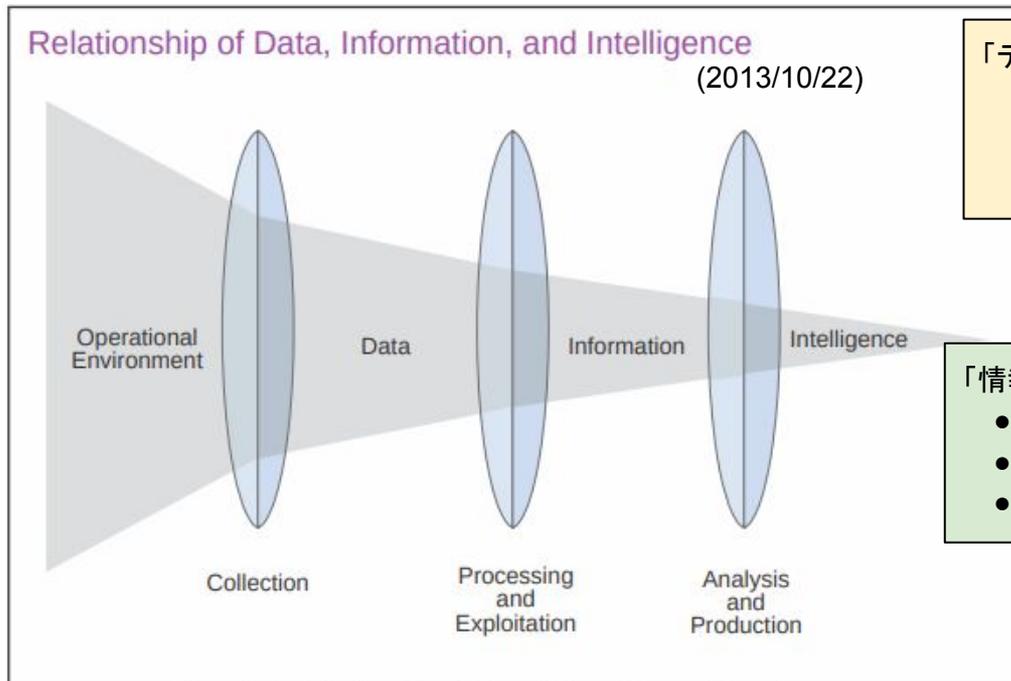
意味のある情報

オリンピックはどうする？
やるとしても無観客？
等の間に答える分析

分析し、意思決定に利
用するもの

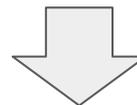
データ／情報／インテリジェンス の違い

□ 国統合参謀本部 “Joint Intelligence Joint publication 2-0” の定義



「データ」は通常、下記のような分析前のもの

- IPアドレス
- アクセスしたPort
- サーバに残されたファイルのハッシュ



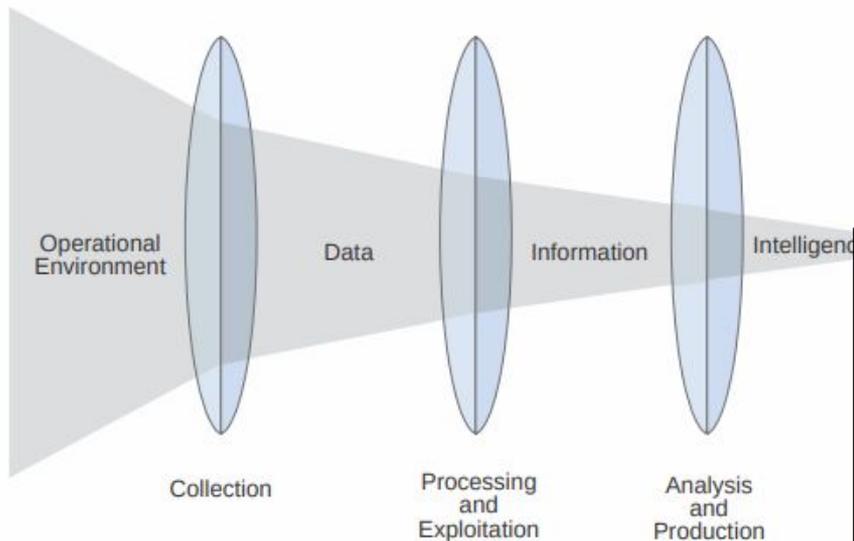
「情報」は、例えば下記のような意味の有るもの

- このIPアドレスが自組織にアクセスした回数は？
- このIPアドレスはどこの組織がどのような目的で使用してる？
- アクセスしたPortはどのような攻撃で使用されているか？

□ 国統合参謀本部 “Joint Intelligence Joint publication 2-0” の定義

Relationship of Data, Information, and Intelligence

(2013/10/22)



「情報」は、例えば下記のような意味の有るもの

- このIPアドレスが自組織にアクセスした回数は？
- このIPアドレスはどここの組織がどのような目的で使用してる？
- アクセスしたPortはどのような攻撃で使用されているか？



「インテリジェンス」は種々の情報から判断して下記を提供

- 現在どのような攻撃が自組織になされているか？
- 同様の攻撃が過去に自組織に行われていたか？
- 同様の攻撃は過去に別の組織で事例があるか？その目的は？
- 過去の攻撃情報から、被害はどのようなものが想定されるか？
- 自組織では同様の被害が発生し得るのか？
- 被害の範囲はどのくらいになるのか？

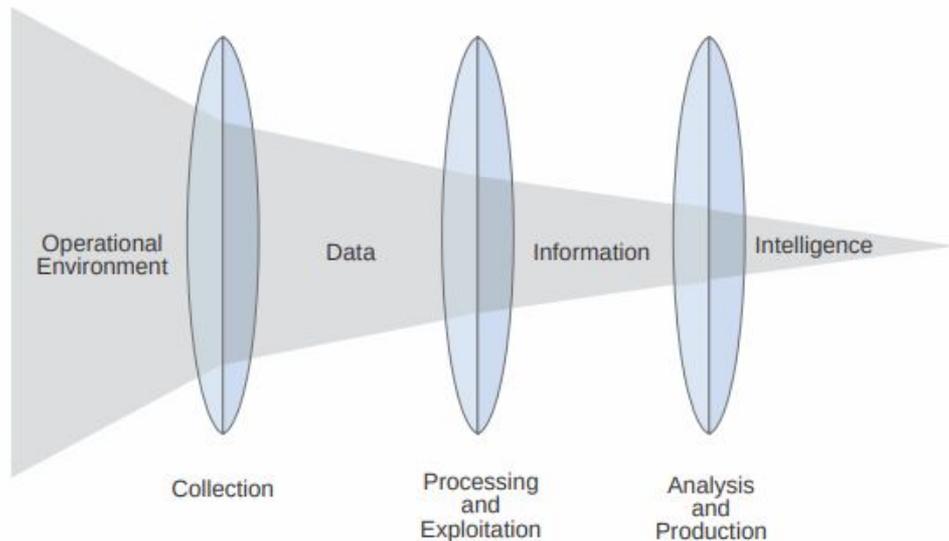
「インテリジェンス」を用いて意思決定を行い、脆弱性の修正やセキュリティ体制の改善・リスク軽減のためのアクション等を実行する。

インテリジェンス 活用の種類

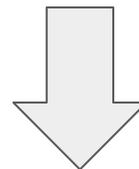
インテリジェンス活用

Relationship of Data, Information, and Intelligence

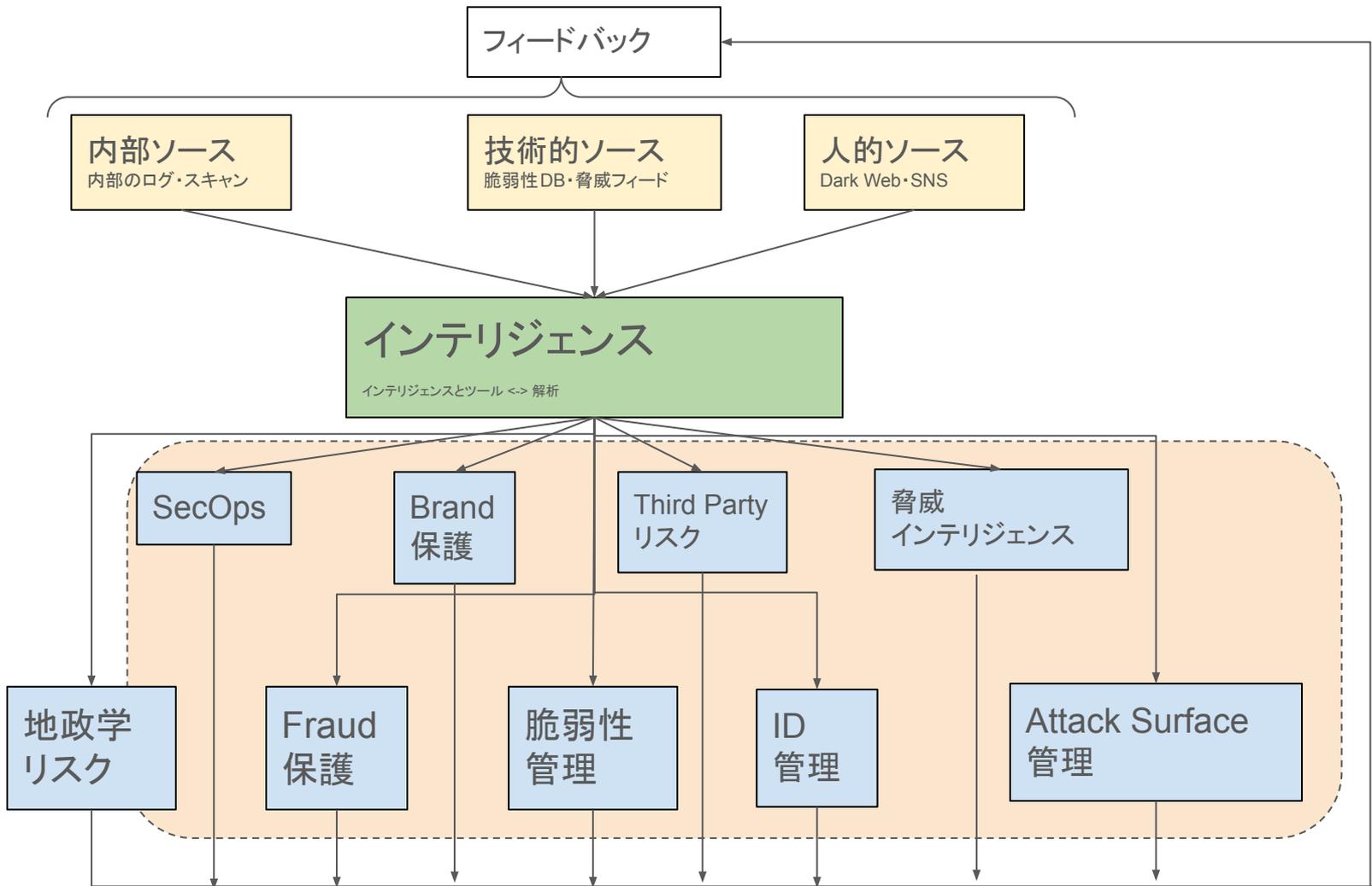
(2013/10/22)



様々なソースからデータ・情報を持ってきてインテリジェンスにします。



では、そのインテリジェンスをどの分野に活用するのか？



3.3.1. 脅威インテリジェンス

脅威をいち早くつかみ組織の防衛に利用する

- 組織にとって最大の脅威となる攻撃者を特定する
- 攻撃者の動機やターゲットを理解する
- 攻撃者のTTP
 - 戦術(Tactics)
 - 技術(Techniques)
 - 手順(Procedures)

を調査し、文書化する

- 業界や地域的特性など、組織に影響する大きな傾向を追跡する

3.3.1. 脆弱性インテリジェンス

脆弱性管理チームで使用されるインテリジェンス

- 膨大な脆弱性に対処するためのプライオリティをつける
- CVSSスコアに過大に頼らない
- ゼロデイ脆弱性にばかり気を逸らされない

ために、脅威アクターや自社ITなどをデータソースにインテリジェンスを用いて適切な脆弱性管理を行っていく

3.3.1. SecOpsインテリジェンス

- 脅威の可能性を監視する
- 疑わしいネットワークアクティビティを検出する
- 進行中の脅威を封じ込める
- 利用可能なテクノロジーによって脅威を取り除く

ためにSecOpsにインテリジェンスを活用

3.3.1. 地政学(Geopolitical)インテリジェンス

組織としてある国や地域に事業所や工場などを持っていた場合

- 政府機関による決定や活動 — 法案の可決、規制の導入、緊急時の警官隊や軍隊の動員など
- 政党、労働組合、活動家グループ、その他の組織の活動 — ストライキ、デモ、抗議、ボイコット、ソーシャルメディアキャンペーン、暴動、物理的な地点や建物を標的とする攻撃など
- 自然災害や人為的災害 — 病気の発生、ハリケーンや地震、軍事行動、テロ攻撃など

の影響を受けるため、インテリジェンスを下記のように利用する。

- 損害を予測、防止する(たとえば、大規模デモの前に施設を閉鎖する)
- 迅速な対応でイベントの影響を軽減する(たとえば、自然災害発生後に従業員を支援したり、物資の別の供給元を探したりする)
- 重要な事実を従業員、顧客、ビジネスパートナー、政府機関に伝達する
- その地域における将来的なリスクを評価し、投資や事業拡大の判断に反映する

3.3.1. ブランド(Geopolitical)インテリジェンス

下記のような企業のブランド失墜から守るためにインテリジェンスを活用する

- 偽のWebサイトやソーシャルメディアアカウントを使って組織またはその従業員になりすまして仕かけられる不正行為やフィッシング攻撃
- Webサイトやソーシャルメディアプラットフォームでの 組織やその商品に関する不正なコンテンツや偽情報の投稿
- デジタルマーケットプレイスやアプリストアでの偽造の 製品やソフトウェアの公開
- データ漏洩、従業員や経営幹部の認証情報の漏洩

3.3.1. サードパーティーインテリジェンス

- サードパーティーへの攻撃はさらに増えて悪化し、サイバーリスク管理が複雑になる
- パートナーからは最も重大な問題についておそらく教えてもらえない
- サードパーティーリスクの評価手法が静的なものに依存しているためダイナミックなリスク変化についていけない

これらから

- リアルタイムのサードパーティーインテリジェンスを使うことで、状況が変化し新たな脅威が出現しても、それに対応して評価を最新に保つ事が可能

3.3.1. Fraudインテリジェンス

Fraud(詐欺)のインテリジェンス

- 主にクレジットカード支払詐欺 や、オンライン取引に関連したその他の種類の不正の防止 に関するもの
- フロードインテリジェンスによって 複数のペイメントカードアカウントが侵害された可能性が明らかになった場合、金融機関や商店などはリスクベースのアプローチを取って取引を許可することになります。
- リスク計算に応じてユーザーはパスワードやセキュリティの質問への回答を求められたり、スマートフォンに送信されたワンタイムコードを入力するように求められたりします。特別の承認があるまで保留になるランザクションや、完全にブロックされてしまうランザクションもあります。
- このように、Fraudインテリジェンスは修復すべき脆弱性や問題を見つけるものではなく、リスク評価を手助けするものとして使われます。

3.3.1. ID管理インテリジェンス

- ID情報のリアルタイム収集
- オープンソース、ダークWeb、技術的ソースの幅広いカバレッジ
- 重複、フェイク、自社組織に脅威とはならない認証情報を排除するための効率的かつ正確なトライアージ
- 漏洩した認証情報の自動検索
- 個別ユーザー、ユーザーグループ、全事業部門のクエリと分析ツール



3.3.1. Attack Surface Managementインテリジェンス

アタックサーフェスインテリジェンスとは、インターネット経由でアクセスできるネットワークやシステムに関する情報や、そこから生じるリスクに関する情報のことです。

アタックサーフェス

- 従業員が使用しているあらゆるPC・モバイルデバイス
- サーバ、ネットワーク機器、セキュリティ機器、プリンタ等
- 仮想上のサーバ、DB、サービス、クラウド上のその他の資産
- Web接続されたセンサー、カメラ、ロボット、その他 IoTデバイス

これらに対して

- 組織のインターネットに接続された資産のすべてを検出する
- 侵害された資産を分析し、脆弱性やセキュリティ上の問題がありそうな資産を判断する
- 組織のアタックサーフェスを継続的にモニタリングしてリスクが生まれそうな新しいドメインや資産を検知する

インテリジェンスの手法

インテリジェンスの手法(ソース)の種類

1. GEOINT (Geospatial Intelligence)
 - 画像
 - IMINT (Imagery Intelligence)
 - i. 衛星写真・ドローンの写真
 - 地理情報
2. HUMINT (Human Intelligence)
 - 報告
 - 尋問
 - スパイ活動
3. SIGINT (Signal Intelligence)
 - COMINT (Communication Intelligence)
 - ELINT (Electronic Intelligence)
4. OSINT (Open Source Intelligence)
 - 学術論文
 - 各省庁間の刊行物
 - ニュース・新聞・定期刊行物
 - メディアの放送
 - 公開された財務情報
 - Internet上の公開情報
5. MASINT (Measurement and Signature Intelligence)
 - 電磁データ
 - レーダーデータ
 - 無線データ
 - 地球物理データ
 - 材料データ
 - 核放射線データ

3.3.1. OSINT (Open Source Intelligence)

オープンになっている情報源から情報を収集

- Web で公開されている情報やニュース記事
- GitHub 等のソースコード共有や会話の場所
- SNS
- 脆弱性データベース
- 公開されている既存の脆弱性の PoC
- ゼロデイ攻撃に関する公開された情報



2.4. OSINTの歴史

米国の OSS(Office of Strategic Services:戦略情報局)が 1941 年に開設した際からある手法。OSSは後のCIA。

OSS の調査分析部門は、世界中から新聞、雑誌、ラジオ放送のレポートを収集し、敵に関する重要な情報を纏めていた。

OSS は、重要なナチスのニュースを求めて、ドイツの地方紙から新しい戦艦、航空機の画像等を取得。これらは入念に照合されてまとめられ、OSS が敵の状態を評価する為に使用されていた。



(参考: <https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/>)

3.3.2. HUMINT (Human Intelligence)

人間を介して情報を収集

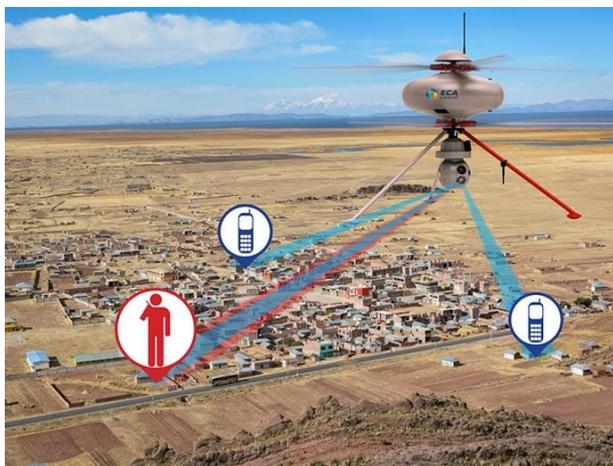
- ・ 標的となる会社から何らかの方法で信頼を勝ち取り、内部情報を入手
- ・ 標的となる会社の社員と個人的な信頼関係を築き、内部情報を収集
- ・ コミュニティ、業界固有の情報共有の場での会話による情報収集
- ・ ダーク Web フォーラム等での会話での情報収集



3.3.3. SIGINT (Signal Intelligence)

電話や無線・GPS・Wifi等から情報を収集

- 電話を盗聴して会話から情報を収集
- 無線 LAN を解読して情報を取得
- 無線傍受による相手の動向の分析



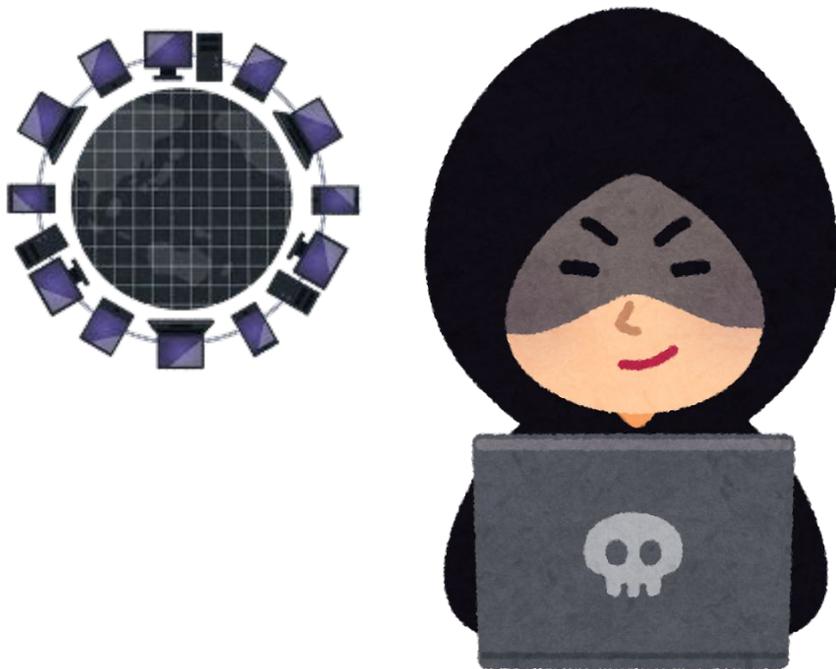
Signals Intelligence (SIGINT) collection
ships of European Navies in 2016

©NAVALANALYSES.BLOGSPOT.COM

			Ships: <i>Oste, Oker, Alster</i> Commissioned: 1988 Displacement f.l.: 3,200t Length: 83.5 m	
			Ship: <i>Dupuy de Lôme</i> Commissioned: 2006 Displacement f.l.: 3,600t Length: 101.7m	
			Ships: <i>Hydrograf, Navigator</i> Commissioned: 1975 Displacement f.l.: 1,675t Length: 73.3 m	
			Ship: <i>Marjata II</i> Commissioned: 2016 Displacement f.l.: ?t Length: 126m	
			Ship: <i>Marjata I</i> Commissioned: 1995 Displacement f.l.: 7,560t Length: 81.5 m	
			Ship: <i>Elettra</i> Commissioned: 2003 Displacement f.l.: 3,000t Length: 93.5 m	
			Ship: <i>Orion</i> Commissioned: 1984 Displacement f.l.: 1,400t Length: 61.2 m	
			Ship: <i>Alerta</i> Commissioned: 1982 Displacement f.l.: 2,290t Length: 76.5 m	

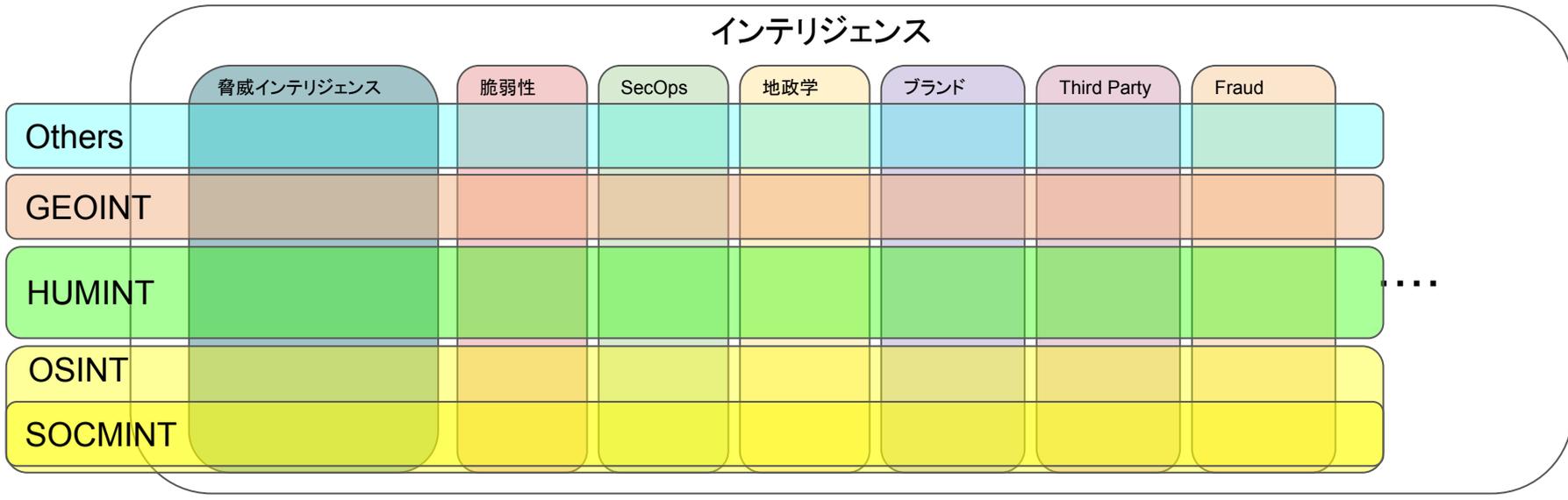
3.3.4. DARKINT (Dark Web Intelligence)

ダークウェブから情報を収集する活動(近年の新しいジャンル)



インテリジェンスの 種類と手法の関係

インテリジェンスの種類と手法の関係



脅威インテリジェンスとは？

脅威インテリジェンス

Gartnerのレポートによる定義 (2013年5月)

「脅威インテリジェンスとは、コンテキスト、メカニズム、指標、影響、実行可能なアドバイスなど、資産に対する既存または新たな脅威またはハザードに関する実際の証拠に基づいた知識であり、その脅威またはハザードに対する対象者の対応に関する決定を通知するために使用できる。」



脅威インテリジェンス (Gartnerレポート定義)

脅威が**脆弱性**を悪用して**インシデント**を発生させる

殆どの場合、脅威は制御出来無い。脅威を認識し、可能な場合は回避、回避できない場合は特定の防御を開発する必要がある。

殆どの場合、脆弱性は制御出来る。

セキュリティインシデントは避けたい。インシデントの結果の制御は限られている。

脅威インテリジェンス : 脅威に関する情報であり、収集・照合・検証・評価・解釈など、**何らかの処理**を通じて生成された特定の情報である。

つまり脅威インテリジェンスとは

- 組織がセキュリティを向上する際に、**追加情報として関連付けることができる情報**
- 詳細な分析または複数のデータの相関から抽出された付加価値情報が含まれる。
 - 攻撃者または開発者の目的／脅威が脆弱性を悪用出来る条件
 - 脅威の亜種／脅威に関連した現在の活動
 - 脅威が実行された場合の組織の受けるダメージ
 - 脅威が組織資産に対して現在作用しているか・損害を与えているか等を示す指標
 - 脅威に対する防御方法
- 脅威を回避する方法や潜在的な影響を軽減する方法など、脅威に備えるために使用できる。
- 識別、評価、検証、修復等、**脅威に起因するインシデントに対応するために使用できる。**

(例) サードベンダーが金融機関Aに対して

以下を纏める

- Lazarusグループ(北朝鮮)が金融機関をターゲットにした攻撃を行っていること
- どの様な攻撃を行うのか、DDoS等のサービス不能か、或いは情報の搾取か、等
- 攻撃を行う際のツール・使用される IPや通信プロトコルなどの技術的な特徴

以上から金融機関Aに対して **脅威に備えられる様な情報を提供** する

- Lazarusグループに狙われる可能性
- 狙われた場合に攻撃から守るような設定情報
- 攻撃が起きた場合の、痕跡の見分け方
- 攻撃を防げなかった場合の被害想定



脅威インテリジェンスとなる

脅威インテリジェンスとは

情報に基づく意思決定を行い対策をとるためのコンテキストを提供するもの

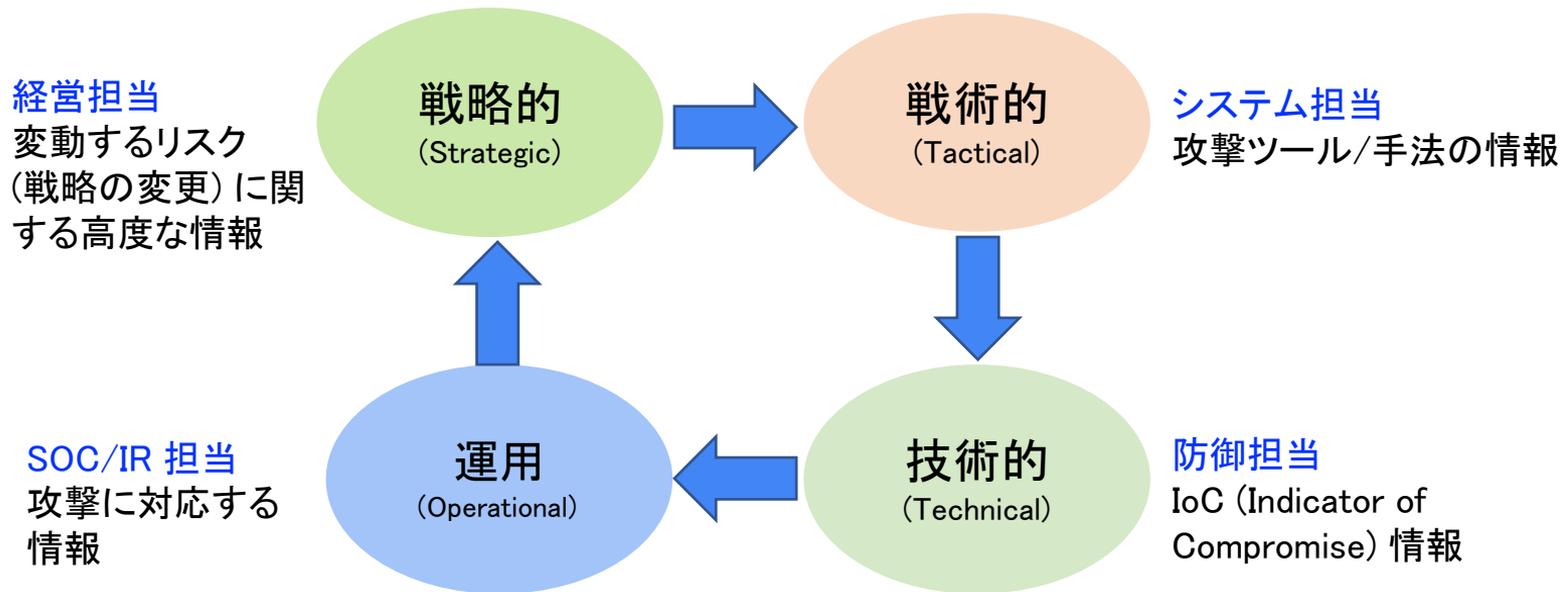
- 豊富なソースを基にした情報と分析が、容易に理解して使用できる形で提示される
- サイバーセキュリティ組織の主要なチームすべてにとって非常に有益である
- あらゆるセキュリティ部門の時間節約に寄与する
- ほとんどの部分を既存のセキュリティ担当スタッフで処理できる（適切なツールとサポートがある場合）



引用: 脅威 インテリジェンス ハンドブック (第3版)

Recorded Future

脅威インテリジェンスの分類



CTI Information Sharing

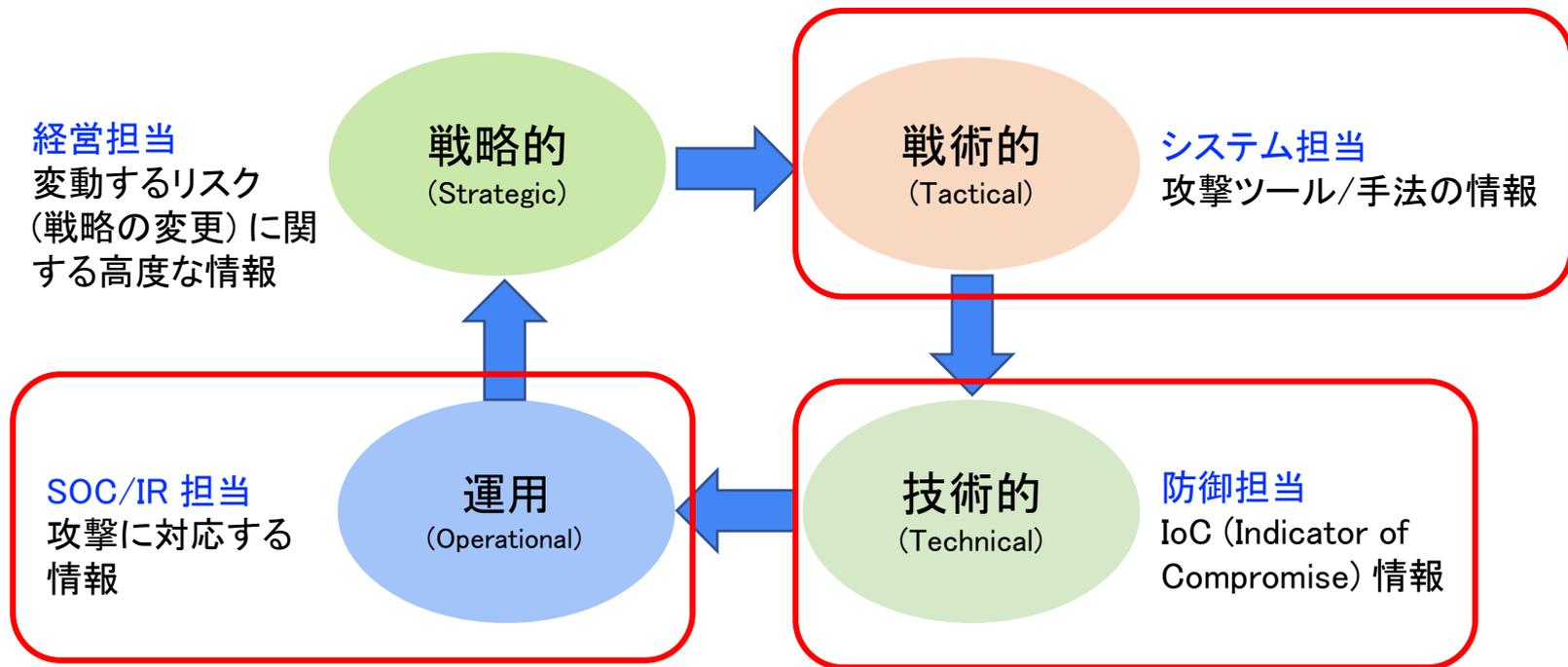
<https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/cti-information-sharing/>

Threat Intelligence: Collecting, Analysing, Evaluating

<https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf>

脅威インテリジェンスのどこで脆弱性が関わってくるのか

脅威インテリジェンスの分類



CTI Information Sharing

<https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/cti-information-sharing/>

Threat Intelligence: Collecting, Analysing, Evaluating

<https://www.foo.be/docs/informations-sharing/Threat-Intelligence-Whitepaper.pdf>

サイバーキルチェーン

サイバーキルチェーンとは

2009年にロッキード・マーチン社が提唱したものです。

攻撃者が標的を決定し、攻撃から目的を達成するまでの一連の行動を

1. 「偵察(Reconnaissance)」
2. 「武器化(Weaponization)」
3. 「デリバリー(Delivery)」
4. 「エクスプロイト(Exploitation)」
5. 「インストール(Installation)」
6. 「C&C(Command and Control)」
7. 「目的の実行(Actions on Objectives)」

の7フェーズに分けています。



RECONNAISSANCE

Harvesting email addresses, conference information, etc.



DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.



INSTALLATION

Installing malware on the asset



ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals



WEAPONIZATION

Coupling exploit with backdoor into deliverable payload



EXPLOITATION

Exploiting a vulnerability to execute code on victim's system



COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

1. 「偵察 (Reconnaissance)」
2. 「武器化 (Weaponization)」
3. 「デリバリー (Delivery)」
4. 「エクスプロイト (Exploitation)」
5. 「インストール (Installation)」
6. 「C&C (Command and Control)」
7. 「目的の実行 (Actions on Objectives)」

1. Reconnaissance (偵察)

攻撃者が外部から被害者の状況を評価し、脆弱性と侵入ポイントを特定します。
この段階では、次の作業が行われます。

- OSINTによるデータ収集
- スパイツールの展開
- スキャンツールやサービス等を利用し、システムやアプリケーションの特定・および(あれば)脆弱性など弱点の調査

平たくいうと、目をつける



2. Weaponization (武器化)

攻撃者はマルウェアや悪意のあるペイロードを作成し、Reconnaissance (偵察) で特定した弱点を悪用します。

このプロセスには、新しいマルウェアの開発や、特定の脆弱性で使用できるように既存のプログラムをカスタマイズすることが含まれます。

目をつけた脆弱性を悪用する
プログラムを作る



3. Delivery (配送)

攻撃者はマルウェアを配送し、標的のネットワークへ侵入を試みます。

一般的には

- フィッシングメールの送信
- SNSツールの使用
- ハードやソフトの脆弱性の悪用

などが含まれます。



4. Exploitation (エクスプロイト)

マルウェアが配送された後に、攻撃者は標的の脆弱性を悪用して侵入をさらに進めます。

多くの場合、攻撃者は標的となる組織のシステムに侵入した後に横方向に移動 (Lateral Movement) して、より多くの侵入ポイントと脆弱性等を特定します。



5. Installation (インストール)

攻撃者は、標的のネットワークの更なる制御のために、マルウェアをインストールします。これには

- トロイの木馬
- アクセストークンの操作
- コマンドラインインターフェース (CLI)
- バックドアを使用した権限の昇格
- アクセス権限の変更

等が含まれます。



6. Command & Control (C&C)

攻撃者はCommand & Control (C2) チャネルを確立し、インストール・展開したツールをリモートで監視・制御します。

攻撃者は難読化技術を使用して痕跡を隠し、DoS等を併用して標的の注意を攻撃の目的からそらしたりします。



7. Action (アクション)

最終段階では、次のような目的を実行します。

- データの盗難
- 暗号化
- サプライチェーン攻撃



MITRE ATT&CK

MITRE ATT&CKはサイバー攻撃を行ってくる攻撃グループ等の「敵対者」側が、そのライフサイクルの間にどのような行動をするのかを、敵対者側の視点に立って分類したものです。

- Tactics: 敵対者のゴール
- Techniques: Tacticsの内容を更に細かく記述したもので「技術」レベル
- Procedures: Techniquesの内容を、更に下位レベルから非常に詳細に記述したもの

となっています。

MITRE ATT&CKとサイバーキルチェーンの関係

ざっくりレベル。元々背後の発想が違うのでそれぞれが対応しているわけではない。

サイバーキルチェーンは大まかな目的別

MITRE ATT&CKは攻撃者の行動を記述するLowレベル

CYBER KILL CHAIN VS. MITRE ATT&CK



脅威アクターと
使用する脆弱性

脅威アクター種別

1. 国家が背後にいる脅威アクター
 - a. 中国、ロシア、イラン
2. 金銭目的とされる脅威アクター
 - a. 代表的なものを取り上げる

MITRE ATT&CKのTTPと脆弱性の結びつき

1. 「脆弱性を悪用して攻撃された・・・」とよく言われるが、果たしてどのフェーズで脆弱性が悪用されているのか？
2. 代表的な脅威アクターを幾つか選び、脆弱性とその脆弱性がどのTactics/Techniquesで使用されていたのかを確認する。

1. 国家が背後にいる 脅威アクター

1-1. ロシア

ロシアが背後にいるとされている脅威アクター(攻撃者)

大凡62組織が該当。以下、代表的なもの

- BlueDelta (APT28, Fancy Bear, Forest Blizzard, Iron Twilight, Pawn Storm, Sednit, Sofacy, Strontium, TAG-75, Tsar Team)
- BlueBravo (APT29, Cozer, Cozy Bear, Cozy Duke, CozyCar, EuroAPT, Midnight Blizzard, NOBELIUM, Office Monkeys, RUS2, The Dukes, UNC2452)
- Sandworm Team (BE2 APT, Quedagh, Seashell Blizzard, UAC-0082)
- Turla Group (Group 88, KRYPTON, Secret Blizzard, Snake, Venomous Bear, Waterbug)
- Berserk Bear (BROMINE, Crouching Yeti, DYMALLOY, Dragonfly, Energetic Bear, Ghost Blizzard, Koala Team, TEMP.Isotope)
- Gamaredon Group (Aqua Blizzard, Armageddon Group)
- BlueCharlie (COLDRIVER, Callisto Group, Gossamer Bear, Iron Frontier, SEABORGIUM, Star Blizzard, TA446, TAG-53)
- GRU 85 Main Special Service Center (85th Central Research Institute, в/ч 26165)
- UAC-0056 (FROZENVISTA, Lorec53, UNC2589)

ロシアが背後にいる脅威アクター

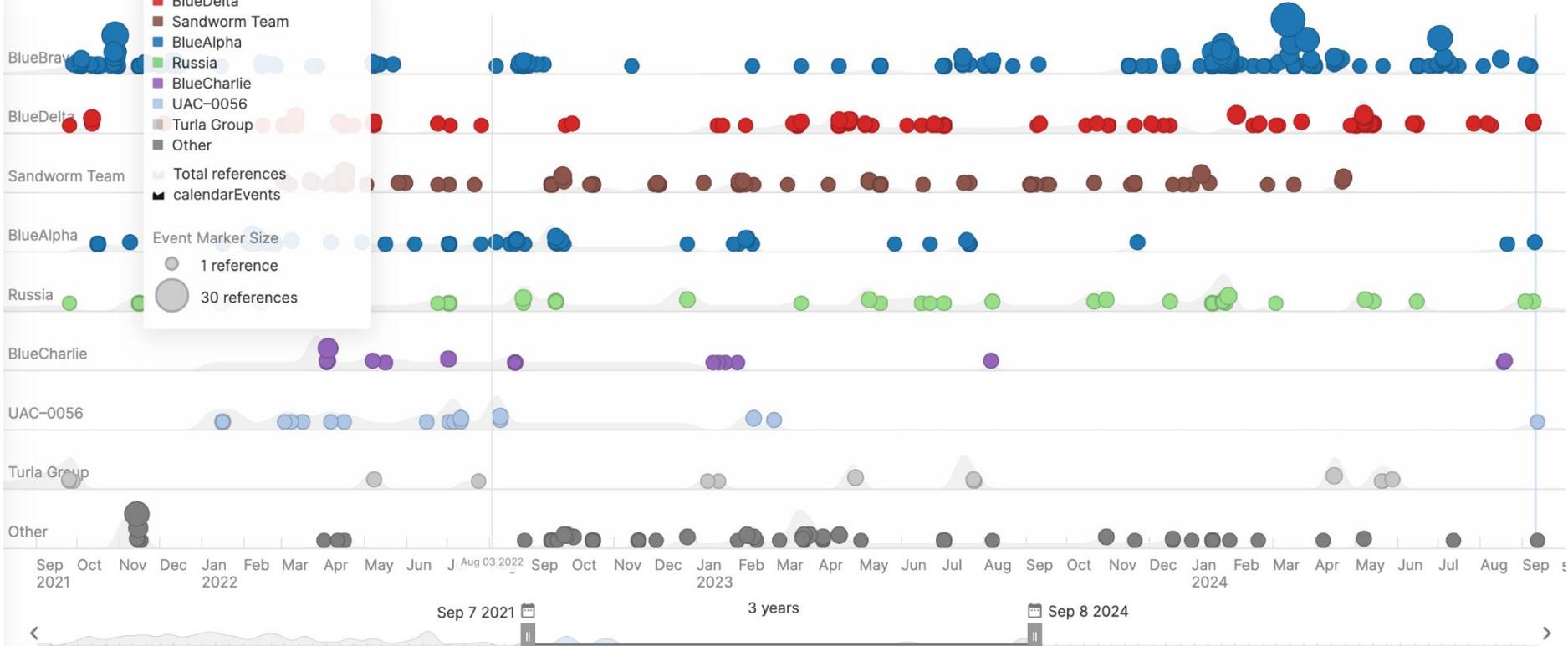
2021-2024

Colors

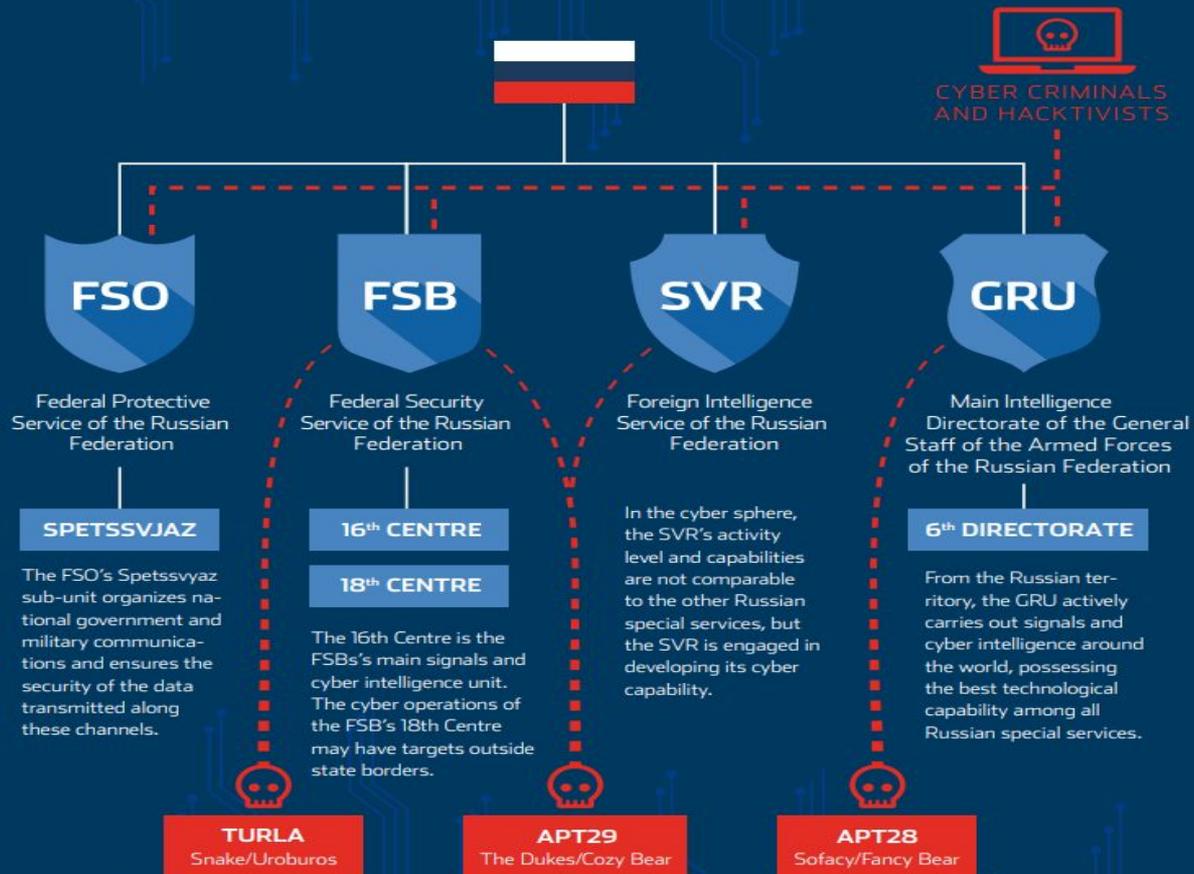
- BlueBravo
- BlueDelta
- Sandworm Team
- BlueAlpha
- Russia
- BlueCharlie
- UAC-0056
- Turla Group
- Other

Event Marker Size

- 1 reference
- 30 references



WHO'S WHO IN RUSSIAN CYBER ESPIONAGE?



2018年時点での分析

- APT29
- APT28
- Turla

APT – or *Advanced Persistent Threat* – carefully targets and combine multiple techniques to obtain the needed information.

1-1. ロシア政府組織と脅威アクター(CISA: 2022)

- ロシア連邦保安局 (FSB) (FSB のセンター 16 およびセンター 18 を含む)
 - BERSERK BEAR(DragonFly)
- ロシア対外情報局 (SVR)
 - **APT29**
- ロシア参謀本部情報総局 (GRU)、第 85 中央特別サービスセンター (GTsSS)
 - **APT28**
- GRU 特殊技術主要センター (GTsST)
 - **Sandworm**
- ロシア国防省、中央化学機械研究所 (TsNIIKhM)
 - XENOTIME

APT29, APT28, Sandwormについて、それぞれ見ていきます。

APT29 TTPs

Tactic	ID	Technique	Procedure
Credential Access	T1110	Brute Force	SVR は、初期感染ベクトルとしてパスワード スプレーとブルート フォースを使用します。
Initial Access	T1078.004	Valid Accounts: Cloud Accounts	SVR は侵害された資格情報を使用して、システムアカウントや休止アカウント等のクラウドサービスアカウントにアクセスします。
Credential Access	T1528	Steal Application Access Token	SVR は盗まれたアクセストークンを使用して、パスワードを使用せずにアカウントにログインします。
Credential Access	T1621	Multi-Factor Authentication Request Generation	SVR は被害者がアカウントへのSVRのアクセスを許可するまで、被害者のデバイスにMFA リクエストをプッシュします。
Command and Control	T1090.002	Proxy: External Proxy	SVR はアクセスログ内の予想されるIPアドレスに紛れ込むために、Home IP Rangeのオーブンプロキシを使用します。
Persistence	T1098.005	Account Manipulation: Device Registration	SVR はアカウントへのアクセス権を取得した後、クラウドテナントに独自のデバイスを登録しようとします。

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Valid Accounts		Scheduled Task/Job		Modify Authentication Process		System Service Discovery	Remote Services	Data from Local System	Data Obfuscation	Exfiltration Over Other Network Medium	Data Destruction
Replication Through Removable Media	Windows Management Instrumentation	Valid Accounts		Network Sniffing			Software Deployment Tools	Data from Removable Media	Fallback Channels	Exfiltration Over Network Medium	Data Encrypted for Impact
		Hijack Execution Flow		OS Credential Dumping					Application Layer Protocol	Scheduled Transfer	Service Stop
Trusted Relationship	Software Deployment Tools	Boot or Logon Initialization Scripts		Direct Volume Access	Input Capture	Application Window Discovery		Replication Through Removable Media	Proxy	Data Transfer Size Limits	Inhibit System Recovery
Supply Chain Compromise		Creates or Modify System Process		Rootkit	Brute Force	System Network Configuration Discovery			Data Staged	Communication Through Removable Media	Defacement
Hardware Additions	Shared Modules	Event Triggered Execution		Obscured Files or Information	Two-Factor Authentication Interception	System Owner/User Discovery		Internal Spearphishing	Screen Capture		Firmware Corruption
Exploit Public-Facing Application	User Execution	Boot or Logon Autostart Execution							Use Alternate Authentication Material	Email Collection	Web Service
Phishing	Exploitation for Client Execution	Account Manipulation	Process Injection		Exploitation for Credential Access			Clipboard Data	Multi-Stage Channels		Network Denial of Service
External Remote Services	System Services	External Remote Services	Access Token Manipulation			System Network Connections Discovery	Lateral Tool Transfer	Automated Collection	Ingress Tool Transfer	Exfiltration Over Web Service	Endpoint Denial of Service
Drive-by Compromise	Command and Scripting Interpreter	Office Application Startup	Group Policy Modification		Steal Web Session Cookie		Taint Shared Content	Audio Capture	Data Encoding	Web Service	System Shutdown/Reboot
		Create Account	Abuse Elevation Control Mechanism		Unsecured Credentials	Permission Groups Discovery	Exploitation of Remote Services	Video Capture	Traffic Signaling	Automated Exfiltration	Account Access Removal
		Browser Extensions	Exploitation for Privilege Escalation	Indicator Removal on Host	Credentials from Password Stores			Man in the Browser	Remote Access Software	Exfiltration Over Alternative Protocol	Disk Wipe
		Traffic Signaling		Modify Registry			File and Directory Discovery	Remote Service Session Hijacking	Data from Information Repositories	Dynamic Resolution	Alternative Protocol
	Inter-Process Communication	BITS Jobs		Trusted Developer Utilities Proxy Execution	Steal or Forge Kerberos Tickets	Peripheral Device Discovery		Man-in-the-Middle	Non-Standard Port	Transfer Data to Cloud Account	
		Server Software Component		Traffic Signaling	Forced Authentication			Archive Collected Data	Protocol Tunneling		
		Pre-OS Boot		Signed Script Proxy Execution	Steal Application Access Token	Network Share Discovery		Data from Network Shared Drive	Encrypted Channel		
		Compromise Client Software Binary		Rogue Domain Controller	Man-in-the-Middle	Password Policy Discovery		Data from Cloud Storage Object	Non-Application Layer Protocol		
		Implant Container Image		Indirect Command Execution		Browser Bookmark Discovery					
				BITS Jobs		Virtualization/Sandbox Evasion					
				XSL Script Processing		Cloud Service Dashboard					
				Template Injection		Software Discovery					
				File and Directory Permissions Modification		Query Registry					
				Virtualization/Sandbox Evasion		Remote System Discovery					
				Unused/Unsupported Cloud Regions		Network Service Scanning					
				Use Alternate Authentication Material		Process Discovery					
				Impair Defenses		System Information Discovery					
				Hide Artifacts		Account Discovery					
				Masquerading		System Time Discovery					
				Deobfuscate/Decode Files or Information		Domain Trust Discovery					
				Signed Binary Proxy Execution		Cloud Service Discovery					
				Exploitation for Defense Evasion							
				Execution Guardrails							
				Modify Cloud Compute Infrastructure							
				Pre-OS Boot							
				Subvert Trust Controls							

LEGEND

- APT28
- APT29
- Both

Comparing APT28 to APT29

3-1-1. 米国／EUへの攻撃 (APT29)

2013年～2019年

「Operation Ghost」

ノルウェー 最新ニュース ドキュメンタリー 気候 NRK声明

ノルウェーが大規模なハッカー攻撃にさらされる

PSTは1月、PST、外務省、労働省、および複数の政府関係者に対するロシアのハッカー攻撃について協力機関から通報を受けた。PSTによると、ハッキングの試みは「悪意のある」ものだったに違いないという。



パー＝ウィリー・アムンセン法務大臣、ハッキングについて語る

スニバ・レベッカ・シエゲグス
タッド
ジャーナリスト
ハラルド・ストルト・ニールセン
ジャーナリスト
ライントムター
ジャーナリスト
エレン・オムランド
ジャーナリスト
アニャ・ストロネン
ジャーナリスト

発行済み 2月3日 2017年 22時08分
更新しました 2月4日 2017年 00:02

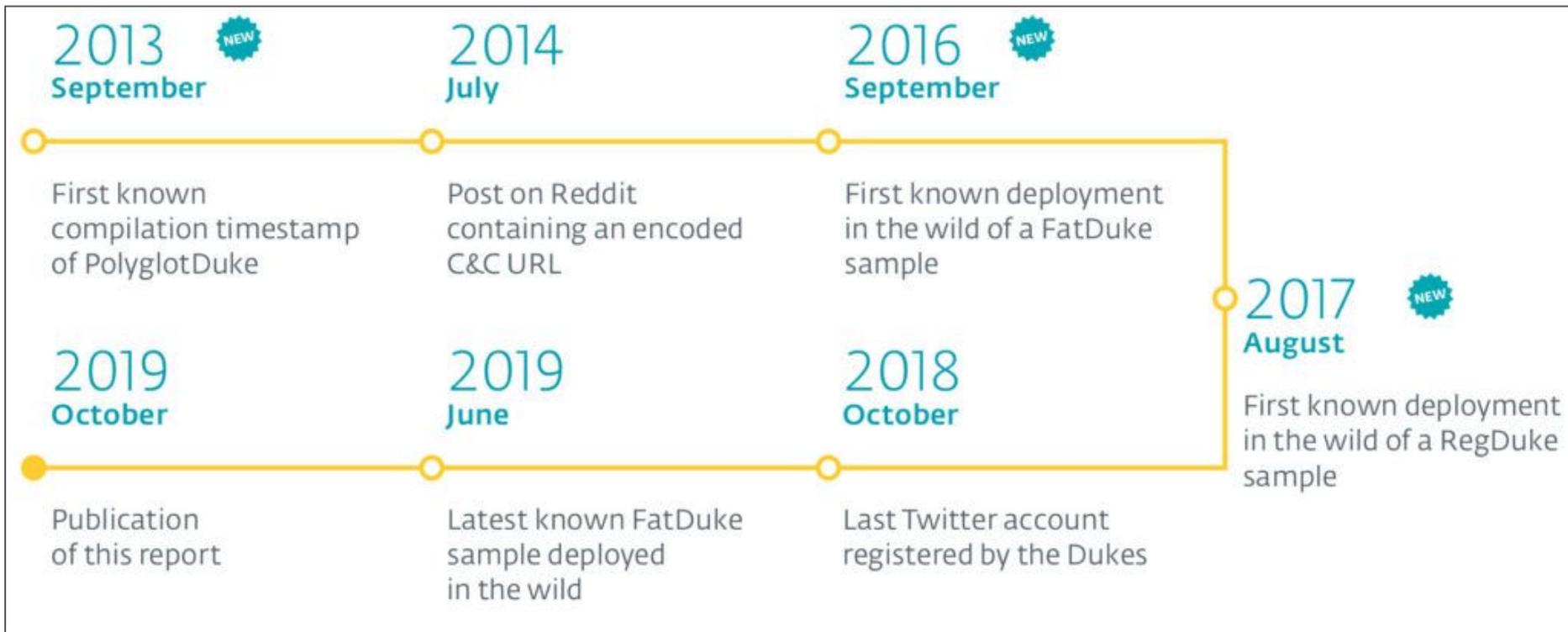


この記事は数年前のものです。

ワシントンD.C.にあるEU加盟国の大使館や、ヨーロッパの少なくとも3か国の外務省に侵入

2017年にはノルウェーへのフィッシング攻撃

「Operation Ghost」タイムライン



この一連の流れをESETが「Operation Ghost」と命名

2016年米国大統領 選挙(APT28, APT29)

2016年

2016年「GRIZZLY STEPPE」(APT28)

REUTERS®

ワールド▼ マーケット▼ 経済▼ ビジネス▼ オピニオン▼ ライフ▼

ワールド

米民主党へのサイバー攻撃、クリントン氏「ロシアが関与」

Reuters

2016年8月1日 午前 7:46 GMT+9 · 8年前更新

Aa <



7月31日、米民主党全国委員会のコンピューターがサイバー攻撃を受けたことについて、民主党大統領候補のヒラリー・クリントン氏は、ロシアの情報機関が関与したと断言した。オハイオ州ヤングスタウンで30日撮影（2016年 ロイター/AARON P. BERNSTEIN）

米国選挙に関連するネットワークやエンドポイント・米国政府・政治・民間の様々な組織を侵害。

- APT28は標的となった組織のドメインを模倣した偽ドメインを使用し、短縮URL等を用いて被害者をだまして、正規の資格情報を入力させていました。
- 2016年春、APT28は偽のWeb メールドメインを通じて同政党(民主党)の受信者をだまし、パスワードを変更させました。APT28は収集した認証情報を使用してアクセスを取得し、コンテンツを盗むことができ、これにより複数の民主党幹部からの情報の流出につながった可能性があります。

2016年「GRIZZLY STEPPE」(APT29)

REUTERS®

ワールド▼ マーケット▼ 経済▼ ビジネス▼ オピニオン▼ ライフ▼

ワールド

米民主党へのサイバー攻撃、クリントン氏「ロシアが関与」

Reuters

2016年8月1日 午前 7:46 GMT+9 · 8年前更新

Aa ↩

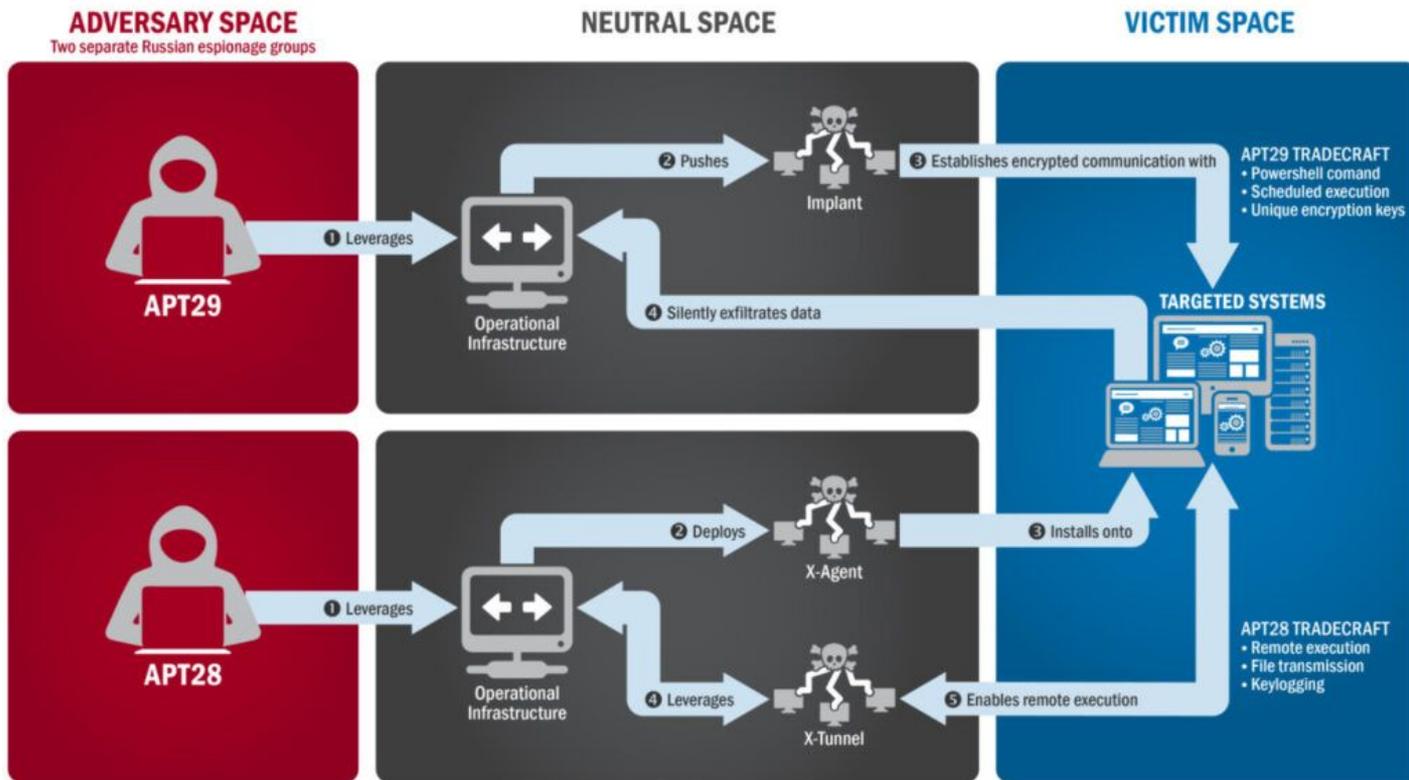


7月31日、米民主党全国委員会のコンピューターがサイバー攻撃を受けたことについて、民主党大統領候補のヒラリー・クリントン氏は、ロシアの情報機関が関与したと断言した。オハイオ州ヤングスタウンで30日撮影（2016年 ロイター/AARON P. BERNSTEIN）

ロシアの文民・軍事情報局(RIS)が、米国選挙に関連するネットワークやエンドポイント・米国政府・政治・民間の様々な組織を侵害。

- APT29は米国の政党(民主党)が使用しているシステムへの侵入に成功しました。
- APT29は民主党のシステムにマルウェアを配信・永続性を確立・権限を昇格させ、Active Directoryのアカウントを列挙して、暗号化された接続を通じて**複数のアカウントから電子メールを流出**させました。

TacticsとTechniques(2016年米国大統領選挙)



APT29は 2015年夏
に民主党のシステム
に侵入

APT28は 2016 年春
に侵入

APT29

CVE-2021-26855	Exchangeサーバ	リモートコード実行	Reconnaissance - Active Scanning	T1595.002
CVE-2019-19781	Citrix Application Delivery Controller (ADC) and Gateway	リモートコード実行	Initial Access - Exploitation	T1190
CVE-2019-11510	Pulse Secure Connect Server	任意のファイル読み込み	Initial Access - Exploitation	T1190
CVE-2018-13379	Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性	システムファイルのダウンロード	Initial Access - Exploitation	T1190
CVE-2019-9670	Zimbra Collaboration Suite	XML Externaly Entity Injection	Initial Access - Exploitation	T1190
CVE-2020-0688	Exchangeサーバ	リモートコード実行	Initial Access - Exploitation	T1190
CVE-2019-1653	Cisco Small Business	ルータ設定ファイルのダウンロード	Initial Access - Exploitation	T1190
CVE-2023-42793	JetBrains TeamCity	認証迂回によるリモートコード実行	Initial Access - Exploitation	T1190
CVE-2019-2725	Oracle WebLogic Server	Oracle WebLogic Serverの操作を奪取	Initial Access - Exploitation	T1190
CVE-2020-14882	Oracle WebLogic Server	Oracle WebLogic Serverの操作を奪取	Initial Access - Exploitation	T1190
CVE-2020-4006	VMware Workspace One Access	コマンドインジェクション	Initial Access - Exploitation	T1190
CVE-2021-21972	vSphere Client	Port443を通じてのコード実行	Initial Access - Exploitation	T1190
CVE-2019-9670	Zimbra Collaboration Suite	XML Externaly Entity Injection	Initial Access - Exploitation	T1190
CVE-2019-7609	Kibana	Java Scriptコード実行	Initial Access - Exploitation	T1190
CVE-2020-5902	BIG-IP	リモートコード実行	Initial Access - Exploitation	T1190
CVE-2023-38831	WinRAR	任意のコード実行	Initial Access - Exploitation	T1190
CVE-2021-36934	Windows	権限昇格	Privilege Escalation - Exploitation for Privilege Escalation	T1068
CVE-2022-30170	Windows Credential Roaming Service	権限昇格	Privilege Escalation - Exploitation for Privilege Escalation	T1068
CVE-2021-27065	Exchangeサーバ	リモートコード実行	Persistence	T1505.003
CVE-2021-26858	Exchangeサーバ	リモートコード実行	Persistence	T1505.003
CVE-2023-42793	JetBrains TeamCity	認証迂回によるリモートコード実行	Executoin - Exploitation for Client Execution	T1203

APT28

CVE-2020-17144	Exchangeサーバ	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2017-6742	Cisco	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2022-30190	Microsoft Support Diagnostic Tool	リモートコード実行	Initial Access - Phishing	T1566
CVE-2020-35730	RoundCube Webmail	XSS	Initial Access - Phishing	T1566
CVE-2021-44026	RoundCube Webmail	SQLインジェクション	Initial Access - Phishing	T1566
CVE-2023-38831	WinRAR	任意のコード実行	Initial Access - Phishing	T1566
CVE-2020-0688	Exchangeサーバ	リモートコード実行	Initial Access - Phishing	T1566
CVE-2022-38028	Windows Print Spooler	権限昇格	Privilege Escalation - Exploitation for Privilege Escalation	T1068
CVE-2015-1701	Windows	権限昇格	Privilege Escalation - Access Token Manipulation	T1134.
CVE-2021-44026	RoundCube Webmail	SQLインジェクション	Execution - Exploitation for Client Execution	T1203
CVE-2023-23397	Microsoft Outlook	権限昇格	Execution - Exploitation for Client Execution	T1203
CVE-2022-30190	Microsoft Support Diagnostic Tool	リモートコード実行	Execution - Exploitation for Client Execution	T1203
CVE-2020-12641	RoundCube Webmail	システムファイルのダウンロード	Execution - Exploitation for Client Execution	T1203
CVE-2020-35730	RoundCube Webmail	XSS	Execution - Exploitation for Client Execution	T1203
CVE-2023-38831	WinRAR	任意のコード実行	Execution - Exploitation for Client Execution	T1203
CVE-2020-0688	Exchangeサーバ	リモートコード実行	Execution - Exploitation for Client Execution	T1203
CVE-2017-0262	Microsoft Office	リモートコード実行	Execution - Exploitation for Client Execution	T1203
CVE-2023-23397	Microsoft Outlook	権限昇格	Collection - Automated Collection	T1119

3-3-1. ウクライナへの攻撃 (Sandworm)

2022-2024年頃

2022年のウクライナ変電所攻撃



コンピューティング

Russian hackers tried to bring down Ukraine's power grid to help the invasion

ロシアがウクライナへ大規模サイバー攻撃、送電網が標的に

ウクライナとの地上戦で苦戦しているロシアが、ウクライナへのサイバー攻撃を強化している。送電網を標的とした大規模な攻撃が確認され、一部は成功した模様だ。

世界最先端の

REUTERS®

ワールド▼ マーケット▼ 経済▼ ビジネス▼ オピニオン▼

ワールド

ウクライナ、電力施設へのサイバー攻撃阻止 ロシア軍ハッカーか

Reuters

2022年4月12日 午後 11:33 GMT+9 · 2年前更新

Aa ↵

A photograph of several Ukrainian national flags (blue and yellow) flying against a blue sky with light clouds.

攻撃の一部は成功した模様

ICS

2022年のウクライナ変電所攻撃

1. 被害者の変電所環境の監視制御およびデータ収集 (SCADA) 管理インスタンスに三ヶ月ほど掛けて侵入していました。
2. 攻撃者はまず、OTにliving-off-the-land攻撃 (LOTL: 所謂ファイルレスマルウェアで検出を困難にする攻撃) を使用して変電所のブレーカーを落とし、ウクライナ全土の重要インフラへの大量ミサイル攻撃と同時に計画外の停電を引き起こしました。
3. Sandworm はその後、被害者の IT 環境に CADDYWIPER (データを完全破壊するワイパー型マルウェア) を用いて2回目の攻撃を実行しました。

2023年8月 ウクライナ軍の Androidから情報を盗み出すスパイウェアについて警告が发せられる。



「Infamous Chisel」マルウェアは、感染端末においてネットワークを監視。

「SSH」や「Tor」経由で外部からアクセスでき、ネットワーク環境の調査やファイルを取得する機能を搭載。端末情報のほか、ウクライナ軍が利用するアプリケーションなどの情報などが窃取されていた。

Sandworm

CVE-2022-30190	Microsoft Support Diagnostic Tool	リモートコード実行	Initial Access - Phishing	T1566
CVE-2023-38831	WinRAR	任意のコード実行	Initial Access - Phishing	T1566
CVE-2019-10149	Exim	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2022-30190	Microsoft Support Diagnostic Tool	リモートコード実行	Execution - Exploitation for Client Execution	T1203
CVE-2014-4114	Microsoft Windows	任意のコード実行	Execution - Exploitation for Client Execution	T1203
CVE-2013-3906	Microsoft Windows	任意のコード実行	Execution - Exploitation for Client Execution	T1203
CVE-2023-38831	WinRAR	任意のコード実行	Execution - Exploitation for Client Execution	T1203

1-2. 中国

中国が背後にいるとされている脅威アクター（攻撃者）

大凡140組織が該当。以下、代表的なもの

- **RedGolf (APT41, BRONZE ATLAS, Barium, Blackfly, Brass Typhoon, Earth Baku, Red Kelpie, Wicked Panda, Winnti Group)**
- APT19 (BRONZE FIRESTONE, Black Vine, CHLORINE, Deep Panda, KungFu Kittens, PinkPanther, Pupa , Shell Crew)
- **RedDelta (BRONZE PRESIDENT, HoneyMyte, Mustang Panda, Red Lich, TA416, Twill Typhoon, Vertigo Panda)**
- **VoltTyphoon**
- APT1 (61398部隊, BRONZE SUNSET, Comment Crew, Comment Panda, FLUORINE, PLA Unit 61398, TG-8223)

中国が背後にいる脅威アクターによる攻撃

2021-2024 9月

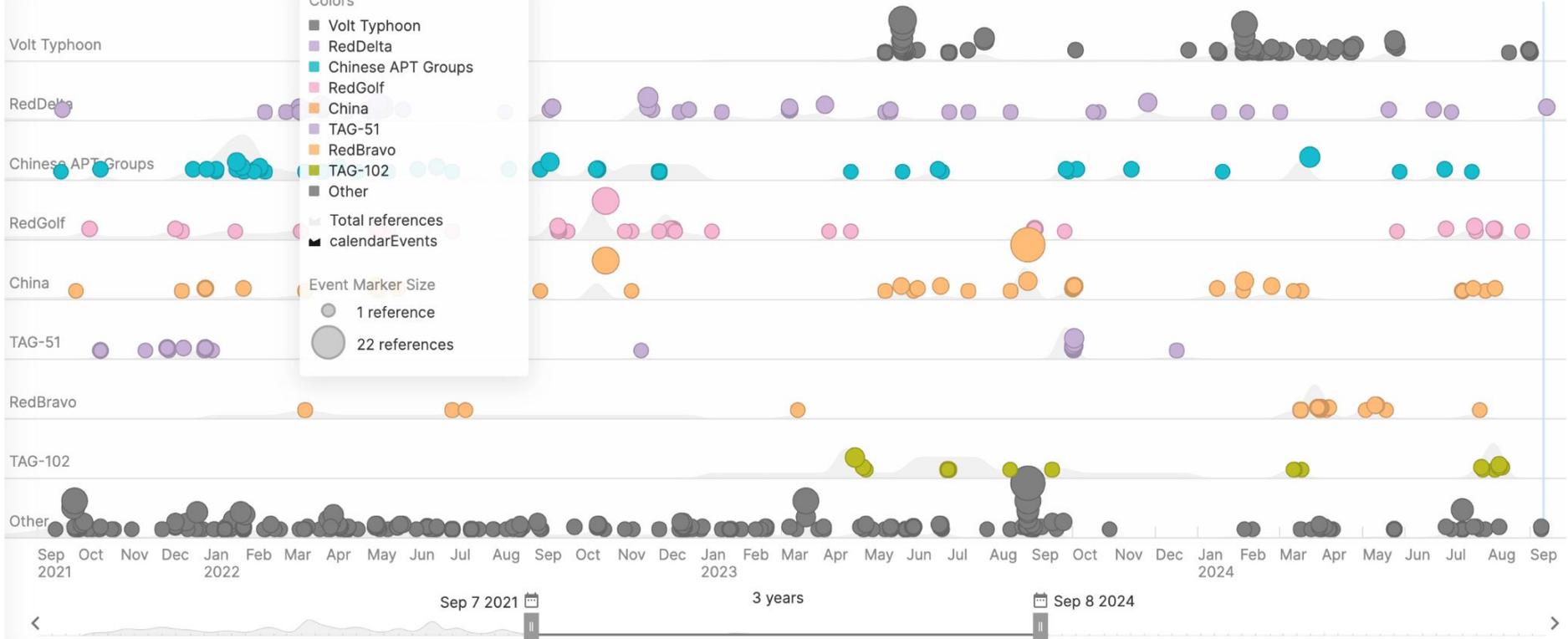
Colors

- Volt Typhoon
- RedDelta
- Chinese APT Groups
- RedGolf
- China
- TAG-51
- RedBravo
- TAG-102
- Other

Event Marker Size

- 1 reference
- 22 references

Total references
calendarEvents

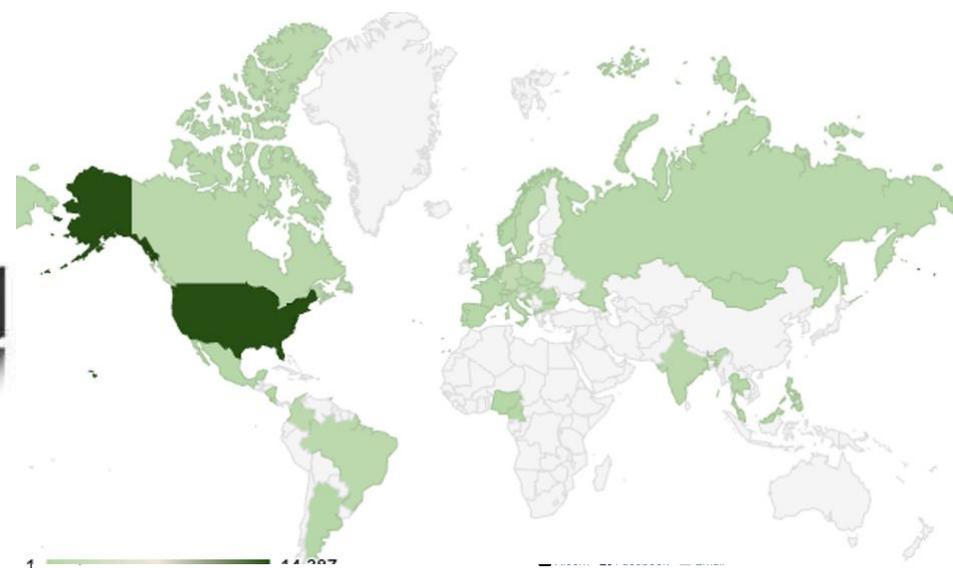


Volt Typhoon (DEV-0391)

- **Guamや米国の重要インフラ** を標的にした攻撃を行っている
- 「**有事の際に米国<->アジア間の通信インフラを妨害できる能力の開発**」が目的



Volt Typhoon



1

China's Hackers Have Entire Nation in Their Crosshairs, FBI Director Warns

More funding for the FBI is crucial to countering the evolving threat



Secure by Design Alert Security Design Improvements for SOHO Device Manufacturers

TLP:CLEAR

SECURE BY
DESIGN

Malicious Cyber Actors Exploiting Insecure SOHO Routers

Threat actors—particularly the People's Republic of China (PRC)-sponsored [Volt Typhoon group](#)—are compromising small office/home office (SOHO) routers by exploiting software defects that manufacturers must eliminate through secure software design and development. Specifically, Volt Typhoon actors are exploiting security defects in SOHO routers to use them as launching pads to further compromise U.S. critical infrastructure entities. CISA and the Federal Bureau of Investigation (FBI) are releasing this Alert based upon recent and ongoing threat activity to urge SOHO router manufacturers to build security into technology products from the beginning and encourage all customers of SOHO routers to demand better security by design.

While PRC-sponsored actors, including the Volt Typhoon group, have made headlines by exploiting SOHO router software defects, the guidance for manufacturers to implement secure software design and development that can eliminate these defects is not new.

VoltTyphoon

CVE-2024-39717	Exchangeサーバ	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2022-42475	FortiOS	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2022-42475	FortiOS	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2021-40539	Zoho ManageEngine	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190

RedDelta(Mustang Panda, Stately Taurus)



UNIT 42
Unit 42について サービス 脅威リサーチ パートナー リソース Unit 42 Blog

現在、攻撃を受けていますか?

Threat Research Center > 脅威アクターグループ > 国家支援型サイバー攻撃

国家支援型サイバー攻撃

東南アジア政府へのサイバースパイ攻撃に Stately Taurus (別名 Mustang Panda) が関与

5 min read

RELATED PRODUCTS

- Advanced DNS
- Advanced URL
- Advanced WildFire
- Cortex XDR

中国が国家支援しているAPT

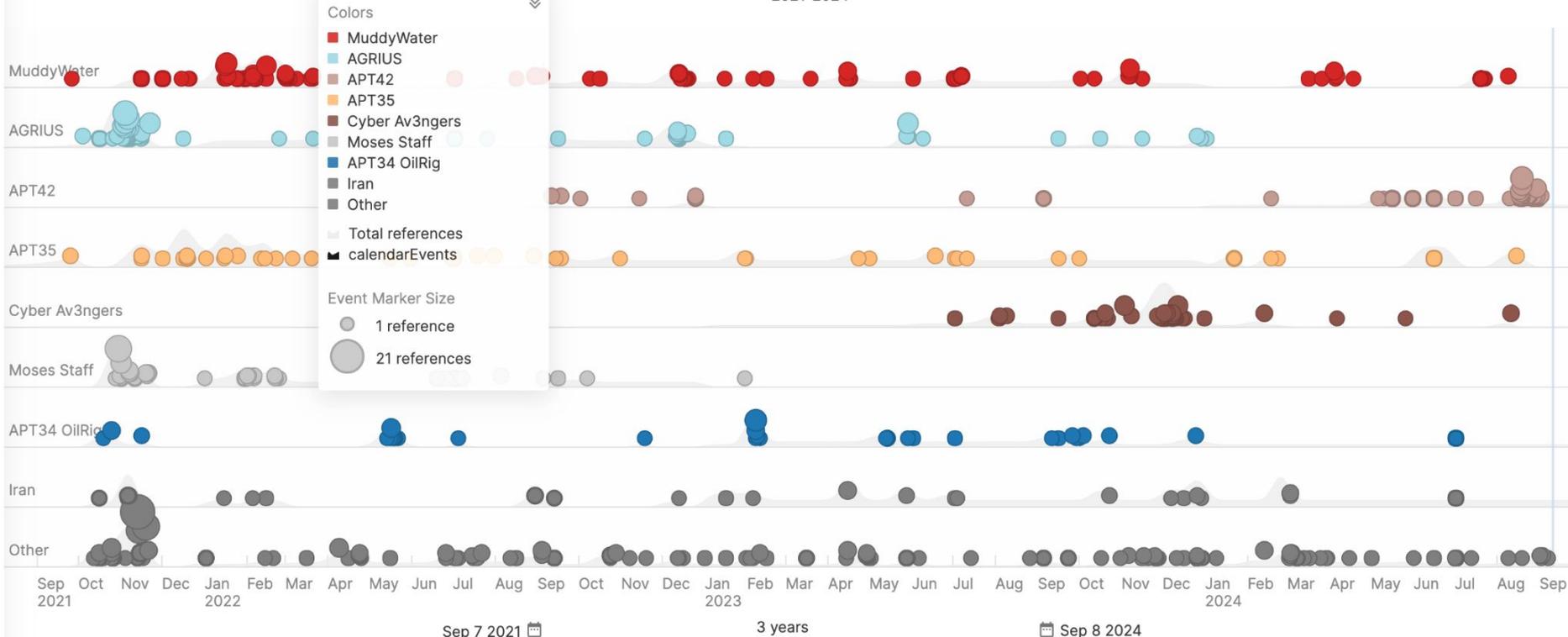
RedDelta

CVE-2021-26855	Exchangeサーバ	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2017-0199	Microsoft Office	リモートコード実行	Execution - Exploitation for Client Execution	T1203

1-3. イラン

イランが背後にいる脅威アクター

2021-2024



Muddy Water

MuddyWaterは、イラン情報安全保障省 (MOIS) 内の組織であると評価されています。少なくとも 2017年には活動が観測されており、中東やアジア・アフリカ・ヨーロッパ・北米などを標的としています。標的となっているのは電気や通信・防衛・石油・天然ガス関連組織など、さまざまな分野の政府および民間組織です。

MuddyWater は、ファイル共有サービスからのマルウェアのダウンロードにつながる、悪意のある PDF 添付ファイルによるスパイ フィッシングなどの高度な戦術を採用しています。

最近の事件では、イスラエルの病院から医療記録を漏洩して犯行声明を出しています。

Muddy Water

CVE-2020-0688	Exchangeサーバ	リモートコード実行	Initial Access - Exploitation	T1190
CVE-2020-1472 (Zerologon)	Microsoft Office	リモートコード実行	Execution - Exploitation for Client Execution	T1203
CVE-2021-44228 (Log4Shell)	log4j	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2017-0199	Microsoft Office	リモートコード実行	Execution - Exploitation for Client Execution	T1203
CVE-2023-27350	PaperCut NG	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190

2. 金銭目的とされる 脅威アクター

金銭目的とされる脅威アクター

2021-2024

Colors

- Lazarus Group
- FIN7
- BlackBasta Ransomware Group
- Desorden
- ShinyHunters
- RansomHub Ransomware Group
- Akira Ransomware Group
- BlackSUIT Ransomware Group
- Other

Total references

calendarEvents

Event Marker Size

- 1 reference
- 16 references

Lazarus Group

FIN7

BlackBasta Ransom...

Desorden

ShinyHunters

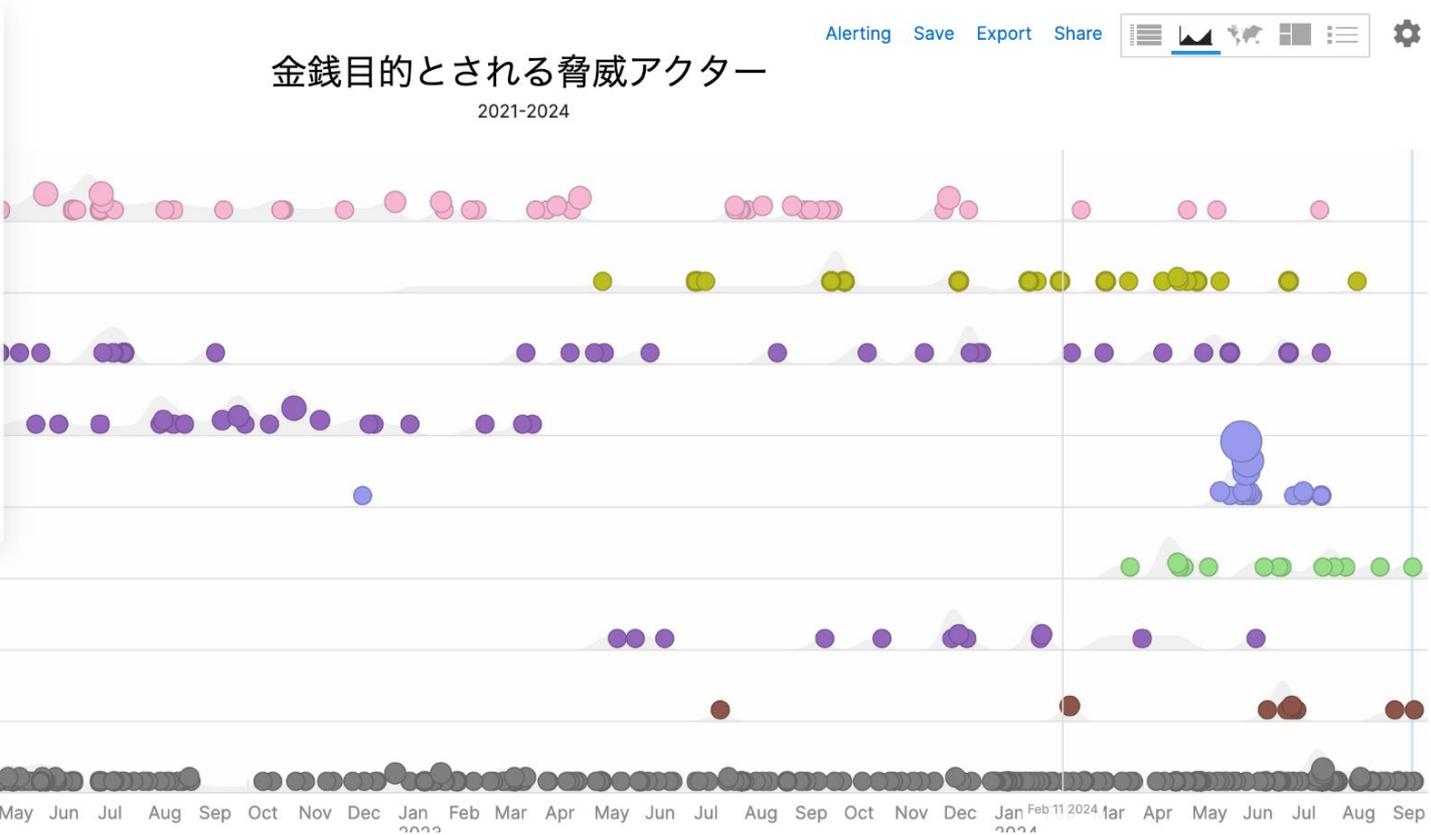
RansomHub Ransomware Group

Akira Ransomware Group

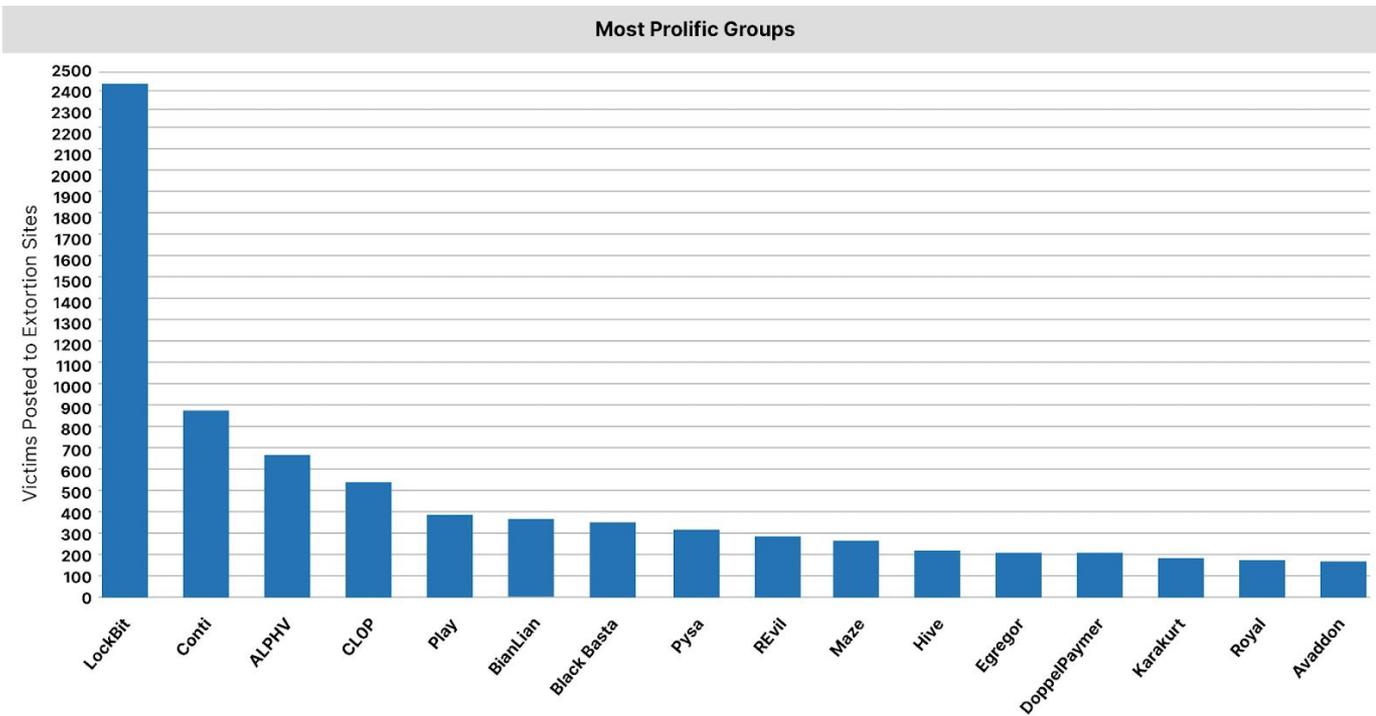
BlackSUIT Ransomware Group

Other

Sep 2021 Oct Nov Dec 2021 Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2022 Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2023 Jan Feb 11 2024 1ar Apr May Jun Jul Aug Sep



ランサムウェアグループの動向(2022年4月～2024年4月)



2022年以降はLockBitによるものがかなりの部分を占めている事がわかる。

またALPHVやCLOP・Playなどのランサムウェアグループも多くを占めている事がわかる。

(画像はTheRecord: [Ransomware tracker: The latest figures \[April 2024\]](#)より引用)

脅威アクター

1. LockBit
2. Akira
3. RansomHub

2-1. LockBit

LockBit

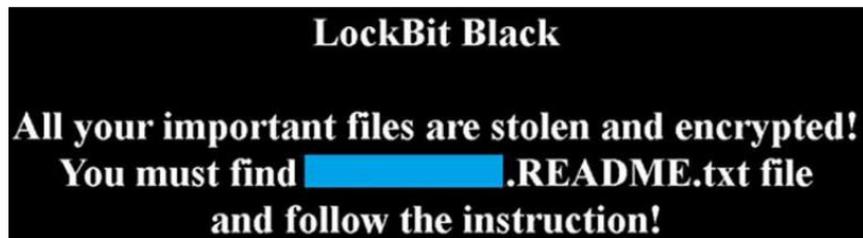
LockBit ランサムウェアグループは2019年に出現し、それ以来重大な脅威をもたらしている脅威アクターです。LockBitは、そのRaaS (Ransomware-as-a-Service) モデルで広く知られており、二重恐喝を専門としています。

2022年、LockBitは世界中で最も多く導入されたランサムウェアの亜種であり、2023年も引き続き蔓延しています。Fortinet, log4j2, VMWare, Microsoft RDP脆弱性等、多様な脆弱性を悪用します。

LockBitを使用するアフィリエイト(affiliate)は

- 金融サービス
- 食品
- 農業
- 教育
- エネルギー
- 政府関連機関
- 医療
- 製造
- 輸送

等を攻撃の対象としてきました。



LockBitの摘発「Operation Cronos」

THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.





LEAKED DATA

THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE



Press Releases

PUBLISHED



Updated: 01 Feb, 2024, 04:12 UTC 3947

LB Backend Leaks

PUBLISHED



Updated: 31 Jan, 2024, 01:44 UTC 1182

Lockbitsupp

PUBLISHED

You've Been Banned From LOCKBIT 3.0

Updated: 31 Jan, 2024, 01:44 UTC 1182

Who is LockbitSupp?

2D 19H 26M 11S



The \$10m question

Updated: 01 Feb, 2024, 04:12 UTC 3947

Lockbit Decryption Keys

PUBLISHED



Law Enforcement may be able to assist you to decrypt your Lockbit encrypted

Updated: 01 Feb, 2024, 04:12 UTC 3947

Recovery Tool

PUBLISHED



Japanese recovery tool key to access encrypted files and expand Europol's #Nomoreransom family

Updated: 01 Feb, 2024, 04:12 UTC 3947

US Indictments

PUBLISHED



FBI Investigation Leads to a Total of 5 LockBit Affiliates Charged by the Department of Justice. Two of Those Indictments Released Today.

Updated: 31 Jan, 2024, 01:44 UTC 1182

Sanctions

0D 3H 56M 11S



United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity

Updated: 31 Jan, 2024, 01:44 UTC 1182

Arrest in Poland

PUBLISHED

On 20/02/2024 a suspected LockBit actor was arrested in Poland on the request of the French judicial authorities.

Updated: 31 Jan, 2024, 01:44 UTC 1182

Activity in Ukraine

PUBLISHED

On 20/02/2024 a suspected Lockbit actor was arrested in Ternopil (UA) by the local authorities.

Updated: 31 Jan, 2024, 01:44 UTC 1182

Report Cyber Attacks!

PUBLISHED

Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and enqae with Law Enforcement

Updated: 01 Feb, 2024, 04:12 UTC 3947

Cyber Choices

PUBLISHED



Updated: 01 Feb, 2024, 04:12 UTC 3947

05/07/2024に米国司法省からLockbitSuppが起訴される



ロシア Voronezh 在住の「Dimitry Yuryevich Khoroshev (Дмитрий Юрьевич Хорошев)」氏 (31歳)

振込詐欺罪1件・保護されたコンピュータに対する意図的な損傷が8件・保護されたコンピュータからの機密情報に関連した恐喝8件。保護されたコンピュータへの損害に関連した恐喝罪8件で、合計するとこれらの容疑には最大で懲役185年の刑が科せられるとの事です。

LockBit

CVE-2023-0669	GoAnywhere MFT	コマンドインジェクション	Initial Access - Exploit Public-Facing Application	T1190
CVE-2023-27350	PaperCut NG	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2021-44228 (Log4Shell)	log4j	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2021-22986	BIG-IP	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2019-0708	MS Remote Desktop	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2018-13379	Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性	システムファイルのダウンロード	Initial Access - Exploitation	T1190
CVE-2023-4966	Citrix NetScaler(CitrixBleed)	情報漏洩	Initial Access - Exploitation	T1190
CVE-2023-4967	Citrix NetScaler(CitrixBleed)	DoS	Initial Access - Exploitation	T1190
CVE-2021-36942	Windows LSA	Spoofing	Initial Access - Exploitation	T1190
CVE-2022-36537	ZK Framework	情報漏洩	Initial Access - Exploitation	T1190
CVE-2021-20028	SRA appliances	SQLインジェクション	Initial Access - Exploitation	T1190
CVE-2021-34473	Microsoft Exchange	リモートコード実行	Initial Access - Exploitation	T1190
CVE-2021-34523	Microsoft Exchange	特権昇格	Initial Access - Exploitation	T1190
CVE-2021-3120	Wordpress Plugin	リモートコード実行	Initial Access - Exploitation	T1190
CVE-2020-1472 (Zerologon)	Microsoft Office	リモートコード実行	Execution - Exploitation for Client Execution	T1203
CVE-2020-0796	Windows SMBv3	リモートコード実行	Remote Services: SMB/Windows Admin Shares	T1021.002

2-2. Akira

Akira

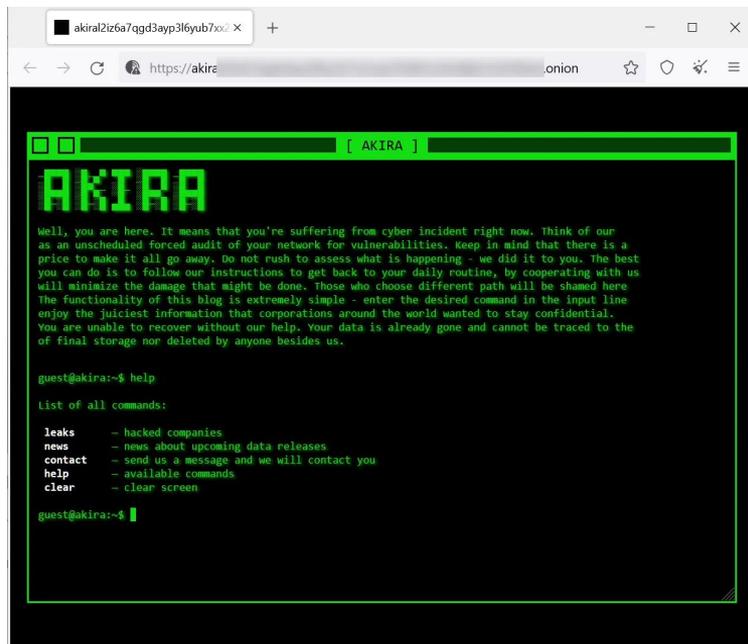
Akiraランサムウェアグループは、2023年3月に発見された、比較的新しい二重脅迫型のランサムウェアグループになります。過去に解散したグループ「Conti」と共通点が多く、Contiの元アフィリエイトが立ち上げたグループの可能性を示唆されています。

Akiraは、1980年代風な(PC-8001時代の様な)レトロなWeb サイト(下図を参照)をデータリークサイトとして使用しています。また、20万ドルから400万ドルに及ぶ高額な身代金を要求しています。

Akiraランサムウェアグループによる攻撃は

- 2023年のスタンフォード大学への攻撃
- 日産オーストラリアへの攻撃
- ヤマハのカナダ部門への攻撃

等になります。日産オーストラリアのデータ侵害では、従業員の個人情報や機密保持契約(NDA)／プロジェクト／クライアント／パートナーに関する情報を含む100GBのデータを盗んだと主張しています。被害者は通常中小企業がメインとなっており、金融・不動産・製造・ヘルスケアなど複数の業種をターゲットにしています。



Akira

CVE-2020-3259	Cisco ASA	情報漏洩	Initial Access - Exploit Public-Facing Application	T1190
CVE-2023-20269	Cisco ASA	ユーザに対するブルートフォース攻撃	Initial Access - Exploit Public-Facing Application	T1190
CVE-2023-20269	Cisco ASA	ユーザに対するブルートフォース攻撃	Initial Access - Exploit Public-Facing Application	T1190

2-3. RansomHub

RansomHub

RansomHubは二重恐喝型のランサムウェアグループで、Cyclops および Knight と呼ばれていたランサムウェアグループがブランドを変更したものと考えられています。

RansomHubがターゲットとする業界

- 水道施設
- 政府関連
- 医療関連
- 輸送
- 通信
- 金融
- 食品
- 商業施設
- 製造業

など多岐に渡ります。多額の身代金を支払う可能性が高い組織に的を絞っているとも言われており、米国 UnitedHealth社などが代表的なインシデントになります。



The screenshot shows a ransomware payment interface. At the top, there is a blacked-out area. Below it, a red timer displays '7D 3h 33m 56s'. The page includes statistics: 'Visits: 368', 'Data Size: 12GB', and 'Last View: 09-03 08:25:53'. A footer bar shows the date and time '2024-09-02 20:28:27'. A large watermark 'KRISK.IO' is visible across the center.

RansomHub

CVE-2023-3519	Citrix ADC (NetScaler)	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2023-27997	FortiOS	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2023-46604	Apache ActiveMQ	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2023-22515	Atlassian Confluenceサーバ	許可されていない管理者アカウント作成	Initial Access - Exploit Public-Facing Application	T1190
CVE-2023-46747	BIG-IP	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2023-48788	Fortinet FortiClientEMS	SQLインジェクション	Initial Access - Exploit Public-Facing Application	T1190
CVE-2020-0787	Windows	特権昇格	Initial Access - Exploit Public-Facing Application	T1190
CVE-2020-1472 (Zerologon)	Microsoft Office	リモートコード実行	Execution - Exploitation for Client Execution	T1203
CVE-2017-0144	Windows SMB	リモートコード実行	Lateral Movement - Exploitation of Remote Services	T1210

3. 集計と考察

集計

			Reconnaissance	Initial Access	Privilege Escalation	Execution	Persistence	Lateral Movement	Collection	Exfiltration
国家支援	ロシア	APT29	1	17	2	1	3	0	0	0
		APT28	0	7	2	8	0	0	1	1
		Sandworm	0	3	0	4	0	0	0	0
	中国	Volt Typhoon	0	4	0	0	0	0	0	0
		Red Delta	0	1	0	1	0	0	0	0
	イラン	MuddyWater	0	6	0	2	0	0	0	0
金銭目的		LockBit	0	17	0	1	0	0	0	0
		Akira	0	3	0	0	0	0	0	0
		RansomHub	0	9	0	1	0	1	0	0

Initial Accessに脆弱性が使用されているケースが多い

- 国家・金銭目的に関わらず、脆弱性の多くがInitial Access

→ 露出している部分の脆弱性を守るのがやはり効果的

ASM (Attack Surface Management) はやはり効果的か。

次にExecutionが多い

- ロシアが多いが、抽出による偏りの可能性が高い
 - ロシアは62, 中国は140ある中で3つずつしか確認していないため。
- Microsoft製品の脆弱性がExecutionに使われているケースが多い
 - Zerologonなど、主にWindows/Microsoft系の脆弱性の悪用が多い
 - 内部のWindows製品に関してのWindows Updateをきちんと行うことで対応

Microsoft	8
JetBrains	1
RoundCube	3
WinRAR	1

その他、脆弱性以外でInitial Accessでよく使われているもの

- Phishing/Spear Phising
- Credential Leak(資格情報の漏洩)

が多い

まとめると

- Initial Accessへの対策としてASM(Attack Surface Management)
 - 脆弱性対策
 - きちんとした設定
 - MFA
- OS周りは(Windows Updateなどで)パッチ確認で対処。
- その他、PhishingやCredential Leakに対する対策を打つ

ことで、これらの脅威アクターへの対策がある程度出来ると考えられる。

脅威インテリジェンスの中で どの様に脆弱性情報を 活用していくのか

(補足) 時間があれば

(補足) 商用製品では

- 脆弱性のリスクを算定して表示
 - 脆弱性が悪用されているかなどでアラートとしてあげる
- 脆弱性を利用している事が判明した脅威アクターを表示
 - 脅威アクターに紐づいたTTP/loCなどをアラートとしてあげる

などを行い、脆弱性情報を脅威インテリジェンスの中で活用している

(例)

- ある脅威アクターで脆弱性の悪用が観測された場合
 - その脅威アクターの TTPやIoCを知ることで
 - Initial AccessとしてPhishingがあれば、Phishingの注意喚起を行う
 - IoCを使ってIDS/IPSやFirewallによる内側からの検知を行ったり、脅威ハンティングに役立てられる
 - 脅威が現時点で社内にもない場合でも、引き続き観測を続けることで何かあった際にいち早く行動ができる

Demo(必要であれば&時間があれば)

(補足) 商用Intelligence製品で確かめてみる(ロシア)

The screenshot shows the Recorded Future AI Insights interface. On the left, a list of vulnerabilities is displayed, with the first 15 items highlighted by a red box. The main content area shows a narrative titled "Recorded Future AI Insights" with a detailed text block and a timeline at the bottom.

Vulnerability (32)

- CVE-2023-23397
- CVE-2022-30190
- CVE-2023-38831
- CVE-2022-27926
- CVE-2020-35730
- CVE-2020-12641
- CVE-2021-44026
- CVE-2022-38028
- CVE-2023-5631
- CVE-2023-41993
- CVE-2023-42793
- CVE-2017-0199
- CVE-2017-0263
- CVE-2017-6742
- CVE-2018-13379
- CVE-2019-10149
- CVE-2019-11510
- CVE-2019-1653
- CVE-2019-19781
- CVE-2020-2725

Recorded Future AI Insights

In November 2023, APT29 compromised Mongolian government sites 'mfa.gov[.]mn' and 'cabinet.gov[.]mn' by adding a malicious iframe that delivered an exploit for **CVE-2023-41993**. [1] The Russian-linked **APT28** exploited the **CVE-2023-23397** vulnerability in attacks aimed at European NATO members since April 2022. [2] **BlueDelta** targeted the Government, Energy, and Transportation sectors using various methods including **CVE-2023-23397** and multiple other exploits. [3] The group TAG-75 targeted numerous entities across **Eastern Europe** employing methods such as **Email Spoofing** and **NLTM Relay**. [4] Additionally, **APT28** was involved in exploiting the **Follina vulnerability (CVE-2022-30190)** against Ukrainian targets. [5] **Gamaredon Group** leveraged **spear phishing** tactics to target **Ukraine**, while Russian APT Primitive Bear/**Gamaredon** actively exploited **Log4Shell** vulnerabilities against Ukrainian entities. [6] In October 2023, **Winter Vivern** used a **zero-day** vulnerability (**CVE-2023-5631**) to breach European government organizations. [7] Furthermore, reports indicate that Sandworm is utilizing the **Follina vulnerability** for ongoing attacks since at least April 2022. [8]

Top 3 Sources: **Insikt Group** | **Security Affairs** | **Cyware** | All News

Generated based on 44 references | Mar 18, 2022 - Aug 29, 2024 | Analyst: Omo Kazuki

Timeline: Sep 15 2021 | 3 years | Sep 16 2024

過去3年間の攻撃
(セキュリティベンダーレポートや政府/NGO、一般的なニュースに情報ソースを絞った場合)

(補足) 商用Intelligence製品で確かめてみる(ロシア+TA0001)

Recorded Future

Search

Alerting Save Export Share

Any Vulnerability, TA0001, Russia Nation State Sponsored Analyst Notes ...

Click to edit title

Time Event Information

Threat Actor Category (2)

- Nation State Sponsored
- Russia Nation State S...

Vulnerability (25)

- CVE-2023-38831
- CVE-2022-27926
- CVE-2020-12641
- CVE-2020-35730
- CVE-2021-44026
- CVE-2022-38028
- CVE-2023-23397
- CVE-2023-5631
- CVE-2017-0199
- CVE-2017-6742
- CVE-2018-13379
- CVE-2019-10149
- CVE-2019-11510
- CVE-2019-1653
- CVE-2019-19781
- CVE-2019-2725
- CVE-2019-2800

Recorded Future AI Insights

BlueDelta is targeting **Microsoft Windows Print Spooler** and various sectors including Government, Education, and Transportation using methods such as **CVE-2022-38028** and **privilege escalation** techniques. [1] **APT29** is focused on exploiting vulnerabilities in **Microsoft Windows Server 2012 R2** and **2008 R2**, employing methods like **T1566** and **CVE-2022-30170**. [2] **Gamaredon Group** is conducting operations in **Ukraine** through **spear phishing** and utilizing malware with specific hashes alongside **CVE-2017-0199**. [3] **UAC-0063** targets Research and Government sectors, employing **CHERRYSPY**, **HATVIBE**, and various **spear phishing** methods including attachments with a focus on scheduled tasks. [4] **DEV-0586** has been seen targeting multiple sectors such as Energy, Healthcare, and **U.S. Defense Industrial Base** with a wide range of CVEs including **CVE-2019-9670** to **CVE-2021-26855**. [5] **TAG-99** employs **exploitation of remote services** with malicious infrastructures linked to **GitHub repositories**. [6] **TAG-70** has targeted several Eastern European governments including **Uzbekistan's** Ministry of Defense using CVE vulnerabilities from 2023 and various **Tactics Techniques Procedures (TTPs)**. [7] **BlueDelta** has also targeted **Ukraine** using methods that include **T1566.001** and **spear phishing** techniques while being associated with malicious infrastructures like **sourcescdn.net**. [8] Furthermore, **BlueBravo** targets numerous international organizations such as the **United Nations** with exploits like **CVE-2023-38831** alongside diverse TTPs for infiltration. [9]

Top 1 Source: **Insikt Group**

Generated based on 18 references | Jan 12, 2022 - Jul 24, 2024 | Analyst: Omo Kazuki

Share feedback? 👍 👎

79d871ff25d9d8a1f50h998h28ff752d...eda18761f3f6822c13cd7heae5af2ed77a9h4f1dc7a71df6ab715e7949h8c78h

Sep 15 2021 3 years Sep 16 2024

過去3年間の攻撃
(セキュリティベンダーレポートや政府/NGO、一般的なニュースに情報ソースを絞った場合)

25/32 = 78%がTA0001

(補足) 商用Intelligence製品で確かめてみる(中国)

The screenshot displays the Recorded Future AI Insights interface. On the left, a sidebar lists various categories and CVE IDs, with 'Vulnerability (50)' highlighted in a red box. The main content area shows a report titled 'Any Vulnerability, China Nation State Sponsored Analyst Notes or Govern...'. The report text discusses APT41's targeting of U.S. government entities, Citrix systems, and other infrastructure activities, mentioning CVE-2021-44207, CVE-2021-44228, CVE-2022-27518, CVE-2022-27518, CVE-2022-27518, CVE-2016-5195, CVE-2021-26855, CVE-2021-34473, CVE-2022-1388, ProxyShell, CVE-2010-3333, CVE-2012-0158, CVE-2017-11882, CVE-2018-13379, CVE-2018-2628, CVE-2018-5713, CVE-2019-11510, CVE-2019-18935, CVE-2019-9621, CVE-2019-9670, and CVE-2020-1472. The report also mentions tools like Cobalt Strike Beacon, Winnti, APT5, TAG-42, DEV-0401, Nightsky ransomware, Log4Shell, VMWare Horizon servers, Deep Panda, Fire Chili toolkit, APT15, BEHINDER, SafetyKatz, RedHotel, ProxyShell, Cobalt Strike, BackdoorDiplomacy, AsyncRAT, ProxyShell, Aozin Dragon, BlackTech, arbitrary code execution, Hafnium, and zero-day exploits like Follina. The report is generated based on 54 references from Dec 16, 2021, to Jun 17, 2024, by analyst Omo Kazuki. The interface includes a search bar, navigation icons, and a timeline at the bottom.

Recorded Future

Search

Alerting Save Export Share

Any Vulnerability, China Nation State Sponsored Analyst Notes or Govern...

Time Event Information

Recorded Future AI Insights

APT41 has targeted **U.S. government** entities using various tactics, including exploiting vulnerabilities like **CVE-2021-44207** and **CVE-2021-44228**, and utilizing tools such as **Cobalt Strike Beacon** and **Winnti**. [1] RedJuliett has been active against numerous organizations in **Taiwan**, including **Taiwanese government** agencies and educational institutions, employing a range of techniques. [2] APT5 focused on **Citrix systems**, leveraging vulnerabilities such as **CVE-2022-27518** to gain access. [3] TAG-42 has been linked to several malicious infrastructure activities with multiple identified hashes associated with its operations. [4] **DEV-0401** has been observed deploying **Nightsky ransomware** through exploitation of the **Log4Shell** vulnerability on **VMware Horizon** servers. [5] **Deep Panda** has launched new attacks against the finance and travel sectors, also targeting **VMware Horizon** servers with the **Fire Chili** toolkit using **Log4Shell** exploits. [6] APT15 utilized various tools and techniques in its operations, including **BEHINDER** and **SafetyKatz**. [7] **RedHotel** has targeted multiple countries and sectors, employing methods like **ProxyShell** and **Cobalt Strike** while utilizing a wide array of malicious infrastructures. [8] **BackdoorDiplomacy** employs tools like **AsyncRAT** and **ProxyShell** while targeting various organizations globally. [9] The Chinese-speaking group known as **Aozin Dragon** is known for exploiting software vulnerabilities such as **CVE-2012-0158** to infiltrate systems. [10] Meanwhile, **BlackTech** targeted **Japan** using methods including **arbitrary code execution** via **CVE-2022-1388**. [11] **Hafnium** exploited **Log4Shell** to attack virtualized infrastructure while **TA413** focused its efforts on Tibetan organizations using **zero-day** exploits like **Follina** for data theft through malicious add-ons. [12] Multiple **Chinese APT groups** are reported to employ sophisticated tactics targeting government networks globally with various identified malware strains at their disposal. [13]

Top 3 Sources: **Insikt Group** **iZOlogic** **Telegram Messenger**

Generated based on 54 references | Dec 16, 2021 - Jun 17, 2024 | Analyst: Omo Kazuki

Share feedback?

100

Sep 15 2021 3 years Sep 16 2024

Recorded Future

過去3年間の攻撃
(セキュリティベンダーレポートや政府/NGO、一般的なニュースに情報ソースを絞った場合)

(補足) 商用Intelligence製品で確かめてみる(中国+TA0001)

Recorded Future

Search

Alerting Save Export Share

Any Vulnerability, TA0001, China Nation State Sponsored Analyst Notes o...

Nation State Sponsored
Ransomware and Ex...

- Vulnerability (37)
- CVE-2021-44228
- CVE-2022-1040
- CVE-2016-5195
- CVE-2022-1388
- CVE-2022-27518
- ProxyShell
- CVE-2010-3333
- CVE-2012-0158
- CVE-2017-11882
- CVE-2018-13379
- CVE-2018-2628
- CVE-2018-5713
- CVE-2019-11510
- CVE-2020-3452
- CVE-2020-5902
- CVE-2021-1472
- CVE-2021-1473
- CVE-2021-2135
- CVE-2021-21975

Time Event Information

Recorded Future AI Insights

BackdoorDiplomacy employs methods such as **AsyncRAT**, **ProxyShell**, and various exploits including **CVE-2020-5902** and T1190, utilizing numerous malicious infrastructures like **185.80.201.87** and **cloud.microsoftshop.org**. [1] APT41 targets the **US** government using techniques like T1190 and **Cobalt Strike**, with infrastructure at **104.18.6.251**. [2] TAG-94 focuses on media and publishing in **Japan**, leveraging **CVE-2023-45727** and T1566.001 among others, with a range of malicious infrastructures such as **www.ninesmn.com** and **167.179.66.89**. [3] RedJuliett targets multiple organizations in **Taiwan's** government and academia while TA413 is involved in cyber operations across South Asia using methods like **Gh0st RAT** and **CVE-2022-1040** with malicious infrastructures connected to various domains. [4] **TAG-68** attacks the **Angolan government** using **CVE-2020-3452** along with several infrastructures including **194.68.26.164** and **knowledge.111leader.com**, whereas **Storm-0062** utilizes **Confluence Data Center** for its operations employing **CVE-2023-22527** among other tactics. [5] **Aoqin Dragon** uses methods such as **T1566** and backdoor strategies targeting multiple sectors while BlackTech attacks **Japan** using techniques like **Arbitrary Code Execution** combined with numerous **IP addresses** including 139.180.201.6 for its infrastructure needs; additionally, TAGs 88 and 5 utilize multiple vulnerabilities targeting information technology sectors across various infrastructures while **Volt Typhoon** focuses on **zero-day** exploits against software solutions like **Versa Director** using **IP addresses** including 207.148.122.171 for its operations related to **unauthorized network access** alongside **DEV-0401** specifically targeting **VMware Horizon** through a series of complex methodologies, utilizing diverse infrastructure for their campaigns against entities such as **Sophos** in various jurisdictions worldwide including multiple countries in **Asia-Pacific** regions reflected in their diverse target list ranging from

Top 1 Source: Inskit Group

Generated based on 25 references | Jan 21, 2022 - Aug 27, 2024 | Analyst: Omo Kazuki

Share feedback?

Sep 15 2021 3 years Sep 16 2024

過去3年間の攻撃
(セキュリティベンダーレポートや政府/NGO、一般的なニュースに情報ソースを絞った場合)

25/32 = 74%がTA0001

(補足) 商用Intelligence製品で確かめてみる(イラン)

The screenshot shows the Recorded Future AI Insights interface. At the top, there is a search bar and navigation icons. The main title of the report is "Any Vulnerability, Iran Nation State Sponsored Analyst Notes or Governm...". On the left sidebar, a list of categories is shown, with "Vulnerability (14)" highlighted in a red box. The main content area displays a "Recorded Future AI Insights" report. The report text states: "Hackers believed to be part of the Iranian APT35 state-backed group have been observed leveraging Log4Shell attacks to deploy a new PowerShell backdoor known as 'CharmPower'. [1] Microsoft has warned that an Iranian state-based threat actor it refers to as Mercury is utilizing Log4Shell vulnerabilities in SysAid applications against organizations in Israel. [2] In April 2023, various ransomware gangs and state-sponsored actors, including ClOp, Muddywater, and APT35, compromised PaperCut servers by exploiting CVE-2023-27350 and CVE-2023-27351. [3] Insikt Group reports indicate that MuddyWater employed multiple methods including social engineering and utilized various malicious infrastructures during their campaigns. [4] Additionally, the same group continues to exploit Log4Shell vulnerabilities in their cyber operations. [5] The Iranian cyber-espionage group Rocket Kitten was also observed exploiting the CVE-2022-22954 RCE vulnerability to deploy the Core Impact penetration testing tool on vulnerable systems. [6] APT34 leveraged CVE-2017-11882 to deploy POWRUNER and BONDUPDATER in a recent campaign. [7] Moreover, Pioneer Kitten targeted sectors such as Aerospace and Defense, Education, Finance, and Healthcare using phishing methods along with other techniques including ransomware deployment. [8]" Below the text is a profile picture of the analyst, Omo Kazuki, and the sources: "Top 3 Sources: Insikt Group, Feedjunkiecom, National Cyber Security News Today". At the bottom, it says "Generated based on 17 references | Nov 3, 2021 - Aug 30, 2024 | Analyst: Omo Kazuki".

過去3年間の攻撃
(セキュリティベンダーレポートや政府/NGO、一般的なニュースに情報ソースを絞った場合)

(補足) 商用Intelligence製品で確かめてみる(イラン+TA001)

The screenshot shows the Recorded Future interface. At the top, there is a search bar with the text "Any Vulnerability, TA0001, Iran Nation State Sponsored Analyst Notes or ...". Below the search bar, there are navigation options: "Alerting", "Save", "Export", "Share", and a menu icon. On the left side, there is a sidebar with a list of categories: "Iran Nation State Sponsored", "Nation State Sponsored", "Hacktivist", "Ransomware and Extor...", "Vulnerability (10)", "Indicators and Observables (125)", "Location (10)", "Organization (1)", "Person (4)", and "Product (2)". The "Vulnerability (10)" category is highlighted with a red box and contains a list of CVE IDs: CVE-2021-44228, CVE-2019-0604, CVE-2019-19781, CVE-2021-26855, CVE-2021-45046, CVE-2022-47966, CVE-2022-47986, CVE-2023-27350, and CVE-2024-3400. The main content area shows a "Recorded Future AI Insights" section with a narrative about MuddyWater and various threat actors. Below this, there is a "Top 1 Source" section for "Insikt Group" and a "Generated based on 6 references" section. At the bottom, there is a timeline view showing a date range from Sep 15 2021 to Sep 16 2024, with a "3 years" duration indicator.

過去3年間の攻撃
(セキュリティベンダーレポートや政府/NGO、一般的なニュースに情報ソースを絞った場合)

10/14 = 71%がTA0001
Share feedback?

<https://app.recordedfuture.com/live/sc/3nFXDDF1pHQD>

(補足) 商用Intelligence製品で確かめてみる(金銭目的)

The screenshot displays the Recorded Future AI Insights interface. On the left, a sidebar lists various vulnerability categories, with 'Vulnerability (103)' highlighted in a red box. The main content area shows a report titled 'Recorded Future AI Insights' with a narrative about the Insikt Group's activities. The report includes a list of CVEs and a timeline from September 2021 to September 2024. The interface also features a search bar, navigation icons, and a 'Share feedback?' button.

Recorded Future

Search

Alerting Save Export Share

Any Vulnerability Analyst Notes or Government or Non-Governmental Or...

Time Event Information

Vulnerability (103)

- CVE-2023-34362
- CVE-2024-24919
- CVE-2021-44228
- CVE-2020-1472
- CVE-2023-0669
- CVE-2023-4966
- CVE-2018-13379
- CVE-2022-47966
- CVE-2023-27350
- CVE-2022-24086
- CVE-2023-20269
- CVE-2024-4358
- MS17-010
- ProxyShell
- CVE-2017-0144
- CVE-2017-11882
- CVE-2017-3506
- CVE-2020-0787

Recorded Future AI Insights

The **Insikt Group** has reported various cyber events involving multiple threat actors, including the **CL0P Ransomware Group**, which exploited **CVE-2023-34362** and targeted organizations such as the **University System of Georgia**, **Metro Vancouver Transit Police**, and **Ernst & Young Global Limited** using malicious infrastructure associated with **Progress MOVEit File Transfer**. [1] **Boris Ostritski** targeted the aviation sector using methods including **MS17-010** and **T1078**. [2] The **BianLian Ransomware Group** employed various techniques, including **ProxyShell** and **Living-off-the-Land** tactics. [3] The **Lazarus Group** exploited **CVE-2022-47966** to deploy **QuiteRAT** malware against healthcare entities in **Europe** and the **U.S.** [4] In November 2023, they were also linked to attacks exploiting vulnerabilities in Zoho's **ManageEngine ServiceDesk**. [5] The **LockBit Gang** targeted significant entities like **Boeing** and the **Industrial And Commercial Bank of China Limited** using multiple CVEs including **CVE-2023-4966**. [6] Additionally, **mont4na** executed attacks on several U.S. state governments employing **CVE-2024-24919** for information disclosure. [7] The **FBI** noted that the **BI00dy Ransomware Gang** accessed education facilities by exploiting **PaperCut** servers vulnerable to **CVE-2023-27350**. [8] Meanwhile, the **8220 Gang** has continued its **cryptocurrency** mining campaigns by targeting vulnerable **Oracle WebLogic** servers through **CVE-2017-3506**. [9]

Top 3 Sources: Insikt Group Security Affairs IZOologic

Generated based on 132 references | Jan 20, 2022 - Sep 7, 2024 | Analyst: Omo Kazuki

Share feedback?

Sep 15 2021 3 years Sep 16 2024

Recorded Future

過去3年間の攻撃
(セキュリティベンダーレポートや政府/NGO、一般的なニュースに情報ソースを絞った場合)

(補足) 商用Intelligence製品で確かめてみる(金銭目的)

Recorded Future

Search

Alerting Save Export Share

Any Vulnerability, TA0001 Analyst Notes or Government or Non-Government...

North Korea Nation St...

Vulnerability (68)

- CVE-2023-34362
- CVE-2022-24086
- CVE-2023-0669
- CVE-2017-0144
- CVE-2022-41080
- CVE-2022-41082
- CVE-2022-47966
- CVE-2024-1708
- CVE-2024-1709
- MS17-010
- ProxyNotShell
- CVE-2015-2291
- CVE-2017-11882
- CVE-2020-0787
- CVE-2020-1472
- CVE-2020-3259
- CVE-2021-22205
- CVE-2021-26855
- CVE-2021-26857
- CVE-2023-27997

Time Event Information

Recorded Future AI Insights

The **Insikt Group** has reported multiple cyber threat events involving various attackers and targets. [1] **Boris_Ostritski** targeted **Abu Dhabi's** electronic equipment, parts, and healthcare sectors using **MS17-010**, T1021, T1133, T1078, and T1586. [2] The **CL0P Ransomware Group** targeted several organizations including **TJX Companies Inc.**, **TomTom**, and the **U.S. Department of Energy** using **CVE-2023-34362**, T1190, T1486, and exploiting **Progress MOVEit File Transfer**. [3] **Stars4** attacked **Panama's** non-US government entities employing **CVE-2021-27065** and related vulnerabilities. [4] The **BianLian Ransomware Group** utilized various methods including **ProxyShell** and **Living-off-the-Land** techniques for their campaigns against information technology sectors. [5] **Scattered Spider** employed multiple techniques including **phishing** to target telecommunications and business process outsourcing industries. [6] **FIN7** focused on **Internet Key Exchange** with methods such as **CVE-2022-34721** and **memory corruption** exploits. [7] **Lazarus Group** attacked fintech with a combination of methods including **CVE-2022-0609** and **resource hijacking** tactics while targeting **cryptocurrency** exchanges as well as aerospace defense industries. [8] Other notable threats including the **BI00Dy Ransomware Gang** targeting education institutions using **Truebot** malware, the **Gualtieri** group exploiting **Magento Open Source** vulnerabilities for eCommerce attacks, and **LockBit Gang** utilizing **CWE** vulnerabilities against **ConnectWise Control** services. [9]

Top 1 Source: Insikt Group

Generated based on 52 references | Nov 11, 2021 - Sep 7, 2024 | Analyst: Omo Kazuki

Share feedback?

CVE-2023-27997 Password Spraying, T1588 Cyber attack against Government, Citrix NetScaler Application Delivery Controller (ADC) SMRu1 by RansomHub Ransomware Group

Sep 15 2021 3 years Sep 16 2024

過去3年間の攻撃
(セキュリティベンダーレポートや政府/NGO、一般的なニュースに情報ソースを絞った場合)

68/103 = 66%がTA0001

(補足) 商用製品を使うと

荒っぽい推定だが、65-70%の脆弱性がTA0001と関係している可能性
ASMとパッチ更新はかなり有効であると考えられる。

Any Question?

以降、ボツスライド

2-2. BlackSuit

(※) BlackSuitはRoyalのリブランディングとされている。

