DARKTRACE

CRIMSON ECHO:

中国系サイバー諜報技術を理解する

～ビヘイビア分析を通じて

目次

はじめに

近年、世界のデジタルシステムおよび経済システムにおける中国の役割は拡大し、それに伴って中国系グループが関係したサイバーアクティビティも着実に増加しています。

これらの脅威アクターは、中国の国家利益に役立つ情報やアクセスを提供するかもしれないネットワークを持つ公的または一般の組織を常に狙っています。

これらのアクティビティの継続に対し、さまざまなセクターの組織が一定のレベルのリスクを予期し、中国系グループが関係した侵入を識別し、管理する備えをしておく必要があります。.

中国系攻撃者からのリスクをよりよく理解し、コミュニティに情報を提供するため、ダーク十レースは過去3年間の顧客ベースでの中国系グループが関与したサイバーセキュリティインシデントの証拠を調査し、長期的レビューおよび脅威ハンティングを実施しました。

このレビューでは、2022年7月中旬から2025年9月までの期間に、国やセクターを問わずDarktraceによって検知された異常なアクティビティを精査し、仮説、シグネチャ、動作、および戦術、技法、手順（TTP）に基づく脅威ハンティングを含む、複数の構造化されたインシデント識別手法を適用しました。

限界と課題

中国系グループによる作戦を特定する

サイバーセキュリティプロフェッショナルは伝統的に複数の情報ストリームや分析リソースを組み合わせて中国系グループの脅威に対抗してきました。

サイバー脅威情報ストリームやシグネチャベースの検知は有益ではありますが、これらの手法に過剰に依存していては回避技術に長けた相手には不十分です。そのため、セキュリティアナリストは国の軍や諜報機関が支援する脅威のような特に高度で能力の高いAPT（Advanced Persistent Threats）についての攻撃者プロファイルを非常に頼りにしています。

しかしこのAPTプロファイリングへの依存はこれらのリソースが増えすぎる結果を招きました。 これらのサービスを提供する組織はしばしば異なる命名規則を使用し、その結果、同じグループについての、冗長で、しかしわずかに異なる理解が生まれることになりました。

これらの脅威グループ間での人的および技術的リソースの共有もさらなる問題を作り出します。中国系グループ間のはっきりした組織の境界線を自信を持って引くことは難しいかもしれません。それは中国の安全保障および軍事機関の間での人的および技術的リソースの共有がされているからです。サイバー防御者は現在、拡大しつづけるグループの境界を似たようなTTPから判別し、重複している可能性のあるプロファイルを分析してSOCのためにアクション可能な情報を抽出するという、さらなる課題に直面しています。

ダークトレースのアプローチ

中国系の脅威ハンティングに対する

各中国系アクターの特徴、動作、ツール、戦術の詳細を分類し続けるのではなく、ダークトレースは Darktrace Cybersecurity Attribution Framework（付録 1）に基づいて、中国系アクターに対する脅威ハンティングのサイバー防御の一般的な枠組みの特定に注力することを選択しました。

これはダークトレースにとって自然なアプローチであると言えます。ダークトレースの特徴である異常ベースの検知は前提に依存しない性質を持っていること、そして本報告書の付録 “Strategic Statecraft” にも詳述されている中国系オペレーションの組織構造を考慮すると、この手法が適しています。人員やリソースの共有により厳密な APT グループの分類がより困難になる一方で、こうした現実はアナリストがより高いレベルでアクティビティを集約することを可能にします。

この目標を達成するため、ダークトレースの脅威調査チームは 2 つのフェーズで調査プロジェクトを実施しました。最初のフェーズにはある種の文献レビューが含まれています。つまり過去 3 年間にわたる回顧的脅威ハンティングを実施することにより、顧客ベース内で中国系によるものと疑われるアクティビティをできるだけ多く特定することです。第 2 のフェーズでは、脅威リサーチチームは特定された各ペースの確度を評価し結果を分析してキルチェーンアクティビティおよび TTP の一般的なパターンを導き出します。

この作業により中国系脅威アクターが関与した中～高確度のサイバー侵入事例を特定するに至りました。その侵害のデータベースからはさまざまなはっきりとしたパターンが確認でき、これは組織内のあらゆるレベルのサイバー実務者にとって有益な情報です。

調査対象期間の中国系サイバー攻撃者は戦略的目標に基づいて幅広い TTP の好み、滞留時間のパターン、そして標的選択のパターンを示していました。ダークトレースの脅威調査チームはこれらの情報を使用して、今後も顧客ネットワーク内において中国系による可能性のあるアクティビティの事例を特定するため、検知メカニズムを形成し継続的に改良を重ねています。

中国系グループが重複し、サブセット間の線引きがしばしばあいまいであることから、このレポートでは中国系サイバーアクティビティがもたらす課題をより幅広い枠組みでコンテキスト化することを目標としています。これにより、SOC アナリストやサイバーセキュリティプロフェッショナルがこれらの考察を利用してより簡単かつ迅速にこうした中国系によるものと疑われるアクティビティのインスタンスを自社の環境内で特定し、脅威に対するサイバーレジリエンス強化に役立てていただけることを願っています。

Project Director: Nathaniel Jones

Project Analyst Lead: Adam Potter

Project Participants: Emma Foulger, Paul Jennings, Nahisha Nobregas, Nicole Wong

Contributors: Nicole Carignan, Margaret Cunningham, Eugene Chua, Owen Finn, Samantha Gonzalez, Keanna Grelicha, Daniel Levy, Angel Lopez, Nathan Ly, Qing Hong Kwa, Will Palmer, Shawn Puckett, Tyler Rhea, Steven Sosa, Priya Thapa, Hyeongyung Yeom

Report Editors: Sarah Murphy, Ryan Traill

主な考察：

中国系サイバーオペレーションは単発的なキャンペーンではなく、**戦略的計画の連続**であると理解するのが最適である。

滞留時間の短い侵入は諜報活動の失敗として解釈するべきではなく、**意図的な作戦上の選択**と見るべきである。

西側のセキュリティモデルは依然として過度にインシデント中心型であり、全体として**持続的なアイデンティティリスクを過小評価**している。

中国のサイバーアクティビティは**知的財産の窃取だけではなく**、ますます一帯一路構想（BRI）や世界の重要インフラへの影響力に基づいたものとなっており、とくに米国に重点が置かれている。

以降のセクションの内容：

調査**手法**の詳細

中～高確度のアトリビューションが行われた事例の詳細な**レポート**、および地域およびセクターレベルの明確な分類

観測されたアクティビティが、2013年に発表された中国の経済圏構想であるBRIに関連した目標とどのように一致しそれを支援するものとなっているかについての**評価**

付録1：Darktrace Cybersecurity Attribution Framework

付録2：侵害インジケータ（IoC）のリスト

付録3：メタモデル作成

付録4： CVE公開前の異常検知例

付録 5: 重要インフラとしての分類

手法

顧客ベースにおける中国系サイバー作戦の包括的な長期レビューを実施するにあたり、ダークトレースの脅威調査チームは、関連性を確保するための明確な指標、定義、および計画を策定しました。それには、経験的証拠に的を絞ったアトリビューションのためのフレームワークも必要でした。

この手法は、Darktrace の AI 駆動のビヘイビア検知を、外部インテリジェンス、セクター別のコンテキスト、既知の脅威アクターの TTP の比較分析を組み合わせ、構造化された多面的なアプローチをアトリビューションに適用します。さまざまなインフラストラクチャからの証拠、ツール、TTP（戦術、技法、手順）、被害者の特徴、アーティファクト、および裏付けを評価することで、アナリストは信頼度レベルを適切に調整できます。

これにより、脅威アクターの境界が重複している場合やあいまいな場合でも**、一貫性のある確実なアトリビューション評価**が可能になります。所見は既知の戦略的優先事項との一致を確認するものであり、方向性や指揮の確認を意味するものではありません。また、任務指示権限や将来の国家による行動を示唆するものではなく、観察された作戦パターンと防御リスク露出を検討することにより評価されたものです。

精度の誤解を避け、分析の整合性を保ち、コミュニティによるダークトレースのアナリストとの Crimson Echo についての議論を促進するため、付録には低、中、高の確度の例を示しています。確度スコアは絶対的な確実性の指標というよりもケース間の比較を意味するものであり、前述の複数の証拠クラスを使った裏付けを反映しています。

ダークトレースの脅威調査チームは、計画、脅威ハンティング、品質管理、分析という 4 つのフェーズのアプローチで顧客ベース内の中国系脅威アクティビティを調査しましたこのセクションでは、結果の文脈をよりよく理解し、脅威ハンティングのパラメーター、そしてケースの確度を評価するためのテクニックについて知りたい方のために、プロジェクト計画の各要素と関連性を確保するための手法についてレビューします。

調査結果は差し迫ったアクティビティではなく構造的なリスクパターンを識別するものであり、また観測されたすべてのアクティビティが脅威アクターの評価を補強しているわけではありません。

Crimson Echo の調査結果は堅牢であるものの、基礎となるデータセットの規模と構成によって制約されています。過去 3 年間の合計で、低・中・高確度のケースは執筆時点で 80 件を超えています。

メタモデルとその後の分析は、中〜高確度と判定された 50 件以上のケースに限定されており、そのこと自体に観察の間違いや分析の漏れという課題が伴います。

これにより統計的検出力が制約され、結果は決定的というよりも記述的なものとして扱うべきであることを意味します。要約統計量、ブートストラップ信頼区間、カーネル密度推定（KDE）および QQ プロットの比較、シャピロ・ウィルク検定のすべてが、滞在時間分布が右に歪んでおり、初期にアクティビティが密集し、ロングテールであるという結論を支持しましたが、サンプルサイズが小さいため、これらの方法の解釈には限界があります。全体として、分析はビヘイビアの傾向を確実に捉えていますが、より大きなデータセットなしにはより高解像度のモデリングをサポートすることはまだできません。

分析の期間

ダークトレースの脅威調査チームは、2022 年 7 月から 2025 年 9 月末までの約 3 年間の脅威ハンティングの期間を設定しました。

中国系グループに対する完全な包括的レビューは数十年にわたる可能性がありますが、調査の期間は複数の理由で制限されていました。個人や組織と同様に、APT も時間とともに進化し、その技術を改良することができます。

選ばれる標的は、資金を提供する政府機関の目標によっても大きく影響を受けます。

戦略レベルでのいくつかの大きな目標は不変かもしれませんが、作戦および戦術的な取り組みは必然的に変化します。侵害インジケータ（IoC）もアナリストにとっての重要性は限定的で、かつて広く利用されていたマルウェアも時間の経過とともに使用が減少することがあります。これらの要因により、中国系エクスプロイトのより古い事例は分析においてあまり重要でない可能性があります。

これらの制約を踏まえて、選択された期間は十分なサンプルサイズを確保しつつ、時代遅れの指標や昔の活動の影響を最小限に抑えることができます。

ログタイプ

すべての脅威ハンティング活動と同様に、脅威ハンティングの性質と結果は、レビューされたログの構成に影響を受けています。

このプロジェクトの脅威ハンティング活動は主に、Darktrace によって識別された動作の逸脱に関するデータを活用しました。IoC、仮説、および TTP に基づく調査を含むさまざまな脅威ハンティング手法を使用して、意味のある動作の逸脱が特定されました。したがって、脅威ハンティング中に識別されたアクティビティには、警告が発生したデバイスに対して異常として既にフラグが立てられています。

脅威ハンティングのフェーズ

ダークトレースの脅威調査チームは作業の重複を避けできるかぎり全体でレビューできるよう、脅威ハンティングのフェーズを 2 つに分けました。これらのフェーズには次の重点が含まれ、それぞれを以下に説明します。

フェーズ 1：キャンペーン / マルウェアの調査

フェーズ 2：TTP とシーケンスを使った
ビヘイビアベースの仮説の調査

各フェーズは、過去に特定されているキャンペーン、マルウェア、または中国系侵入事例に関連した主要な TTP に基づく**標準的な脅威ハンティング**で構成されています。調査には厳格に管理されたシーケンスベースの脅威ハンティングフレームワーク（仮説ベース等）が含まれています。

フェーズ 1：キャンペーン / マルウェアの調査

最初のフェーズでは、外部のセキュリティ研究者によって詳細に報告されている中国系サイバー活動をまずレビューすることに焦点を当てました。アナリストは、中国系グループに関するオープンソースインテリジェンス（OSINT）ソースおよび記事の集約を作成しました（第三者によって評価されたもの）。

第三者によって詳細に報告された各特定のキャンペーンまたは一連のエクスプロイトを基に、その作戦に関連する顧客ベース内の過去の活動について対応する調査が行われました。このフェーズはプロジェクトの「文献レビュー」の部分を中心としています。さらに、ダークトレースのアナリストは、中国系グループと高い関連性が知られているマルウェアの証拠を特定するための調査も行いました。

これらのマルウェアの亜種には、以下のものが含まれていましたが、これらに限定されません：

- ShadowPad
- PlugX
- SnappyBee

しかし、ダークトレースのチームは、マルウェアの使用だけでは中国系グループの活動の強い指標とはならないことを認識しています。なぜなら、他の国家を背後に持つ組織も同じマルウェアを使用して彼らの国家安全保障の目標を達成しつつ、セキュリティチームをミスリードする「偽旗」作戦を実行するからです。

そのため、マルウェアについての調査は、事前のダークトレース専有情報、OSINT ソース、および確立された業界の関係に基づくその他のインテリジェンスによって補完されました。

フェーズ 2：TTP ベースの調査

脅威ハンティングの第 2 のフェーズは、特定された TTP を使用して、特定されたキャンペーンや対応する作戦に関連しない中国系グループの活動の他の事例を検知することに重点を置きました。

アナリストは、以前のキャンペーン / マルウェア調査フェーズの情報からこれらの TTP を導き出しました。過去のキャンペーンのそれぞれをレビューする過程で、一般的な手順や作戦上のアプローチにおける主要なテーマが浮かび上がり始めました。

これらのテーマは、その後、顧客ベース内で見つかった実際のエクスプロイト事例によって補強されました。「文献レビュー」から得られたテーマとモデルアラートデータ内で特定された作戦の組み合わせは、脅威ハンティングクエリを構築するために使用される TTP の主要な要素として機能しました。使用された TTP のサンプルには以下が含まれます：

- インターネットに接続されたインフラ
- LOLBin
- DLLサイドローディングと検索順序ハイジャック
- トンネリングおよびC2のためのDNS

各戦術や技法には実行方法にバリエーションがあったため（それにより正確な脅威ハンティングクエリの作成が困難でしたが）、調査チームはアクティビティに共通する核心要素に基づいて、シーケンスベースの脅威ハンティング手法を用いてエクスプロイトの証拠を探しました。

品質コントロールと確度の判定

脅威ハンティングの両フェーズで特定されたすべてのケースに対して、少なくとも 2 回の品質コントロールプロセスを実施しました。アナリストは最初に、そのアクティビティが中国系グループの侵入を含まない他の脅威アクター、マルウェア、または作戦に合理的に帰属または関連付けられるかどうかを判断するためのレビューを行いました。すべてのネットワークベースの IoC は、複数の OSINT 手法および情報源を通じてレビューされ、無関係なマルウェアとの関連の可能性が検討されました。

また、アナリストはキルチェーン全体が存在していたケースをレビューし、悪意ではないアクティビティ（例:侵入テスト / 攻撃シミュレーション）や関係のない悪意ある活動（例:犯罪グループによるランサムウェア）を排除しました。その悪意ある性質、あるいは組織への所属が不確かなアクティビティに対してはさらに品質コントロールプロセスが適用されました。

関係のないすべてのイベントが取り除かれた後で、各ケースに対して中国系グループとの関連性についての総合的確度のレベルが設定されました。確度レベルは個別のスコアの値に対応するものであり、このスコアはアトリビューションフレームワークの基盤となるさまざまな入力データの組み合わせを使用して導き出されました。Darktrace Cyber Attribution Framework については付録 1 を参照してください。

結果と主な所見

代表値

ー侵害のデータセットから

侵害イベントの調査の結果得られたデータベースは、2022年7月以降の中国系脅威アクターの作戦の傾向に関する重要な情報をもたらしました。これらの数値は、滞在時間、モデルアラートのシーケンス、およびTTPデータから得られる、より具体的な情報をコンテキスト化するのに役立ちます。

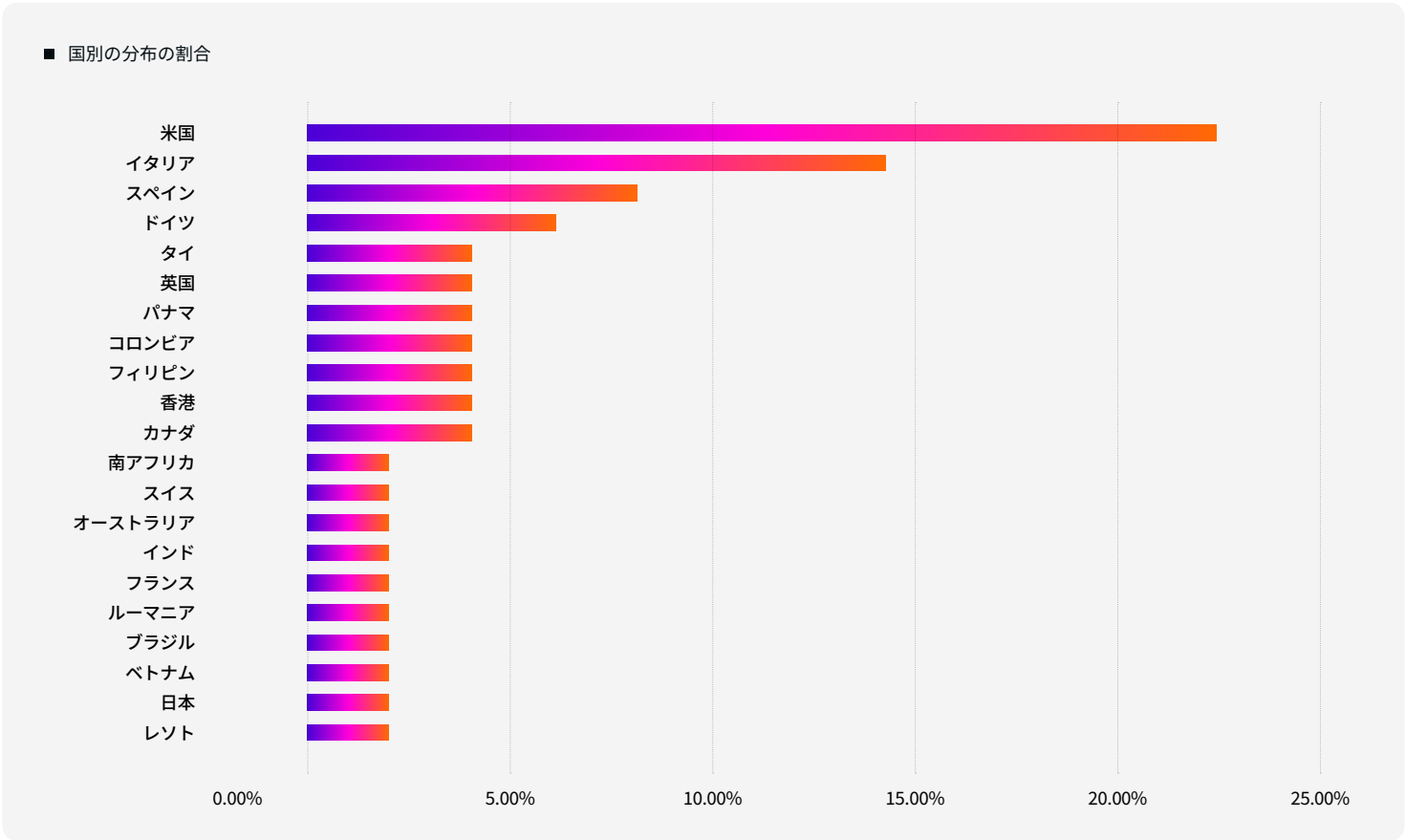
すべての数値と情報は、DCAFスコアリングシステム（付録1）で詳細に定義された少なくとも中程度の確度を持つケースから導出されています。低確度のケースであってもSOCアナリストやセキュリティ研究者にとって有用な情報をもたらすことがありますが、誤ったアトリビューションにつながる可能性があるため、これらのケースは除外されました。

以下のセクションにまとめられたデータは、現在および過去のダークトレースの顧客ベースの構成によって影響を受けます。この制約にもかかわらず、得られたエクスプロイト事例のデータセットは、中国の戦略的目標や作戦キルチェーンのパターンに関する考察を導き出すための確実な情報基盤として機能します。

地域およびセクター別の被害者の特徴および標的の傾向

観測された事例の中で**米国を拠点とする組織**が最も大きな割合を占めており、全世界のイベントのほぼ4分の1（22.5%）を占めています。また、米国の顧客はアメリカ大陸（AMS）地域全体のイベントの60%以上を占めていました。ダークトレースの顧客ベースの構成が結果に影響を与える可能性はありますが、データセットにおける米国の顧客の高い割合は、米国が中国の主要な地政学的ライバルであることを反映している可能性が高いでしょう。米国はまた、国内総生産（GDP）で世界最大の経済を有しており、産業スパイ活動が中国系グループによる侵入の重点となっていることを裏付けています。

米国内の事例のセクター分類および重要国家インフラ（CNI）の分類を考慮すると、この論理がデータに現れていることがわかります。このプロジェクトは、重要インフラストラクチャ（CNI）セクターの特定に米国サイバーセキュリティ・社会基盤安全保障庁（CISA）のフレームワークを利用しており、侵害イベントの圧倒的多数（88%）はCNIに分類される顧客に関わっていました。より厳格な欧州連合（EU）NIS2フレームワークを使用しても、データセットの事例のほぼ4分の3（72%）が、欧州の基準で “critical” または“important” セクターに分類されるものでした。



地域別の傾向：米国

米国は、CNI顧客に関わるすべての事例の約5分の1（約20%）を占め、以下のセクターが含まれていました：

輸送システムセクター

医療および公衆衛生セクター

政府サービスおよび施設セクター

情報技術セクター

地域別の傾向：ヨーロッパ、中東およびアフリカ（EMEA）

米国を除くと、データセット内で最も多い上位5か国のうち3か国はすべてEU加盟国であり、イタリア、スペイン、ドイツです。

これらの国々には、ユーロ圏で最大の経済のいくつかが含まれており、脅威ハンティングプロセス中に特定された多くの組織は、中国政府にとって経済的に重要な中核分野であるデジタルインフラ、先端テクノロジー、製造業、合成素材、農業技術分野に属します。

ヨーロッパ、中東、アフリカ（EMEA）地域全体において、CNI事例の75%以上が以下のCISAセクターに関与していました。

米国とともに、これらの国々はCNIセクターに関わるすべての侵害事例のほぼ半分を占めています。

輸送システムセクター

通信セクター

重要製造業セクター

情報技術セクター

食品および農業セクター

中国は長い間、BRIを通じた貿易を盛んに行う国々および/またはインフラ開発のための経済資金を受け取る国々のデジタルおよび経済の基盤においてさまざまなサイバー作戦を展開してきました。米国およびEMEA地域のCNIセクターに対する全体的な標的の集中は、これらの目標についてのさらなる証拠を提供しています。EMEA地域では、観測された事例の約半数が、標的とされた組織が重要国家インフラ（CNI）に分類されているかどうかにかかわらず、製造業、通信/デジタルインフラ、そして海運/物流の3つのセクターに集中していました。

米国およびEMEAにおける電気通信および輸送インフラの標的化は、中国系アクターが西側諸国との直接対決に備えて事前に配置しようとしていることを示しています。

電気通信インフラに関わる事例の80%はEMEA地域で発生しており、鉄道、空港、港湾などの交通インフラに特に関わる事例はすべて米国、英国、カナダで発生しています。このカテゴリーでは米国がイベントの60%を占めています。

地域別の傾向：アジア太平洋および日本（APJ）

低確度のイベントを含めても、データセット内で最も出現頻度が低かった地域はアジア太平洋および日本（APJ）でした。

特定された侵害イベントの中で、事例はこの地域内の国の間で比較的均等に分布しているようです。しかし、APJ地域内で記録されているすべての国は、東南アジア諸国連合（ASEAN）または日米豪印戦略対話（QUAD）のいずれかのメンバーであることに注意すべきです。この地域内で標的となった組織は、特に南シナ海および台湾に関して、中国の安全保障体制を強化するためのサイバー作戦の重要性を裏付けています。

しかし、香港内でのITサービスの標的化は、国内の治安目標を反映している可能性が高いでしょう。

また、APJ内の事例は、公的機関やメディア分野に偏っています。APJ地域の事例の半分は政府または通信関連の組織で構成されているのに対し、EMEA地域には製造業、医療システム、海運および物流、防衛など、より幅広い重要な経済的目標が含まれています。ここでも、ダークトレースの顧客ベース内に偏りの可能性があることをアナリストは考慮しておくべきでしょう。

このパターンは、標的の選定の一部は戦略的目標によって決定されることを表しているように見えます。APJ地域のサイバーアクティビティはこの地域での中国の安全保障問題（南シナ海、台湾、等）について戦略的アドバンテージを得るためのより伝統的な諜報活動に重点を置いているように見えますが、EMEA地域でのサイバー侵入はBRIに沿った活動と経済的スパイ活動というより広い焦点を反映している可能性があります。

米国、カナダ、およびEMEA地域での事例の大部分が特に輸送システム分野（重要国家インフラ）に関係していることは、中国が台湾をめぐる直接的な軍事衝突の場合に混乱を引き起こすために事前の配備を進めている様子を示している可能性があります。

目標/目的のバリエーション

期間が短いケースと長いケース

このプロジェクトのアプローチは、中国系グループの脅威ハンティングのための一般化された枠組みの定義が可能であるという考えに基づいています。

しかし、ダークトレースのアナリストは、すべての侵害が同じキルチェーンのシーケンスや攻撃要素を持つとは想定していません。調査の結果得られた侵害データベースにはまだ大きな変動性が含まれています。攻撃チェーンの期間、技法、戦術の順序、および観測される活動はさまざまです。

すべての変動性を説明する単一の要因は特定されませんでしたが、データセットの一般的な不一致は主に滞在時間にありました。具体的には、期間が短い事例では、より特徴的なモデルのシーケンスや戦術.技法のグループが見られる傾向があり、これはより長期間の侵害と比較して顕著でした。短期と長期の期間を判断する基準は、1か月に設定されました。滞留時間がこれを超えると事例の変動性が大きくなっていたためです。それでも各グループ内には逸脱が存在しますが、一般的に短期間の事例では、インターネットに接続されたデバイスのエクスプロイトによる初期アクセスが特徴であり、迅速なツールの流入、C2通信の確立および/または流出アクティビティが行われる傾向があります。

これと比較して、滞留時間が長い事例では、最初のデバイス群を超えてより広範なネットワーク侵入を特徴とする傾向があります。

ダークトレースのアナリストは、中国系グループのサイバー作戦の性質と被害者のパターンを考慮すると、この違いは中国系アクターの目的セットの分割によるものと考えています。産業スパイおよび伝統的な諜報活動を目的とした作戦は、当然ながら観測される侵害期間が長くなり、継続的なデータ流出のためのネットワーク内での永続化につながると思われます。これは、より機会主義的な「スマッシュアンドグラブ（smash-and-grab）」型作戦や、「待ち伏せ（lay-and-wait）」型の事前配置とは対照的です。この分岐の性質については、以降のセクションで解説します。

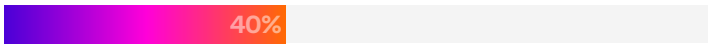
テクニックの分布と同時発生

中国系グループの活動に関連していると少なくとも中程度の確信を持って特定された事例に対しては、特に重要な一連の戦術と技法についての評価も行われました。これらの戦術の具体的な実装は、既存のオープンサーチ研究のレビューおよび脅威ハンティング作業中に観察されたパターンの両方で特定されました。これらのアクティビティの一部のサブセット、特にホストレベルのデータにはいくつかの制限がありますが、より広範な傾向を明らかにすることは可能です。

地域別のテクニックの頻度と分布

事例の大半（63%）はインターネットに接続されたインフラのエクスプロイトが関係しており、多くの場合環境内への初期アクセスを得るためでした。

それ以外の事例でも公開インフラを介したやり取りがあった可能性はありますが、このテクニックに関連するイベントは、確認された共通脆弱性識別子（CVE）のエクスプロイト（またはその可能性）に応じて特定のモデルアラートを発生させています。CVE公開前のエクスプロイトに関連する直接的な事例およびモデル検知の証拠は付録に含まれています。その他データセット全体で広く観測されたテクニックには、特定のコマンドラインユーティリティ、C2アクティビティおよび/またはペイロードのホスティングでのクラウドプロバイダーの使用、トンネリングのためのDNSプロトコルの使用が含まれ、それぞれがすべてのケースの40%以上で発生しています。



戦術 / テクニックの地域別の分布も重要な傾向を示しています。割合で見ると、中国系グループによる侵害のケースは、EMEA および AMS 地域では周辺機器を標的としたものがより一般的に見られました。EMEA のケースの 75% 以上、AMS のケースの 60% にこのテクニックが含まれています。米国をグループから除外しても、このパターンは一貫しています。この周辺機器のエクスプロイトへの依存は、APJ ではこの初期アクセス方法を通じて開始された事例が 30% であったことと対照的です。初期アクセスは常に直接確認可能とは限りませんが、アクティビティの可能性と OSINT ソースで報告されている同時進行中のキャンペーンを相互に参照することにより、これらの事例はフィッシングまたはより広範な検索エンジン最適化（SEO）ハイジャックから始まっている可能性が示唆されています。

APJ および EMEA 地域での侵害事例には AMS 地域では見られない共通した特徴があります。侵害の期間に関係なく、EMEA および APJ 地域の顧客に関係した事例ではアプリケーションまたはトランスポートレイヤーの偵察活動が含まれている場合が多く、これはより迅速なゼロ /n デイ侵害への偏りの可能性を示すものかもしれません。米国および AMS 地域の顧客では他の地域と比較した場合「ローアンドスロー」を目指すケースが多くみられます。特に米国内の標的を精査すると、この違いはさらに大きくなります。米国は DLL サイドローディングや検索順序ハイジャックが含まれる事例の割合が最も低く、こうしたテクニックの明示的な証拠が含まれる事例は 10% 未満でした。EMA と APJ 地域での頻度はそれぞれ 40% と 60% であり、対照的な数値です。

DLL サイドローディングと検索順序ハイジャックは主にキルチェーンのうち 2 つのフェーズ、すなわち最初のツールダウンロードと水平移動のフェーズで見られました。したがって、攻撃の期間はこのテクニックの頻度に影響するかもしれませんが、内部偵察関連テクニックと比較してその影響は小さいものと思われます。しかし、米国の標的において広範なネットワーク侵入の割合が低いことからも、このことは侵害と永続化に対する選好を示している可能性があります。これは前述のセクター別のケースの分布に見られた傾向とも一致しています。

テクニックの同時発生

アナリストは侵害データセットにおける戦術およびテクニックの同時発生についても評価しました。

同時発生指標は最初にすべてのケースについて評価され、その後データを短期グループと長期グループに分けた後で再度評価されました。侵害データセット全体をレビューし、アナリストは 2 つの重要な数値に注目しました：インターネットに接続されたデバイスのエクスプロイトとツール流入の高い同時発生率、そしてツール流入と明示的コマンドラインユーティリティの中程度の同時発生率です。データセット全体で見るとケースの大半は何らかの形の周辺デバイスエクスプロトが関係していました。そのため、このテクニックとツール流入の同時発生率が高いことは予期されることです。このような侵害の多くはこうしたイベントの連続で始まる可能性が高いからです。さらに、サーバーのエクスプロイトではファイル取得にリモートコマンド実行が関係することが多いため、ツール流入アクティビティと明示的コマンドラインユーザーエージェントの同時発生も予期される通りです。

データセット全体と同様、短期のケースのマトリクスではインターネットに接続されたデバイスのエクスプロイトとツール流入の同時発生の傾向が強く、またツール流入とコマンドラインユーティリティの同時発生も観測できました。

しかし、短期のケースではインターネットに接続されたデバイスのエクスプロイトと DNS トンネリングおよび HTTP/SSL ビーコニングの両方が高い割合で同時発生していました。インターネットに接続されたデバイスのエクスプロイトが含まれるケースで DNS トンネリングの発生頻度が高いことは、その一部はエクスプロイトの検証手段として DNS トンネリングと bin サービスが使用されていることに由来します。滞留時間が短い侵害ではさらにクラウドプロバイダーの使用とツール流入および DNS トンネリングといったテクニックの同時発生が高い傾向にありました。

データ流出、Active Directory（AD）偵察、Registry/Service オペレーションに関する明確な傾向はみられず、比較して弱いものの中程度のネットワークスキャンと LOLBin の使用の同時発生がみられました。しかし、水平移動と偵察関連手順の同時発生頻度が低いのは、短期間の侵害の性質に起因している可能性があります。そのようなケースは、キルチェーンの後半段階に進展していない場合、および / またはより広範なネットワークの侵害を目的としていない場合があります。

このデータセットでは、インターネットに接続されたデバイスのエクスプロイトとツール流入、そしてツール流入とコマンドラインユーティリティの同時発生がベースラインと比較して高くなっています。

短期間のケース、特に「ローアンドスロー」あるいは「スマッシュアンドグラブ」型の作戦を伴うものは、リモートコード実行やトロイの木馬のダウンロードのための迅速なエクスプロイトへの偏りの可能性を示しています。

短い滞留時間のケースでは、クラウドプロバイダーの使用とツール流入の同時発生の頻度が高くなっておりこれは長期のデータでは見られない傾向です。これは、短期間のケースにおける迅速なエクスプロイトと永続性確立のために、C2 およびペイロードのホスティングにクラウドプロバイダーを使用していることを示すものかもしれません。また、短期間のケースでは、匿名化インフラと DLL サイドローディング組み合わせが多くみられ、これらのサービスが特に DLL ベースの実行を目的としたペイロードのホスティングに使用されていることを示唆しています。

データセットのすべての分類で最も高いテクニックの同時発生は長期ケース内で見られました。ネットワーク偵察（アプリケーションレイヤー偵察とトランスポートレイヤースキャンの組み合わせ）が関係しているケースにおいて、ネットワークスキャンのインスタンスのほぼ 80% で DLL サイドローディングまたは検索順序ハイジャックも発生していました。

前述の通り、キルチェーンが長くなる性質上、侵害期間が長くなると、偵察アクティビティと水平移動アクティビティの同時発生の増加につながる可能性があります。

しかし、この高い同時発生率は、DLLサイドローディングが特に水平移動フェーズの一部として機能する場合、アクセスと永続化のための小規模な作戦よりも、広範なネットワーク侵入においてより多く見られることも示しています。また、DLLサイドローディングは、このデータセット内ではDNSトンネリングと共に発生することが多いようです。

送信関連のアクティビティはクラウドプロバイダーの使用とともにより多く発生していました。これは、長期間にわたる侵入において、中国系グループがクラウドサービスをペイロードのホスティングだけでなく、データの抜き出しやC2にますます活用している可能性を示唆しています。

リモート管理ツールは、DLLサイドローディング、インターネットに接続されたデバイスのエクスプロイト、より広範なツール使用など、複数の手法と同時に使用されており、長期的な作戦中にリモート監視および管理（RMM）機能への依存が高まることを示しており、このことは攻撃者の適応能力と標的となった組織の特徴の両方を反映している可能性があります。

長期的なケースでは、水平移動、偵察、その他のTTPの同時発生率も高い傾向が確認されています。

その一部は長い滞留時間に起因するものですが、幅広い重複がみられることは、これらのグループが長期にわたる侵害の間に意図的にテクニックを拡大および変化させ、作戦時間が長いことを利用して環境内でピボットし、アクセスを深め、足掛かりを広げていることを示唆しています。

滞留時間の指標

ダークトレースの脅威調査チームは、すべての侵害事例についてタイミングと期間に関して分析しました。これらを総称して「滞留時間」と呼びます。

脅威ハンターやサイバー防御者は、脅威ハンティングの期間を設定し、調査の範囲を設定するために、滞留時間を使用する場合が多いと言えます。見つかった侵害の期間に関連する指標は、将来のモデルや検知ヒューリスティックにおけるタイミングの遅延情報に生かし、適切な検知を可能にすることができます。したがって、両方のユースケースをサポートするために、アナリストは「滞留時間」の 3 つのサブセット、すなわち全体の時間、送信の時間、および水平移動の時間に注目しました。

すべての Darktrace モデルアラートは、顧客の環境内で記録が行われた瞬間に対応する標準化されたタイムスタンプを保持しています。

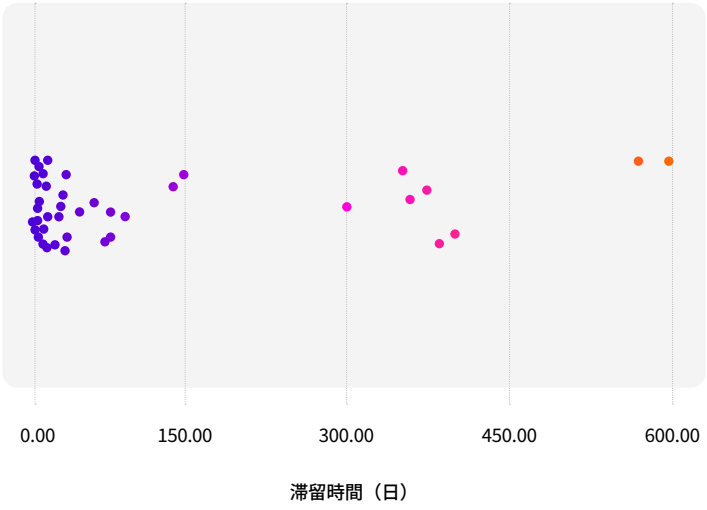
各滞在時間カテゴリーは、特定された終了時点のタイムスタンプとキルチェーンの開始として識別された最初のモデルアラートとの時間の差分として計算されました。多くの侵害事例は初期アクセスに関連するモデルアラートから始まっていましたが、一部の事例では、キルチェーンの開始と合理的に見なせる 2 つまたはそれ以上のモデルアラートが存在していました。あいまいな場合には、滞在時間の指標が過大とならないよう、より保守的な推定値が開始点として使用されました。

すべての開始モデルアラートについても一貫性を保つため、人手によって評価および品質コントロールが行われました。ただし、このアプローチは、最も早く観測されたモデルアラートが悪意あるサイバーアクティビティの真の開始を正確に反映していると仮定していますが、顧客環境の中で Darktrace がカバーしていない部分でより早いアクティビティがあった場合には当てはまらないことがあります。

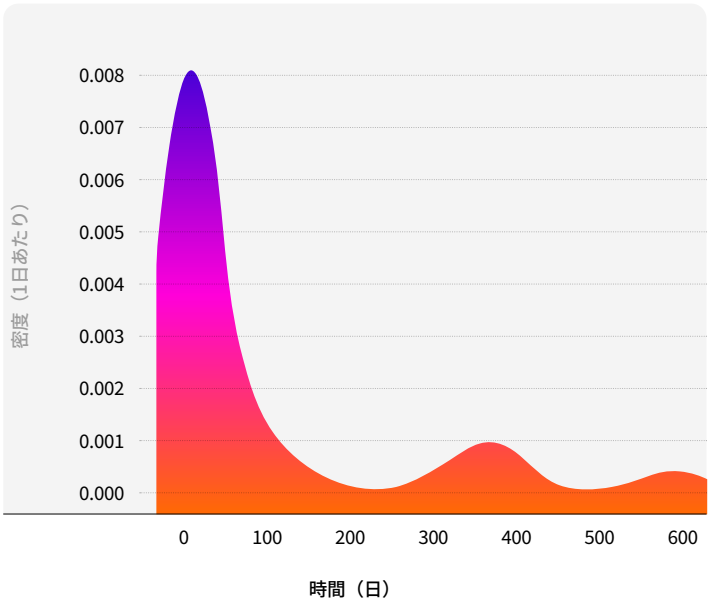
全体の滞留時間

このレポートの文脈において、全体の滞留時間とは、単に各侵害事例のキルチェーン内で最初のモデルアラートと最後のモデルアラートの間の期間を指します。全体の滞在時間の分布は右に歪んでおり、中央値は237.63時間（約10日）ですが、600日を超えるより高い値も少数存在します。中央値と95パーセンタイルをブートストラップするとそれぞれ標準的な信頼区間は3.5日から26日、および246日から584日となります。

■ 全体の滞留時間



■ 全体の滞留時間 KDE



これらの区間の対比は、ほとんどの観測値が比較的狭い中央領域に集中し、長い尾を持つ分布であることを示しています。事例の約半数は0.5時間から10日以内に発生しています。全体のデータ分布を説明するために、対数正規分布やマルチモーダル分布などの理論モデルが提案されましたが、仮説検定は結論を出せませんでした。いずれにせよ、データの右に偏った分布はほぼ予想されるパターンを反映しており、より迅速で機会主義的な、nデイエクスプロイトを伴う短期的な侵害が多数を占める一方で、戦略的な標的に対する長期の持続性を特徴とする事例は少数であることを示しています。

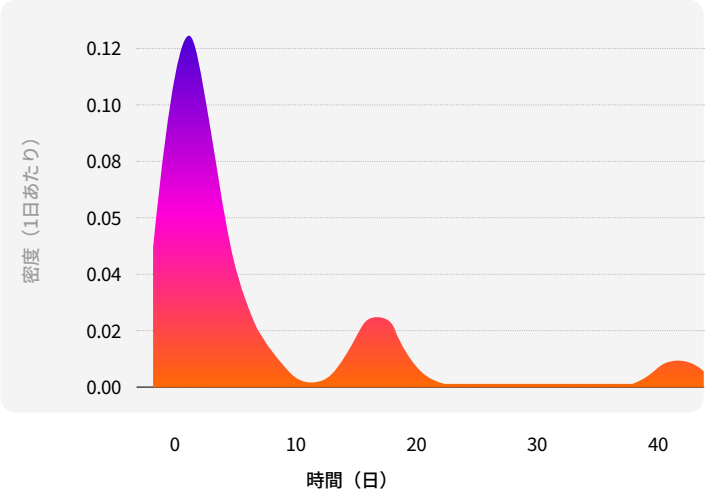
送信の滞留時間

送信の滞在時間も同じ開始タイムスタンプを使用しましたが、終了点として最初の送信関連モデルアラートのタイムスタンプを使用しました。C2やビーコニングに関連するいくつかのモデルは、ある種のデータ送信に関わるアクティビティを合理的に識別できますが、この数値については、特にデータ抜き出しの検知に焦点を当てたモデルのみが使用されました。全体の滞留時間分布と同様に、流出滞留時間の分布も右に歪んでおり、中央値は48.54時間ですが、算術平均は842.81時間（35日）です。

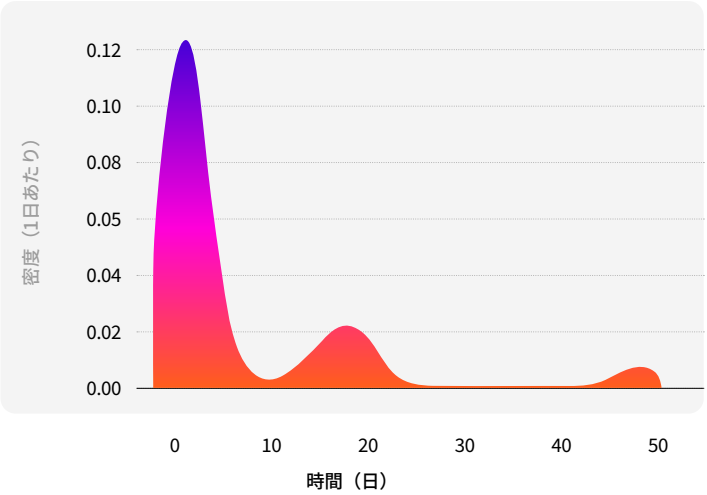
中央値および95パーセンタイルの95%信頼区間はそれぞれ、0.5 ～7.1日、 16.9 ～341.1 日でした。ここでも、低い値で点の密度が高く、左裾が非常に軽く、いくつかの孤立した極端に高い値が右尾を支配している分布が見られます。全体の滞留時間の分布とは異なり、最初のアラートから最初の流出モデルまでの時間の長さは、対数正規分布にかなりよく従っています。対数変換したデータに対してシャピロ・ウィルク検定を実行したところ、p値は0.36であり、対数正規性の仮定を棄却できないことを意味します。

これらの考察も、一般化された中国系グループの活動に関する作業仮説/モデルを支持しています。ここでは、流出とデータの抜き出しが主要な目的であり、侵害の大多数はより迅速な「スマッシュ・アンド・グラブ」スタイルの作戦を特徴としています。しかし、より価値が高く戦略的に重要な産業や標的に対しては、まず長期的な持続性が確立され、その後、より長い期間にわたる流出が行われます。

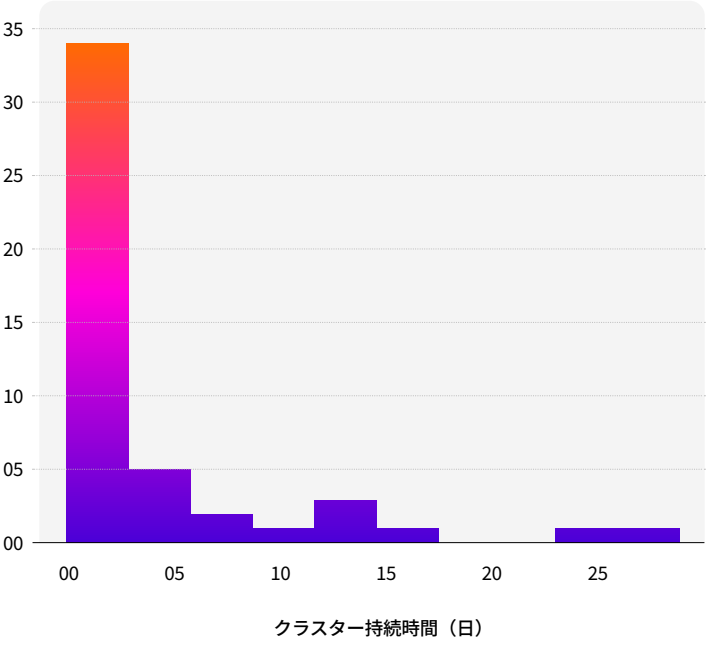
■ 流出滞留時間 KDE



■ 水平移動滞留時間 KDE



■ 水平移動クラスターのヒストグラム



水平移動の滞留時間

最初の水平方向移動アラートを活動の開始とマークするのではなく、アナリストは初期の探査や偵察を完全なネットワーク侵入と誤分類しないように、水平方向移動モデルの密集した「急増」を特定しました。モデルはHDBSCANを使用してクラスタリングされ、最初のクラスタの開始点が滞留時間の基準点として使用されました。初期の水平方向移動についてのアラートは脅威ハンターにとって依然として有用であるものの、アナリストは初期アクセスと最初の持続的な水平方向移動クラスターとの間の間隔をより意味のある指標と判断しました。

結果の分布は右に歪んでおり、中央値は27.7時間、平均値は147.6時間（6.15日）、95パーセンタイル値は478時間（19.9日）です。データは概ね対数正規分布のパターンと一致していますが、適合度は流出よりも弱いと言えます。

流出に比べて、水平移動の分布は狭く、極端な値は少数でした。中央値は流出の約半分であり、平均値はほぼ6分の1でした。つまり、攻撃者は通常、流出を実行するよりも水平移動をより迅速に実行し変動も少ないと言えます。

右方向への偏りは必ずしも予想されていたわけではありません。高度な攻撃者は検知を避けるために水平移動を遅らせると考えられるからです。しかし、明確な水平移動のクラスタリングを伴うケース（より深刻なネットワーク侵害を示す）では、流出は内部での広範な拡散の後まで遅延されることが多いことが示されています。水平移動のクラスターと流出が両方含まれる侵入の75%では、広範な水平移動が最初に発生しており、重要な作戦では、攻撃者がデータ抜き出しや目的の実行の前にネットワーク全体への浸透と長期的な配置を重視していることを示唆しています。

前述の通り、流出の滞留時間にはより大きな変動があり、また裾側のデータのギャップが広いことが確認されています。しかし、これらの外れ値のケースを除外すると、2つのデータセットの比較から興味深いパターンが現れます。

流出と水平移動の滞留時間の密度グラフを見ると、対数正規分布に典型的な初期アクティビティの全体的な急増が見られますが、どちらのグラフにおいても、10日から20日の間にアクティビティの特異な急増が発生しています。アクティビティが流出であれ水平移動であれ、長期型の侵害が進行中であれば、10日から20日程度の期間で活動の急増がある程度予想できると言えます。このパターンは、侵害が初期の安定化期間を超えて続くと、およそ10〜20日目あたりで活動をエスカレートさせることが多いことを示唆しています。これは脅威アクターが環境を十分に把握してアクティビティの拡大やデータのステージングに進む準備ができるタイミングと見られます。

最後に、水平移動クラスターに限定した分析が行われました。クラスター持続時間の中央値は約1日であり、クラスターが検知された場合、クラスターの平均数は4つでした。クラスター持続時間の中央値は0.96日で、25パーセンタイルと75パーセンタイルはそれぞれ0.1075日と2.965日であり、標準偏差は6.13日でした。このパターンは、水平移動アクティビティが通常は短時間の断続的な動作で実行されるものの、特定の作戦ではより大規模または複雑なネットワーク内で長時間の内部の移動が必要となり、その結果、はるかに長い尾が発生することを示しています。

モデルアラートアクティビティのクラスター

分析の最終段階では、非構造化クラスタリングを適用して、キルチェーン全体にわたるアラートアクティビティの「急増」を特定しました。

このアプローチは、滞留時間が長い場合にも侵害内の高密度なサブコンポーネントを識別するのに役立ち、SOC は作戦のテンポがいつどこで早まっているかをよりよく解釈することができます。ダークトレースのアナリストは、水平移動の分析に適用したのと同じクラスタリング手法を使用しましたが、キルチェーンのフェーズに関係なくすべてのモデルアラートにこれを拡大しました。

クラスタリングアルゴリズムはすべての侵害で急増を特定することはできませんでした。一部の侵入は基準を満たすほど十分に密集したアクティビティを示さなかったためです。この変動性は、侵入スタイルの多様性と脅威アクターの適応力の両方を表しています。クラスターが存在する場合、それらは通常、単一の戦術が支配的であり、最も頻繁に見られたのは C2、内部偵察、水平移動、またはツールの配備であり、シーケンス内の次のアラートも最も多くの場合、同じ戦術の繰り返しでした。ほとんどのクラスターは 5 ～ 15 件のアラートを含み、15 時間未満で終了していました。

アナリストは、連続するチェーンを凝縮することによって、戦術間の遷移についても分析しました。すべてのクラスターにおいて、ツール配備、権限昇格、および流出は最も一般的にはC2に続き、内部偵察と水平移動は頻繁に相互に遷移していました。これらのパターンは、Darktraceモデルデッキの設計および一般的な侵入ワークフローの両方と一致しています。特に、クラスターの長さとクラスターのエントロピーとの間に関係は見られませんでした。 つまり、アラートのより長いシーケンスは、必ずしもより多様なTTPを含むものではないということです。

エントロピーがゼロでない場合、単一の戦術が同時に発生している他の戦術を抑えて圧倒的に支配することはありませんでした。

■ **分析のポイント 1**

クラスターは、短い、戦術に的を絞ったアクティビティが突発的に発生する傾向を示しています。攻撃者は多くの場合、広範に複数のテクニックを多数実行するよりも、迅速な、集中した作業を複数のフェーズで実行しているとみられます。

■ **分析のポイント 2**

クラスターの規模と戦術の多様性に強い相関がみられないことは、活動のエスカレーションが必ずしもより複雑あるいは変化のある振る舞いにつながらないことを示しています。多くのケースにおいて、攻撃者は優先度の高いフェーズにおいて単に同じテクニックを強めています。

これらの調査結果は、アラート密度のクラスタリングが攻撃者のワークフローを理解するための有意義な視点を提供します。敵対者がより高強度の作戦段階に移行するタイミングを明らかにし、これらのアクティビティの急増に対する防御者による効果的な検知および対応を可能にします。

ケーススタディ

中国系グループによる攻撃の例

以下のセクションでは、全体のデータセット内の 3 つの事例における具体的なキルチェーンおよび攻撃シーケンスの要素について詳述します。これらのイベントを振り返ることにより、前のセクションで述べられたパターンや主張に文脈を加え、これらの分析がどのように導き出されたかについての考察を提供します。

さらに、これらの事例は、テクニックの同時発生、滞留時間、戦術のシーケンス、ならびに前述のセクター / 地域別の内訳に関する、重要な傾向を浮き彫りにしています。方法論の説明以外に、このセクションは、さまざまな環境における中国系グループの作戦の実行例を示すことで、サイバー防御者を支援することも目的としています。

■ **事例**

SAP NetWeaverの迅速なエクスプロイトおよびクラウドでホスティングされたツールの投下

2025 年 4 月、ダークトレースはヨーロッパの運輸業組織のネットワーク上にあるサーバーデバイスがエクスプロイトの初期の兆候を示していることを特定しました。

システムは、Out-of-Band Security Testing（OAST）ドメインへのリクエストを含む、bin サービスへの異常な DNS クエリおよびトンネリングを開始しました。セキュリティプロフェッショナルはテストのために OAST ドメインを使用することがありますが、これらのエンドポイントはしばしば侵害イベントと共に現れ攻撃の検証手段としても使用されています。その後のサーバーの挙動は、このようなプラットフォームの使用を裏付けることになりました。アナリストは後に、最初のアクセスはおそらく CVE-2025-31324 の脆弱性エクスプロイトであると結論付けました。この脆弱性により、SAP NetWeaver Visual Composer を通じて認証されていないリモートコード実行が可能になります。

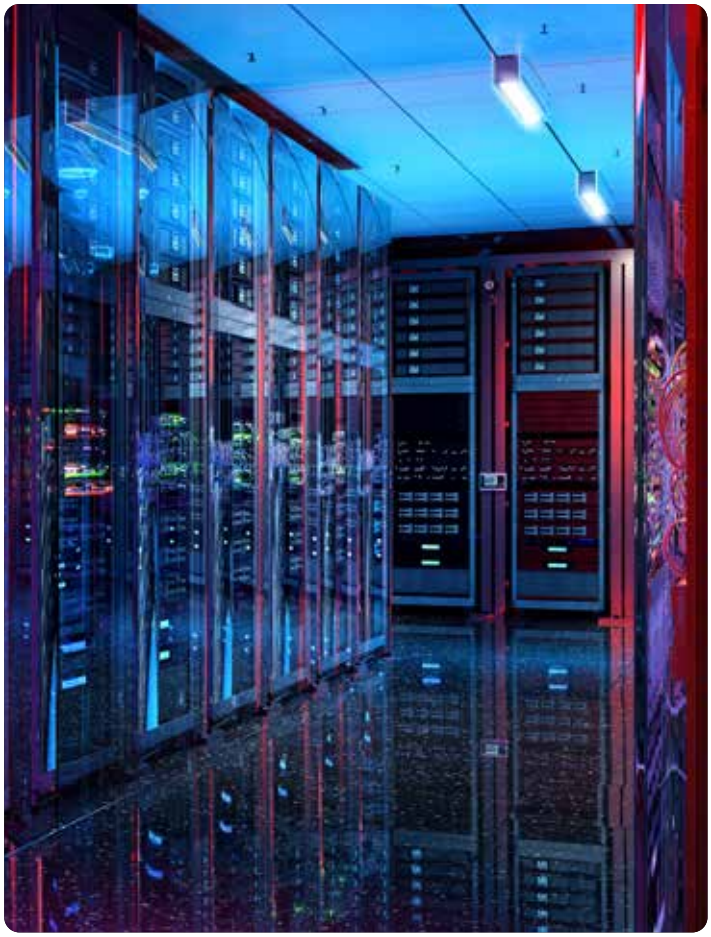
エクスプロイトの検証と初期アクセスから数日以内にさらなるツール流入が開始されました。サーバーは Amazon S3 バケットにホストされているバイナリを要求する、いくつかのアウトバウンド HTTP GET リクエストを行いました。これらの HTTP リクエストのユーザーエージェントとして curl コマンドラインツールが現れ、異なるファイルタイプを装っていた可能性のある、データを要求しました。クラウドサーバーからのさらなるバイナリ / オクテットストリームのダウンロード要求は数日間続き、さらに PowerShell の使用も含まれており、これはユーザーエージェントの HTTP ヘッダーフィールドに記載されていました。

侵害イベントの期間は約4〜5日間続いたと見られ、明確な流出、偵察、または水平移動アクティビティは含まれていませんでした。

追加のHTTPリクエストの一部は、以前のファイルダウンロードがシステムにインストールできなかったことが原因である可能性があります。

いずれにせよ、受信した複数のバイナリは、おそらく永続性を確保するためのツールの流入、およびアクセスを維持し、環境内でさらなる目的を達成するための追加のツールと思われます。この顧客が輸送セクターの主要な組織であることを考えると、これは長期的な、「待ち伏せ」目標と一致した挙動と見られます。この侵害では、短期間の侵害でよく見られる主要なテクニックの同時発生、特にインターネットに接続されたデバイスのエクスプロイトがツールダウンロードのためのコマンドラインユーティリティ実行につながったことが確認されました。

これは、ツールのダウンロード、クラウドサービスプロバイダーの使用、および流出操作を特徴とする他の短期的なケースとは対照的でした。APJ地域内の比較的短期間のケースの1つでは、ツールのダウンロードとクラウドプロバイダーの使用が含まれていました。この侵害は、



クラウドストレージサービスへの明示的なデータ流出を伴い、コマンドラインユーティリティを使った複数回のバイナリツールの実行は含まれていませんでした。注目すべき点は、このイベントは公共部門の顧客のネットワーク内で発生しており、初期アクセス手段としてフィッシングが用いられたと見られることです。

■ 事例

米国のCNI環境における段階的偵察と認証情報悪用

ダークトレースは、CVE-2025-0994 Trimble Cityworksのエクスプロイトに関連するモデルアラートを公表の18日前に確認し、さらにそれ以前にも悪意あるアクティビティを示すアラートを確認していました。

これは、国家レベルの機能を支える環境に対する敵対者の行動を検知するために、挙動に対する可視性を持つことの価値を示す事例です。影響を受けた環境は、国全体の交通、緊急救援、そして国防兵站を支える、継続的な航空運用を維持するその役割から、CNI（国家重要インフラ）カテゴリーに該当します。この環境は広範なマルチモーダル輸送および物流システムに統合されていることから、いかなる混乱も経済的、運用上、そして安全保障上の影響を連鎖的に引き起こす可能性があります。これは高価値なCNI標的固有の特徴です。

早期に検知できる機会があること、そして運用環境の重大性は、これらの顧客の戦略的重要性と、脆弱性公開前のビヘイビアベースの検知の持つアドバンテージを裏付けています。

2024 年 12 月中旬には、Darktrace は米国の公共部門の顧客ネットワーク内のデバイスが予期された動作から逸脱しているのを観測し、デバイスのエクスプロイトの可能性を確認していました。そのデバイスは、後に Trimble Cityworks CVE-2025-0994 のエクスプロイトに関連づけられる、複数の指標を示しました。Trimble Cityworks はインターネット露出の程度がさまざまな、多様なデバイスにインストール可能であるため、Darktrace が既存の生活パターンからの逸脱が始まる数週間前に、インターネットへの露出を検知していることは注目に値します。

影響を受けたホストは12月上旬から中旬にかけて一般的でないWMIリクエストを開始しています。これだけでは侵害を確認することはできません。分析されたケースにおいてはWMI等のLOLBinsの使用が頻繁に出現していますが正規のトラフィックからの区別が難しいためです。

1週間後、ホストはDRSGetNCChangesリクエストをドメインコントローラーに対して発行し、月末になるころにはこのデバイスにとって珍しい管理者認証情報を使用しました。

アナリストは DRSGetNCChanges アクティビティがその後の認証情報の使用を可能にしたとみています。この認証情報を使って、ホストは .ini ファイルの SMB ドライブ書き込みを相手先サーバーの TEMP フォルダーに対して実行しました。.ini ファイルはソフトウェアインストールの際にこのディレクトリに正当に存在することもありますが、アナリストは新たに使用された認証情報と普通ではないファイル名からこの挙動を不審なものと判断しました。

1 週間後、脅威アクターは内部偵察を開始し、これは 1 週間単位の 2 つのフェーズにわたり実行されました。

最初のフェーズはポート 445 が開放されているデバイスを見つけるための SMB スキャニングで構成されていました。次の週には、おそらく事前のスキャンの結果をうけて、ホストから RDP 関連の内部接続が開始されました。キルチェーンの最終段階において、このホストはさらにツールをダウンロードするためアウトバウンド HTTP GET リクエストを発行し、未知の外部 IP アドレスから英数字の実行ファイルを取得しました。アラートに PowerShell ユーザーエージェントが含まれていたことはコマンドラインアクティビティを示し、HTTP での珍しい宛先ポート（3219）の使用は、境界ベースの検知を回避して防御をすり抜けようとしたものと思われます。

この事例では、テクニックの同時発生、戦術のシーケンス、そして滞留時間の指標において長期的侵害のいくつかの属性が表れています。この顧客は米国の輸送セクターに属し主要な CNI 組織であることが、経済的スパイ活動でよく標的とされるセクターでの長期的侵入とは異なり、明確な流出関連のモデルアラートが存在していないことにつながった要因であるかもしれません。

この事例は長期にわたる作戦においてドメイン列挙と偵察行動が多いこと、特に DRSGetNCChanges リクエストが特徴的である例でもあります。 水平移動の可能性を示すアラートが 2 件観測されましたが、アナリストは広範な水平移動の証拠を確認するには至りませんでした。そのため、SMB 書き込みを通じた DLL サイドローディングアクティビティがなかったこと、また広範なネットワーク浸透がなかったことは想定通りです。

興味深いことに、コマンドラインユーティリティはツールのダウンロードの文脈では出現していません。しかし HTTP リクエストは侵害の最初ではなく、観測可能な最後に向けて発生しています。この事例は、高度な侵入は最初からドラマチックに見えることは稀で、静かに時間をかけて進行していくこと、したがってわずかな挙動の変化を検知できる能力が高価値なシステムを保護する上できわめて重要であることを示しています。

重要製造業環境での深いネットワーク浸透

2022 年 10 月と 11 月、APJ 地域の重要製造業顧客の社内ネットワーク内で、数台のデバイスが感染の初期兆候を示しました。

直接的なエクスプロイトや初期アクセスのイベントは確認されなかったものの、影響を受けたホストは匿名のNTLM認証を試みることでアプリケーションレイヤーの偵察を開始し、ポート445を介した広範な内部接続を行っていました。この初期のスキャンとネットワーク列挙は、より広範なネットワーク侵害のための確認であった可能性があります。

12月までに、1台のデスクトップは正当な管理者アカウントを使用していましたが、そのアカウントはおそらくローカルホストから盗まれたもので、SMBセッションを確立し、複数のネットワークサーバーのDISK共有にファイルを書き込んでいました。具体的には、システムは疑わしいDLLファイルとおそらくXMLコンフィギュレーションファイルと見られるファイルを宛先サーバーのDISK共有の「vss」フォルダーに転送しました。この期間中のネットワークインジケータの分析は、DLLサイドローディング/検索順序のハイジャック技術の両方と、PCExterマルウェアの使用の可能性を示唆しています。

ダークトレースのアナリストは、同じ期間中にSMBを介して書き込まれたさらなるバイナリおよびファイルを検知しています。これには、ツールの追加と見られるもの、および/またはコンフィギュレーションおよび暗号化されたペイロードが含まれていました。

書き込まれたこれらの実行可能ファイルには、データの抜き出しを可能にしたとみられるバイナリも含まれています。たとえば“Onedrive.exe” という名前のファイルや、流出のためにチャンク化されたデータを含むと思われるさまざまなアーカイブファイルなどです。

このアクティビティは2022年12月全体を通じて見られ、これには顧客の環境に含まれるPSEXESVC管理ツールを含むLOLBinsの使用が含まれます。この脅威アクターは12月中旬に流出アクティビティを開始したとみられます。

影響を受けたシステムの多くは前述のようなバイナリを書き込みまたは受け取っており、11月に集積されたと思われるTLSで暗号化された大量のデータを正当なクラウドサービスプロバイダーに送信しました。 この脅威アクターは最初の流出アクティビティの後、休眠状態に入ったようにみえました。

しかしその後、2022 年の秋から冬にかけての初回の作戦時に関与していたデバイスが、2023 年から少なくとも 2024 年の 7 月にかけて、突発的な偵察活動や水平移動を行っているというパターンが発生しました。 アナリストは少なくとも 2 回の DLL および RAR ファイルの SMB を介した書き込み、LOLBin の使用 (WMI)、および DRSGetNCChanges リクエストを介したドメイン列挙を特定しています。またアナリストはこのサイクル中にさまざまなクラウドストレージプラットフォームを使ったデータ抜き出しが起こっていることも確認しています。

この事例においても、侵害の期間、キルチェーンで確認されたテクニックおよび戦術の進行は、標的の戦略的重要性を反映しています。

この侵害の背後にいた攻撃者はネットワーク内のアクセスを数か月間にわたって維持していました。「スマッシュアンドグラブ」型や「待ち伏せ」型の他の重要インフラ部門を対象とした攻撃と比較して、中国政府にとっての戦略的重要性は、おそらく経済スパイ活動や一帯一路（BRI）目標にとって重要な産業における顧客の立場をより反映しています。この場合は、ICT/ 半導体産業です。

この戦略的意図は、より長い滞在時間と、それに伴うより深いネットワーク侵入およびアクセスに関連する特定の技術や戦術に現れていると思われます。この事例では、数か月にわたり、広範なスキャン、水平移動フェーズでの複数回の DLL サイドローディング、および複数のツール転送が確認されています。

さらに、滞留時間がより長いケースで確認されているように、流出イベントが遅延されています。データ抜き出しの最初の証拠はアクセスの最初の兆候が見られてから何週間も後に発生しています。さらに、クラウドプロバイダーが関係した以後の流出関連モデルアラートも準備的な水平移動アクティビティからかなり後に発生しています。流出関連操作の遅れは、長期的な持続と繰り返しの流出操作を実行しようと計画している標的に対する作戦の初期フェーズでは、脅威アクターがより広範なネットワーク侵害を優先していることを意味するものかもしれません。

まとめ & コミュニティの議論

この報告書は、過去3年間にわたる中国系グループのサイバー活動のハイレベルなパターンを解説するものです。個別の脅威グループやキャンペーン名に焦点を当てるのではなく、この研究によって防御者が中国系グループの活動をより早く、より確信を持って認識できるようにするための一般化されたオペレーションフレームワークを構築しようとしています。

調査結果はセキュリティ研究者にとって重要であり、またその影響は経営幹部やCISOから日々の監視を担当するSOCアナリストに至るまで、組織全体に及びます。

これらの作戦の戦略的ロジックを理解することは、組織が異常なアクティビティを解釈し、それに応じて防御の優先順位を調整するのに役立ちます。この報告書には、CEO、CISO、アナリスト、政策立案者向けのフォローアップディスカッションの視点を提供する短い所見も含まれています。

要約すると、ダークトレースの調査チームがこの研究から得た主な考察は以下の通りです。

中国系サイバーオペレーションは単発的なキャンペーンではなく、**戦略的計画の連続**であると理解するのが最適である。

滞留時間の短い侵入は諜報活動の失敗として解釈するべきではなく、**意図的な作戦上の選択**と見るべきである。

西側のセキュリティモデルは依然として**過度にインシデント中心型**であり、全体として持続的なアイデンティティリスクを過小評価している。

中国のサイバーアクティビティは知的財産の窃取だけではなく、ますます一帯一路構想（BRI）や世界の重要インフラへの影響力に基づいたものとなっており、とくに米国に重点が置かれている。

戦略的影響

このデータセットは、中国系グループの活動が、重要な国家インフラのカテゴリーや、輸送、通信、製造、医療、デジタルインフラなどの戦略的に重要な分野に属する組織を明確に好むことを裏付けています。

これらの標的パターンは、中国政府が戦略的優位のための伝統的なスパイ活動と、一帯一路（BRI）および産業スパイ活動の目標の両方を支援するために設定した目標を概ね反映しているように見えます。

この文脈データは、最高責任者レベルの経営幹部が自社がCNIフレームワークのどこに位置し、どのように機能しているかを理解することの重要性を表しています。サイバー防御リソースへの投資、プロアクティブな脅威ハンティングへの注力、およびITセキュリティコントロールのレビューの頻度は、中国系アクターがこれらの重要なセクターで戦略的目標に基づいて行動する意図を考慮すれば、再評価する必要があるかもしれません。

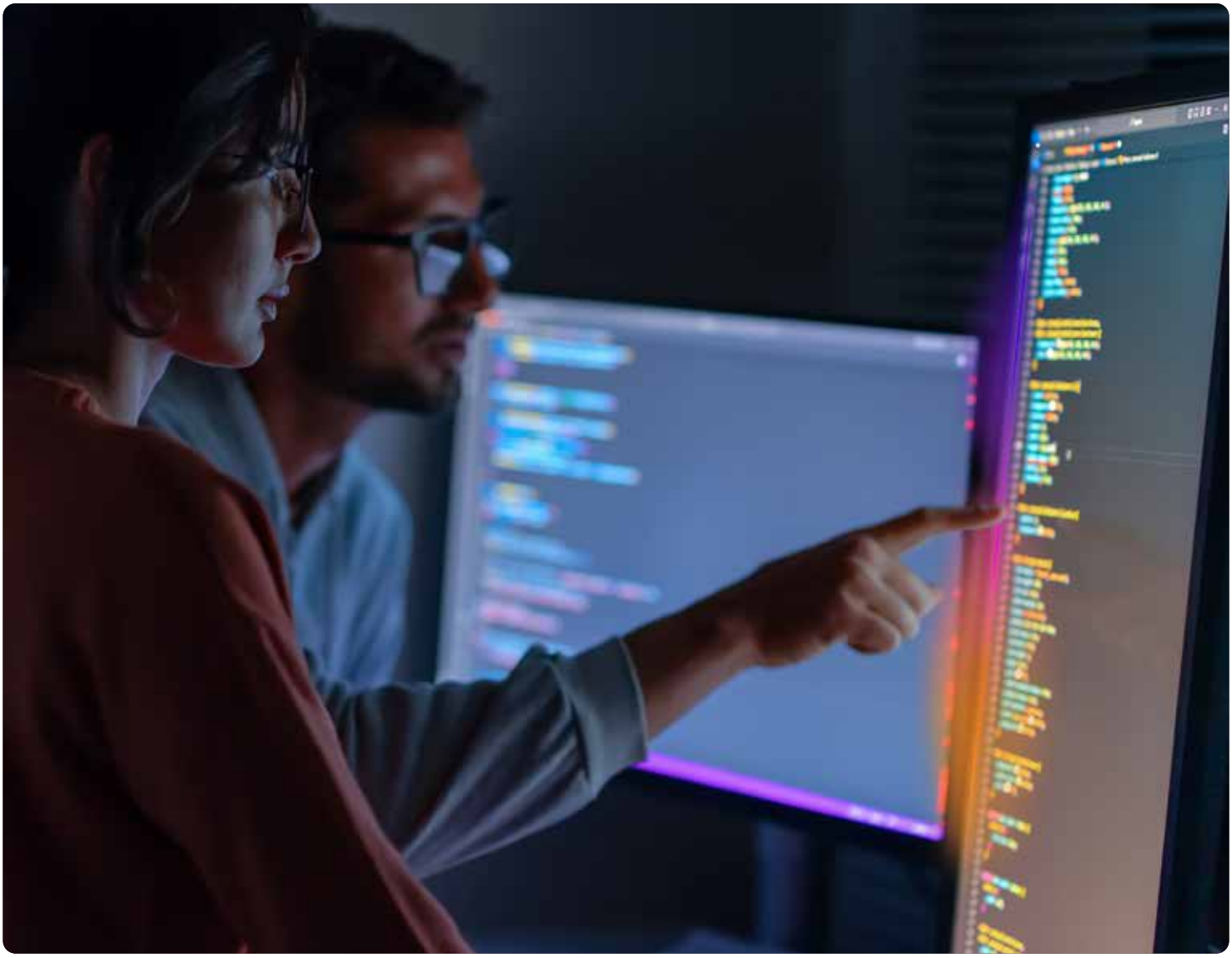
このデータに暗示されているのは、中国の国家機構による中長期的な戦略的計画を理解することが、組織のリスクに直接的に影響し、その緩和に役立つという事実です。CISOや意思決定者にとって、自社組織がそのような目的の潜在的な標的としてどのように見られるかについてのより詳細な理解を持つことは有益です。

このレポートから得られる情報、たとえば滞留時間の傾向、テクニックの同時発生、キルチェーンのシーケンスなどは、SOCチームが脅威ハンティングの期間などのパラメーターを精緻化し、防御的な監視の優先順位を決定するのに役立ちます。

防御者は、静的な指標や特定の攻撃者のプロファイルのみに依存するのではなく、認証情報の異常な使用、偵察アクティビティ、通常とは異なるクラウド接続、そして突発的な水平移動等、繰り返される動作のパターンに注目することができます。

これらの調査結果は、異常ベースの検知がますます重要となることも示しています。中国系アクターは、従来のシグネチャベースのコントロールを回避するために、環境寄生（LOTL）テクニック、クラウドインフラ、および正規の管理ツールを頻繁に使用します。

したがってこれらを検知するには、確立されたネットワーク動作パターンからの逸脱を特定することがますます必要となります。



コミュニティのディスカッションのための問い

Crimson Echoの調査結果はサイバーセキュリティ、ビジネス、および政策立案者コミュニティでの議論にいくつかの戦略的な問いを投げかけています：

インシデント中心型のセキュリティモデルから、永続的アクセスのリスクに焦点を当てたフレームワークにどうシフトすべきか？

長期的な侵入を検知するにはどのレベルのアイデンティティ管理、テレメトリー保持、監視の可視性が必要か？

政府や業界はデジタルサプライチェーンやクラウドへの依存により生じる体系的な露出にどう対処すべきか？

敵対者が直接的な妨害や窃盗よりもアクセスの維持を優先している場合、どのような防御戦略が最も効果的か？

組織はエグゼクティブレベルでのリスクの理解と、セキュリティチームが直面する業務の現実をどのように整合させていくことができるか？

最終的な考察

中国系サイバーアクティビティは、単発的なキャンペーンというよりも、長期にわたる戦略的な計画を反映するようになってきています。これらの作戦は一貫した活動のリズムを示しています。攻撃者はアクセスを確立し、その戦略的価値を評価し、状況がエスカレーションを正当化するまで辛抱強くアクセスを維持します。

防御者にとっての課題は、単に個々の侵入を防ぐことではなく、複雑なデジタル環境全体にわたって継続的に露出を管理することです。アクター中心のアトリビューションから動作パターンの認識へとシフトすることで、組織は新たに出現する脅威をより効果的に検知し、防御への投資の優先順位をつけ、戦略的サイバー競争のダイナミクスの変化に対するレジリエンスを強化することができます。

この研究の結果および考察が、複雑な脅威のエコシステムから政策立案者、CEO、CISO、アナリスト、企業にとっての実行可能な防御指針を解明し、組織が中国系アクターの活動を予測し、戦略的なサイバー競争の次なるフェーズに備えて防御を強化するのに役立つことを期待しています。

1 International Monetary Fund: Datamapper [referenced Jan. 2026] https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWORLD

付録 1

Darktrace Cybersecurity Attribution Framework

複雑なサイバーアトリビューション問題をナビゲートする

サイバーアトリビューション、つまり悪意あるサイバーアクティビティの起源と犯人を特定するプロセスは、現代の脅威インテリジェンスにおいて最も複雑かつ重要な結果を伴うタスクの1つです。これは単なる技術的練習課題ではなく、特に国家が関与するアクターが関係する場合には、戦略的かつしばしば政治的な判断となります。

アトリビューションは説明責任の基盤であり、防御的および攻撃的サイバー戦略に情報と提供し、外交的、法的、場合によっては軍事的対応のきっかけとなる可能性があります。

国家的フレームワークと戦略的重要課題

各国は自国の国家安全保障機構の中で強力なアトリビューション能力を構築してきました。例えば、米国の国家安全保障局（NSA）や英国の国家サイバーセキュリティセンター(NCSC)は、アトリビューション調査に専念する豊富な人的、技術的、財政的資源を有しており、しばしば民間の脅威インテリジェンスベンダーと連携して活動しています。国家アクターは、国際舞台における戦略的手段として、脅威アクターの公的なアトリビューション（特に他の国家グループに対する）をますます活用するようになっています。

この地政学的な下地は、業界内で公的なアトリビューションに関する多くの議論を生み出しており、さまざまな枠組みが公表され、また多くの民間企業が独自のものを発表しています。同様に、IISS Cyber Power Matrix は、非国家アクターから国家に組み込まれた組織までの 6 段階の枠組みを示しており、アクターと国家の関係を評価し、アトリビューション判断を導くために使用されています。ダークトレースは、透明性を促進し、アナリストによる再現性を支援し、正当化可能な方法論に対する公共部門の期待と一致する、アトリビューションフレームワークを公開しています。

アトリビューションの課題

国家や民間によるさまざまなアトリビューションフレームワークが存在するにもかかわらず、アトリビューションには依然として多くの課題があります。

- **技術的複雑性：**脅威アクターは、難読化、偽旗作戦、多段階作戦を使用して素性を隠します。
- **法的あいまい性：**国際法にはサイバーアトリビューションについて、明確な基準が欠けており、特に武力紛争の閾値未満の作戦については扱いがあいまいです。
- **政治的リスク：**間違ったアトリビューションは緊張を高めあるいは信頼を損なう可能性があり、政府は公的な宣言については注意深くなります。
- **リソースの必要性：**アトリビューションには深いフォレンジック分析、地政学的コンテキスト、そして複数のインテリジェンス領域にわたる裏付けが求められます。

これらの問題からしばしば責任のギャップが生じ、悪意あるアクティビティが検知されるものの確信をもってそれを加害者や国家と結びつけることができない状況になります。

Darktrace Cyber Attribution Frameworkの役割

サイバー脅威のアトリビューションには、挙動についてのアナリティクス、外部のインテリジェンス、それらに重ねるコンテキスト情報を組み合わせた、多面的アプローチが必要です。これは意図の評価を行おうとするものではありません。時間を超え、セクターを超えて、ツールの変化に関係なく存在する再現可能な動作のパターンを説明しようとしているのです。

Darktrace Cyber Attribution Frameworkはダークトレース独自のAI駆動の検知モデルを既知の脅威アクターのTTPと整合させることによりこのアプローチをサポートし、次の6つの柱を中心に確信を持ってアトリビューションを構築することを可能にしています：

01 インフラ

この柱はIPアドレス、ドメイン、VPN等、脅威アクターが使用するネットワークインフラに焦点を当てたものです。アナリストはインフラについて次を評価します：

- 複数のキャンペーンで再利用されているか
- 既知の脅威アクタークラスターにリンクされているか
- 以前のインシデントからのパターンと一致するか

アクターの例：

APT41 （aka Barium / Winnti）参照：CISA (2021)– Pulse Secure VPNの中国によるエクスプロイト

Darktraceモデルの例：

- Compromise::Beaconing to Rare Endpoint
- Anomalous Connection / Unusual External Connection

02 マルウェア / ツールの使用

この柱は攻撃に使用された悪意あるソフトウェアおよびツールを精査します。アナリストは次を探します：

- 既知のマルウェアファミリー（例：PlugX、gGh0st RAT）
- カスタムツールまたはサイドローディングされたDLL
- IoC

アクターの例：

APT41 （Winntiファミリークラスター） 参照：Mandiant (2020) – 二重スパイおよびサイバー犯罪作戦

Darktraceモデルの例：

- Compromise::Unusual Process Execution
- Anomalous File Transfer
- Anomalous File Download

3. TTP

TTPは攻撃者がどのように作戦を展開するかを表します。これには次のようなアクティビティが含まれます：

- 認証情報窃取
- スケジュールされたタスクの作成
- データ抜き出し

アクターの例：

APT29 （Nobelium） 参照：Palo Alto Unit 42 (2021) – SolarStorm サプライチェーン攻撃

Darktraceモデルの例：

- Unusual Admin Credential Use
- Compromise::Suspicious Scheduled Task
- Unusual Data Exfiltration

04 被害者の特徴

この柱は誰が標的とされているかについて、セクター、地理、戦略的価値などから分析します。次の場合にアトリビューションが補強されます：

- 被害者プロファイルがアクターの既知の関心と一致
- 標的化のパターンが地政学的動機と一致

アクターの例：

- APT10 （Cloud Hopper） 参照：UK NCSC Advisory (2020) – 通信企業の標的化

アナリストによるコンテキスト / エンリッチメント

- アナリストがコンテキストを重ね合わせます（セクター、地理等）

05 言語 / アーティファクト

この柱は次のような言語的および技術的アーティファクトに注目します：

- 特定の言語で書かれたおとり文書
- ファイルの命名規則
- コンパイル時間やメタデータ

アクターの例：

- Mustang Panda - 参照：CrowdStrike (2021) –中国語のおとり文書と悪意あるRARアーカイブ
- アナリストによるエンリッチメント（例：おとり文書、ファイル名、コンパイル時間）

06 外部の裏付け

最後の柱は、結果を次の資料と交差検証することです：

- ベンダーの脅威レポート
- 政府の勧告
- インテリジェンス評価

参考資料の例：

US DNI (2021) – People's Republic of China (PRC)persistent targeting of healthcare

アナリストの追加情報：

アナリストが結果を外部情報ソース（ベンダー/政府のレポート）と比較

アトリビューションの確信レベル

サイバーインシデントを特定の脅威アクターまたは国家に帰属させる作業は二分決定であることはめったにありません。これには、複数の調査の柱に関する証拠の品質、量、収束に基づいた確信のレベルを割り当てる作業が伴います。NSA（米国）や NCSC（英国）等のインテリジェンス機関はしばしば階層化された確度フレームワークを使用します。低、中、高など確信のレベルに基づいて、存在するデータがあるアトリビューションをどの程度強く支持するものであるかを表します。

これらのレベルは技術的インジケータ（例：マルウェアのシグネチャ、インフラの再利用）、動作のパターン（TTP）、地政学的コンテキスト、および外部ソースからの裏付けに基づいて設定されます。

確信が低いアトリビューションは状況証拠や弱い相関関係に基づいている場合があるのに対し、確信が高いアトリビューションは通常複数の独立した情報ソース、一貫したアクターの挙動、既知の動機との戦略的な整合などに基づいています。重要な点として、確信のレベルはアナリストや意思決定者が対応を調整し、防御アクションや公式発表、あるいは外交的対応をアトリビューションの確実性に応じて行うことができます。

確信スコアを調査ワークフローに組み込むことにより、アナリストは透明性を維持し、バイアスを抑え、再現可能、防御可能な結論を出すことができます。特に構造化されたフレームワークを使うことで、これらの原則に対応するチェックポイントを使ってアトリビューションを導き出すことができます。

- **高い確信 →** 複数の独立した、裏付けとなるインジケーターが整合（例：インフラの再利用 + マルウェアファミリー+ 被害者の特徴）。
- **中程度の確信 →** 複数のインジケーターが整合、しかし証拠のギャップが存在。
- **低い確信 →** インジケーターが弱い、状況に依存 または主として第三者のレポートに基づく。

アトリビューションワークフロー決定木の例

ステップ 1：インフラ

もし “Compromise::Beaconing to Rare Endpoint” または “Anomalous Connection” の場合 → WHOIS/OSINT に移動してインフラの再利用をチェック

ステップ 2:マルウェア / ツール使用

もし “Unusual Process Execution” または “Anomalous File Transfer” の場合 → ファイルハッシュおよびコードの類似性を公的な報告書に照らしてチェック

ステップ 3:TTP

もし “Unusual Admin Credential Use” または “Suspicious Scheduled Task” の場合 → MITRE ATT&CKにマッピング、既知のAPT手法と比較

ステップ 4:被害者の特徴

標的の選択が過去のAPTの優先事項と一致する場合（例：通信、防衛、非政府組織（NGO）等） → アトリビューションを強化

ステップ 5:アーティファクト

アナリストがおとり文書、ファイル名、コンパイル時間等をチェック → アトリビューションのナラティブを支持

ステップ 6:裏付け

調査結果を外部の脅威報告と比較（CISA、NCSC、Mandiant、CrowdStrike Palo Alto等）

確度の割り当て：簡単な計算

- 3つ以上の強力な柱の整合 → 高い確信
- 2つの柱が整合 → 中程度の確信
- 1つの弱い柱 → 低い確信

柱	なりすまし可能性	調整された重み	ティア
インフラ	低	0.80	戦術
マルウェア / ツール使用	中	0.80	戦術
TTP	中	0.85	作戦
被害者の特徴	低	0.70	作戦
言語 / アーティファクト	高	0.40	戦術
外部の裏付け	低	0.95	戦略

アナリストの確信レベル

確度の評価：
各ステップで以下に基づいて重みづけを付加：

- なりすましの容易性（例：言語のアーティファクトは インフラの再利用よりも偽装が容易）
- 過去の信頼性（例：マルウェア/ツール使用はより アクター固有の傾向があるが必ずしもそうとは限らない）
- アナリストの確信（過去の調査に基づき）

4. ワークフローの例（高い確信）：
DARKTRACE → アトリビューション

通信企業においてDarktraceがビーコニングを検知

ステップ 1:インフラ → Compromise::Beaconing to Rare Endpoint. インフラがCISA Alert A21-110Aと重なる

ステップ 2:マルウェア → Compromise::Unusual Process Execution. DLLサイドローディングがMandiant APT41レポートと一致

ステップ 3: TTP → Suspicious Scheduled Task. 永続化テクニックがPalo AltoのUnit 42でSolarStorm攻撃に関連して報告されている

ステップ 4: 被害者の特徴 → 通信セクター、NCSC Cloud Hopper勧告と一致している

ステップ 5: アーティファクト → 中国語のデコイファイル、CrowdStrikeが確認したMustang Panda キャンペーンと類似

ステップ 6: 裏付け → ODNI 2021 ATA により通信セクターに対する中国の関心を確認

式のサンプル

スコア =（調整された重み × 証拠の強度） + ブースト

インフラに対して：

- 調整された重み = 0.80
- 証拠の強度 = 1.00 （CISAアラートと強い一致）
- ブースト= 0.10 （外部キャンペーンデータによる裏付け）

それぞれの柱が強力な証拠により支持される：

- **インフラ：**CISA アラートとの重なり → +0.10 ブースト
- **マルウェア / ツール使用：**DLLサイドローディングがMandiantと一致 → +0.15 ブースト
- **TTP：** Palo Altoの確認したSolarStorm手法と一致
- **被害者の特徴：**通信セクターが標的、NCSCの情報と一致
- **言語 / アーティファクト：**中国語のおとり文書 → +0.10 ブースト
- **外部の裏付け：**ODNIにより中国の関心を確認
- **0.90+0.95+0.85+0.70+0.50+0.95=4.85**
  4.85 = 高い確信

- スコア = (調整された重み x **証拠の強度**) + ブースト

柱	調整された重み	証拠の強度	ブースト
インフラ	0.80	1.00	0.10
マルウェア / ツール使用	0.80	1.00	0.15
TTP	0.85	1.00	0.00
被害者の特徴	0.70	1.00	0.00
言語 / アーティファクト	0.40	1.00	0.10
外部の裏付け	0.95	1.00	0.00

最終的アトリビューションステートメントの例（高い確信）：:

「この侵入がインフラストラクチャの重複（CISA）、マルウェア/ツール使用（Mandiant）、永続化の手法（Palo Alto Unit 42）、被害者の特徴（NCSC）、およびアーティファクト（CrowdStrike）に基づき、中国（PRC）に関連するスパイ活動（APT41クラスター）に関連していると高い確信を持って評価します。」

ワークフローの例（中程度の確信）：DARKTRACE → アトリビューション

- インフラが既知のアクターのインフラと重複（CISAアラート）
- マルウェアが既知のツール使用と部分的に一致（Mandiant）
- TTPが確認されていない
- 被害者の特徴はセクター標的と整合
- アーティファクトの一致がない
- 強い外部の裏付け
- **生スコア: 3.16**
  最大スコア 4.85
  正規化されたスコア.65 > 中程度の確信

柱	重み	強度	ブースト
インフラ	0.80	1.00	0.10
マルウェア / ツール使用	0.80	0.80	0.15
TTP	0.85	0.00	0.00
被害者の特徴	0.70	0.60	0.00
言語 / アーティファクト	0.40	0.00	0.10
外部の裏付け	0.95	1.00	0.00

ワークフローの例（低い確信）：DARKTRACE → アトリビューション

- インフラまたはマルウェアの一致がない
- 被害者の特徴およびアーティファクトの指標は弱い
- TTPや外部の裏付けが確認できない
- **生スコア .90**
  最大スコア 4.85
  正規化されたスコア .19 = 低い確信

柱	重み	強度	ブースト
インフラ	0.80	1.00	0.10
マルウェア / ツール使用	0.80	0.80	0.15
TTP	0.85	0.00	0.00
被害者の特徴	0.70	0.60	0.00
言語 / アーティファクト	0.40	0.00	0.10
外部の裏付け	0.95	1.00	0.00

このフレームワークが有効な理由

- **Darktraceファースト：**アナリストが日々確認している実際のモデルに基づいている
- **参考資料の裏付け：** 権威ある情報源にリンクしている（CISA、NCSC、Mandiant、Palo Alto、CrowdStrike、ODNI）
- **確度の補正：** 構造化されたICスタイルの言語を使った一貫性のあるアトリビューションステートメント

ダークトレースが今このフレームワークを構築したのは、脅威ランドスケープが根本的に変化したからです。私たちが顧客ベース全体で目にしているのは、もはや断片的なインシデントの集まりではなく、スパイ活動、サプライチェーンの侵害、長期的な作戦上の配置が融合した、持続的かつ国家と連携した活動です。この環境において、アトリビューションは政治的な行為ではなく、リスク管理上の必須要件です。

組織は、自分たちが対処しているのが機会主義的な侵入なのか、商業的動機による侵害なのか、あるいは国家の戦略的目標に沿った作戦なのかを理解する必要があります。その区別を行うことは、コントロールの優先付けから、レジリエンス、情報開示、長期的なリスク対応の考え方に至るまで、すべてに影響を与えます。

このフレームワークの強みは、静的な指標ではなく、実際の動作に基づいていることです。

脅威アクターはインフラを偽装したり、マルウェアを再利用したり、誤解を招くアーティファクトを仕込んだりすることができますが、時間の経過とともにどのように活動しているかという深いパターンを隠すことは困難です。アトリビューションをこれらの確実なビヘイビアシグナルに結びつけ、公共部門およびベンダーの情報と照合することで、推測ではなく情報の収束に基づいて確信を構築することができます。

その結果、構造化された、繰り返し可能で透明性のあるプロセスが実現され、アナリストは定義された一連の柱に沿って分析を進め、それぞれのデータの重要性を理解し、検証に耐えうる確信レベルに到達することができます。

また、私たちは制限についても明確にしています。サイバー空間においてアトリビューションは常にあいまいさを伴います。ツールの共有、アクターの重複、偽旗作戦、そして意図的な誤誘導はすべてこの環境の一部です。そのため、私たちはこのフレームワークをさまざまな事例の回顧的レビューで検証しました。過去の侵入事例を 6 つの柱を使った手法で調べ、このフレームワークが一貫性のある防御可能な結論を生み出すことを確認しました。

目標は絶対的な確実性ではなく、規律正しい、校正された判断です。これにより、防御者は侵入の背後にある戦略的な文脈を確実に理解し、適切なレベルの緊急性、投資、および経営層からの確認とともに対応することができます。

付録 2

侵害インジケータ(IoC)のリスト

備考：TLP Clearインジケーターは以下の通りです。一部のインジケーターについてはセキュリティ上の理由で開示していません。TLP Amberインジケーターの情報が自社組織にとって有益であると思われ正当な理由を示すことができる場合には、crimsonecho@darktrace.comまでEメールでお問い合わせください。

IoC	タイプ	確度
shell.cdn-sina[.]tw	ホスト名	高
xxl17z.dnslog[.]cn	ホスト名	高
asljkdqhkhasdq.softether[.]net	ホスト名	高
aar.gandhibludtric[.]com	ホスト名	高
plugins.jetbrians[.]net	ホスト名	高
dscriy.chtq[.]net	ホスト名	高
cybaq.chtq[.]net	ホスト名	高
ns1.akacur[.]tk	ホスト名	高
ns2.akacur[.]tk	ホスト名	高
trkbucket.s3.amazonaws[.]com	ホスト名	高
tnegadge.s3.amazonaws[.]com	ホスト名	高
fconnect.s3.amazonaws[.]com	ホスト名	高
times.windowstimes[.]online	ホスト名	高
applr-malbbal.s3.ap-northeast-2.amazonaws[.]com	ホスト名	高
beansdeals-static.s3.amazonaws[.]com	ホスト名	高
bringthenoiseappnew.s3.amazonaws[.]com	ホスト名	高
brandnav-cms-storage.s3.amazonaws[.]com	ホスト名	高
abode-dashboard-media.s3.ap-south-1.amazonaws[.]com	ホスト名	高

IoC	タイプ	確度
maxdesigns[.]top	ホスト名	高
asdasw21[.]icu	ホスト名	高
micheeasodh[.]top	ホスト名	高
a.micheeasodh[.]top	ホスト名	高
lsls.casacam[.]net	ホスト名	高
meetls.kozow[.]com	ホスト名	高
vals.bumbleshrimp[.]com	ホスト名	高
4.232.170[.]137	IP	高
185.238.251[.]244	IP	高
45.251.240[.]55	IP	高
137.175.30[.]36	IP	高
192.74.254[.]229	IP	高
107.148.219[.]227	IP	高
107.148.149[.]156	IP	高
107.148.219[.]54	IP	高
107.148.219[.]55	IP	高
103.27.108[.]62	IP	高
103.27.110[.]83	IP	高
103.13.28[.]40	IP	高
89.31.121[.]101	IP	高
16.162.188[.]93	IP	高
5.181.132[.]95	IP	高
63.245.1[.]34	IP	高
158.247.213[.]167	IP	高
158.247.199[.]185	IP	高
94.131.110[.]28	IP	高
193.56.255[.]214	IP	高
15.188.246[.]198	IP	高

IoC	タイプ	確度
149.104.23[.]171	IP	高
192.210.239[.]172	IP	高
107.155.56[.]87	IP	高
156.244.28[.]153	IP	高
154.90.63[.]250	IP	高
45.76.191[.]59	IP	高
45.77.170[.]188	IP	高
38.54.29[.]25	IP	高
154.205.139[.]12	IP	高
45.76.209[.]205	IP	高
64.176.59[.]232	IP	高
149.28.28[.]9	IP	高
17d65a9d8d40375b5b939b60f21eb06eb17054fc	SHA1	高
da23dab4851df3ef7f6e5952a2fc9a6a57ab6983	SHA1	高
fa645f33c0e3a98436a0161b19342f78683dbd9d	SHA1	高
4a8b8a164e20748e23fbded8b048bacb9c3d715c	SHA1	高
b5367820cd32640a2d5e4c3a3c1ceedbbb715be2	SHA1	高
8da0489e4d6307b461cb4090dd661d0fbeef9928	SHA1	高

付録 3

メタモデル作成

このプロジェクトは、特定のサブグループの区分に関係なく、中国系グループの活動を特定するための準備的な枠組みを提供することを目的としています。この目的を追求するために、アナリストは脅威ハンティングの成果を活用して、ネットワーク環境における一般的な中国系グループの活動をモデル化した Darktrace / NETWORK ™モデルを作成しました。このモデルは「メタモデル」であり、特定の期間内に他の基礎モデルの特定の組み合わせがアラートを発生させることを意味します。

サブコンポーネントを構成するモデルは、確認されたモデルアラートおよび中～高確度の事例のキルチェーン進行状況、ならびに「文献レビュー」プロセスの一環として OSINT ソースに共通して見られる特定のテクニックおよび手順に基づいて特定されました。

各サブコンポーネント内のモデルの組み合わせは、どのアクティビティの組み合わせがモデルのアラートに寄与できるかを示しており、これはテクニックの同時発生の指標に基づいています。Darktrace がサブコンポーネントのモデルアラートを発動するまでの時間の長さには、滞留時間も反映しています。IP 範囲 /ASN ブロック、クラウドプロバイダー、ファイル命名パターンなど、より限定的な指標も一部のコンポーネントのパラメーターに含まれており、誤ったアラートの発生を防いでいます。

2 つのモデルにより、より高い確度の事例で頻繁に見られる中心的キルチェーン要素を検知します。最初のモデルは、初期のエクスプロイト、実行、および足場の確立に焦点を当てています。このモデルは「短期的」なアクティビティを把握することを目的としていますが、顧客が長期にわたる攻撃の標的となりやすいセクターに属している場合でも、検知が制限されるわけではありません。さまざまな基礎モデルの組み合わせによりこのモデルのアラートが発生し、それぞれの組み合わせは以前に特定された各種の短期的な侵害の開始シーケンスを表しています。

例えば、インターネットに接続されたシステムのファイルのダウンロードや新しいユーザーエージェントに関連するものなど、境界デバイスのエクスプロイトに関するアラートは、モデルのコアコンポーネントに含まれています。このカテゴリー内のアラートは、将来の DLL サイドローディングを示唆するツールの流入、ツールの流入に使用される certutil/BITS ユーティリティ、および DNS トンネリングアクティビティなどに関する追加のモデルアラートが発生した場合に、全体のモデルをトリガーする可能性があります。他のコンポーネントモデルは、DLL 操作テクニックを示唆するツールの流入、DNS トンネリング、SSH 等のアウトバウンドリモートプロトコル、TLS に関連するビーコニング、新しいユーザーエージェントなどのアクティビティを特定します。ここでも、誤った関連のないアラートの発生を防ぐために、よりシグネチャベースのインジケーターが使用されます。

長期モデルも同じアプローチを使用しており、特定の期間内の基礎モデルの組み合わせが全体のメタモデルをトリガーします。短期モデルは初期アクセスや足場確立などの準備的なキルチェーン要素のみに焦点を当てていますが、その後のモデルは準備的な要素と少なくとも 1 つの二次的なキルチェーン要素の両方が観察された場合にのみアラートを生成することができます。これらの後続のコンポーネントは、流出および偵察 / 水平移動アクティビティに焦点を当てています。

短期モデルをトリガーするアクティビティは、たとえ長期間の侵害を試みる一環として行われた場合でも、検知され対応が行われると想定しています。したがって、長期モデルの準備的要素は、より広範なパラメーターを持っています。

この検知のバリエーションは、初期要素を満たす他の変数を伴う、繰り返される HTTP/S ビーコニング関連のアクティビティも許容します。これらのビーコニング /C2 関連のアラートは、Darktrace のビヘイビア分析および通信パターンの監視に基づいています。これにより、存在するテレメトリーから中国系であるとの評価を強化する追加のシグナルが欠如しているシナリオにも耐えることができます。

Darktrace のモデル検知メカニズムの性質上、モデルは関連する動作が現れたときにトリガーされ、長時間持続した後ではありません。したがって非常に長い永続化シーケンスは単一の検知として扱われません。これらのケースにおいては、このユースケースモデルは攻撃ライフサイクルのあらゆるフェーズをカバーするというよりも早期の警告を提供するように意図的に設計されています。繰り返しになりますが、この場合の目標はこれらのグループが関与した攻撃のシーケンス全体を検知するモデルではありません。そうではなく、そうした作戦に対する信頼性の高い早期検知メカニズムを提供することを目的としています。

しがたって、継続時間（流出または偵察 / 水平移動コンポーネントがアラートを発生させるためのモデル遅延）は流出あるいは水平移動の最初のインスタンスに対する滞留時間指標を反映しています。侵害事例内で特定された流出アクティビティは、対応するモデルアラートの範囲がより狭いことが確認されています。これらの生の検知は流出アクティビティの 2 番目のコンポーネントの条件を満足します。水平移動のモデルアラートは主に LOLBin の使用、珍しい LDAP アクティビティおよび DRSGetNCChanges リクエスト等の Active Directory 偵察オペレーション、永続化のための registry/service/task オペレーション等に焦点を当てています。

基礎コンポーネント自体も異常ベースの検知メカニズムを表していることは再度強調しておく価値があるでしょう。つまり、Darktrace はキルチェーンアクティビティの特定の組み合わせを検知できるだけでなく、これらのコンポーネントはシグネチャまたはヒューリスティックベースの検知の落とし穴を回避しているのです。実際には、戦術 / テクニックとシーケンシャルなアラートの組み合わせはデバイスの通常の生活パターンを考慮しています。たとえば、LOLBin の使用だけでは水平移動コンポーネントを満足するには不十分です。LOLBin の使用自体がデバイスにとって通常とは異なるあるいは予期しないものでなければなりません。同様に、ツールのダウンロードのために特定のクラウドプロバイダーを使用したこともパラメーターをトリガーしません。クラウドプロバイダーエンドポイントがネットワークにとって稀であり、そのダウンロード / 流入アクティビティがデバイスの確率された生活パターンと異なるものでなくてはなりません。そうすることにより、このメタモデルはアクティビティの潜在的逸脱をより幅広くカバーすると共に、関係ないアクティビティがアラートを発生するのを防ぐことができます。

付録 4

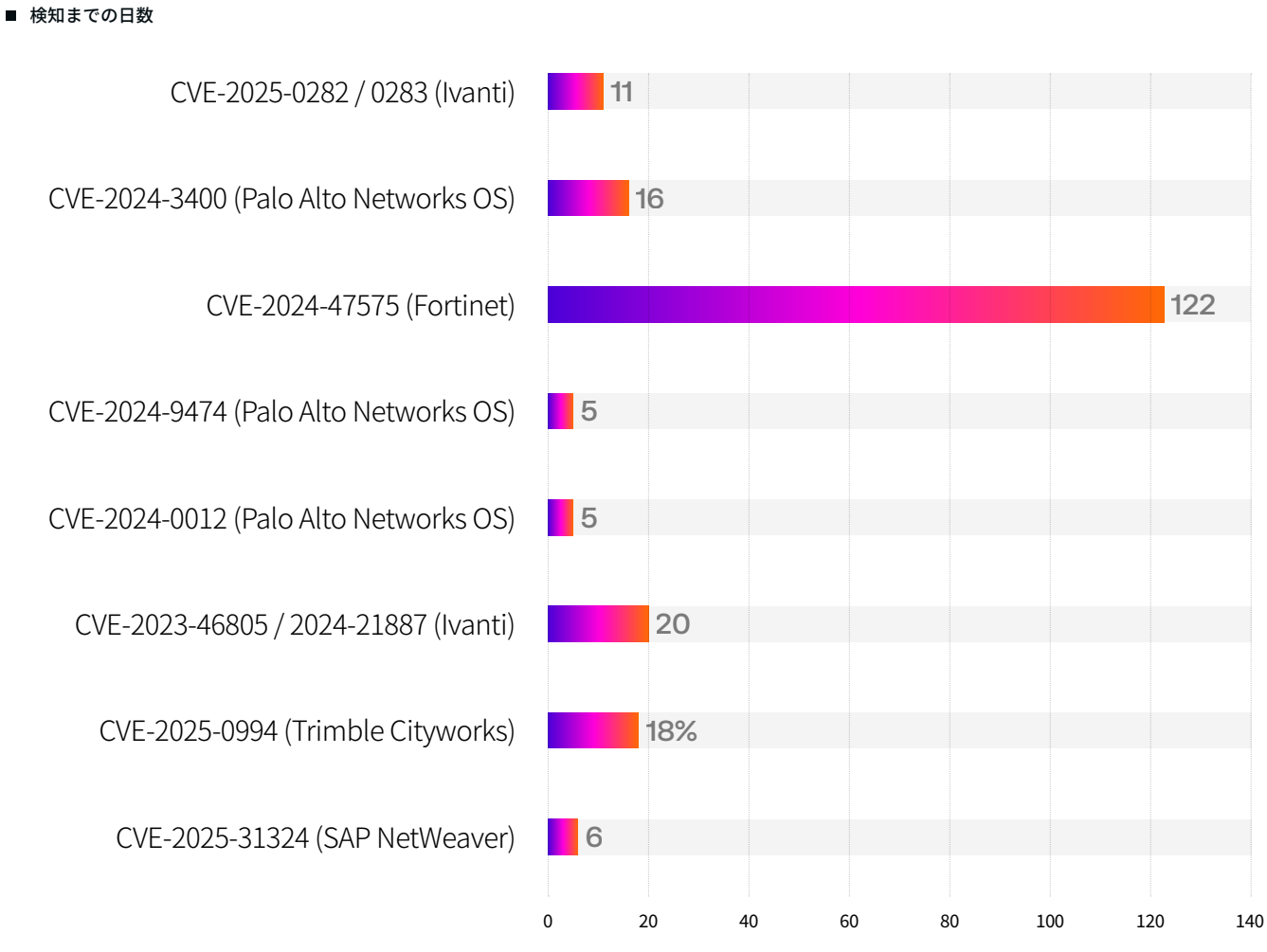
CVE公開前の異常検知例

2025年には48,000件以上のCVE（Common Vulnerabilities and Exposures）が報告されました（前年比20.6%の増加）。ゼロデイエクスプロイトと脆弱性の開示の間にはしばしば大きなギャップがあり、ネットワーク内で発生したエクスプロイトを遡及的に特定することが継続的な課題となっています。

ネットワークやシステム内で発生した異常な動作、例えば普段とは異なるログインパターンや予期しないデータ転送は、サイバー攻撃の試行、内部関係者による脅威、あるいは侵害されたアセットを示している場合があります。Darktraceは事前に定義されたルールや既知のシグネチャに依存しないため、特定のデバイスやアセットに関する完全なコンテキストが利用できない場合でも、確立された動作の基準から逸脱した、悪意あるアクティビティを検知することができます。

Darktraceが動作のパターンを継続的に分析することで、組織はエクスプロイトの可能性を早期に特定し、封じ込めることができます。これらの異常検知パラメーターを活用して、ダークトレースのアナリストは回帰分析を行い、より広範な脅威ランドスケープにおける検知結果をよりよく理解し、分析結果にさらなるコンテキストを追加します。このビヘイビアに基づくアプローチはCVE公開前の検知も可能にします。ダークトレースは攻撃者の動作に基づいて、脆弱性が公開されるまたはCVEが割り当てられる前に、新手のまたは未知のエクスプロイト技術を特定することができます。

ダークトレースは、本研究に関連するいくつかの注目すべきケースにおいて、公開前に悪意ある活動を特定する能力を実証しました。これは以下の表に概要が示されています。



付録 5

重要インフラとしての分類

組織を重要インフラとして分類する際、ダークトレースは被害者の国の国家または地域のポリシーを使用しました。例えば、アメリカ合衆国の事例においては、国家安全保障政策における16の重要セクターと、CISAからの適用に基づいて設定しています。

EUの事例においては、European Union Agency for Cybersecurityの分類法を利用しました。

セクターの分類：

情報技術

- ソフトウェア/ハードウェア製品、非重要ソフトウェア・アズ・ア・サービス（SaaS）/プラットフォーム・アズ・ア・サービス（PaaS）/インフラストラクチャ・アズ・ア・サービス（IaaS）プロバイダー、マネージドサービスプロバイダーを含むIT製品およびサービス

製造

- 重要および非重要製造業
  - 製鉄所や金属製品、産業機械、セメント/建設/合成素材の製造業者、ハイテクハードウェア製造業者（プロセッサー、マイクロチップなどを含む）を含む重要製造業
  - 繊維、消費財、加工食品および飲料製造業を含む非重要製造業

芸術、エンターテインメント、レクリエーション

- 映画/テレビ/音楽スタジオ、音響工学、視覚効果、制作会社、文字起こしサービスを含む映画関連サービス、エンターテインメントおよびスポーツ会場、スポーツリーグおよび統括団体、ゲーム/カジノ、博物館および文化施設/研究所

教育

- 公立および私立の初等、中等、および高等教育機関

農業、林業、漁業

- 大規模な産業農業、主要食料生産者、公園、野生生物管理、農業/畜産機械

専門、科学技術サービス

- コンサルティング会社、技術アドバイザリー組織、非健康関連研究機関

電気、ガス、蒸気および空調供給

- 電力網、エネルギー市場、石油およびガスの生産者/精製所、水処理施設、発電所、太陽光発電運営者および生産者、風力発電所、原子力発電所を含むあらゆるエネルギー、水、冷却関連の事業体

メディアおよび放送

- 放送および印刷媒体の代理店や組織、出版物、新聞、テレビおよびラジオ局

金融および保険

- 銀行、信用組合、貸付機関、信用調査機関、株式市場、保険代理店、その他の金融関連組織

輸送インフラ

- 空港、航空会社、港、鉄道/運営、橋/灯台/港の運営、交通システム、バス運行

行政機関および政府サービス

- 連邦、県、州、地方、部族、および準州の政府機関、公的資金によるプロジェクトおよび組織

法務サービス

- 法律事務所、顧問組織、その他の法務サービス

健康関連製品およびサービス

- 病院や診療所、医療サービスおよび管理、製薬会社および生物医学研究機関

通信/デジタルインフラ

- 電話およびインターネットプロバイダー、重要クラウドオペレーター、公開鍵基盤（証明書機関、中間機関、鍵管理プロバイダーなど）を含む電気通信製品およびサービス

海運、倉庫、物流

- 貨物および製品のトラック輸送、鉄道輸送、海上輸送組織

鉱業および採石

- 鉱物および鉱石の採掘と抽出
  - 希少/重要元素および非重要元素と鉱石の両方を含む

その他のサービス活動

- 健康、専門/科学、法律、財務、またはビジネスのニーズや関心に直接関連しないサービス

防衛セクター

- 武器および弾薬製造業者、警備請負業者、公共/防衛コンサルティングアドバイザリーサービス

建設

- 建設および設計会社

CISA CNIカテゴリー:

CISAのCNIセクター指定に基づいて分類されたセクターおよび組織：

- 情報技術セクター
- 重要製造業セクター
- 商業施設セクター
- 食品および農業セクター
- 金融サービスセクター
- エネルギーセクター
- 通信セクター
- 輸送システムセクター
- 政府施設セクター
  - 政府施設セクター - 教育施設サブセクター
- 医療および公衆衛生セクター
- 防衛産業基盤セクター

参照: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

■ **ダークトレースについて**

ダークトレースは AI サイバーセキュリティのグローバルリーダーであり、日々変化する脅威ランドスケープに立ち向かう組織を支援しています。2013 年に英国ケンブリッジで設立されたダークトレースは、それぞれのビジネスからリアルタイムに学習する AI を使用して未知の脅威から組織を保護する、必要不可欠なサイバーセキュリティプラットフォームを提供しています。ダークトレースのプラットフォームおよびサービスは 2,700 名を超える従業員により支えられ、世界でおよそ 10,000 社の組織を保護しています。より詳しい情報については、www.darktrace.com/ja をご覧ください。

北米: +1 (415) 229 9100 | ヨーロッパ: +44 (0) 1223 394 100 | 日本: (03) 5456 5537 | ラテンアメリカ: +55 11 4949 7696

darktrace.com/ja | japan@darktrace.com