脅威インテリジェンスと脆弱性

面　和毅

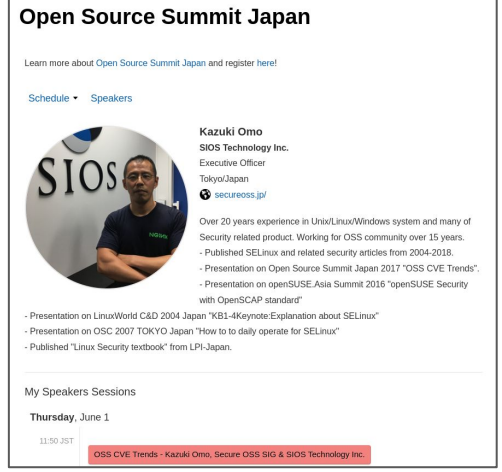
略歴

- 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
試験番号 LPI 303
Security Exam
改訂新版
LPIC
Level 3 303 [Version 2.0] 対応
教科書
解説がより充実
合格力が身
[詳しい解説] + [演習問題] +
「重要ポイント」がひと目でわかる。
試験対策


@IT > Security&Trust > スイッチ・オン！ SELinux（7）
Security&Trust
ツイート
B! 0
いいね！ 1
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.


LinuC open your NEXT future LPI-JAPAN
資格・試験概要
受験案内
受験申込み
学習のすすめ方
よくあるご質問
受験者マイページ
標準教科書シリーズ
Linuxセキュリティ標準教科書
いいね！ 37
シェアする
ツイート
B! 17
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
製本版：Ver. 1.0.0


メニュー
キーワードで検索
IT
電機
会員情報更新キャンペーン実施中 12/11まで
特集
Linuxで怪しい実験やってみた
＋ 特集をフォロー
面 和毅 SIOSテクノロジー
virus
PR
【データ・マネジメントの新戦略】近未来に実現する「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)
X
Facebook
LINE
コピー
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し


セキュ塾TOPに戻る
セキュ塾 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


cybertrust
企業・IR 情報
事業内容
ニュース
導入事例
採用情報
お問い合わせ
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
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）イセトーへの攻撃
を見てみたいと思います。
最新 BLOG 記事
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！
中村行宏
面和毅
Open オープン
Source ソース
INTelligence インテリジェンス
OSINT
実践ガイド
脅威インテリジェンス
IoC
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などを紹介
MITRE ATT&CK
SCAP
KEVカタログ
「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

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

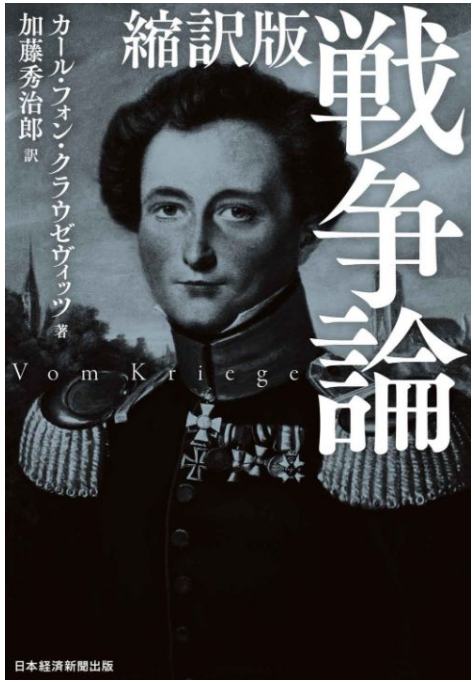
インテリジェンスとは

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取ると

東京の感染者900人

東京の感染者900人
先週と比べて最多
病床使用率も逼迫

オリンピックはどうする？
やるとしても無観客？
等の問に答える分析

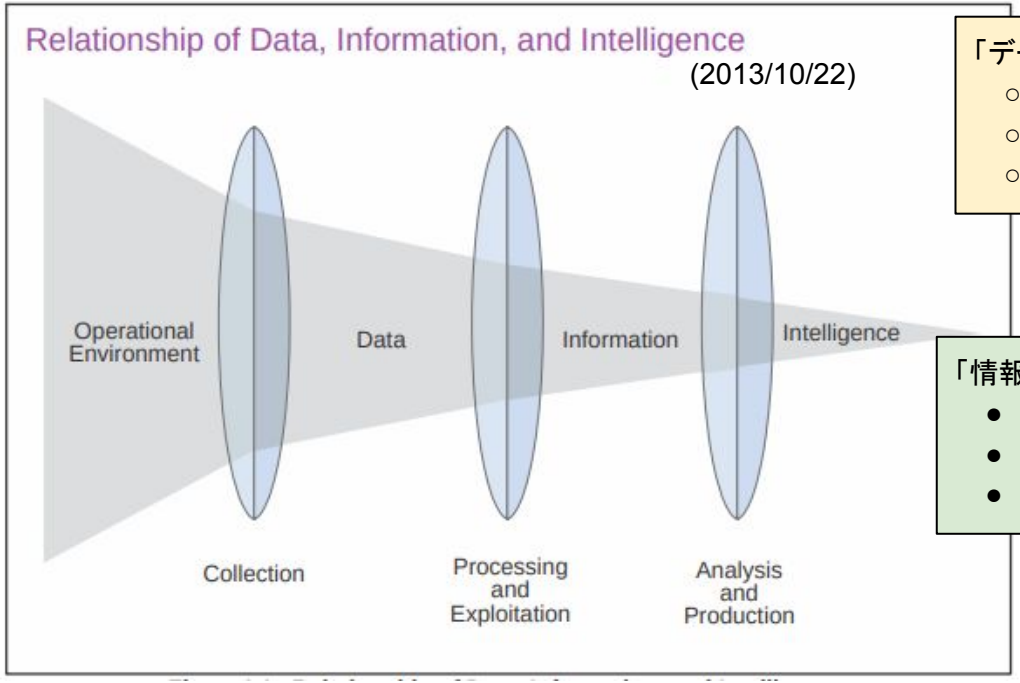
存在する情報

意味のある情報

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

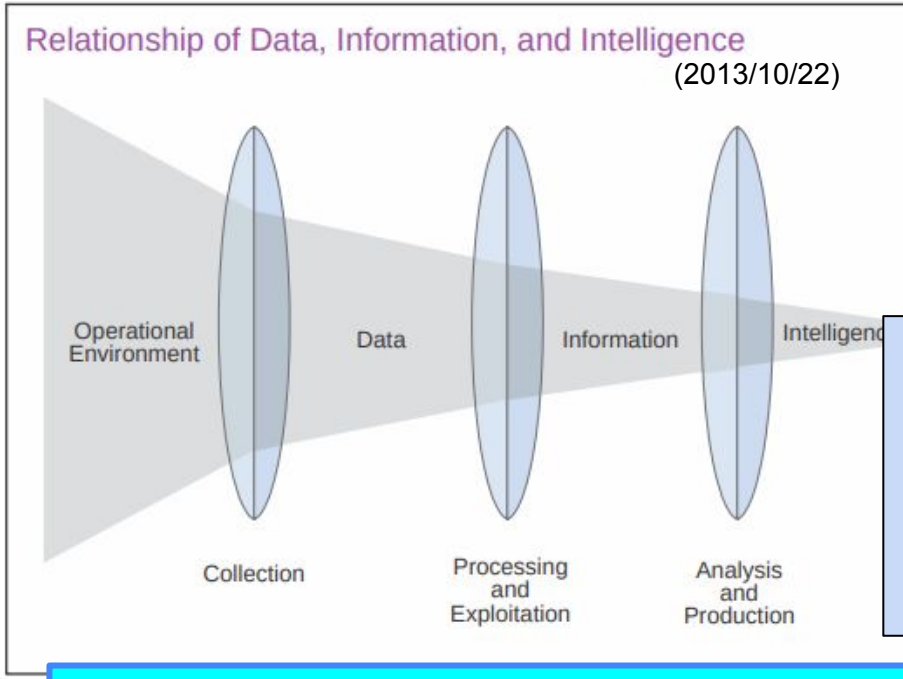
□国統合参謀本部 “Joint Intelligence Joint publication 2-0”の定義



「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様な目的で使用してる？
- アクセスしたPortはどの様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



「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様な目的で使用してる？
- アクセスしたPortはどの様な攻撃で使用されているか？

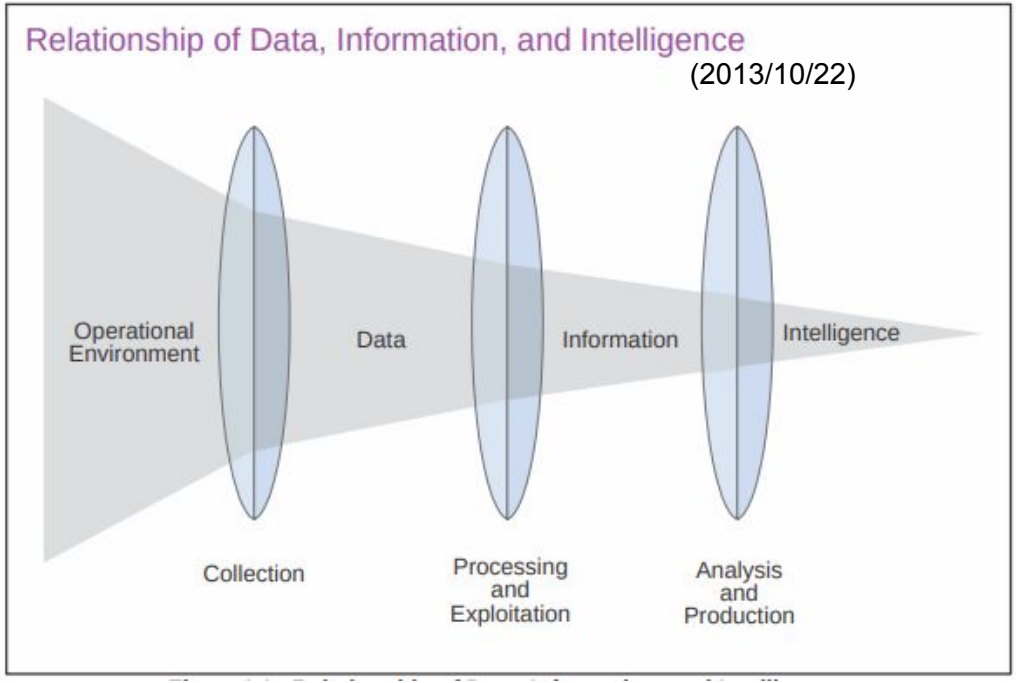
「インテリジェンス」は種々の情報から判断して下記を提供

- 現在どの様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有るか？その目的は？
- 過去の攻撃情報から、被害はどの様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。

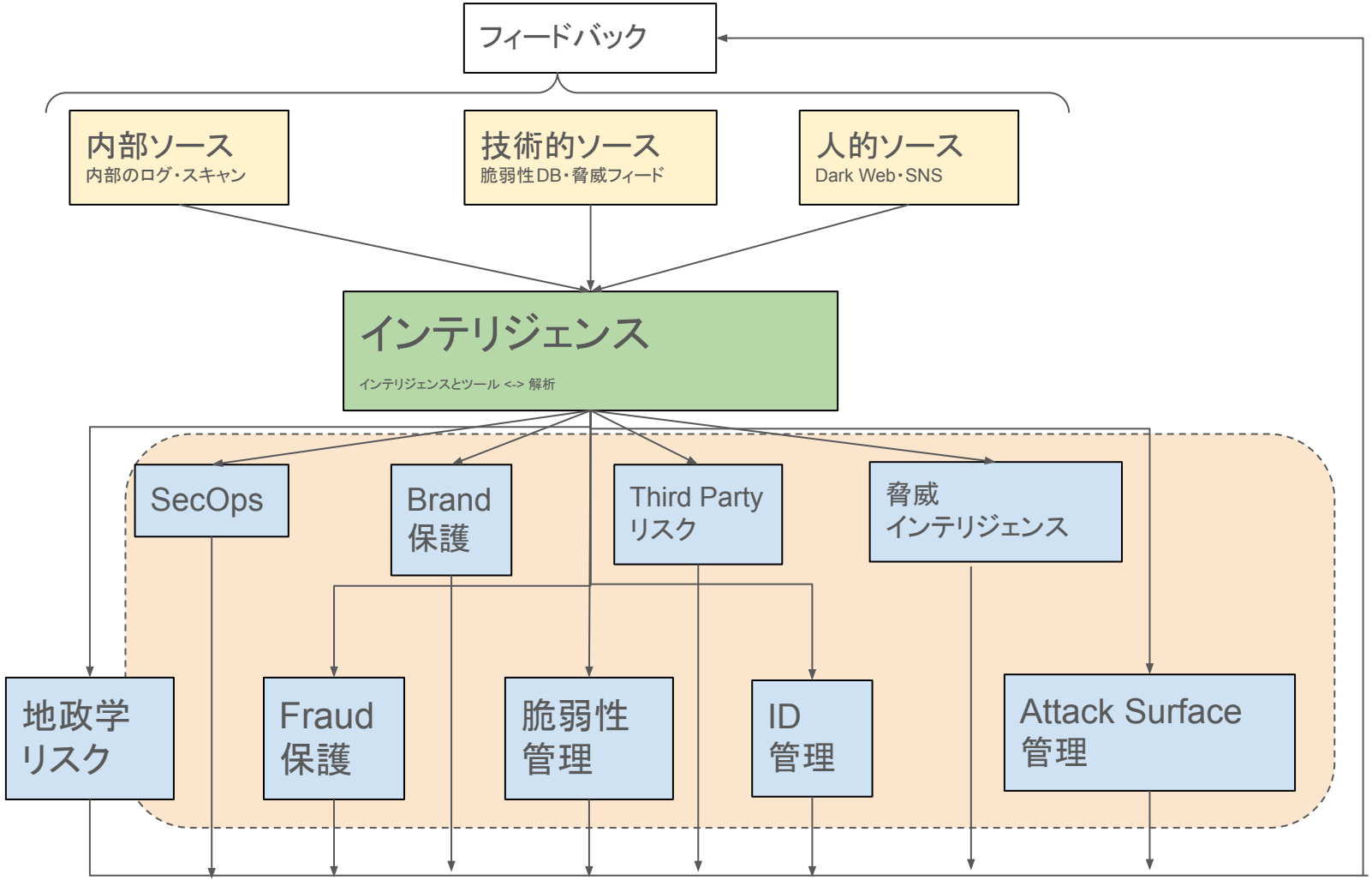
インテリジェンス活用の種類

インテリジェンス活用



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？


フィードバック
内部ソース
内部のログ・スキャン
技術的ソース
脆弱性DB・脅威フィード
人的ソース
Dark Web・SNS
インテリジェンス
インテリジェンスとツール <-> 解析
SecOps
Brand
保護
Third Party
リスク
脅威
インテリジェンス
地政学
リスク
Fraud
保護
脆弱性
管理
ID
管理
Attack Surface
管理

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タリジェンスを用いて適切な脆弱性管理を行なっていく

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

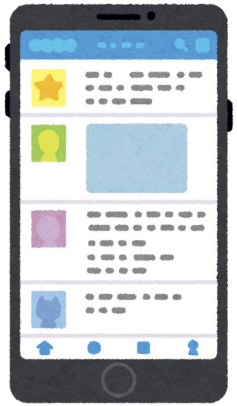
3.3.1. Fraudインテリジェンス

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トランザクションや、完全にブロックされてしまうト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リアージ
- 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。

アタックサーフェース

- 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

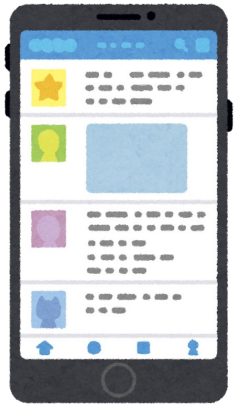
インテリジェンスの手法（ソース）の種類

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

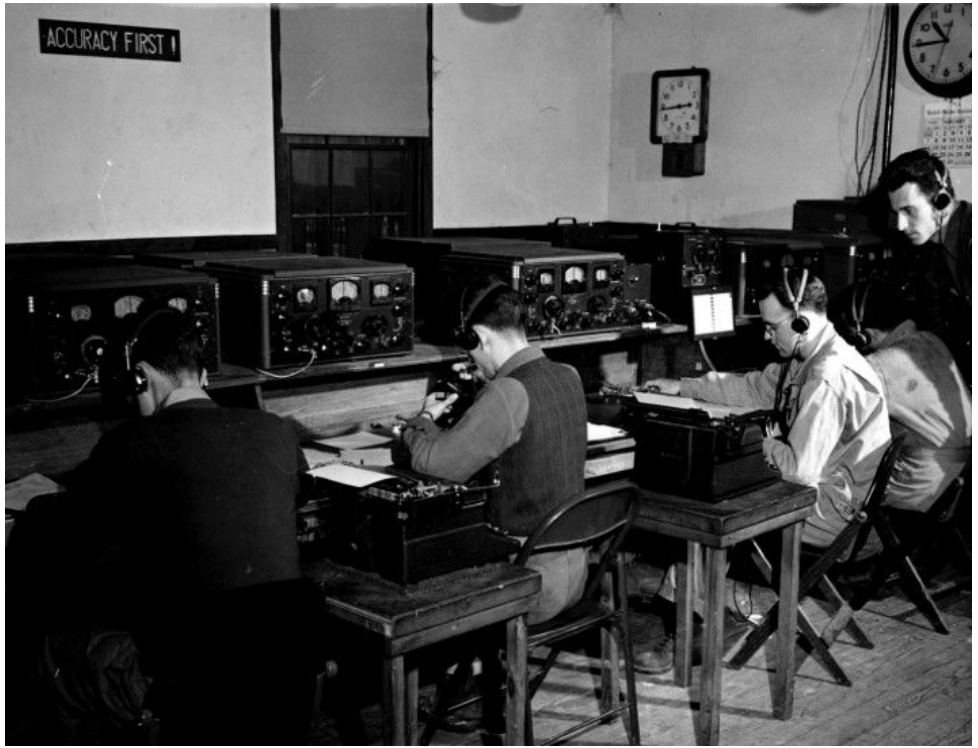


2.4. OSINTの歴史

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。

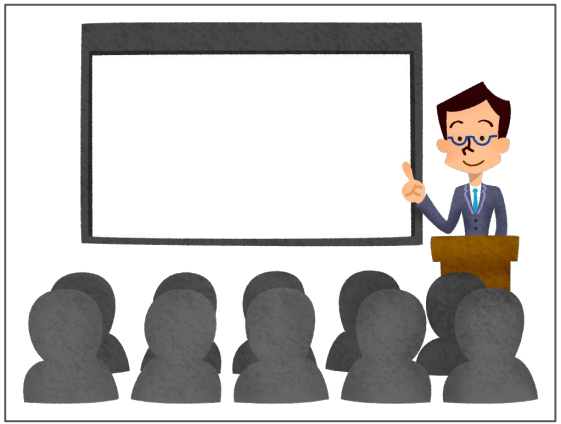


（参考：https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/）

3.3.2. HUMINT (Human Intelligence)

人間を介して情報を収集

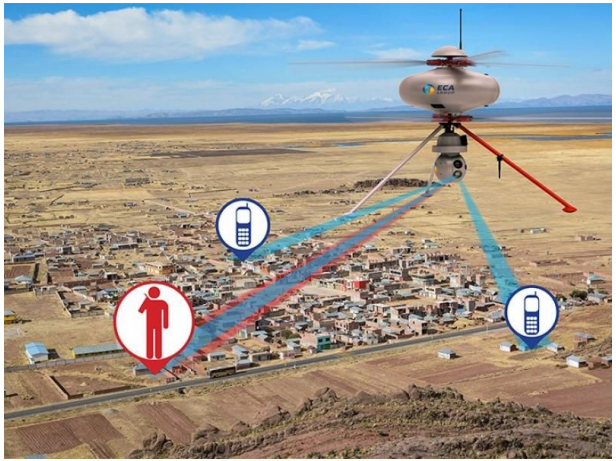
- 標的となる会社から何らかの方法で信頼を勝ち取り、内部情報を入手
- 標的となる会社の社員と個人的な信頼関係を築き、内部情報を収集
- コミュニティ、業界固有の情報共有の場での会話による情報収集
- ダーク Web フォーラム等での会話での情報収集



3.3.3. SIGINT (Signal Intelligence)

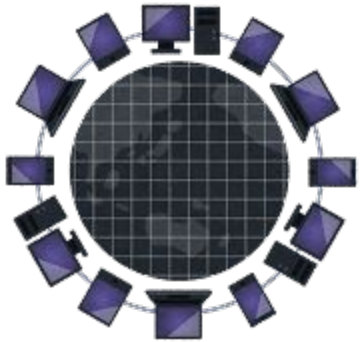
電話や無線・GPS・Wifi等から情報を収集

- 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



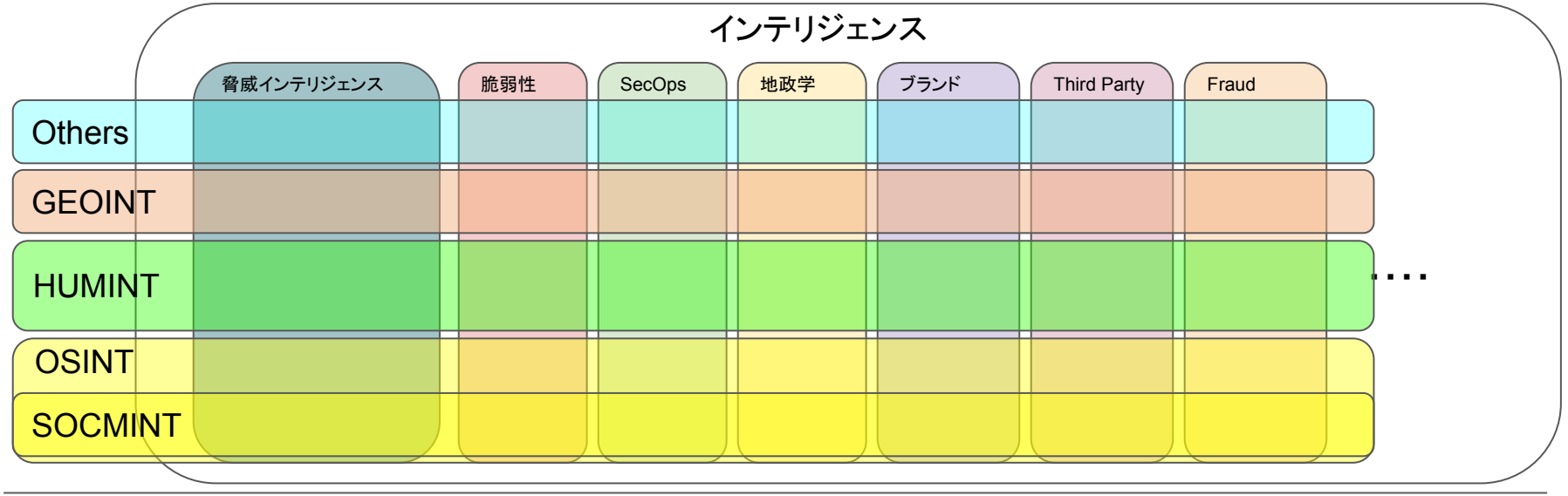
3.3.4. DARKINT (Dark Web Intelligence)

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

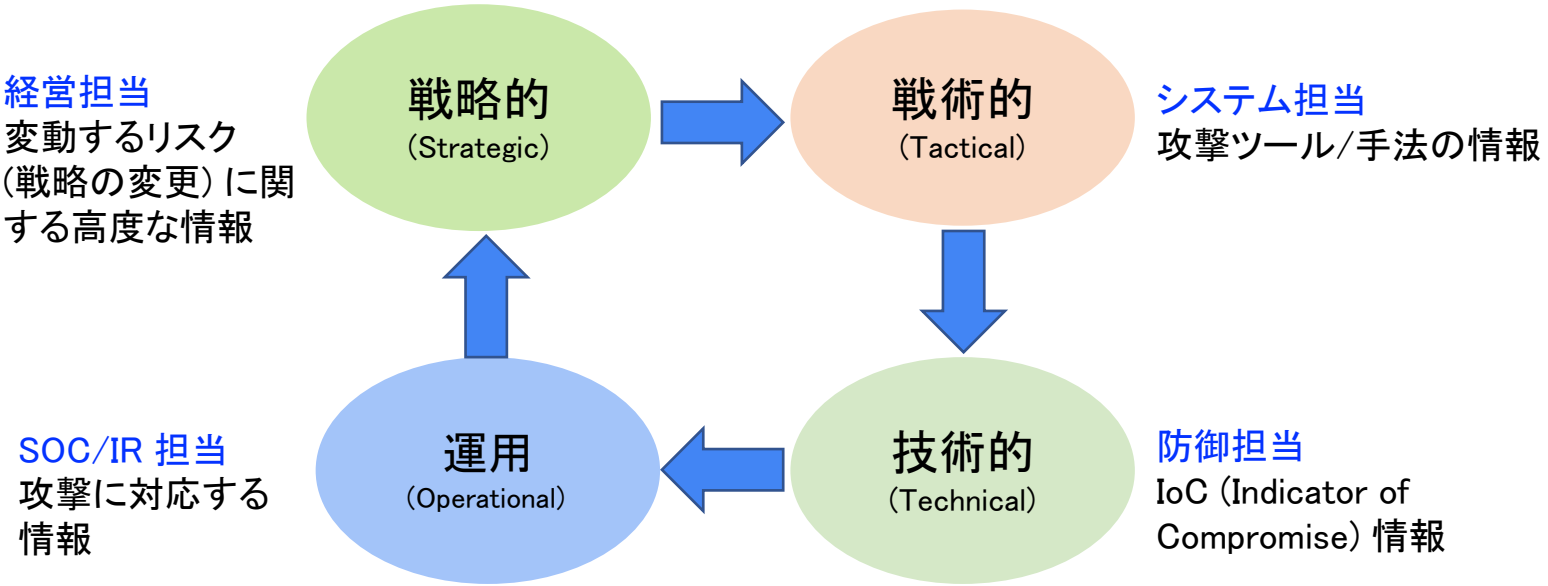
脅威インテリジェンスとは

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

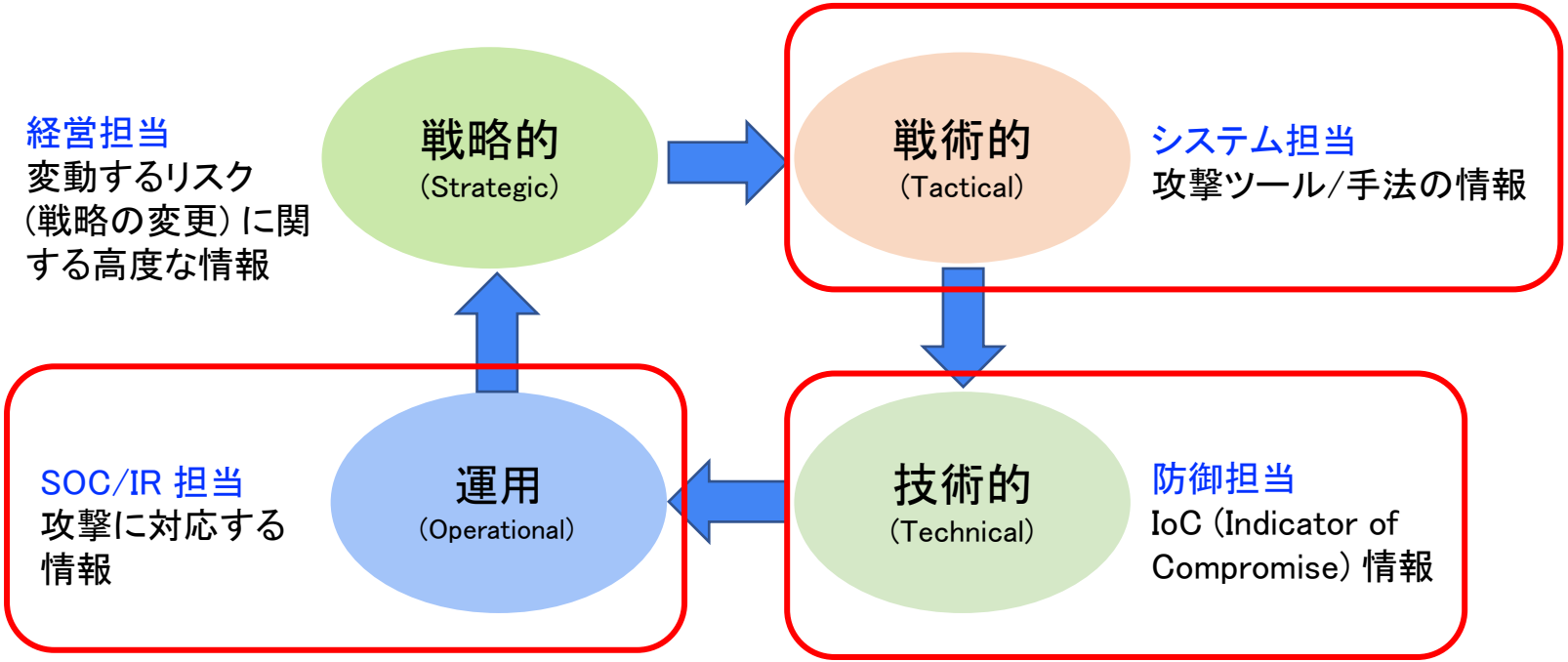


CTI Information Sharing
https://www.enisa.europa.eu/events/cti-eu-event/cti-eu-event-presentations/cti-information-sharing/

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

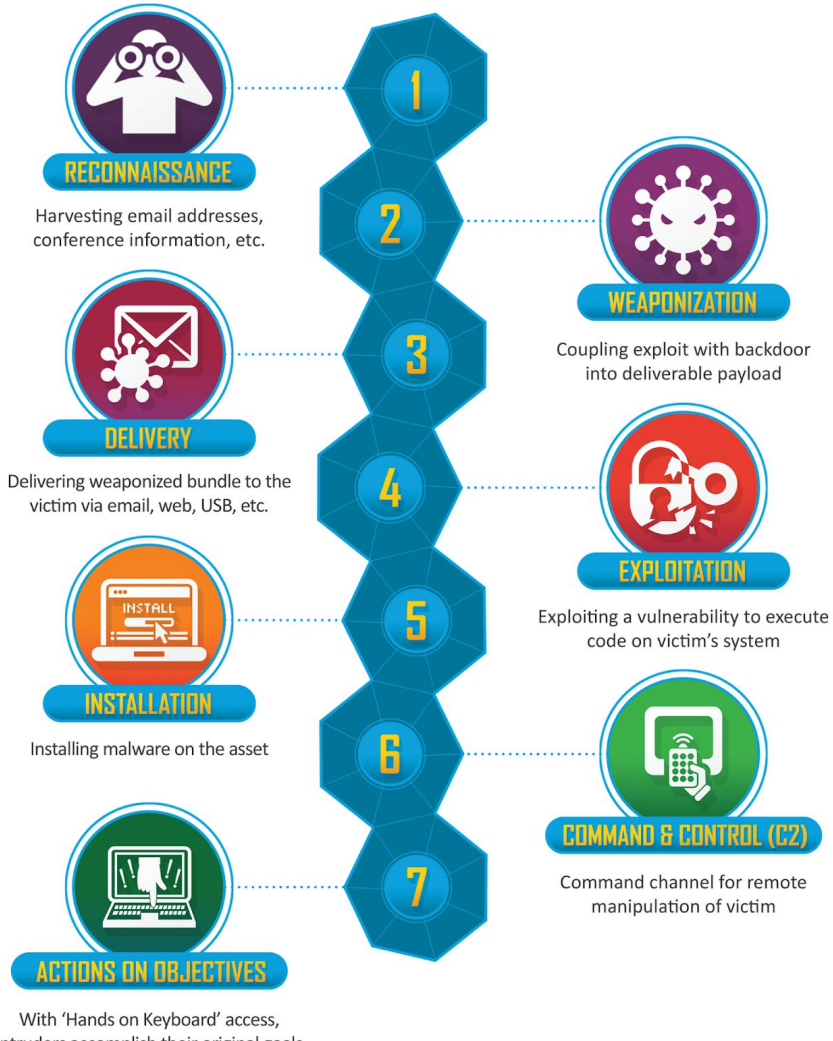
サイバーキルチェーンとは

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。



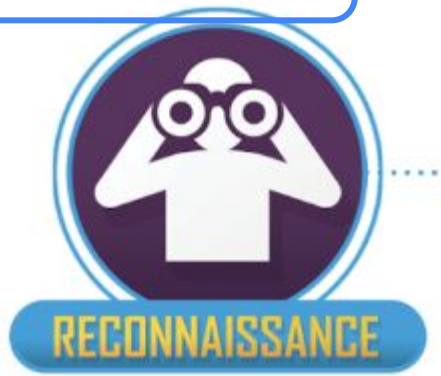
1. **「偵察（Reconnaissance）」**
2. 「武器化（Weaponization）」
3. **「デリバリー（Delivery）」**
4. **「エクスプロイト（Exploitation）」**
5. 「インストール（Installation）」
6. 「C&C（Command and Control）」
7. 「目的の実行（Actions on Objectives）」

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様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

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。

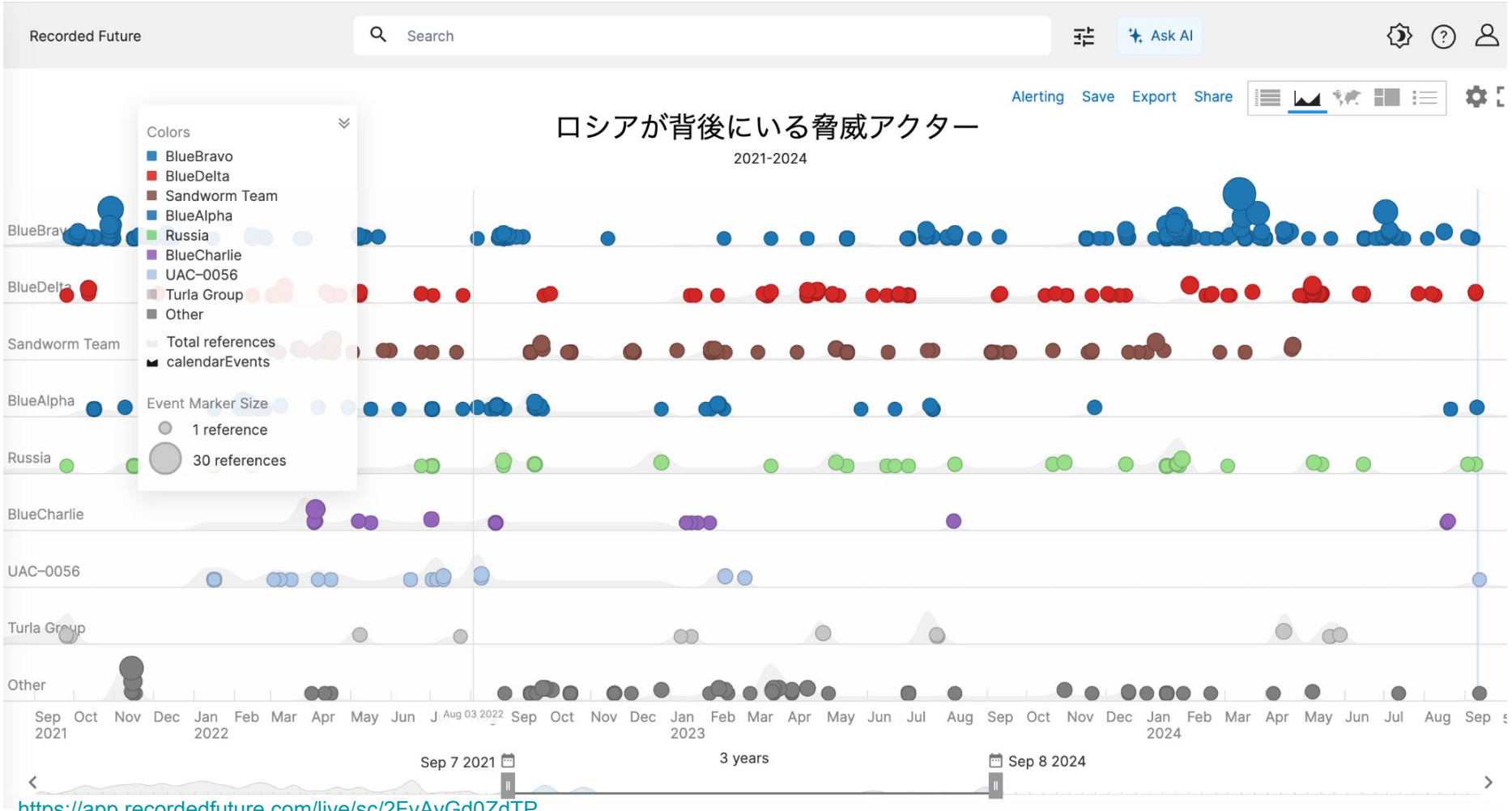
1. 国家が背後にいる脅威アクター

1-1. ロシア

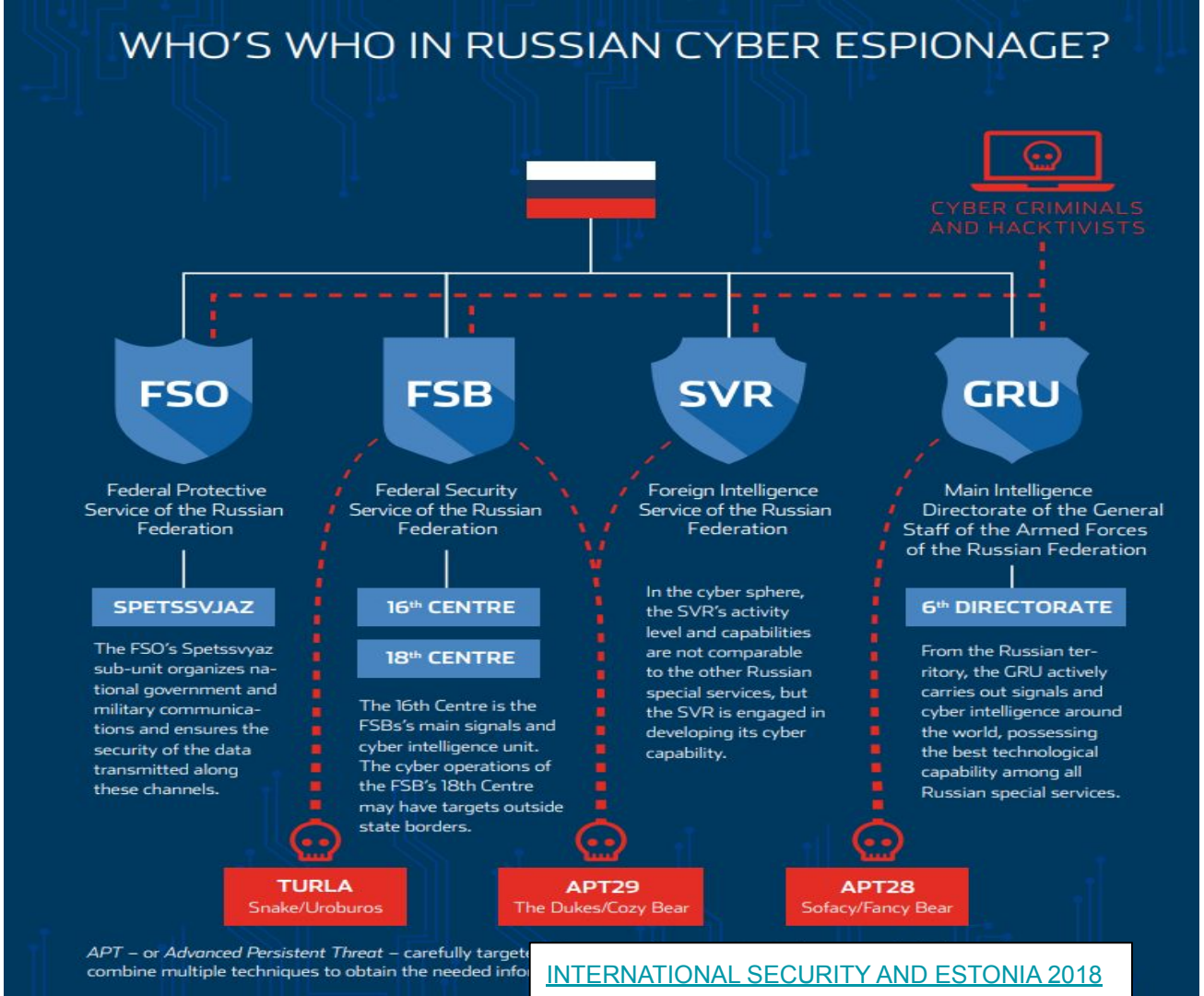
ロシアが背後にいるとされている脅威アクター（攻撃者）

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)



https://app.recordedfuture.com/live/sc/2FvAyGd0ZdTP



[INTERNATIONAL SECURITY AND ESTONIA 2018]

2018年時点での分析

- APT29
- APT28
- Turla

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のオープ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	Valid Accounts	Process Injection	Modify Authentication Process	Network Sniffing	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	Hijack Execution Flow	Valid Accounts	Valid Accounts	OS Credential Dumping	Application Window Discovery	Software Deployment Tools	Data from Removable Media	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Trusted Relationship	Software Deployment Tools	Boot or Logon Initialization Scripts	Access Token Manipulation	Direct Volume Access	Input Capture	System Network Configuration Discovery	Replication Through Removable Media	Input Capture	Application Layer Protocol	Data Transfer Size Limits	Service Stop
Supply Chain Compromise	Shared Modules	Create or Modify System Process	Group Policy Modification	Rootkit	Brute Force	System Owner/User Discovery	Internal Spearphishing	Data Staged	Proxy	Exfiltration Over C2 Channel	Inhibit System Recovery
Hardware Additions	User Execution	Event Triggered Execution	Abuse Elevation Control Mechanism	Obfuscated Files or Information	Two-Factor Authentication Interception	System Network Connections Discovery	Use Alternate Authentication Material	Screen Capture	Communication Through Removable Media	Exfiltration Over Physical Medium	Defacement
Exploit Public-Facing Application	Exploitation for Client Execution	Boot or Logon Autostart Execution	Exploitation for Privilege Escalation	Indicator Removal on Host	Exploitation for Credential Access	Permission Groups Discovery	Lateral Tool Transfer	Email Collection	Web Service	Exfiltration Over Web Service	Firmware Corruption
Phishing	System Services	Account Manipulation	Process Injection	Modify Registry	Steal Web Session Cookie	File and Directory Discovery	Taint Shared Content	Clipboard Data	Multi-Stage Channels	Automated Exfiltration	Resource Hijacking
External Remote Services	Command and Scripting Interpreter	External Remote Services	Access Token Manipulation	Trusted Developer Utilities Proxy Execution	Unsecured Credentials	Peripheral Device Discovery	Exploitation of Remote Services	Automated Collection	Ingress Tool Transfer	Exfiltration Over Alternative Protocol	Network Denial of Service
Drive-by Compromise	Native API	Office Application Startup	Group Policy Modification	Traffic Signaling	Credentials from Password Stores	Network Share Discovery	Remote Service Session Hijacking	Audio Capture	Data Encoding	Transfer Data to Cloud Account	Endpoint Denial of Service
	Inter-Process Communication	Create Account	Abuse Elevation Control Mechanism	Signed Script Proxy Execution	Steal or Forge Kerberos Tickets	Password Policy Discovery		Video Capture	Traffic Signaling		System Shutdown/Reboot
		Browser Extensions	Exploitation for Privilege Escalation	Rogue Domain Controller	Forced Authentication	Browser Bookmark Discovery		Man in the Browser	Remote Access Software		Account Access Removal
		Traffic Signaling		Indirect Command Execution	Steal Application Access Token	Virtualization/Sandbox Evasion		Data from Information Repositories	Dynamic Resolution		Disk Wipe
		BITS Jobs		BITS Jobs	Man-in-the-Middle	Cloud Service Dashboard		Man-in-the-Middle	Non-Standard Port		Data Manipulation
		Server Software Component		XSL Script Processing		Software Discovery		Archive Collected Data	Protocol Tunneling		
		Pre-OS Boot		Template Injection		Query Registry		Data from Network Shared Drive	Encrypted Channel		
		Compromise Client Software Binary		File and Directory Permissions Modification		Remote System Discovery		Data from Cloud Storage Object	Non-Application Layer Protocol		
		Implant Container Image		Virtualization/Sandbox Evasion		Network Service Scanning					
				Unused/Unsupported Cloud Regions		Process Discovery					
				Use Alternate Authentication Material		System Information Discovery					
				Impair Defenses		Account Discovery					
				Hide Artifacts		System Time Discovery					
				Masquerading		Domain Trust Discovery					
				Deobfuscate/Decode Files or Information		Cloud Service Discovery					
				Signed Binary Proxy Execution							
				Exploitation for Defense Evasion							
				Execution Guardrails							
				Modify Cloud Compute Infrastructure							
				Pre-OS Boot							
				Subvert Trust Controls							

Comparing APT28 to APT29

3-1-1. 米国／EUへの攻撃 (APT29)

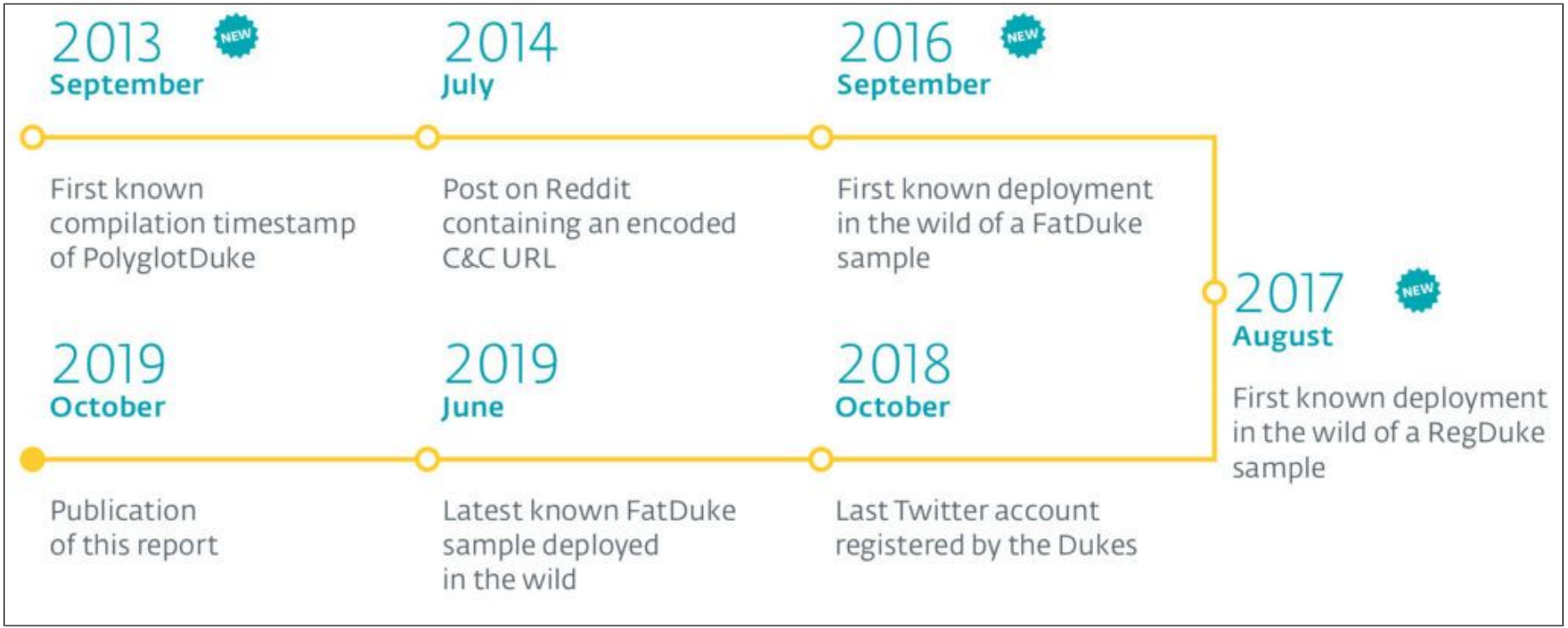
2013年～2019年

「Operation Ghost」

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

「Operation Ghost」

C&C サーバーのアドレスは、Twitter等の公開ページから取得されます。

左はエンコードされたC&C URLを含むツイートサンプルになります。

2016年米国大統領選挙(APT28, APT29)

2016年

2016年「GRIZZLY STEPPE」(APT28)

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。

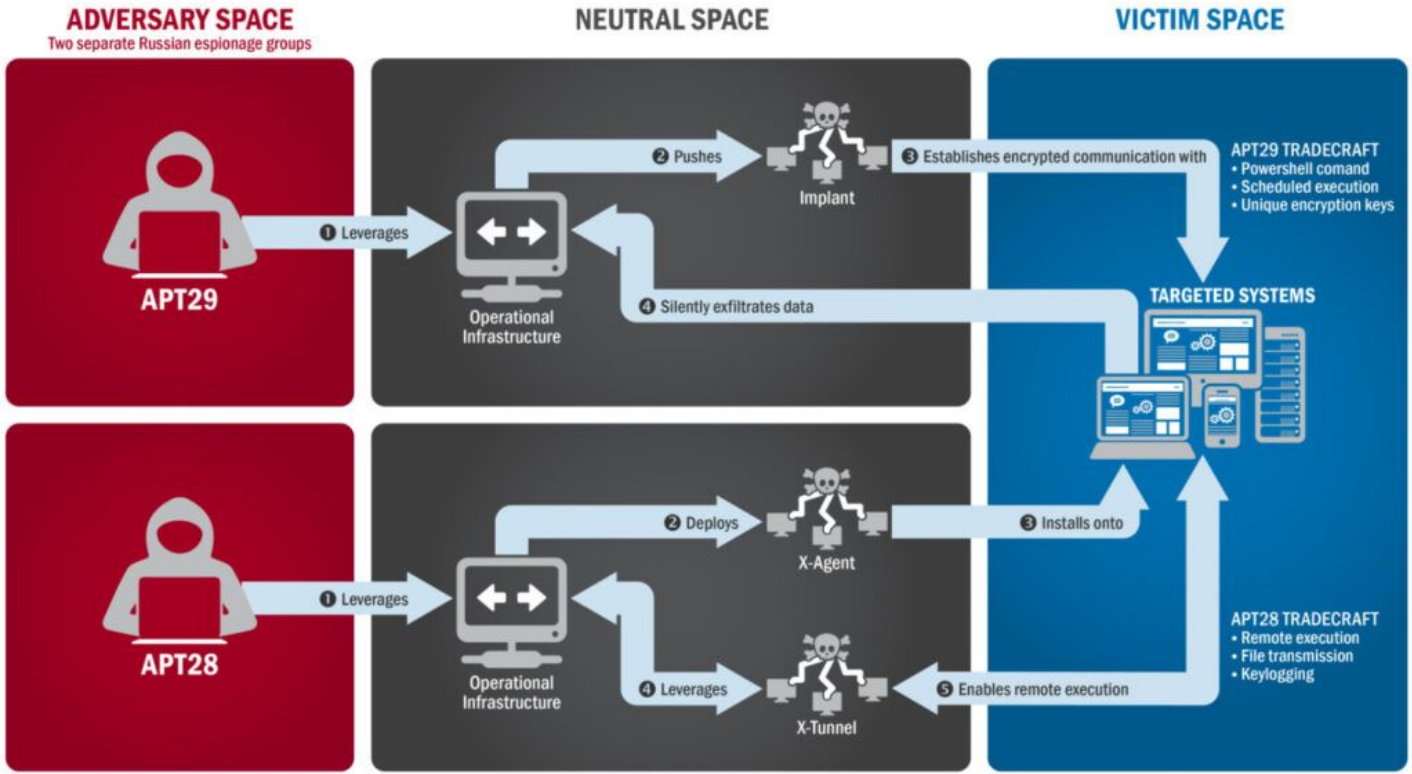
- APT28は標的となった組織のドメインを模倣した偽ドメインを使用し、短縮URL等を用いて被害者をだまして、正規の資格情報を入力させていました。
- 2016年春、APT28は偽のWeb メールドメインを通じて同政党（民主党）の受信者をだまし、パスワードを変更させました。APT28 は収集した認証情報を使用してアクセスを取得し、コンテンツを盗むことができ、これにより複数の民主党幹部からの情報の流出につながった可能性があります。

2016年「GRIZZLY STEPPE」(APT29)

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	Persistance	T1505.003
CVE-2021-26858	Exchangeサーバ	リモートコード実行	Persistance	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 - Phissing	T1566
CVE-2020-35730	RoundCube Webmail	XSS	Initial Access - Phissing	T1566
CVE-2021-44026	RoundCube Webmail	SQLインジェクション	Initial Access - Phissing	T1566
CVE-2023-38831	WinRAR	任意のコード実行	Initial Access - Phissing	T1566
CVE-2020-0688	Exchangeサーバ	リモートコード実行	Initial Access - Phissing	T1566
CVE-2022-38028	Windows Print Spooler	権限昇格	Privilege Escalation - Exploitation for Privilege Esc	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	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

AP

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

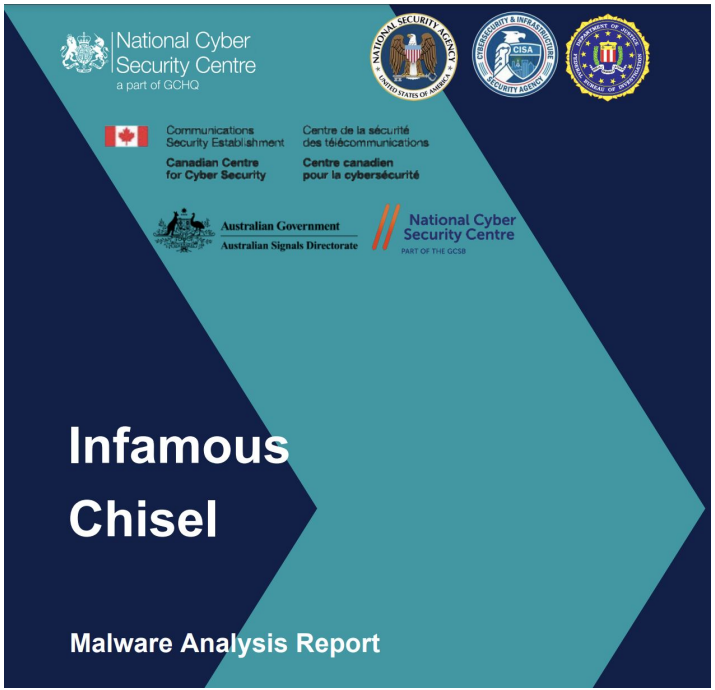
攻撃の一部は成功した模様

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発せられる。



「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。

NCSC「Infamous Chisel」

Sandworm

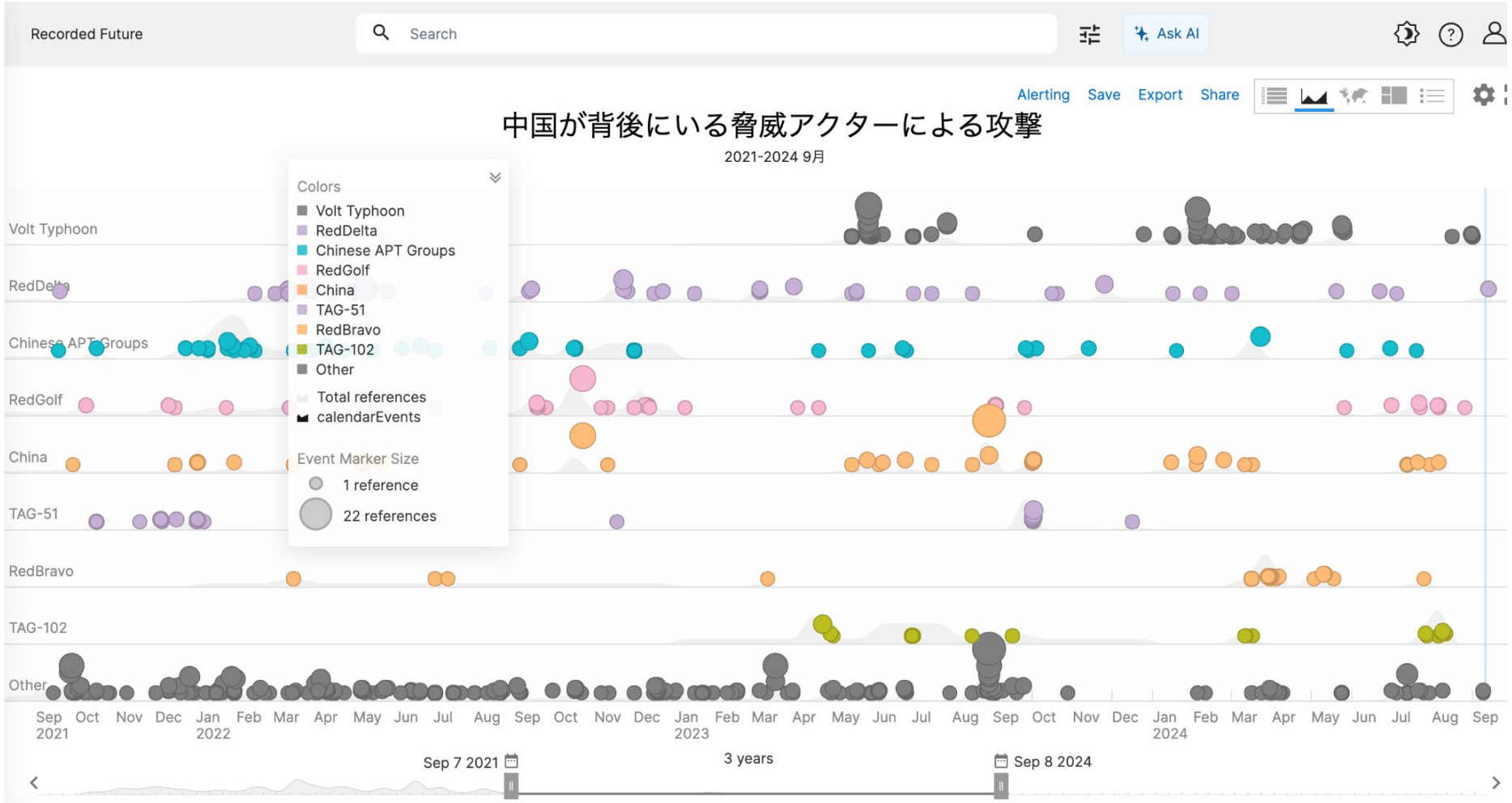
CVE-2022-30190	Microsoft Support Diagnostic Tool	リモートコード実行	Initial Access - Phissing	T1566
CVE-2023-38831	WinRAR	任意のコード実行	Initial Access - Phissing	T1566
CVE-2019-10149	Exim	リモートコード実行	Initial Access - Exploit Public-Facing Application	T1190
CVE-2022-30190	Microsoft Support Diagnostic Tool	リモートコード実行	Execution - 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部队, BRONZE SUNSET, Comment Crew, Comment Panda, FLUORINE, PLA Unit 61398, TG-8223)

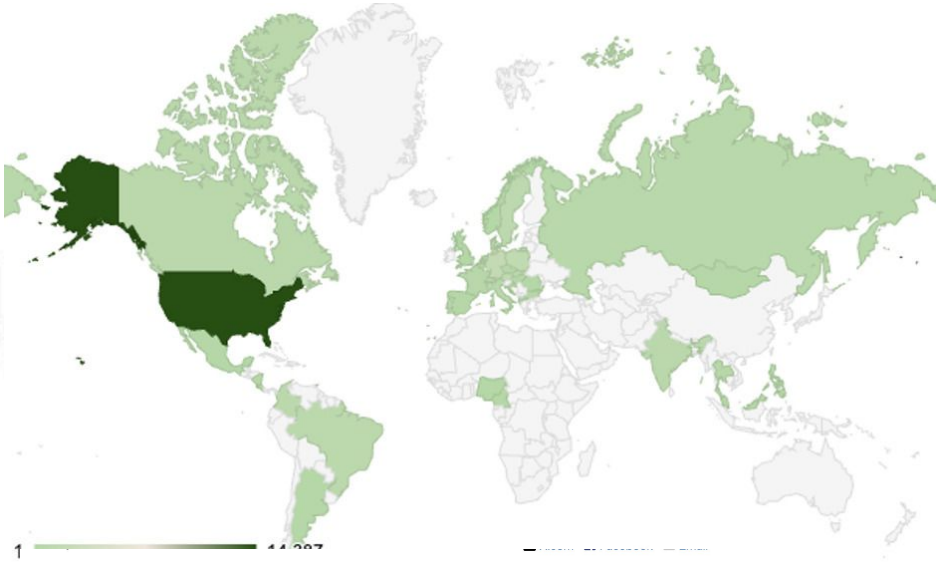


https://app.recordedfuture.com/live/sc/26qCSUGYxU8D

Volt Typhoon (DEV-0391)

- **グアム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



TLP:CLEAR

Secure by Design Alert

Security Design Improvements for SOHO Device Manufacturers

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.

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

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

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

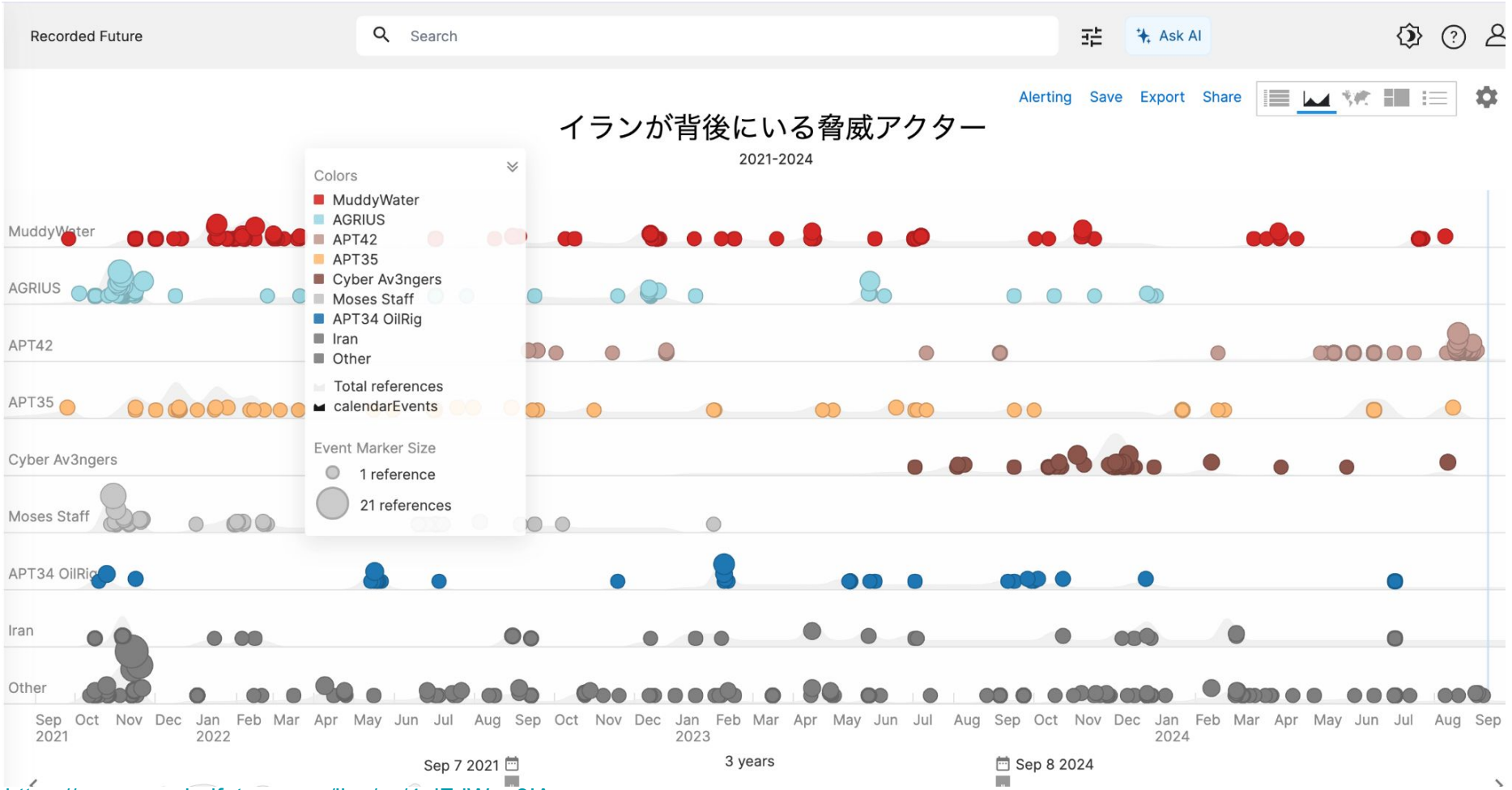
RedDelta(Mustang Panda, Stately Taurus)

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



https://app.recordedfuture.com/live/sc/4elFdWnn9IAr

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。

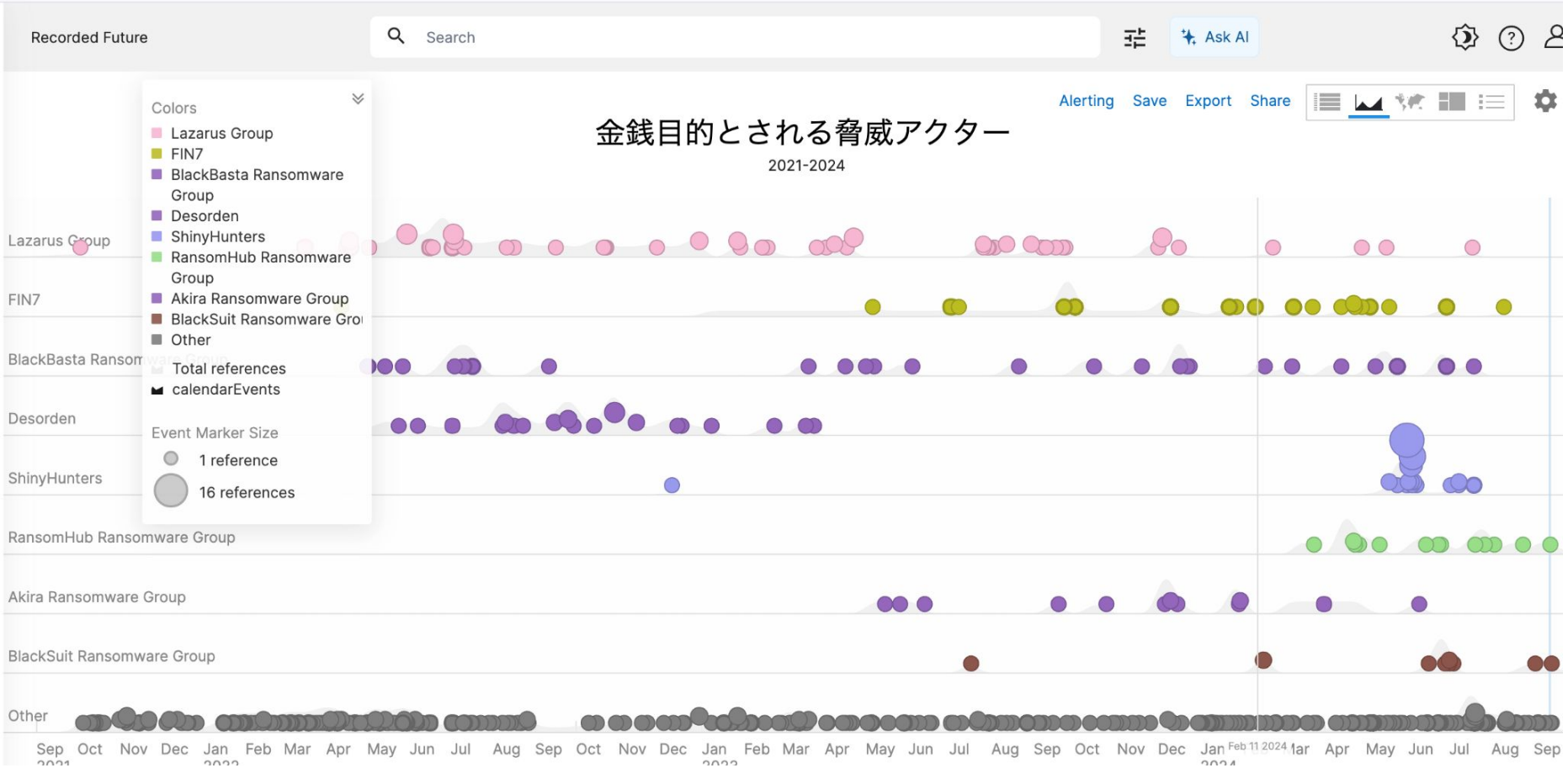
MuddyWater は、ファイル共有サービスからのマルウェアのダウンロードにつながる、悪意のある PDF 添付ファイルによるスピア フィッシングなどの高度な戦術を採用しています。

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。

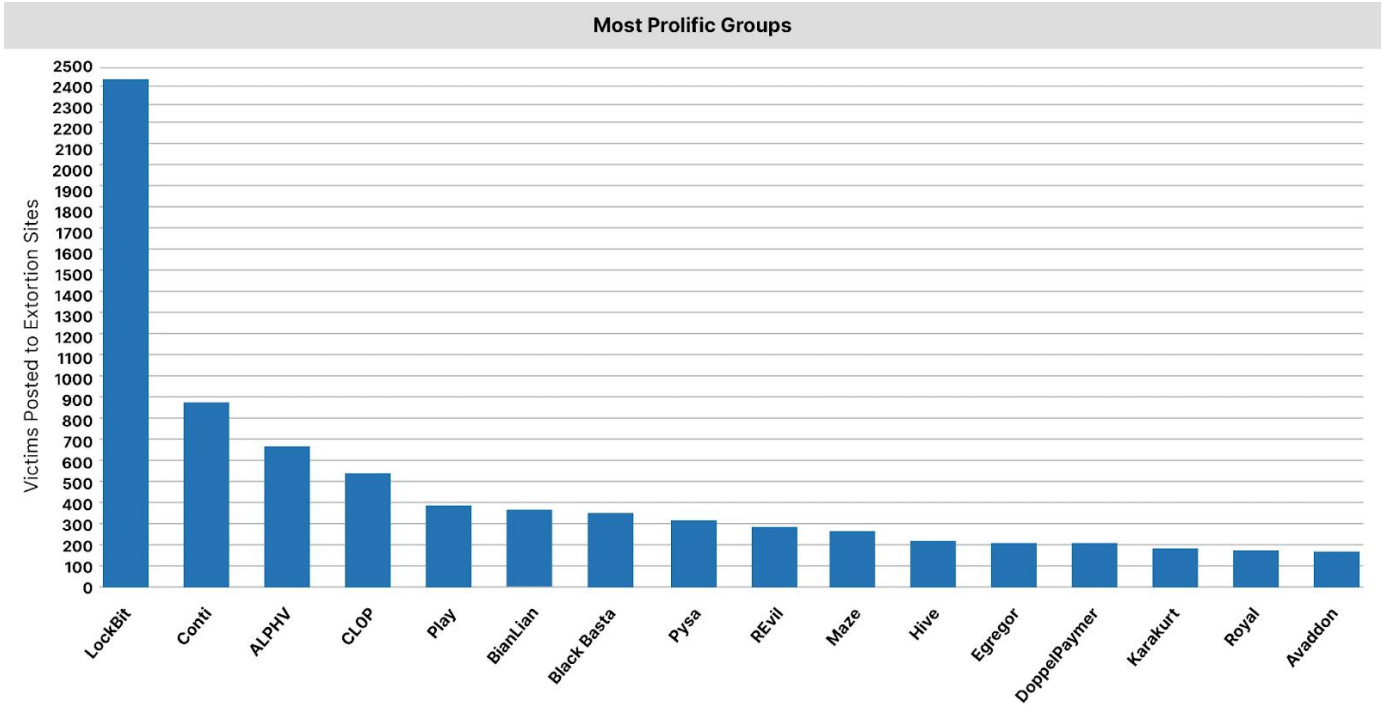
Muddy Water

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


Recorded Future
Search
Ask AI
Alerting
Save
Export
Share
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 Grou
Other
Total references
calendarEvents
Event Marker Size
1 reference
16 references
Lazarus Group
FIN7
BlackBasta Ransomware Group
Desorden
ShinyHunters
RansomHub Ransomware Group
Akira Ransomware Group
BlackSuit Ransomware Group
Other
Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan Feb 11 2024 Mar 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CL0P・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）

The Record.
Recorded Future® News

脅威アクター

1. LockBit
2. Akira
3. RansomHub

2-1. LockBit

LockBit

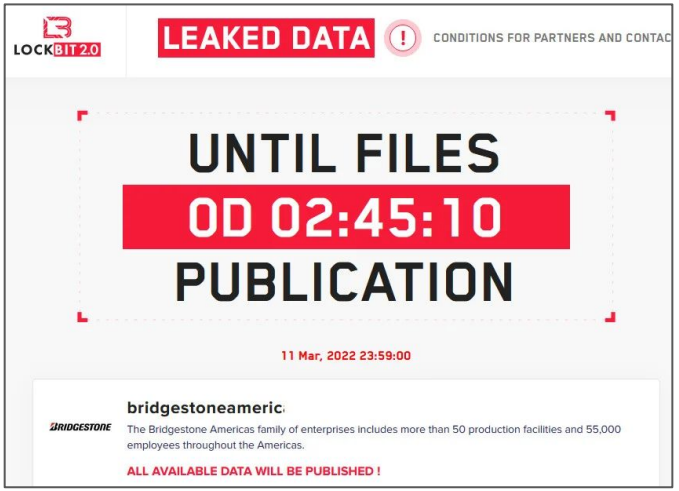
LockBit ランサムウェアグループは2019年に出現し、それ以来重大な脅威をもたらしている脅威アクターです。LockBitは、そのRaaS（Ransomware-as-a-Service）モデルで広く知られており、二重恐喝を専門としています。

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」

SEIZED LOCKBIT 3.0

LEAKED DATA

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

NCA National Crime Agency · EUROPOL

Press Releases
PUBLISHED

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

LB Backend Leaks
PUBLISHED

NCA National Crime Agency

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

LOCKBIT 3.0

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 engage with Law Enforcement

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

Cyber Choices
PUBLISHED

CYBER CHOICES

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

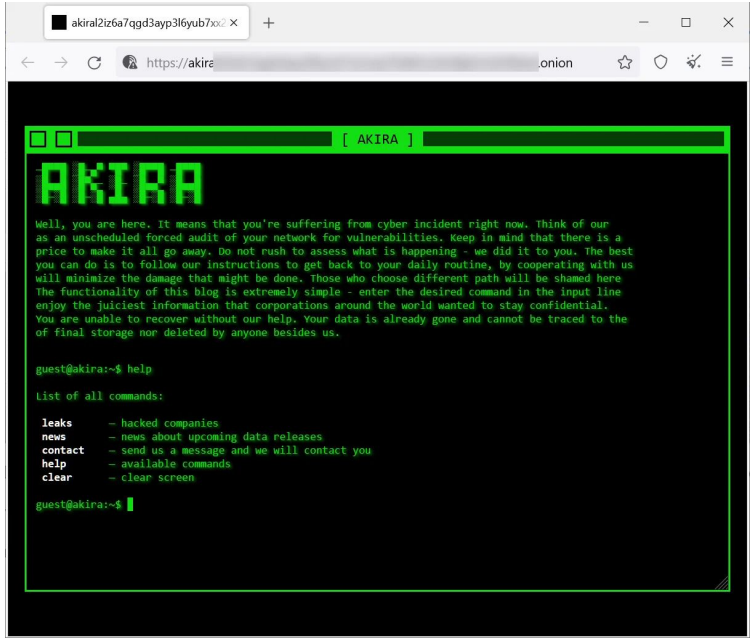
Akiraランサムウェアグループは、2023年3月に発見された、比較的新しい二重脅迫型のランサムウェアグループになります。過去に解散したグループ「Conti」と共通点が多く、Contiの元アフィリエイトが立ち上げたグループの可能性を示唆されています。

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

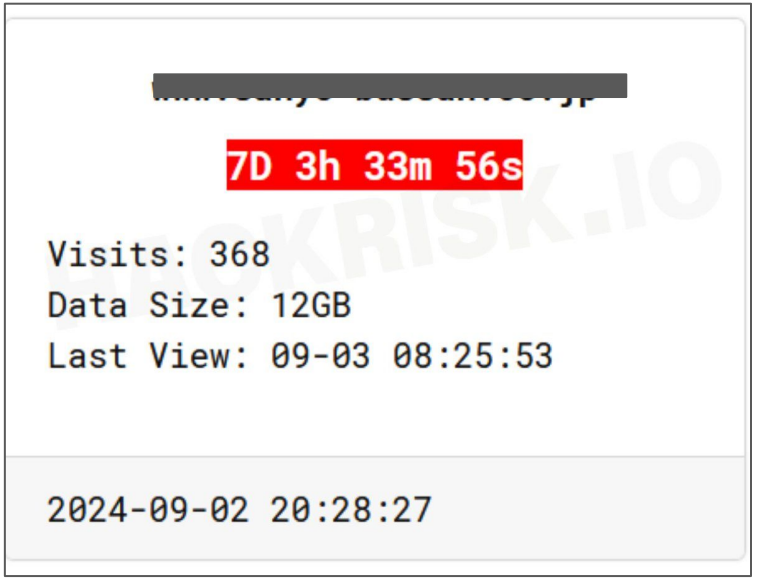
RansomHub

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。



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	Persistance	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/IoCなどをアラートとしてあげる

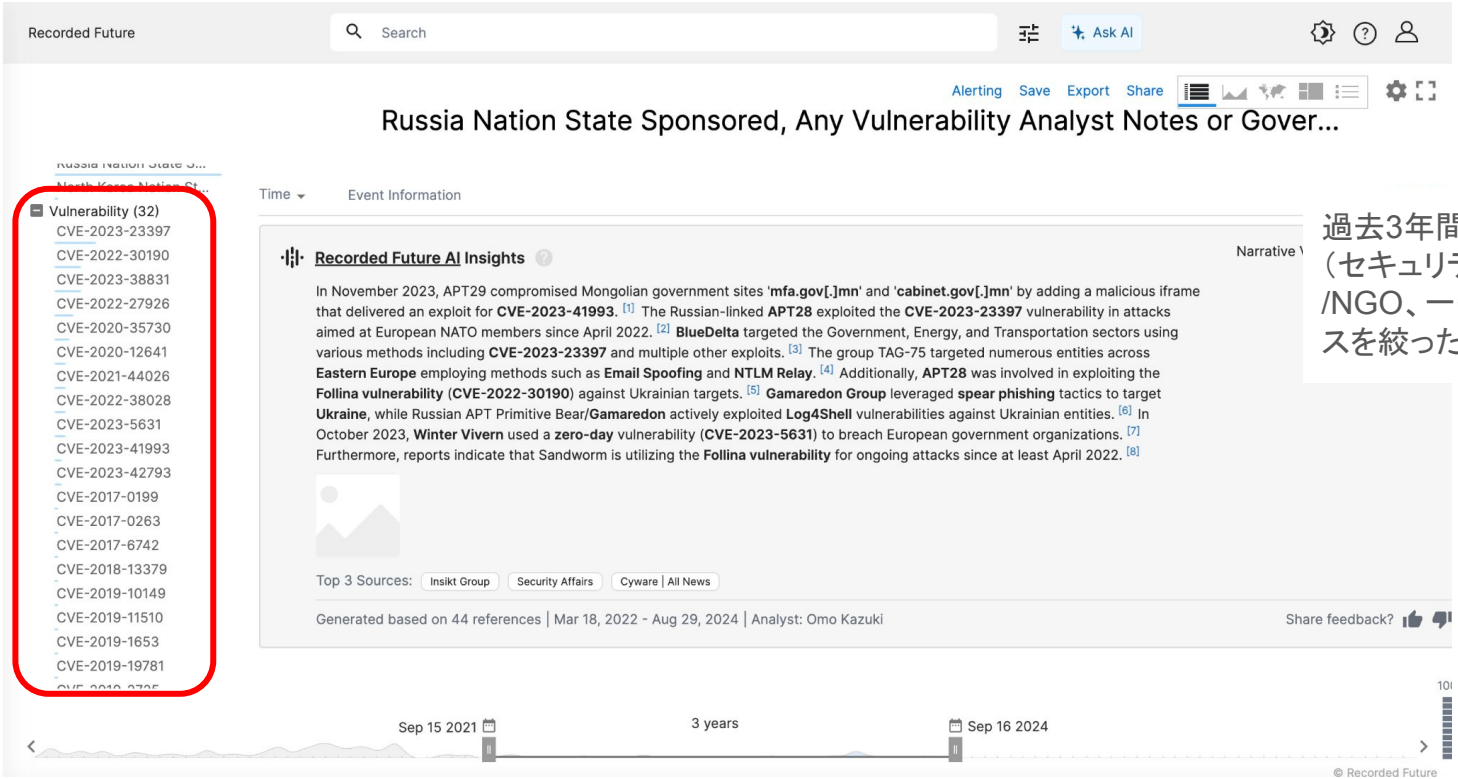
などを行い、脆弱性情報を脅威インテリジェンスの中で活用している

(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）

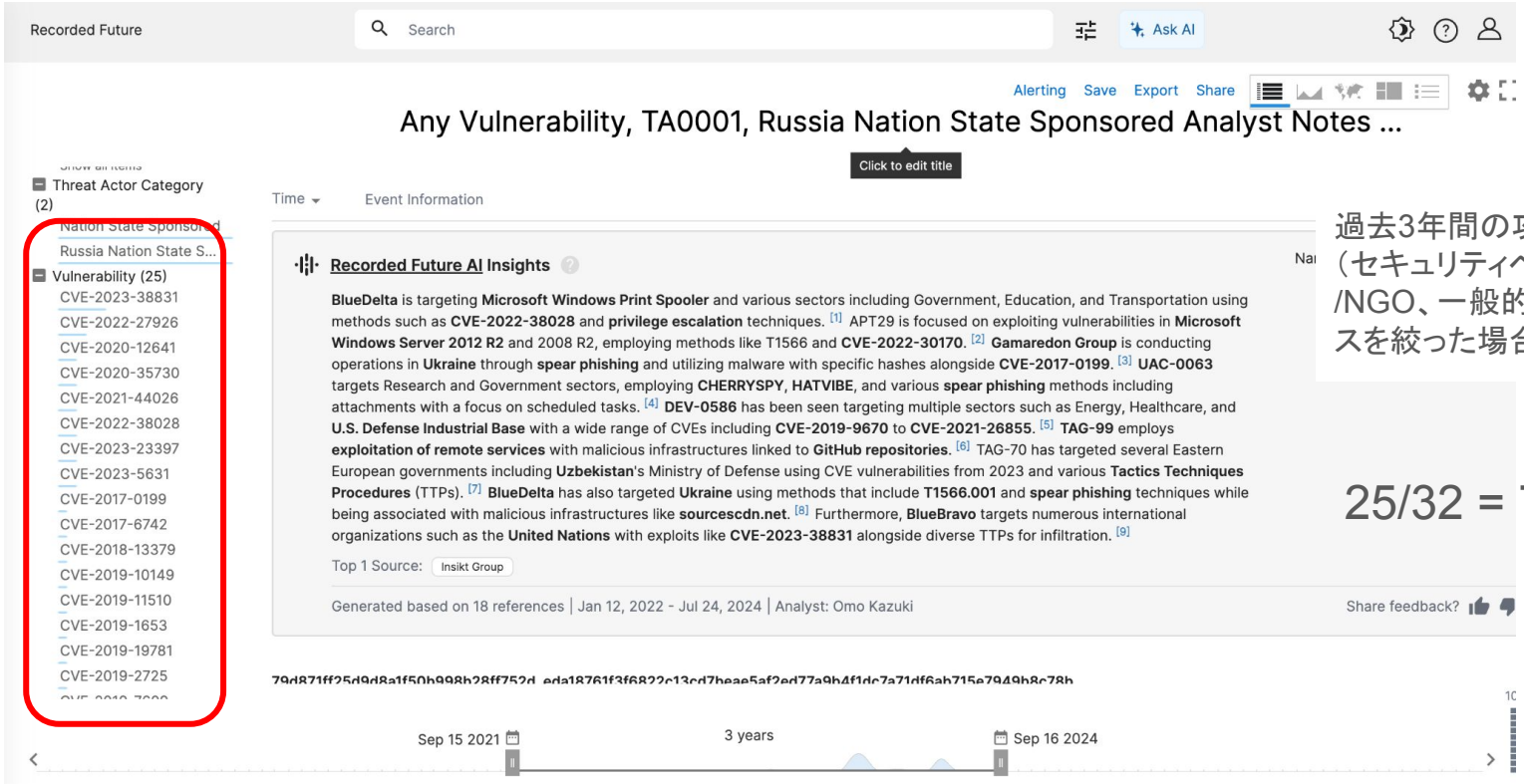
(補足) 商用Intelligence製品で確かめてみる(ロシア)



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）

https://app.recordedfuture.com/live/sc/BnSB4qWcEQkP

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

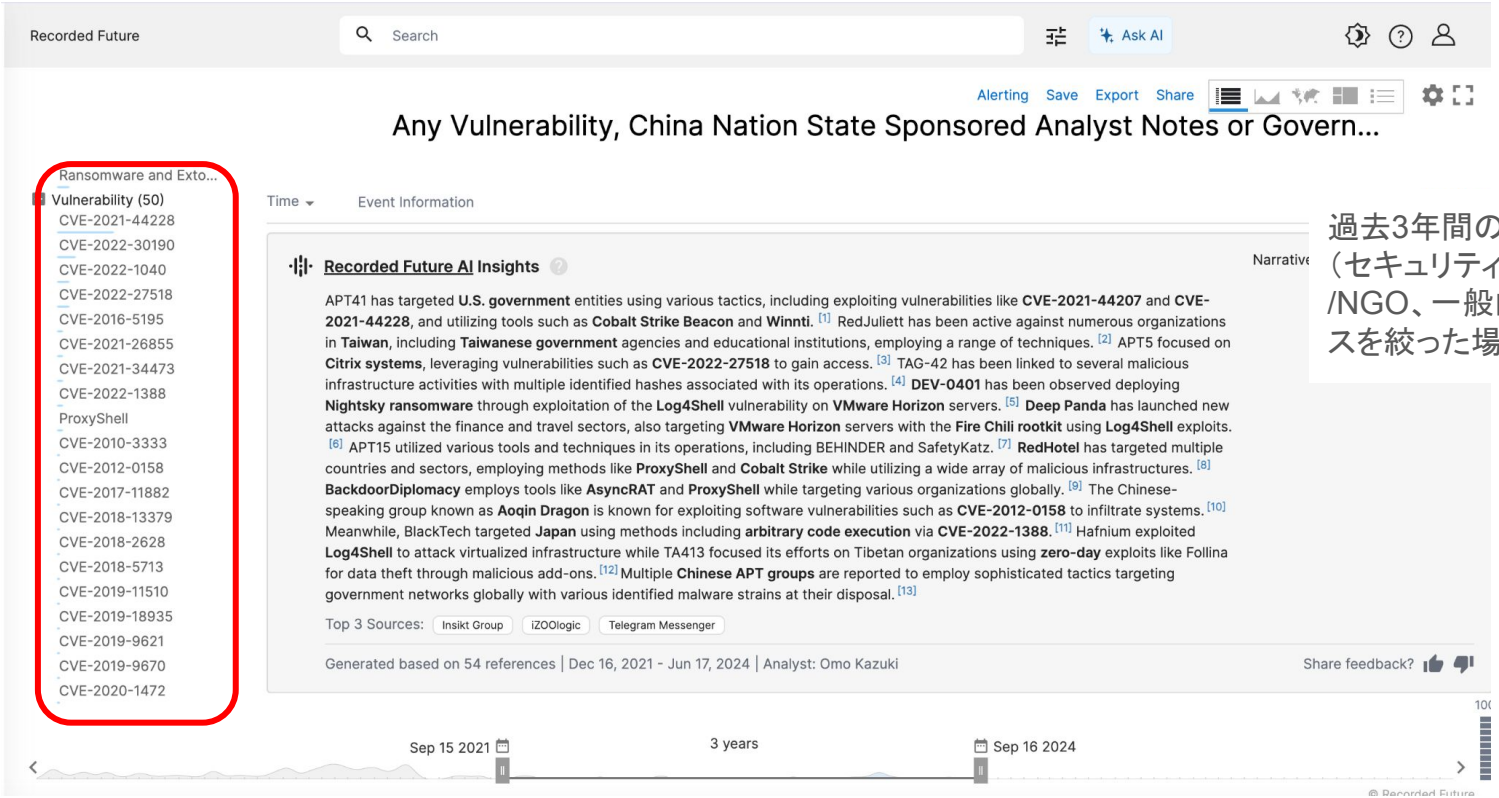


過去3年間の攻撃
（セキュリティベンダーレポートや政府/NGO、一般的なニュースに情報ソースを絞った場合）

25/32 = 78%がTA0001

https://app.recordedfuture.com/live/sc/BnSB4qWcEQkP

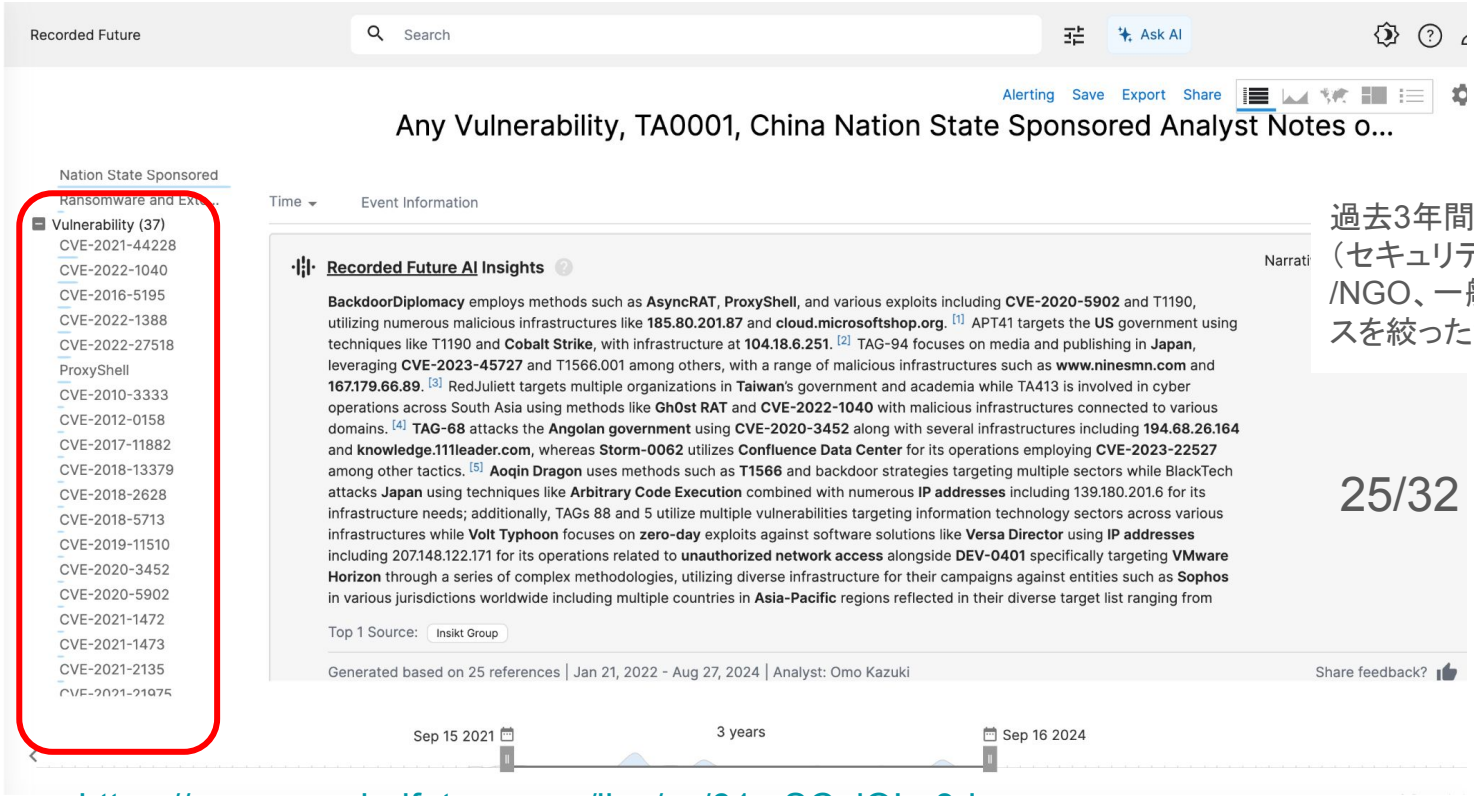
(補足) 商用Intelligence製品で確かめてみる(中国)



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）

https://app.recordedfuture.com/live/sc/4yqOcXPK1T0v

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

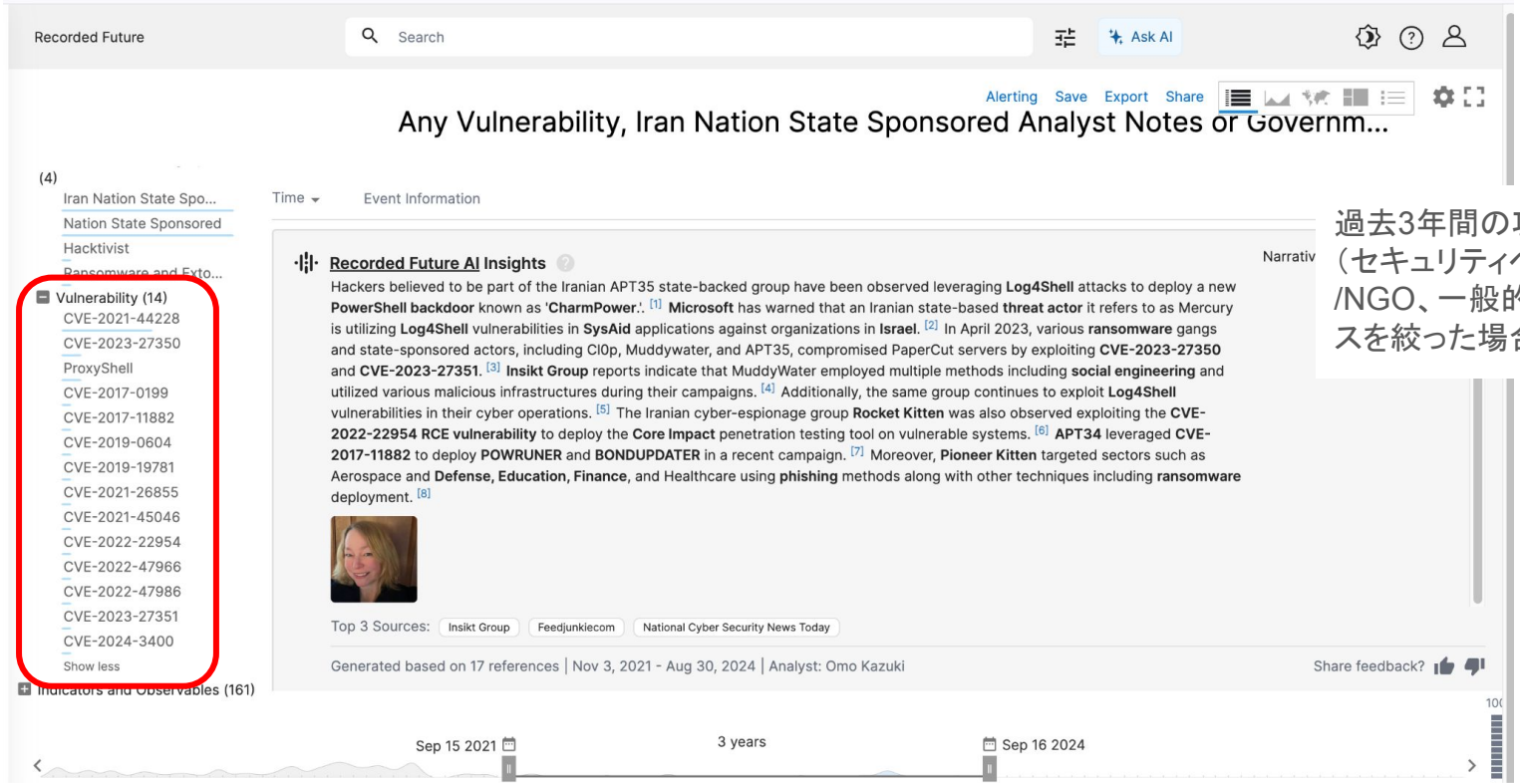


過去3年間の攻撃
（セキュリティベンダーレポートや政府/NGO、一般的なニュースに情報ソースを絞った場合）

25/32 = 74%がTA0001

https://app.recordedfuture.com/live/sc/61mSCniQLe3d

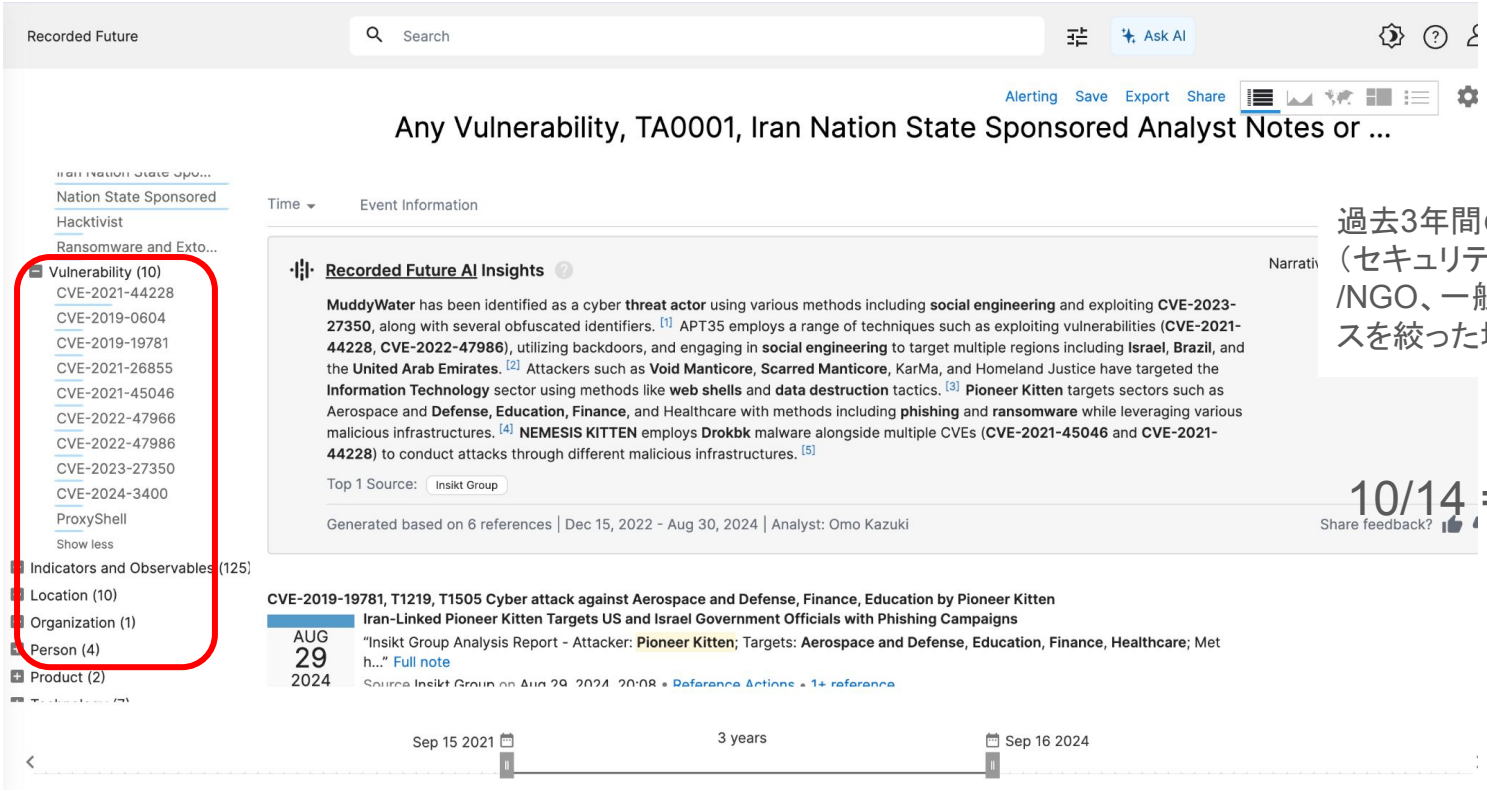
(補足) 商用Intelligence製品で確かめてみる(イラン)



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）

https://app.recordedfuture.com/live/sc/ultUULWPRtVT

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

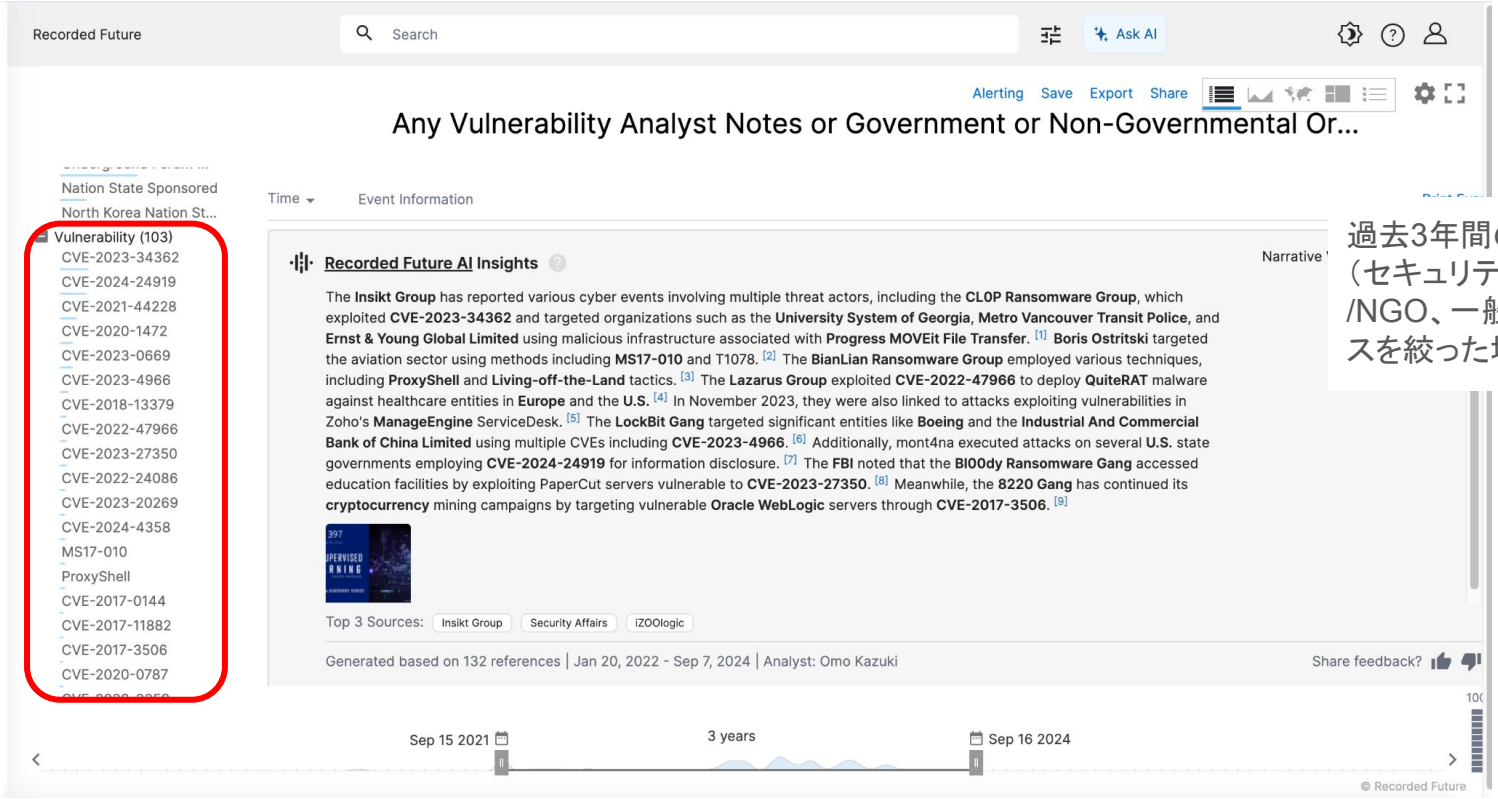


過去3年間の攻撃
（セキュリティベンダーレポートや政府/NGO、一般的なニュースに情報ソースを絞った場合）

10/14 = 71%がTA0001

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

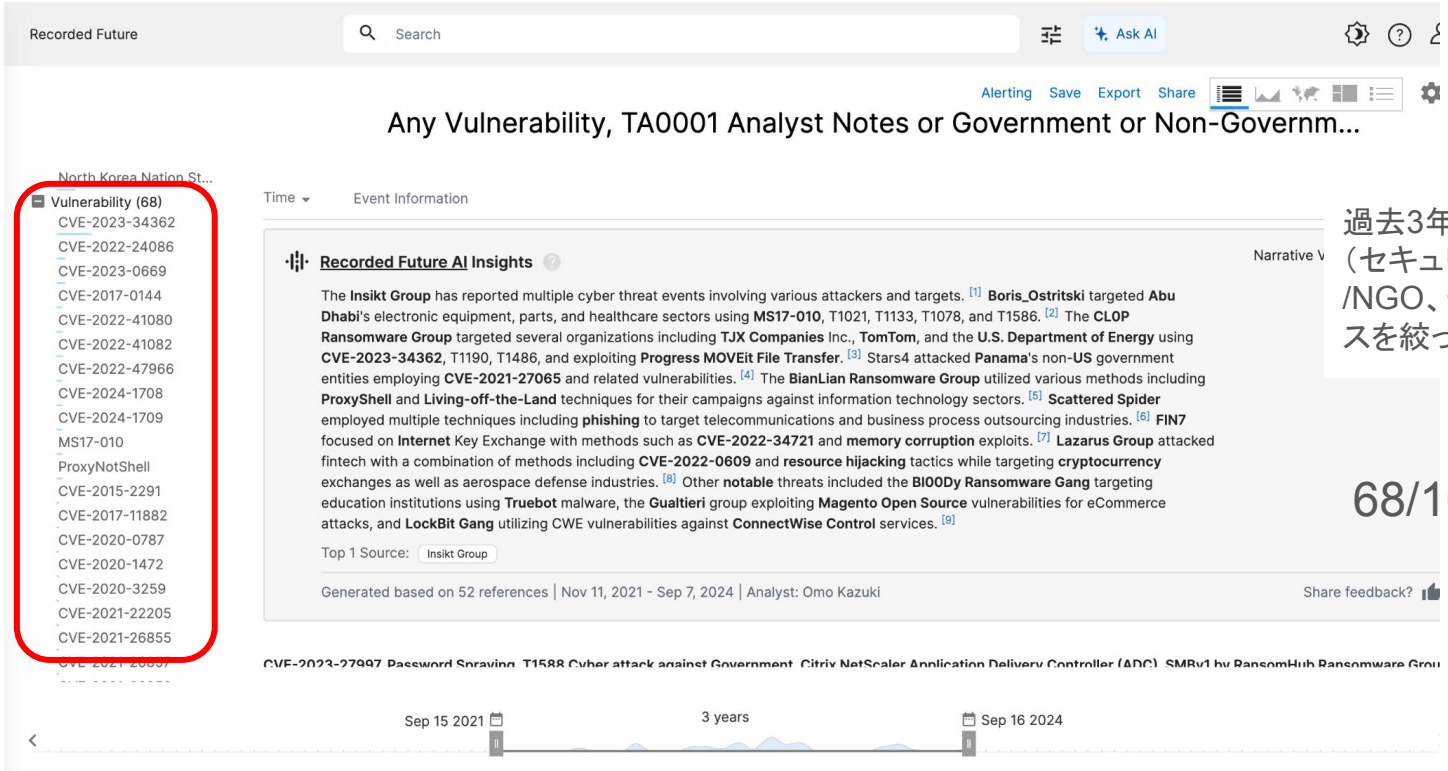
(補足) 商用Intelligence製品で確かめてみる(金銭目的)



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）

https://app.recordedfuture.com/live/sc/6QERGeQ7jdCA

(補足) 商用Intelligence製品で確かめてみる(金銭目的)



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

https://app.recordedfuture.com/live/sc/1jxjZ6Rp4k1D

(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。