2023

CISCO
TALOS

一年の総括

2023 一年の総括

はじめに

2023 年は、ランサムウェア、コモディティ型ローダー、APT の脅威が猛威を振るいました。2 回目になるこの Cisco Talos『一年の総括』で概説するように、世界規模の紛争がサイバーセキュリティの動向に影響を与え、スパイ活動からサイバー犯罪活動に至るまで、多くの攻撃グループの戦術と手法を変化させました。

シスコはグローバルに事業を展開しており、Talos の専門技術は世界トップクラスです。こうした背景から大量のデータが利用でき、徹底的な調査が可能になりました。提供されたのは、エンドポイント検出やインシデント対応業務で収集したデータ、ネットワークトラフィック、メールコーパス、サンドボックス、ハニーポットのデータなど、さまざまです。ありがたいことに、Talos にはサイバーセキュリティのあらゆる分野の専門家が集まっており、こうしたインテリジェンスを防御担当者やユーザーにとって実用的な情報に変えることができます。これらの豊富で複雑な情報源を活用し、2023 年の脅威環境を形作った主要な動向を分析しました。

ランサムウェアは 2023 年も世界の企業を脅かし続け、LockBit が 2 年連続でこの領域の最大の脅威となりました。今年最も狙われた業界は医療です。サイバーセキュリティの資金に制約があり、ダウンタイムの許容度が低い組織が重点的に狙われたからです。Clop などの攻撃グループがゼロデイエクスプロイトを大規模に展開するのが確認されました。必ずしもそうとは限りませんが、これは通常、Advanced Persistent Threat（APT）グループの活動とされる動きです。同時に、ランサムウェアのソースコードが流出したことで、スキルの低い攻撃者の参戦が可能になりました。さらに問題を複雑にしているのは、ランサムウェア攻撃グループが純粋な恐喝に転じるという新たな動向が見られることです。これは、暗号化をまったく行わずに機密データを流出させると脅す手口です。

これらのランサムウェアの脅威を送り込むためにコモディティ型ローダーが相変わらず使用されており、Qakbot や IcedID など、昨年と同じランサムウェアファミリの多くが依然として蔓延していました。金融サービス業と運送業の企業が最も頻繁になりすましの対象になるなど、これはテレメトリにも反映されています。しかし、これらのローダーは、バンキング型トロイの木馬の過去の名残をすべて捨て去り、ペイロードを送り込むためのより高度な方法と化しています。開発者と攻撃実行者は、強化された防御に適応し、増加するセキュリティアップデートをバイパスして被害者を侵害する新しい方法を見出しています。また、今年も大規模ボットネットの解体（今年は Qakbot）がありましたが、経験上、これは必ずしも脅威が排除されたことを意味しません。

今年 Talos が観測した地域横断的な新たな動向の 1 つは、APT グループとランサムウェアグループによるネットワークデバイスへの攻撃の増加です。どちらのグループも、最近公開された脆弱性と、デフォルトまたは安全性の低いログイン情報を悪用します。これが Talos のインシデント対応業務で見られた弱点の中で、有効なアカウントの使用が一貫して上位であった理由の 1 つです。攻撃者がどの程度巧妙であれ、またその意図が何であれ、ネットワークデバイスが狙われる理由は同じです。価値が非常に高いにもかかわらず、ネットワークデバイスにはセキュリティ上の弱点が多いのです。

地政学的な不安定さが APT グループの活動に現れています。これはテレメトリに反映されており、重大な地政学的出来事の際には不審なトラフィックが増加しています。中国のグループについては、西側諸国やアジア太平洋地域との関係が緊迫化するにつれ、破壊を引き起こす意図が強まるなど活動が勢いづくことが確認されています。グアムや台湾のような戦略的に重要な地域に重要なインフラ資産を多数所有する通信事業者を攻撃対象にしている点からも、この傾向が確認されます。ロシアの APT グループについては、Gamaredon と Turla によるウクライナへの攻撃が急増しましたが、2023 年のロシアの活動全般では、過去に見られたような幅広い破壊的なサイバー攻撃能力は反映されませんでした。これは防御側の協力した取り組みのためかもしれません。

今年の明るい点の 1 つは、シスコの断固とした取り組みで、パートナーの防御の強化に役立つ独創的なセキュリティソリューションを生み出して提供したことです。Talos のウクライナタスクフォースは、ウクライナの重要なパートナーに対する攻撃を阻止し続けています。今年は、戦場における全地球測位システム（GPS）ジャミング（電波妨害）の影響を受けたウクライナの送電網を安定させる取り組みを率先して行いました。改造したシスコのスイッチを戦闘中の地域に届けるというものです。シスコはまた、業界を牽引するパートナー数社と Network Resilience Coalition（ネットワークレジリエンス連合）を立ち上げ、ネットワークセキュリティを改善するために意識を高め、実用的な推奨事項を提供することに注力しています。これに関連して、Talos の脆弱性検出および調査チームは、スモールオフィス ホームオフィス（SOHO）用ルータと産業用ルータを優先すべき重要課題として調査し、これまでに 289 件の脆弱性をベンダーに報告し、全部で 141 の Talos アドバイザリを発表しました。

中東情勢が悪化するなか、Talos はまたしても、お客様とパートナー様の防御を支援する立場にあります。ですから、おそらく 2023 年の報告で何よりも重要なメッセージは、攻撃側がより大胆不敵になり、巧妙化し、しぶとくなっている以上、防御側も決意を固くし、可能なあらゆる方法で阻止しなければならないということです。

目次

cisco Talos

一年の総括

2023

テレメトリの動向

本セクションのハイライト

- シスコのセキュリティ製品が捉えた不審なネットワークトラフィックから、重大な地政学的出来事や世界規模のサイバー攻撃が発生すると、多くの場合それに呼応して活動が急増することが明らかになりました。
- 最も狙われた脆弱性は一般的なアプリケーションに以前からあるセキュリティの欠陥で、米国セキュリティ インフラストラクチャ セキュリティ庁（CISA）の近年の調査結果と一致しています。Talos が確認した脆弱性のうち、標的上位のほとんどは、Cisco Kenna と共通脆弱性評価システム（CVSS）で最大または高の深刻度スコアが付けられており、CISA の「悪用が確認された脆弱性カタログ（KEV）」にも掲載されています。これらの脆弱性が頻繁に攻撃され、かつその影響が甚大であることから、重大な混乱を引き起こすことになりかねないパッチ未適用のシステムが優先的な攻撃対象に選ばれていることが明らかになっています。
- 攻撃者は一般的なファイル拡張子を悪用し、有名ブランドになりすましました。これはよく目にした手法であり、フィッシング攻撃やビジネスメール詐欺（BEC）などを成功させるためにソーシャルエンジニアリングが使用されていることが浮き彫りになっています。2022 年に Microsoft 社はマクロを無効化しました。攻撃者は PDF など別の種類のファイルにマルウェアを潜ませることでこれに対応しているようです。PDF は今年最も数多くブロックされたファイル拡張子でした。
- メールのテレメトリで、金融サービス業と運送業の企業のブランドが最も頻繁になりすましの対象になったことが確認されました。これは、Emotet、Qakbot、Trickbot など、メールベースのコモディティ型ローダーを送り込むために長く使用されているフィッシングのテーマがいまだに現役であることを示唆しています。これに関連して、Talos の今年のインシデント対応業務では、フィッシングが既知の初期アクセス手法の 4 分の 1 を占め、攻撃者が引き続きこの手口を多用していることが明らかになりました。
- MITRE ATT&CK 手法では、有効なアカウントの使用が最も頻繁に確認されました。このことは、侵害されたログイン情報を攻撃者が悪用し、さまざまな攻撃段階で既存のアカウントを使用している状況を浮き彫りにしています。これは、侵害されたログイン情報と有効なアカウントが、既知の初期アクセス手法の 3 分の 1 近くを占めたことを示す 2023 年の Talos IR のデータと一致しています。

地域別動向の経時変化

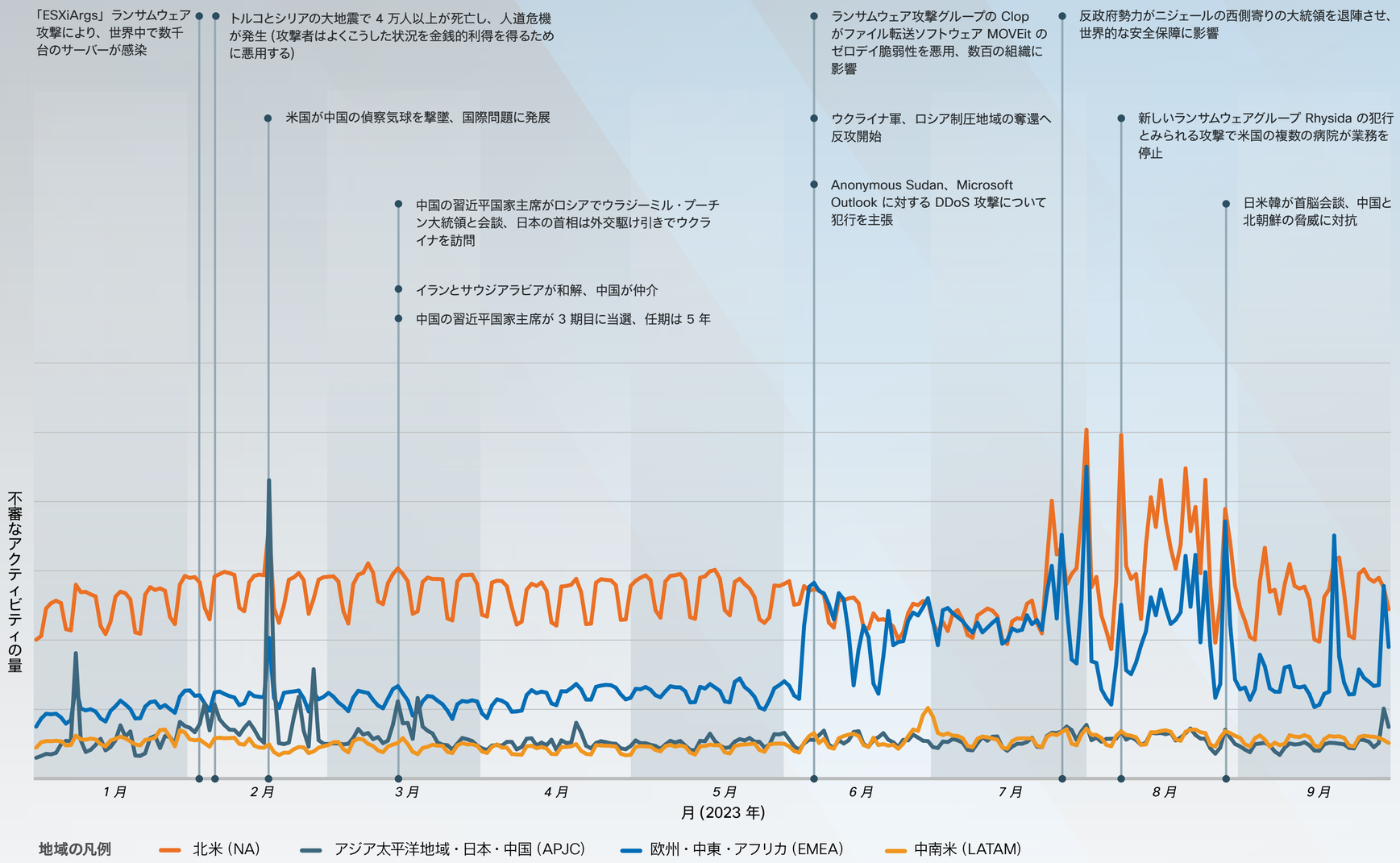
不審なトラフィックには、Cisco Umbrella、Cisco Secure Endpoint、Cisco E メール セキュリティ アプライアンス（ESA）、Meraki、SSE、Cisco Secure Firewall など、シスコの複数のセキュリティ製品から収集した多種多様な分類の情報が含まれています。たとえば Cisco Umbrella でブロックされた悪意のあるドメイン、Cisco Secure Endpoint から収集された悪意の性質を伴うレコード、Cisco E メール セキュリティ アプライアンスのフィッシングメール情報、Cisco Secure Firewall や Meraki からトリガーされた Snort シグネチャなどで、他にも多数あります。

北米、欧州・中東・アフリカ（EMEA）、中南米では不審なネットワークトラフィックが周期的に発生し、1 年の大半は月曜から金曜までの平日パターンが続きました。年の半ばから、このパターンから外れる状況が確認され、シスコのセキュリティ製品によってブロックされたトラフィックが劇的に増加し、年初の通常時の 4 倍に達することが多くなりました。

これらの地域では、2 月中旬に Web スパムが急増しました。スパムの量が世界的に増加する中で、アジア太平洋・日本・中国（APJC）地域だけ突出して影響がありました。

APJC では、不審なトラフィックはあまり周期的でなく、1 月から 4 月にかけて大きく変動しました。その後、春から初夏にかけてトラフィックの変動は横ばいになりました。

グラフに重ねて示したさまざまな国際的な出来事や大規模なサイバー攻撃は、そうした活動が脅威環境にどのような影響を与える可能性があるかを示唆しています。因果関係を証明することは不可能ですが、世界的または地域的に確認された不審なトラフィックパターンと世界の重大な出来事との間には明らかな相関関係があります。



狙われることが多かった上位の脆弱性

2023 年、攻撃者は広く使用されているアプリケーションに以前からあるソフトウェアの脆弱性を悪用しました。多くの場合、10 年以上前に公開された脆弱性であり、攻撃者が近年、新しく公開された脆弱性よりも古くからあるセキュリティの欠陥を標的にしているという CISA の調査結果と一致しています。実際 Talos が確認した脆弱性のうち、標的上位 5 件のうち 4 件は、CISA も過去数年間で頻繁に悪用された脆弱性として挙げており、この点がさらに浮き彫りになっています。攻撃対象となった脆弱性が公開されてから時間が経っていることを考慮すると、これらのシステムの多くがパッチ未適用であった可能性が高いので、組織が定期的にソフトウェアの更新プログラムをインストールする必要があるのは明らかです。

狙われることが多かった上位の脆弱性は、Microsoft Office など広く使用されているアプリケーションで見つかっています。この調査結果は 2022 年の CISA の報告でも裏付けられており、標的のネットワークに広く存在する脆弱性を攻撃者は優先すると指摘されています。攻撃者が広く存在する脆弱性を優先して攻撃する理由は、そうした脆弱性に対して開発されたエクスプロイトは長期にわたって使用でき、大きな影響を与える可能性があるからだと考えられます。

最後に、このリストにある脆弱性のほとんどは、悪用された場合に大きな影響を及ぼすものであり、6 件は Cisco Kenna の脆弱性リスクスコアで最高の 100 点となっており、7 件は共通脆弱性評価システム（CVSS）のスコアで最も深刻な「緊急」と評価されています。ほとんどの脆弱性は CISA の「悪用が確認された脆弱性カタログ（KEV）」にも掲載されています。このカタログは、優先的に修復すべきセキュリティ上の欠陥をユーザーに知らせるためのものです。これらの脆弱性に対する攻撃頻度の高さは、そのシビラティ（重大度）とともに、パッチ未適用のシステムのリスクを明確に示しています。

ランク付け	脆弱性	ベンダー	製品	CISA の調査結果	CISA の KEV カタログ	Kenna/CVSS
1	CVE-2017-0199	Microsoft	Office とワードパッド	2022 年には日常的に悪用	✓	100/9.3
2	CVE-2017-11882	Microsoft	Exchange サーバー	2022 年には日常的に悪用	✓	100/9.3+
3	CVE-2020-1472	Microsoft	Netlogon	2022 年には日常的に悪用	✓	100/9.3
4	CVE-2012-1461	Gzip ファイルの解析ユーティリティ	複数のウイルス対策製品		✗	58/4.3
5	CVE-2012-0158	Microsoft	Office	中国政府、イラン政府、北朝鮮政府、ロシア政府の支援を受けた攻撃者による悪用が多発（2016 年～2019 年）	✓	100/9.3
6	CVE-2010-1807	Apple	Safari		✗	84/9.3
7	CVE-2021-1675	Microsoft	Windows（印刷スプーラー）		✓	100/9.3
8	CVE-2015-1701	Microsoft	Windows(カーネルモードドライバ)		✓	72/7.2
9	CVE-2012-0507	Oracle	Java SE		✓	100/10
10	CVE-2015-2426	Microsoft	Windows（フォントドライバ）		✓	100/9.3

情報源： Cisco Secure Endpoint
CISA の情報源： 「日常的に悪用された上位の脆弱性」2022 年、2016 年～ 2019 年

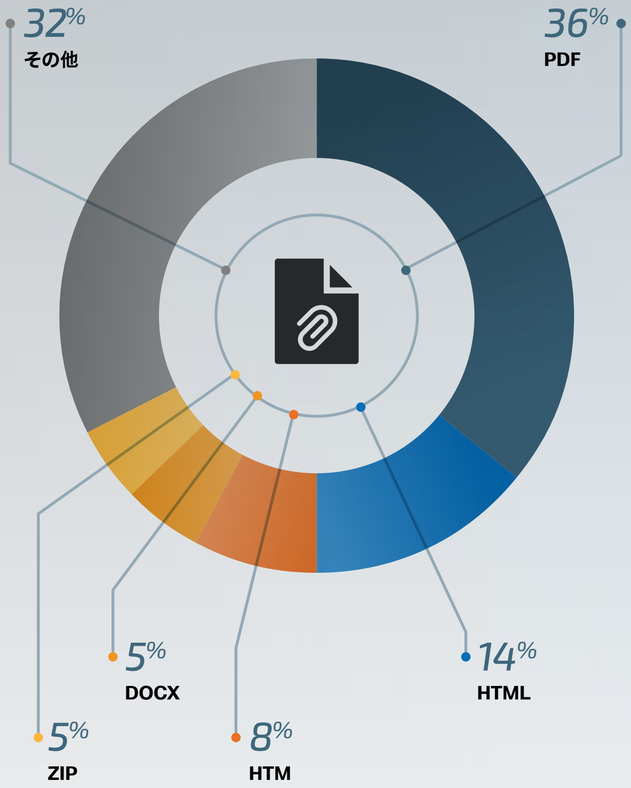
メールの調査結果

ブロックされた添付ファイルの上位のファイル拡張子

フィッシングメールは、攻撃者が被害者を危険にさらす最も一般的な方法の 1 つであり、Talos IR の調査結果でも、長年にわたって常に上位にランクされている脅威です。昨年 1 年間だけを見ると、Talos のインシデント対応業務で特定された初期アクセス手法の 25% がフィッシングメールでした（図 3b 参照）。これは米国政府の調査結果と一致しており、米インターネット犯罪苦情センター（IC3）に 2022 年に報告された最多のインシデントはフィッシングだったことを FBI が指摘しています。

攻撃者は一般的に、マルウェアを送り込むために迷惑メールを送信し、ユーザーが添付ファイルをダウンロードするか開くように仕向けます。ファイル拡張子は必ずしもファイルの種類を示すものではありませんが、攻撃者はよく知られた拡張子のファイルにマルウェアを潜ませて不審に思われないようすることが多いので、ユーザーが開いてしまう可能性が高くなります。たとえば今年初め、日本のコンピュータ緊急対応チーム（JP-CERT）は、攻撃者が検出を回避するために悪意のある Word 文書を PDF ファイルに埋め込んでいると警告しました。これは、攻撃者が何年も使用してきた手口です。

攻撃者によるファイルの種類の選好は、Microsoft が 2022 年に、攻撃者がそれまで盛んに悪用してきたマクロのブロックを決定したことにも影響されたと思われます。この変更に伴い、攻撃者は Word や Excel といった Microsoft Office のファイルを以前ほど頻繁に使わなくなりました。そして 2023 年、コモディティ型ローダーの Ursnif が、悪意のある PDF の添付ファイルをフィッシング攻撃に取り入れたことが初めて確認されました。Ursnif を拡散させている攻撃グループや他のグループは、マクロへの依存を避ける方法を探していたのです。



***情報源：**Cisco E メール セキュリティ アプライアンス*

***注：**一般的な画像関連のファイルの種類（JPG、JPEG、PNG、GIF など）は、送信者の署名やメール本文に画像を含むものなど、圧倒的に大量の問題のないメールに頻繁に出現するため、このリストから除外しました。*

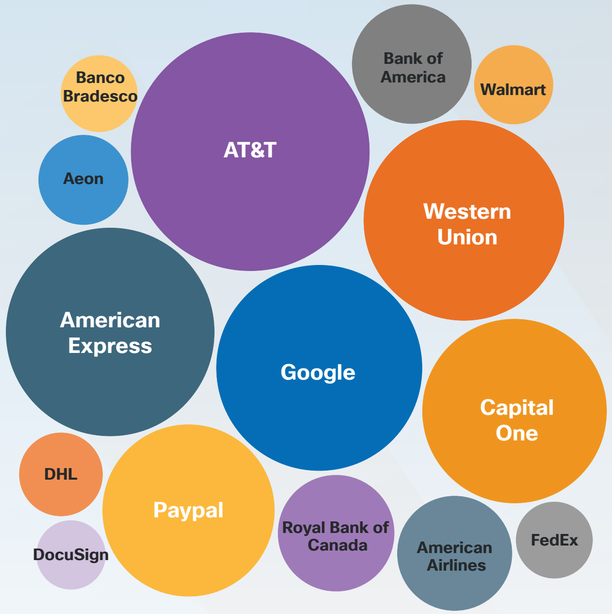
上位の初期アクセス手法（Talos IR の調査結果）

***注：**初期アクセス手法は、さまざまな理由（ログが不十分、影響を受けた環境への可視性が不足している、など）のために特定するのが難しく、結果的に「不明」がかなりの割合を占めています。*

送信元を偽装するなりすましの対象にされた上位のブランド

サイバー犯罪者などの攻撃者は、ユーザーを危険にさらすためにソーシャルエンジニアリングの手口を多用します。フィッシングメールで有名企業になりすますことが多いのはそのためです。たとえば Emotet、Qakbot、Trickbot のようなコモディティ型ローダーは、フィッシングのテーマとして偽の請求書、銀行取引明細書、発送通知などを日常的に使用し、本物のメールに見せかけています。このことは、なりすましの対象にされた上位のブランドのリストに反映されており、金融サービス業や運送業の企業のブランドが、最も頻繁になりすましの対象にされていることがわかります。

ビジネスメール詐欺でも、本物に見せかけるために企業の名前を装います。ビジネスメール詐欺は、攻撃対象にされた人が知っている送信者が正当な要求をしているように見えるメールをサイバー犯罪者が送りつけてくる詐欺です。その狙いは、受信者に不正送金を実行させることです。攻撃者は、ここにリストアップしたような有名で信頼されているブランドを装い、ユーザーを騙します。近年、ビジネスメール詐欺は増加傾向にあり、FBI によれば 2022 年の被害額は 27 億ドルになりました。



***情報源：**Cisco E メール セキュリティ アプライアンス*

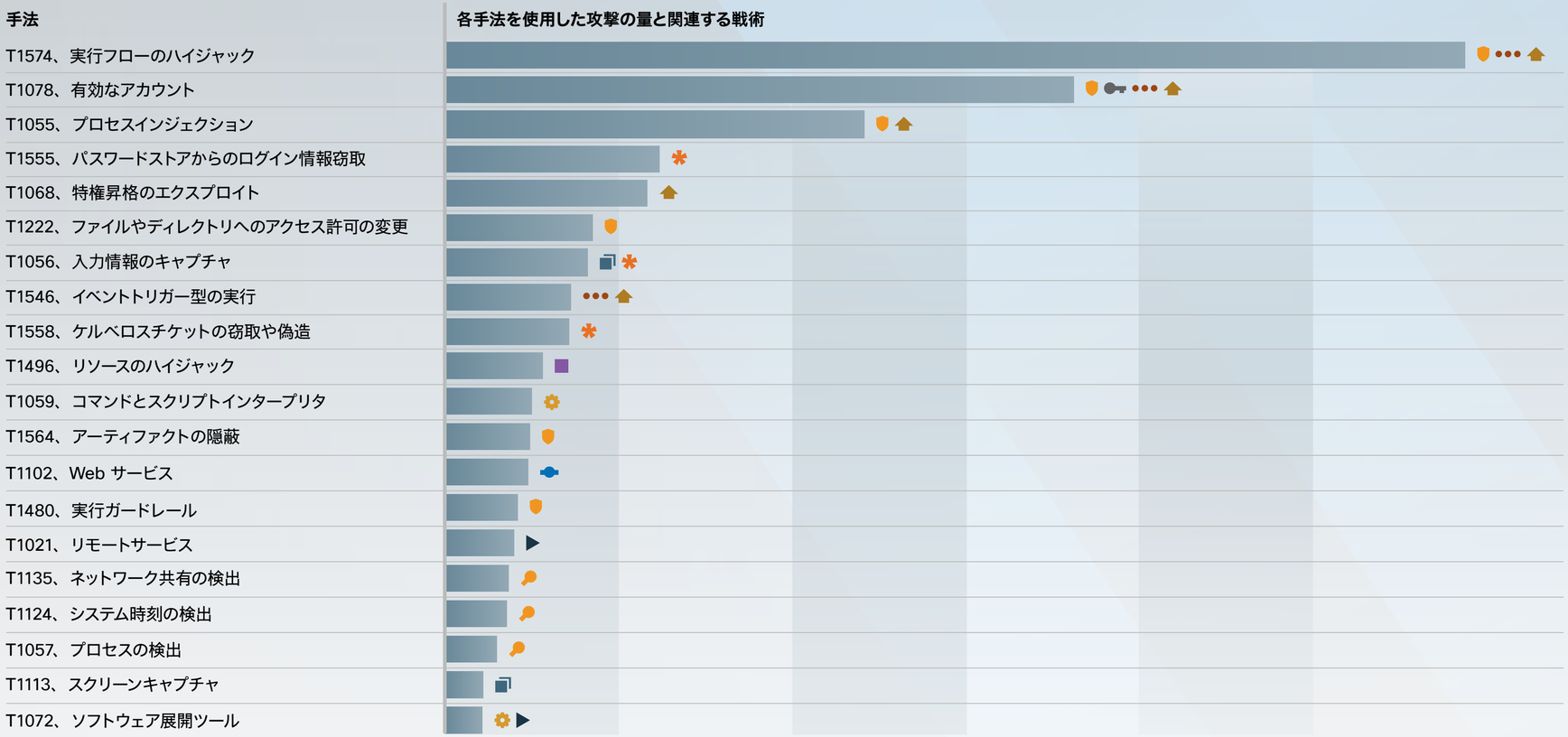
上位の MITRE ATT&CK 手法

注目すべきは、MITRE ATT&CK 手法の最も一般的な上位 20 の手法の約 3 分の 1 が**防御の回避**の戦術に該当することであり、攻撃チェーンのこの段階に攻撃者がかなりのリソースを割いているとことが推測されます。**特権昇格**と**永続化**に関連する手法も上位にランクされており、攻撃ライフサイクルにおけるこれらの手法の重要性が浮き彫りになっています。

実行フローのハイジャックが最もよく用いられた手法で、次に多かった手法の 2 倍近くになりました。実行フローのハイジャックとは、オペレーティングシステムがエンドポイントでプログラムを実行する手法を攻撃者が利用することを言います。DLL サイドローディングがこの一般的な例です。これは基本的には、攻撃者がマルウェアを被害者のアプリケーションの近くに配置し、プログラムが正規の DLL を検索するときに悪意のあるペイロードが実行されるようにする手法です。信頼できる正規のソフトウェアを実行しているように見せかけて攻撃を隠蔽するのに有効な方法であり、APT グループやサイバー犯罪者がよく利用しています。

有効なアカウントの使用が、2 番目によく確認された手法です。攻撃者が侵害されたログイン情報を悪用し、既存のアカウントを使用していることが明らかになりました。攻撃者は、攻撃チェーンのさまざまな段階を実行可能にするためにこの手法を使用します。コモディティ型ローダーがまさにこの目的で情報窃取型マルウェアを展開している状況がよく確認されています。これに関連して、**パスワードストアから**のログイン情報窃取がトップ 5 に入り、攻撃者がユーザーのログイン情報の取得に重点を置いていることがさらに浮き彫りになりました。これらの調査結果は、侵害されたログイン情報と有効なアカウントが、既知の初期アクセス手法の 4 分の 1 近くを占めたことを示す 2023 年の Talos IR のデータと一致しています。

トップ 10 に入ったリソースのハイジャックは、仮想通貨のマイニングマルウェアの展開に関連してよく確認される手法であり、収益を得るためにエンドポイントの処理能力を奪う手口です。仮想通貨マイニングの脅威は、通常はスキルの低い攻撃者による高度とは言えない種類の攻撃なので、非常に一般的です。この種類のマルウェアは、特に新しい脆弱性が検出されてすぐ、被害者がパッチを適応する前によく確認されます。もっと複雑な他のマルウェアと同時に確認されることもあります。



CISCO TALOS

一年の総括

2023

ランサムウェアと恐喝

本セクションのハイライト

- ランサムウェアとランサムウェア感染前のインシデントは、引き続きお客様に一貫した割合で影響を与えており、Talos のインシデント対応業務では両者を合わせると昨年と同じ 20% を占めています。最も狙われる業界は医療です。
- Talos の調査結果では LockBit が 2 年連続で最も活動が活発だった Ransomware as a Service (RaaS) グループでした。最も多く展開されているランサムウェア亜種は LockBit だという CISA のアセスメントと一致しています。今年 Talos IR で最も頻繁に確認されたランサムウェアの脅威の 1 つは LockBit でした。Talos が監視している約 40 のランサムウェアグループのデータリークサイトの被害者の投稿総数の 25% 以上を LockBit アフィリエイトが占めています。
- ALPHV、Clop、BianLian の脅威も猛威を振るい、合計すると同じく、ダークWeb 上の攻撃グループのサイトで公表されたすべてのランサムウェアやデータ恐喝による被害の 4 分の 1 を占めました。
- Clop アフィリエイトが一貫してゼロデイ脆弱性を悪用することが確認されていますが、このようなエクスプロイトの開発に必要な専門知識、人材、アクセスを考えると極めて異例な戦術です。これは、APT (Advanced Persistent Threat) グループだけが匹敵するレベルの高度な知識とリソースを同グループが保有していることを示唆しています。
- 他の RaaS グループから流出したソースコードを利用した新たなランサムウェア亜種が出現しています。この手法を用いると、スキルの低い攻撃者であってもこの領域に参入できるようになります。同時に Clop のような極めて高度な知識を持ったグループがかつてないペースでゼロデイ脆弱性を悪用することが確認されています。二分される攻撃者の存在は、この領域における攻撃グループの幅広さを示しており、興味深いことです。
- 攻撃グループはかつてないほどデータ恐喝に目を向けており、Talos IR が 2023 年第 2 四半期 (4 月~ 6 月) に対応した最大の脅威になりました。データ窃取による恐喝はランサムウェア感染前の活動によく似ており、防御側にとっては課題になっています。
- さらに、ランサムウェアの使用を完全にやめて恐喝を選ぶ攻撃グループもあります。この動向は、法執行機関の継続的な活動、業界の検出力の向上、活動コストの低さが影響しているようです。

ランサムウェアの情勢は、グループが名称変更や合併を繰り返したり、攻撃者が複数の Ransomware as a Service（RaaS）グループで同時に活動することが多かったり、新たなグループが絶え間なく登場したりして、2023 年も引き続き大きな動きがありました。スキルレベルも実にさまざまで、経験豊富な攻撃者がゼロデイ脆弱性を狙う高度なエクスプロイトを開発している一方で、スキルの低い攻撃者は独自のコードを作成するために他のランサムウェアコードを再利用しています。さらに、ランサムウェアの利用をやめ、ファイルを暗号化せずにデータ窃取による恐喝だけを行うようになった攻撃グループが増えており、この領域での新たな動向になっています。これは防御側にとっては新たな課題です。このように変化はありますが、世界中でランサムウェアが引き続き最大の脅威であることに変わりありません。

着手に持続するランサムウェア攻撃

Talos IR が今年対応した全インシデントの 20% をランサムウェアとランサムウェア感染前のインシデントが占めました。昨年に比べてわずかに減少しています。ランサムウェアのバイナリが実行されず、暗号化も行われない場合、防御側がランサムウェア感染前の攻撃の内容を見極めるのは場合によっては困難です。ただし、最終的な目的がランサムウェア感染かどうかを評価するためにアナリストが判断材料にするものがいくつかあります。Cobalt Strike などの攻撃シミュレーション フレームワークや Mimikatz のようなログイン情報収集ツールの使用、バックアップなど特定の重要な資産が攻撃対象にされていること、列挙や検出の手法などです。

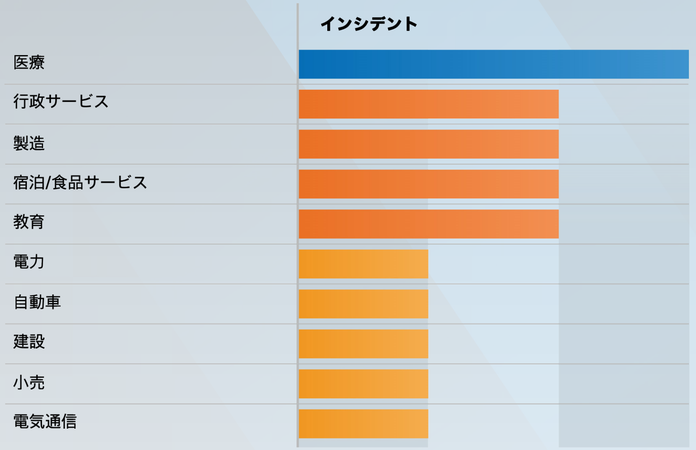
Talos IR におけるランサムウェアとランサムウェア感染前の年間対応件数をみると、昨年の『一年の総括』レポートで報告したように 2022 年に最も狙われた業界は教育セクターでしたが、2023 年は医療と公衆衛生セクターでした **（図 1 参照）**。ダウンタイムの許容度が低いこと、サイバーセキュリティ予算が不足している場合が多いこと、攻撃者にとって価値の高い保護医療情報（PHI）を保有していることから、医療機関はサイバー攻撃に対して非常に脆弱です。近年はコロナ禍で医療機関がリソース面から窮地に立たされ、ダウンタイムがさらに許容されなくなり、状況が悪化したようです。

LockBit が引き続き最大の脅威となるなか、以前から活動している攻撃者が上位を占める

2 年連続で LockBit が最も活発な RaaS グループとなり、データリークサイトへの投稿総数の 25% 以上を占めました。今年は、リークサイトへの投稿総数の 50% 近くを LockBit、ALPHV、Clop、BianLian が占めました **（図 2）**。

図 1

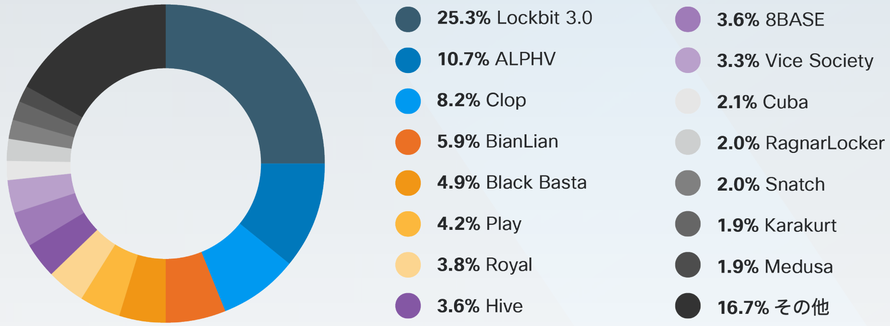
Talos IR が対応したランサムウェアとランサムウェア感染前のインシデント（業界別）



「Talos IR におけるランサムウェアとランサムウェア感染前の年間対応件数をみると、2022 年に最も狙われた業界は教育セクターでしたが、2023 年は医療と公衆衛生セクターでした」

図 2

ランサムウェアのデータリークサイトへの投稿件数

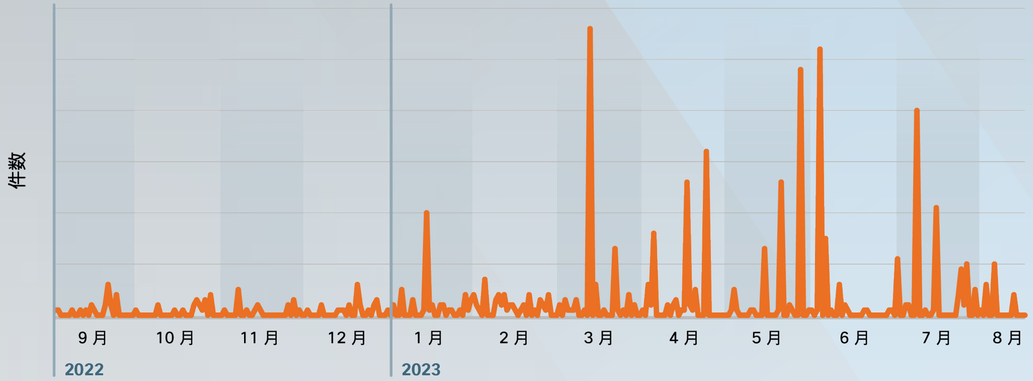


Talos IR は IT ネットワークと OT ネットワークに影響を与える LockBit のインシデントに対応

Talos IR は、電力会社に影響を与えたランサムウェア LockBit のインシデントに対応しました。このインシデントでは、ランサムウェアが企業の IT ネットワークと OT ネットワークに侵入し、被害企業に重大な影響を与えて下流に位置する顧客にも混乱をもたらしました。このランサムウェア アフィリエイトは、多要素認証（MFA）が導入されていない VPN 経由で認証されるルータの有効なログイン情報を使用して初期アクセスを取得しました。攻撃者は、送電網を監視するサーバーなど実稼働中のサーバーを暗号化し、さらに 4 台のドメインコントローラのうち 3 台も暗号化しました。

LockBit は、2023 年も引き続き非常に多くのランサムウェア攻撃を行いました。この調査結果は、最も多く展開されているランサムウェア亜種は LockBit だという CISA のアセスメントと一致しています。LockBit の攻撃は大きな影響をもたらす可能性があり、Talos のインシデント対応業務で確認したように、組織のインフォメーション テクノロジー（IT）ネットワークと、物理プロセスを担うハードウェアやマシンであるオペレーショナル テクノロジー（OT）に影響を与えます。10 月に CISA は、OT 環境を保護するガイダンスを公開し、これらのシステムに対していかに大きな影響をもたらす可能性があるかを強調しました。LockBit は、PaperCut ソフトウェアの 2 件の脆弱性が悪用された際も展開されました。PaperCut は、特に政府機関と教育業界で広く使用されている印刷管理ソリューションです。

図 3
年間を通じた LockBit の活動



LockBit グループのデータリークサイトへの投稿は 1 年を通して波があり、3 月には同グループの活動の検出が急上昇しました。印刷管理ソフトウェアである PaperCut の脆弱なインスタンスへの LockBit の展開と時期が部分的に重なっており、その後も高い検出状況が続いています **(図 3)**。

新たなグループや名称を変更するグループでランサムウェアの分野は依然として活発

ランサムウェアグループの絶え間ない名称変更や交代は、今年の顕著な動向でした。ランサムウェアの作成と改造に不可欠なコンポーネントであるソースコードとビルダーが何度も流出し、ランサムウェアの脅威環境に重大な影響をもたらしました。こういった流出によって、ランサムウェアグループの名称変更が可能になったり、スキルの低い攻撃グループが労力をほとんどかけずに、あるいは知識がほとんどなくても自前のランサムウェアを簡単に作成できるようになったりします。この分野に参入する攻撃グループが増えるにつれ、流出したランサムウェアのコードを利用したランサムウェア亜種の出現数が多くなっています。これが攻撃頻度の増加につながり、特に攻撃グループの特定に関して、新たな課題をサイバーセキュリティ専門家や防御側に突きつけています。

流出したソースコードを基にした新たなランサムウェアの亜種の多さは、攻撃グループがそのような公開情報を利用するスピードが速いことも浮き彫りにしています。直近では、Yashma ランサムウェアビルダーで作成された新種のランサムウェアが急増していることが確認されました。2022 年 5 月に初めて登場した Yashma は、2022 年 4 月に流出した Chaos ランサムウェアビルダー（V5）を名称変更したものです。2023 年の初めから、ANXZ、Sirattacker などの Yashma の新種が複数出現したことを確認しています。広く使用されているランサムウェアではなく、知名度も低いことを考慮すると、小規模なアフィリエイトまたはリソースの少ないアフィリエイトグループによって展開されたものと思わ

れます。4 月、Talos は RA Group という新たなランサムウェア攻撃グループが、流出した Babuk のソースコードを基に作成したランサムウェア亜種を展開していることを発見しました。2021 年 9 月、Babuk グループのメンバーとされる人物がランサムウェアの完全なソースコードを流出させて以来、その流出コードを基にして数種類の亜種が作成されています。2023 年には ESXiArgs、Rorschach、RTM Locker など多くの亜種が登場しました。

脅威環境のこのような変化はアフィリエイトに大きなメリットをもたらしてきましたが、その一方で、セキュリティ研究者と防御側にも、流出したコードを入手できるという利点があります。セキュリティ研究者は、ソースコードの分析によって攻撃者の TTP を理解し、効果的な検出ルールを開発できるようになります。復号プログラムの開発に役立つ可能性もあり、ランサムウェアの脅威に対抗するためのセキュリティ製品の機能強化が可能になるかもしれません。

複数のアフィリエイトがランサムウェアの展開からデータ窃取による恐喝へ転向

RaaS の選択肢は増えていますが、ランサムウェアを展開せずに恐喝金の獲得に成功した攻撃グループもいます。このような恐喝の場合、攻撃者は被害者のデータを盗みますが暗号化はしません。そのため、攻撃者はファイルのロックを解除する代わりに支払いを要求するのではなく、情報を漏らすと脅すだけになり、よくある二重恐喝の戦術はとりません。この傾向は Talos のインシデント対応業務にも反映されており、2023 年第 2 四半期には恐喝が最も多く確認された脅威となり、前四半期（1 月から 4 月）比で 25% 増え、ほぼ 3 分の 1 を占めました **（図 4）**。

Babuk、BianLian、Clop などの有名なランサムウェア集団は、これらのグループの典型的なランサムウェア攻撃チェーンから逸脱し、ランサムウェアを展開せずにデータ窃取による恐喝を選択しています **（図 5）**。

ランサムウェアを展開する代わりにデータ窃取による恐喝を選好する攻撃者が現れた背景には、いくつかの要因が考えられます。近年、米国や世界各国の法執行機関が精力的にランサムウェア攻撃グループを追跡し、有名なグループに対する大掛かりな差し押さえを実行しました。Endpoint Detection and Response（EDR）機能の進歩が、ランサムウェアを展開し、データを暗号化しようとする攻撃者にとっては大きな障害になっていると思われます。攻撃者はこの手法が支払いを受け取る有効な手段であると考えているようで、ランサムウェア攻撃グループが EDR の進歩、法執行機関の取り締まり、その他の障壁に対して常に何らかの手を打とうとしていることがうかがえます。

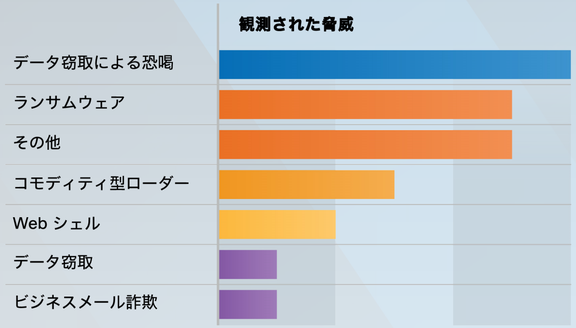
恐喝が深刻で有効な脅威であることは証明されていますが、組織や防御担当者にとって過去数年来問題となっているランサムウェアの脅威をまだ超えてはいません。Talos は、この動向の長期的な影響を今後も監視していきます。

一部のランサムウェアグループが一貫してゼロデイを利用し、多くの場合、複数の組織に影響を与えている

今年は多くの経験の浅い攻撃者がコードの再利用に頼りましたが、極めて高度な知識を持つグループがかつてないペースでゼロデイ脆弱性を悪用している状況も引き続き確認されており、この分野における攻撃グループの幅広い技術的多様性と TTP を浮き彫りにしています。機会をうかがっていることで知られるランサムウェア攻撃グループは、欠陥が公表されるとすぐに悪用します。知名度が高くデータ恐喝を行うランサムウェアグループの Clop が ゼロデイ脆弱性を悪用したという声明を公開するとすぐに、別のランサムウェア アフィリエイトが後に続き、パッチが出される前に影響を受けたシステムを調べていました **（図 6）**。

図 4

第 2 四半期（2023 年 4 月～ 6 月）ではデータ窃取による恐喝が最大の脅威（Talos IR の調査結果）



ランサムウェアのソースコード流出がどのような影響をもたらしているか

ランサムウェアのソースコードやビルダーが流出すると、技術力のない野心的なサイバー犯罪者が、元のコードにわずかな改変を加えるだけで独自のランサムウェア亜種を簡単に開発できるようになります。さらに、流出したソースコードを使用して調査担当者を混乱させたり、判断を誤らせたりすることもできます。セキュリティの専門家が他の攻撃グループの犯行だと誤って特定する可能性が高くなるからです。

（Talos のブログに投稿されたリサーチから引用）

図 5

近年、知名度の高いグループがデータ窃取による恐喝へ転向する傾向が増加

Babuk

2021 年 4 月にデータ窃取による恐喝への転向を表明した以前からのランサムウェア

Karakurt

2021 年 6 月に初めて登場したデータ窃取による恐喝を行うグループ

RansomHouse

2021 年 12 月に初めて登場したデータ窃取による恐喝を行うグループ

Lapsus$

2021 年 12 月に初めて登場したデータ窃取による恐喝を行うグループ

Clop

2023 年にデータ窃取による恐喝を用いた攻撃でも利益を上げたランサムウェアグループ

BianLian

2023 年 1 月からデータ窃取による恐喝を行っているランサムウェアグループ

図 6
注目されている脆弱性を悪用したランサムウェアのタイムライン

2023 年 1 月
Clop ランサムウェアグループがゼロデイ脆弱性（CVE-2023-0669）を利用して GoAnywhere MFT のプラットフォームを標的とする攻撃を開始

2023 年 4 月
2023 年 4 月中旬から攻撃者が PaperCut の脆弱性（CVE-2023-27350）の悪用を開始

PaperCut 社がパッチ未適用のサーバーが実際に悪用されていることを認識、Clop の犯行であることを特定

PaperCut へのエクスプロイトが多発、攻撃者がリモートコード実行によりランサムウェアの LockBit を展開

2023 年 5 月
ランサムウェア集団の BI00dy が PaperCut の脆弱なサーバーを悪用

Clop がそれまで知られていなかった Progress Software 社のマネージドファイル転送（MFT）ソリューションに存在する SQL インジェクションの脆弱性（CVE-2023-34362）の悪用を開始

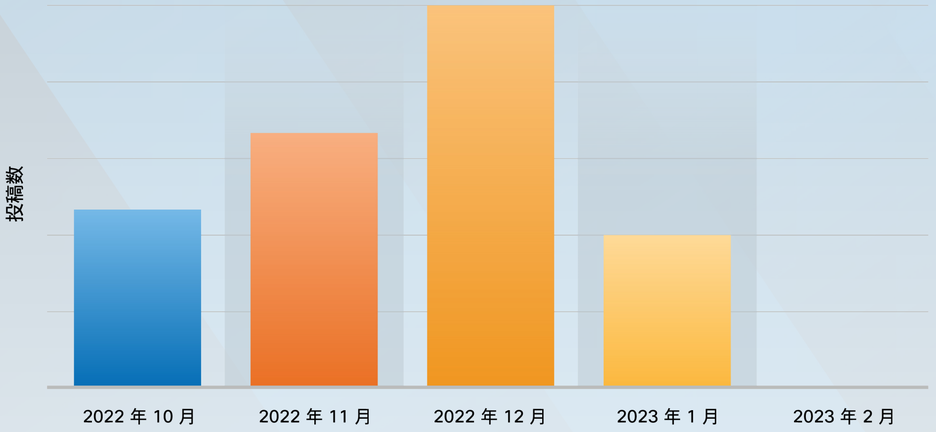
4 月に、印刷管理ソフトウェア会社の PaperCut は、パッチ未適用のサーバーが Clop によって実際に悪用されていることに気づきました。するとまもなく、他のランサムウェアグループが重大なリモートコード実行（RCE）の脆弱性（CVE-2023-27350）を、その攻撃チェーンの一部として悪用し始めたのです。これは、この活動に見られる広範な特徴とランサムウェアグループの戦略を浮き彫りにする事例です。多くの場合、被害者から支払いを引き出すチャンスを増やすために、他のグループの開示情報を基に注目されているセキュリティ上の欠陥を利用します。

繰り返しゼロデイ脆弱性を悪用する Clop の取り組みは、機能の開発に必要なリソースを考慮すると、ランサムウェアグループとしては極めて異例です。2023 年にはこのような事例が数多く見られ、1 月には Clop ランサムウェアグループがゼロデイ脆弱性（CVE-2023-0669）を利用して GoAnywhere MFT のプラットフォームに対する攻撃を開始しました。5 月に Clop グループが出した声明では、Progress Software のファイル転送ソリューションである MOVEit Transfer に影響を与える別のゼロデイ脆弱性（CVE-2023-34362）に対する攻撃についても言及されています。これらの攻撃は Clop のツールキットが拡張されたことも示しており、同グループは、これまで確認されていなかった LemurLoot という Web シェルを展開し、MOVEit を実行しているシステム上の被害者データを流出させて身代金を要求しました。

前述したランサムウェア アフィリエイト / グループに利用された脆弱性はすべて、高または緊急の CVSS スコアが付けられており、容易に悪用できることを Cisco Kenna が確認しています。また、CISA の「悪用が確認された脆弱性カタログ（KEV）」にも掲載されています。

このようなエクスプロイトの開発や特定に必要なリソースを考えると、Clop グループ（特定のメンバー）が、APT グループだけが匹敵するレベルの高度な知識や資金を保有している可能性があります。Clop がどのようにこれらのエクスプロイトを手に入れたかに関する地下フォーラムでのやり取りは見当たりません。しかし、同グループはサードパーティのファイル管理システムや他のネットワーク周辺機器の脆弱性を特定することに注力していると思われる、高度な専門知識を持つ開発者と接触している可能性があると Talos は見ています。

図 7
Hive のデータリークサイトへの投稿（2022 年末以降）



法執行機関による解体を受け RaaS 領域の情勢が変化

ランサムウェアグループは解体を経験した結果、他の RaaS グループに適応または参画せざるを得ませんでした。2023 年 1 月、米国司法省はランサムウェアグループ Hive を撲滅したと発表しました。Talos のデータにもこのことが反映されており、1 月下旬までに Hive のデータリークサイトの投稿数が全面的に下落したことを確認しました **（図 7）**。

ランサムウェアのインフラが解体された場合、攻撃グループが他のグループと協力して活動を続け、法執行機関やネットワークの防御側にとってはもぐらたたき状態になることがよくあります。Talos の調べによると、たとえば Hive のインフラが解体されたときは、数日以内に Hive の元メンバーの多くが他のランサムウェアグループに参画しようとしました。同じランサムウェアビルダーのコードを利用する新たなグループが参入することでこのような「民主化」が進むと、TTP がグループ間で変わらないものになるため、防御側が攻撃活動を特定のグループと結びつける作業が複雑になります。

CISCO TALOS

一年の総括

2023

ネットワーク インフラ

本セクションのハイライト

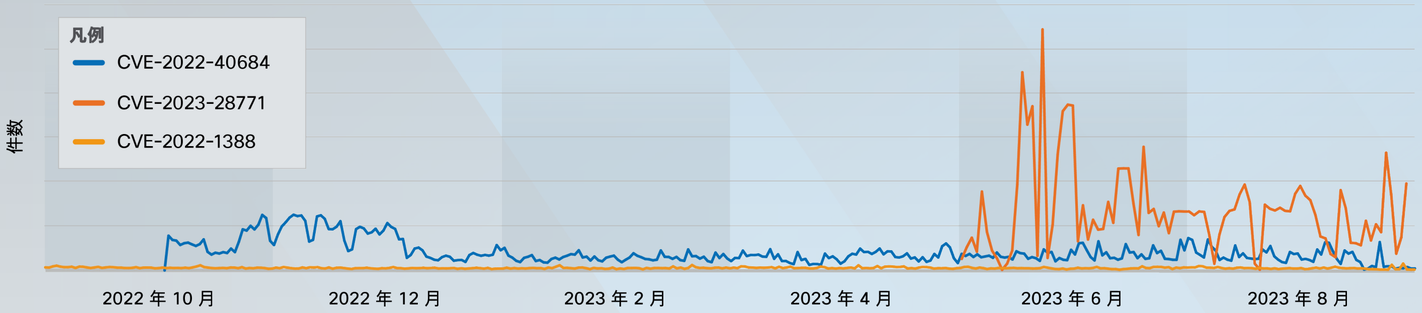
- 今年は懸念されるほどに、高度な攻撃者がネットワークデバイスを攻撃しています。特に目立つのは中国とロシアを拠点とするグループで、その狙いはスパイ活動の目的を達成し、次の標的に対するステルス作戦を円滑に展開することです。
- 他のサイバー犯罪者もこれに追随するようになっており、同じ手法を採用してネットワークデバイスへの不正なアクセス権限をダーク Web で販売したり、標的のネットワークに侵入してランサムウェアを展開したりしています。
- 攻撃者は、デフォルトのログイン情報やパッチを適用していない脆弱性などのセキュリティの弱点を利用し、攻撃対象のデバイスへの初期アクセスを取得します。
- この領域で最も狙われたデバイスの脆弱性 5 件のうち 3 件は緊急または深刻であり、悪用されると、場合によってはデバイスが完全に乗っ取られる可能性があります。その結果、標的のネットワークとセキュリティ境界のコアコンポーネントに攻撃者が自由にアクセスできるようになってしまう恐れがあります。
- この領域での脆弱性に対する悪用の試みは 2023 年を通してほぼ一貫して続き、脆弱性の公開後に時折急増しました。このことは、攻撃を受けた組織がタイムリーにデバイスにパッチを適用していないことが多いので、脆弱性が公開されてから時間が経っても攻撃者が公開済みの脆弱性を悪用することに価値を見出し続けていることを示唆しています。
- ネットワーク侵入後に検出されないようにし、アラームが発報されることなく追加のアクセス手段を確立するために、攻撃者は環境内の防御を弱める対策を講じるほか、新たな脆弱性を導入して悪用することすらあります。
- Talos は、Network Resilience Coalition (ネットワークレジリエンス連合) を支持することにより、この脅威との戦いを支援しています。この組織は、ネットワーク機器ベンダー、ネットワーク事業者、セキュリティ企業の業界リーダーからなるグループであり、重要なデータネットワークの保護に重点を置いています。

Talos はこの 1 年、ネットワークデバイスに対する高度な攻撃が増加していることを確認しました。特に増えているのは国家の支援を受けたグループによる攻撃で、その狙いはスパイ活動の目的を達成し、ステルス作戦を円滑に展開することです。Talos の調査では、主にロシアと中華人民共和国とつながりのある脅威グループが関与していましたが、こうした攻撃の成功に注目が集まっていることから、十分に能力のある APT グループであれば、ネットワークインフラを攻撃対象にする能力を現在開発しようとしているか、今後開発するはずだと考えるのが妥当です。また最近では、標的のデバイスへの不正なアクセスで利益を得ようとする初期アクセスブローカーやランサムウェアグループなど他のサイバー犯罪者による攻撃活動も確認されています。

ネットワーク機器はアタックサーフェス（攻撃対象領域）が広く、被害者のネットワークにアクセスできる可能性があるので、サイバー攻撃者にとっては魅力的な攻撃対象です。IT インフラの重要な構成要素であり、機密性の高いネットワークトラフィックの通信経路であることが多いにもかかわらず、セキュリティの観点からネットワークデバイスが検査されることはまれであり、一般的にパッチも十分に適用されていません。さらに、標準のオペレーティングシステムではなく、ベンダー独自のカスタムファームウェアで稼働することが多いので、汎用のセキュリティソリューションでは保護や監視ができないことになります。価値は高いのにセキュリティが弱いため、ネットワークデバイスが真っ先に悪用の対象になっているのが現状です。シスコのネットワークインフラは世界中に広く存在するため、Talos は最上位の攻撃者とその攻撃活動を調査し、報告するのに適した立場にあります。

図 8

2022 年から 2023 年にかけてのネットワークデバイスの脆弱性に対する悪用の試み



弱いセキュリティは初期アクセスで悪用されることが多い

Talos は、パッチ未適用の脆弱性、弱いログイン情報やデフォルトのログイン情報、安全でないデバイス設定を攻撃者が悪用して、ネットワークデバイスへの初期アクセスを取得することが圧倒的に多いことを確認しています。前述のとおり、セキュリティ専門家がネットワークデバイスに標準の EDR ソリューションを導入することはできないかもしれませんが、日常的なパッチ適用、監視の強化、ログイン情報管理の改善を行うだけで、このような脅威に対する組織の防御が大きく改善される可能性があることがわかります。初期アクセスを取得すると、攻撃者は通常、デバイスのセキュリティの弱さにさらにつけ込みます。ログを消去したり無効化したりして、侵入の証拠隠滅を図るのです。

情報公開後に脆弱性の悪用が急増

Talos のテレメトリによると、この 1 年、ネットワークデバイスの脆弱性を悪用する活動がほぼ一貫して続きましたが、情報公開後に急増することもありました。悪用の試みが急増した要因はいくつか考えられます。高度な攻撃グループが非常に大規模な単発の攻撃を行っていた、あるいは大々的に報じられパッチが推奨されたせいで突然阻止された広範な攻撃活動だったといったことです。これと比べ、脆弱性の公開後数か月間にわたって攻撃が一定のレベルを保っている状況は、攻撃を受けた組織がタイムリーにデバイスにパッチを適用していないので、脆弱性が公開されてから時間が経っても攻撃者が古い脆弱性を悪用することに価値を見出し続けていることを示唆しています。

たとえば、以前取り上げた Fortinet の脆弱性（CVE-2022-40684）を悪用する試みを警告する Snort ID（SID）60726 と 60725 の検出数は、セキュリティの欠陥が 2022 年 10 月中旬に公開された直後に急増し、その後 2023 年初めまでに著しく低下してそのまま一定のレベルを保っています **（図 8）**。それと比べ、脆弱な Zyxel デバイス（CVE-2023-28771、SID 6185）に対する試みは、2023 年 4 月に脆弱性が公開されてから間もない 5 月中旬に始まり、その後数か月間にわたって比較的一定のレベルのまま続いています。

攻撃された上位の脆弱性は極めて重大で悪用されやすく、デバイスが広く普及

2023 年に最も頻繁に攻撃を受けたネットワークデバイスに影響を与えた脆弱性は、シビラティ（重大度）スコアが高く、簡単に悪用されて業務に重大な影響をもたらす可能性があります。この領域で攻撃を受けた脆弱性 5 件のうち 3 件は CVSS スコアが 9.8 点または 10 点でしたが、このスコアが付けられるのは最も深刻な少数の脆弱性だけです。ネットワークデバイスの重大で深刻なセキュリティ上の欠陥が悪用されると、場合によっては、デバイスが完全に乗っ取られ、標的のネットワークとセキュリティ境界のコアコンポーネントに攻撃者が自由にアクセスできるようになってしまう恐れがあります。

そのうえ、影響を受けるデバイスの多くは世界中の企業や政府で広く使用されているので、侵害が成功した場合の影響や範囲がより一層大きくなる可能性があります。攻撃者が欠陥の公開後に大量のスキャンを実行して、何千もの脆弱なデバイスを発見するかもしれません。また、公開されているエクスプロイトを見つける可能性も大いにあります。

最後に、以下のリストに挙げているベンダーの多様さは、この問題がデバイスを提供している企業にとっていかに普遍的な問題であるかを示しています。このことは、Talos がこの 1 年にサンプルを入手した、Vulkan ファイルとも呼ばれるロシアの諜報機関の契約文書でもさらに裏付けられています。同文書は、どの企業のネットワークデバイス製品にも攻撃対象にされる脆弱性があることを示しており、あるスキャンコンポーネントでは、ルータやスイッチのメーカー 20 社近くが標的とされていました。

以下にリストアップしたほとんどの脆弱性は、一般的に攻撃されている脆弱性やすでに悪用が確認されている脆弱性として CISA のリストにも掲載されています。Talos の上位 2 つの脆弱性も、米国の重要インフラに対する脅威に関する CISA のアドバイザリに含まれており、これらの脆弱性の悪用がいかに重大な影響をもたらす可能性があるかを示しています。

1. **CVE-2020-5902 (SID 54462)：**F5 BIG-IP のトラフィック管理ユーザーインターフェイスにおけるリモートコード実行の脆弱性
2. **CVE-2019-1653 (SID 48949)：**Cisco RV シリーズ ルータの情報開示の脆弱性
3. **CVE-2022-40684 (SID 60725、60726)：**Fortinet 社製 FortiOS、FortiProxy、FortiSwitchManager の認証バイパスの脆弱性
4. **CVE-2023-28771 (SID 61865)：**複数の Zyxel ファイアウォールにおける不正なコマンドインジェクションの脆弱性
5. **CVE-2020-3452 (SID 54598)：**Cisco 適応型セキュリティアプライアンス（ASA）ソフトウェアおよび Cisco Firepower Threat Defense（FTD）ソフトウェアのディレクトリトラバーサルの脆弱性

脆弱性の説明の情報源は国立標準技術研究所（NIST）の Web サイト、Snort ID の情報源は Snort の Web サイトです。

侵入後に足掛かりを構築するためにマルウェアがインストールされることもある

Talos はいくつかの事例で、中国系の APT グループをはじめとして、攻撃者が侵入後にデバイスにマルウェアをインストールしてネットワークに足掛かりを構築し、後に続く攻撃活動を可能にしていることを確認しました。Talos が確認したマルウェアによって有効になる機能には以下のようなものがあります。

- トラフィックがルータ本来の動作によってブロックされないようにアクセス制御リスト（ACL）をバイパスする
- 通常の認証方式以外で、デバイスへの認証済みアクセスを許可する
- デバイスを破壊して無効化する機能を有効にする
- 攻撃者が定義したトラフィックを、攻撃者が制御するインフラにリダイレクトする

多くの事例で、攻撃者がマルウェアの展開と同時に、あるいはマルウェアの代わりに環境寄生型バイナリ（LoLBin）を使用して活動を進展させ、検出を回避することが確認されました。侵入後にマルウェアがインストールされた最近の事例では、攻撃者は 2023 年 9 月と 10 月に、それまで知られていなかった重大な脆弱性（CVE-2023-20198）を悪用して、Cisco IOS XE ソフトウェアが動作する特定のネットワークデバイスにアクセスし始めました。これにより、攻撃者はデバイスへの権限レベル 15 のアクセスを取得することができ、その権限を使用して別のゼロデイ脆弱性（CVE-2023-20273）を悪用し、マルウェアを展開しました。

注目すべきは、CVE-2023-20198 の脆弱性が、インターネットに公開されていて HTTP または HTTPS サーバー機能が有効になっているデバイスに特に影響するという点です。これは米国政府が前に警告していた特徴です。

この活動は、インターネットに公開された管理インターフェイスに起因するリスクの軽減に関して米国政府が過去に提示したベストプラクティスおよびガイダンスと一致するシスコの推奨事項の重要性を浮き彫りにしています。また、シスコが Network Resilience Coalition のメンバーとして、業界のパートナーと進めている取り組みもこれに関するものです。詳細については、後で詳しく取り上げます。

極めて重要な活動にはネットワーク情報の収集が不可欠

ロシアと中国の APT は侵害したデバイスを独自に可視化して、機密性の高いネットワーク情報をキャプチャし、より価値の高いデータへアクセスしやすくします。攻撃者は、正規のログイン情報、ドメインの信頼関係の詳細、ネットワーク構成図、ネットワークの顧客との契約、設定情報などのデータを横取りして悪用しようとします。こういった情報は、攻撃者が権限を昇格させて関心のあるネットワークへ侵入し情報収集するためのロードマップとなります。

APT はまた、環境内の防御を弱めて長期的なアクセスのための経路を切り開くための手段を講じます。例を挙げると、ログの無効化、パッチが適用された脆弱性を再導入するためのメモリの変更、特権が必要な操作を可能にする設定変更、メモリ内で変更可能な古い正規のファームウェアと現在のファームウェアとの入れ換えなどです。こうした手口の幅広さは、攻撃者が、侵害を受けたネットワーク機器について非常に高いレベルの技術と専門知識を有していることを示しています。さらに攻撃者は、攻撃対象の環境内でこれらの足掛かりを築きながら、組織の多層防御セキュリティアーキテクチャ内の切り崩すことが可能な障壁を侵食しようとします。組織は、システム強化の取り組みとネットワーク監視機能の最新化と高度化を図り、これらの脅威グループから防御しなければなりません。

侵害を受けた多数のデバイスが悪意のあるトラフィック用に匿名のネットワークを形成

これまで見てきたような手法は通常、特定の被害者を狙うために高度に専門化されています。一方で攻撃者は、次の標的に対するステルス作戦を円滑に展開するために、ネットワークデバイスに対する広範で無差別の攻撃も行います。Talos は、中国系の APT が、デバイスの所有者をほとんど考慮せずに世界中の多数のネットワークデバイスを侵害し、Tor と同じように機能する匿名のネットワークを形成していることを確認しました。攻撃者は侵害したデバイスのネットワークを使用して、標的のネットワークとの間で悪意のあるトラフィックを送受信します。この方法により、攻撃元をわかりにくくしているのです。これらの APT は、地理的な特定地域からのトラフィックをブロックする標的のセキュリティ防御を、C2 トラフィックが被害者の地域のインターネット サービス プロバイダー（ISP）から発信されるようにすることによってバイパスすることもできます。

Talos は、ネットワークデバイスに関連する重大な脆弱性が公開されてから数日以内に、中国系の攻撃グループがそれらの脆弱性を悪用する広範な攻撃を実行することを確認しています。これは、攻撃者がネットワークインフラの種類に関係なく、ほぼ無差別に攻撃を仕掛けていることを意味します。

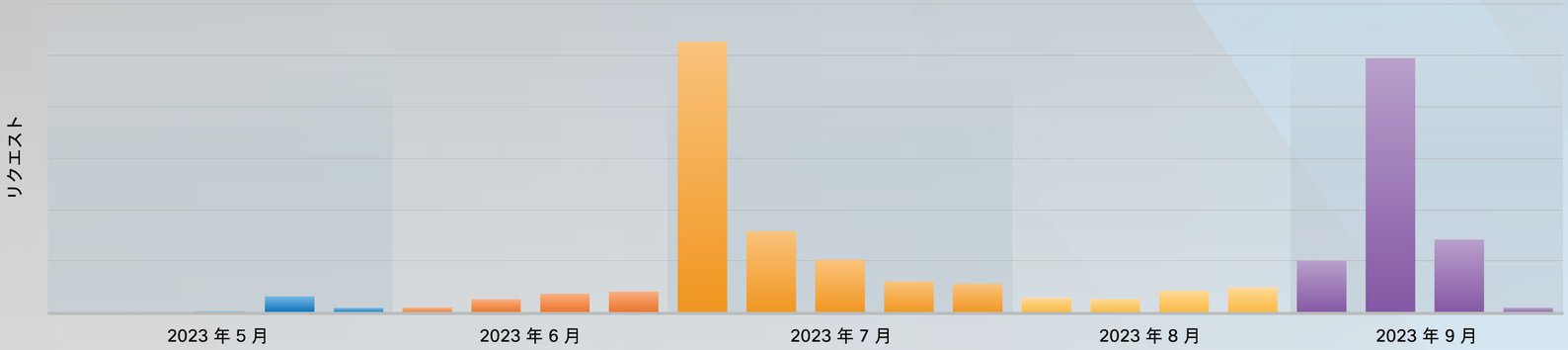
Talos はこの拡大する脅威にどのように対抗しているのか

シスコは 2023 年 7 月に、業界を牽引するパートナー企業数社と Network Resilience Coalition を立ち上げました。このアライアンスは、この問題に対する意識を高め、その全容を理解し、世界経済と国家安全保障を支えるネットワークセキュリティを改善するための実用的な推奨事項を提供することに重点を置いています。

Talos はこの脅威に対処する取り組みを主導し、かなりの量の研究情報と技術情報を提供しました。Talos が提供した情報は米国政府のこのトピックに関するアドバイザリとして公表されています。また、ネットワークインフラの復元力を改善する方法についての、お客様とネットワーク防御担当者へのメッセージ発信を強化しました。デバイスのセキュリティ全体を強化するために、他のベンダーとの研究活動や情報共有にも積極的に取り組んでいます。たとえばこの 1 年、Talos の脆弱性検出および調査チームは、スモールオフィス ホームオフィス（SOHO）用ルータと産業用ルータを優先すべき重要課題として調査しました。この取り組みの成果として、これまでに 289 件の脆弱性をベンダーに報告し、全部で 141 の Talos アドバイザリを発表しました。Talos の報告により Snort ネットワーク侵入検知のカバレッジが新たに拡張され、各ベンダーから複数のセキュリティ修正プログラムが提供されました。これらの修正プログラムは Cisco Security ソリューションを導入しているお客様の役に立つものであり、パッチを適用すれば、脆弱性のあるルータを使用しているすべてのユーザーにとってセキュリティ態勢が改善します。

図 9

ASA デバイスを標的とした活動の増加と同時に WebVPN 関連のリクエストが急増



「この 1 年、ネットワークデバイスを標的とした初期アクセスブローカーやランサムウェア アフィリエイトの活動が活発になっています。主に侵害されているのは、弱いログイン情報やデフォルトのログイン情報です」

ランサムウェア攻撃グループと初期アクセスブローカーが弱いログイン情報を悪用し、アクセス権を収益化

この 1 年、ネットワークデバイスを標的とした初期アクセスブローカーやランサムウェア アフィリエイトの活動が活発になっています。主に侵害されているのは、弱いログイン情報やデフォルトのログイン情報です。その不正なアクセス権をダーク Web のマーケットプレイスで販売したり、これを使用し標的のネットワークでランサムウェアを展開したりしています。

今年 Talos は、WebVPN で設定された Cisco 適応型セキュリティアプライアンス（ASA）のデバイスを標的とした攻撃に対応しました。これらの攻撃では、サイバー犯罪者がブルートフォース攻撃やパスワードスプレー攻撃によってデバイスへの不正なアクセスを取得したと思われます。7 月に WebVPN で設定された ASA のデバイスを標的とした活動が著しく急増したことを確認しました。ASA のデバイスを狙った実際の攻撃に関して多くの公開レポートが発表された時期と一致しています **（図 9）**。さらに 2023 年 9 月には、CVE-2023-20269 の脆弱性公開に関するシスコのセキュリティアドバイザリと同時に WebVPN のリクエストが急増しました。この脆弱性が悪用されると、リモートの攻撃者がブルートフォース攻撃を行ったり、認証されたリモートの攻撃者が不正なユーザーとクライアントレス SSL VPN セッションを確立したりできるようになります。ブルートフォース攻撃を実行する能力と、弱いログイン情報やデフォルトのログイン情報が広く使用されている状況とが相まって、多数のデバイスが大きな影響を受けやすくなりました。こういった活動も、脆弱性の公開直後に攻撃者が悪用を試みる頻度が高まる現状を浮き彫りにしています。

ランサムウェアグループの Akira と LockBit が 2023 年 8 月からこの活動に関与していることが公表されましたが、これらの攻撃グループがログイン情報のスプレー攻撃を行ったのか、初期ブローカーからアクセス権を購入したのかは不明です。この 2 つの脅威グループが FortiGuard など他のデバイスベンダーに対して類似の活動を行っていることも確認されています。攻撃活動の規模や時期と、侵入後に行われる活動の特徴から判断すると、多くのランサムウェア事例では、サードパーティのブローカーが初期アクセスを取得する役割を担っている可能性があると Talos は考えています。前述のセキュリティアドバイザリには、推奨される軽減策と侵害の兆候が記載されており、防御側がこの脅威を防ぐのに役立ちます。適切な MFA の導入や連続するログイン試行の失敗回数制限の重要性を強調しており、これらの手段により、脅威にさらされる可能性を大幅に削減できます。

CISCO TALOS

一年の総括

2023

Advanced Persistent Threat（APT）：中国

本セクションのハイライト

- 今年は中国に関連した活動が活発化しました。これは、西側諸国およびアジア太平洋地域と中国との関係を悪化させた地政学的な出来事を受けてのことだと考えられます。
- 多数の攻撃活動を Talos が分析したところ、中国政府がより積極的な情報収集を指示しており、それらの地域の標的に対する将来の攻撃に備えている可能性があると思われます。
- 標的のネットワークに深く潜入し、検出やインシデント対応の取り組みを回避するという点で攻撃者は進歩を見せており、攻撃対象の組織にとっては、ネットワークを安全に維持するための負担が増しています。
- ランサムウェアグループが、APT が長く使用してきた侵入方法に厳密に従って標的を侵害している事例を Talos はいくつか確認しました。類似の手口で初期アクセスを行い、ランサムウェアを展開しています。APT とランサムウェアグループの結びつきがあるかどうかは不明ですが、活動の時期と TTP の共通点は、ランサムウェア攻撃者が少なくともスパイ活動の予備知識を持っている可能性を示唆しています。
- 2023 年は、通信事業者、特に中国が戦略的に関心を寄せるグアムや台湾などの地域でサービスを提供している事業者が、中国によるサイバー攻撃活動の上位の標的となりました。通信事業者に不正アクセスすれば複数の重要セクターについて広範な情報を収集できるので、攻撃グループにとっては特に魅力のある標的です。
- 通信事業者の組織構造や被害組織の地理的な位置のために、影響を受けるすべてのネットワークを可視化することに限界があることや、中国の関与を調査したり判断したりする際に触れる政治的な機微などが、多くの場合、インシデント対応者にとって課題になります。

世界各地に現れる APT は依然として活発でしたが、今年の Talos の調査研究の大半は、中国、ロシア、中東に焦点を当てたものでした。このレポートの本セクションでは、それらの調査結果を取り上げます。

Advanced Persistent Threat（APT）：中国

今年は中国とつながりのある APT が非常に活発に活動し、多数の重要な標的のネットワークに巧妙な方法でひそかに侵入しました。Talos の調査によれば、これらの攻撃を実行するグループは、多くの場合、標的のネットワークに長期間アクセスしようとし、標的の検出の仕組みを回避しながら永続性を維持するために複数の手段を確立します。

TTP の中心は検出と犯行主体特定の回避

中国系の APT は、検出された場合やインシデント対応の取り組みに気づいた場合、ネットワーク上での悪意のある活動をかなり減らすようです。足掛かりが検出されないように保ち、標的が強い警戒を解くまで活動再開を待っているものと思われます。このことは、積極的な修復や削除の取り組みと、インシデント対応計画を最新に保つことの重要性を浮き彫りにしています。APT がこのようなアクセスの維持に成功していることは、侵害されたネットワークでの長期の滞留時間によって証明されており、Talos がこの 1 年で調査したある侵入事例では、滞留期間が短くても 7 年でした。これは、この種の攻撃が、標的となる組織に深刻な影響をもたらす可能性があることを示しています。完全に修復するには、多くの場合、すべてのネットワーク資産の包括的な分析、高度なインシデント対応チームによる長期的なサポート、パスワードのリセットやシステム更新など、組織を挙げての対策が必要となります。攻撃を受けた組織がこれらの対策に取り組むことができなければ、もう環境は安全だと組織が感じていることを察知すると、攻撃グループはすぐにひそかに活動を再開する可能性があります。

中国につながりのある APT がこの 1 年間に使用した他の TTP には、検出を回避するための LoLBin、公開された脆弱性の悪用、ネットワークデバイスへの攻撃、共有されているオープンソースや商用ツールの使用などがあり、これらはすべて昨年とほとんど変わっていません。標的の組織にアクセスすることで、これらの APT が数多くの被害者に対する侵害行為を促進していることも継続的に確認されています。攻撃グループは、特に通信事業者に対してこの方法を用いています。

長期的なスパイ活動に続くランサムウェアの展開における新たな動向

Talos は、長期にわたる高度なスパイ活動を目的とした APT グループによる侵入後、別の脅威グループが、外部公開された脆弱性の悪用をはじめとする同様の手段で初期アクセスを取得して被害者のネットワークを攻撃し、その後ランサムウェアのペイロードを展開した例をいくつか観測しました。この動向は、半導体などの特定の業界や、中国が戦略的に重視しているグアムなどの地域で観測されました。これらの事例で 2 つの攻撃グループの間につながりがあるかどうかはまだわかりませんが、いくつかのシナリオが考えられます。

- APT が破壊的な攻撃を行っていることを示している可能性があります。Bronze Starlight や APT41 のように、中国の APT がランサムウェアを攻撃に取り入れている事例はいくつかあります。
- 虎視眈々と金銭的な利益を得ようとしている仲間など、元の攻撃者と関連のある攻撃者で構成されたグループである可能性があります。
- これらのグループが中国とはまったく関連がないこともあり得ます。ただし、後に続くランサムウェア活動の時期や初期アクセスの取得方法の共通点を考えると、その可能性はおそらく低いでしょう。

戦略的提携や資金協力、あるいは、元の攻撃者の方がスパイ活動に必要なノウハウを持っているといった何らかの他の要因により、無関係だった攻撃者が参入した結果にすぎないのかもしれません。そのどれが理由であっても、こうした攻撃は中国に関連する APT 攻撃に危険な破壊的要素が新たに加わった可能性を示しており、この動きが数年前からエスカレートしているというのが Talos の見解です。

猛烈な勢いで拡大する活動は、地政学的な環境の変化に関連している可能性

この 1 年、中国系の APT の活動頻度が高まったのは、部分的には、中国指導部が中国共産党の統治に対する脅威と受け止めた地政学的な要因のためと思われます。活動の増加を定量化するために用いたのは、政府パートナーとの情報共有、CISA との協力プロジェクト、関連インフラに対する攻撃事例、シスコのお客様に影響を及ぼす中国関連の活動に関する優先度の高い調査の件数です。

活動頻度の変化は、これまでとは異なる意図や、ここ数年観測されてない種類の兆候を反映している可能性があります。中国政府は通常、中国共産党の経済的、政治的、戦略的目標を達成するための情報収集を目的としてサイバー活動を指揮しています。「五カ年計画」のように長期的な成長目標として定期的に設定されるものもあれば、中国と他国との関係に基づいて一時的なニーズが発生し、目標が決められることもあります。たとえば、中国と重要な輸出相手国との関係が悪化した場合、中国の攻撃グループはスパイ活動に重点を置きながらも意図的に沈黙し、輸出品が何であれ、開発における自国の信頼性を

「この 1 年、中国系の APT の活動頻度が高まったのは、部分的には、中国指導部が中国共産党の統治に対する脅威と受け止めた地政学的な要因のためと思われます」

Advanced Persistent Threat（APT）：中国

攻撃グループのハイライト：Volt Typhoon

Volt Typhoon は中国系の脅威グループであり、この 1 年、米国の重要インフラ組織や軍事基地を標的とした長期的な活動で話題になりました。

Talos は、グアムの通信事業者を標的とした Volt Typhoon による持続的な侵入を調査しました。グアムには、台湾の防衛にとって重要な米軍基地があります。同グループが少なくとも 1 年半の間、あるサービスプロバイダーと特定の重要顧客のネットワークへの不正アクセスを維持し、データを流出させていたことが調査で明らかになっています。Talos は、この脅威グループの活動を突き止め、その匿名化されたインフラを調査するために公的部門と民間部門のパートナーと継続的に緊密に協力しています。

高めることのできる独自データを漏洩させようとするかもしれません。ある国との関係で対立が深まれば、中国はその国の重要インフラのネットワークに足掛かりを築き、将来の破壊的攻撃に備えるかもしれません。

今年は数々の地政学的な出来事が中国と西側諸国およびアジア太平洋地域との関係に影響を与えたので、中国共産党がより積極的な攻撃活動を指示した可能性があります。Talos は、両地域において戦略的な攻撃の対象にされた組織で発生したインシデントへの対応を集中的に行いました。

深まる中国と西側諸国の溝

今年、中国と西側諸国の溝が深まった大きな要因の 1 つは、中国とロシアの同盟関係です。特に、ロシアとウクライナの戦争におけるロシア政府の行動を、他の世界の指導者たちが激しく非難していることが背景にあります。両国は貿易関係を強化しており、中国からロシアへの輸出が急増したことで、ウクライナ侵攻以来ロシアに課されていた数々の西側諸国の制裁措置の影響が緩和されています。ロシアと中国は、中東や発展途上国で存在感を拡大する目的でも結束しており、2023 年 3 月にはオマーン湾で合同軍事演習を行い、2023 年 8 月には多数の国々に BRICS グループへの加盟を要請して西側諸国との競争に対抗する貿易圏を強化しています。

中国に関する米国の政策や立場は今年に入っても軟化しておらず、米国は引き続き中国を安全保障上の最大の脅威と位置づけています。2023 年に米国家情報長官が中国を米国の国家安全保障にとって「最も重大な脅威」と指摘し、米国はそうした懸念から中国企業や組織に対する制裁を着実に拡大してきました。こうした安全保障上の問題は、2023 年初頭に中国の偵察気球がアメリカ上空を飛行して軍事基地から情報を収集し、撃墜される前に収集した情報を中国政府に送った事件で実証されています。2023 年に日米韓 3 か国も同盟関係を強化し、8 月にはキャンプデービッドで首脳会談を行い、中国と北朝鮮からの安全保障上の課題に協力して取り組むことを約束しました。中国政府はこの会談を即座に批判し、アジア太平洋地域で軍事ブロックを形成しようとする試みは「警戒と反発」を招くだろうと声明を発表しました。

アジア太平洋地域で深まる対立

一方、中国はすでにアジア太平洋地域の近隣諸国との対立に直面しています。中国と台湾の緊張が高まっており、台湾の自衛能力拡大を米国が支援していることで関係が悪化しています。人民解放軍は台湾への軍事的圧力を強め、日常的に台湾海峡の中間線を越えて戦闘機、無人機、船舶を送り込み、軍事力を誇示しています。中国は南シナ海でもますます強硬姿勢を取るようになっており、係争地域のほぼ全域に対する領有権の主張を強めています。この 1 年間を通して、この地域における中国の強力な軍事的存在感は、領土をめぐって相反する主張を行う近隣諸国および駐留米軍との膠着状態と対立を招いてきました。最後に、この 1 年は、中国と日本の関係も困難に直面しています。日本が半導体の輸出を制限したり、日本政府が福島第一原子力発電所の処理水放出を決定して中国政府から批判を浴びたりしました。

通信事業者を狙って情報収集を拡大し、将来の攻撃の下準備を進める攻撃グループ

Talos は今年、特に中国政府が戦略的に関心を寄せている分野で、中国系の APT による通信事業者への侵入事例に何度か対応しました。

通信事業者は、国の衛星システム、インターネットサービス、電話網など、民間部門と公共部門にとって極めて重要なその国の重要インフラ資産を多数管理していることが多いため、APT グループにとっては魅力的な標的です。標的国との紛争が発生した場合に、中国系の APT が不正アクセスを利用して足がかりを築き、通信インフラなどの重要なサービスを停止させる可能性があります。また、中国政府が関心を寄せる他の重要な標的のネットワークに侵入し、広範な機密データを流出させるかもしれません。

後者の手口を使用して修復作業を困難にする方法が複数あります。ネットワークに侵入されたことにサービスプロバイダーがすぐに気づかなかったり、他の企業や加入者、サードパーティの通信事業者に対する不正アクセスの範囲まで可視化できていなかったりする可能性があるため、ネットワークのさらに深くに潜入する十分な時間を攻撃グループに与えてしまいます。不正アクセスを顧客に通知するガイダンスも国によって異なるので、最初の被害者の地理的位置によってはインシデント対応が遅れる可能性があります。最後に、攻撃を受けた国と攻撃した国が微妙な外交関係にある可能性を考慮すると、米国を拠点とするインシデント対応チームが特定の地域で支援を行う際に、課題や政治的な機微に直面することも考えられます。国によっては被害者が特定の脅威グループの犯行だと断定するのをためらうことも考えられ、中国と強い組織的なつながりがある可能性も否めません。侵害の重要な詳細情報を米国のチームと共有することを警戒する可能性もあります。

CISCO TALOS

一年の総括

2023

Advanced Persistent Threat（APT）：ロシア

本セクションのハイライト

- ロシア政府の支援を受ける APT グループ Gamaredon は依然としてウクライナに対する重要プレーヤーであり、Cisco Talos ウクライナタスクユニットが今年対応した脅威としては最多となりました。
- 2023 年、Gamaredon は主に北米と欧州の組織を標的にし、西ヨーロッパで被害者数が突出して多くなりました。さらに、標的となった組織の半数以上が運輸部門と電力部門であり、これはロシアが重要インフラに重点を置いていることを反映しています。
- ロシア政府系の別の APT グループである Turla は、2022 年 9 月から 2023 年 2 月にかけて活発に活動していましたが、米国司法省が Turla の Snake マルウェアを無効化したのと時を同じくして、2023 年 5 月頃にその活動を大幅に縮小しました。
- 両グループでは、影響を受けた部門の数と被害者数が大きく異なっており、Gamaredon が広範な標的を攻撃しているのに対し、Turla は攻撃対象をかなり絞って活動しています。
- Gamaredon と Turla の活動以外にも、4 月下旬から 5 月上旬にかけて、多種多様なグループが使用する SmokeLoader マルウェアの活動が急増したことが確認されており、ウクライナの組織を標的として SmokeLoader が大量に配布されているというウクライナのコンピュータ緊急対応チーム（CERT-UA）の報告と一致しています。
- 戦場における全地球測位システム（GPS）ジャミングの影響を受けたウクライナの送電網を安定させるため、シスコのハードウェアとソフトウェアのエンジニアはシスコの商用ネットワークスイッチの 1 つを改造し、停電中はウクライナの送電網設備がホールドオーバー状態になるようにしました。

Advanced Persistent Threat（APT）：ロシア

ロシア政府の支援を受けた APT や政府に同調する APT による脅威は、今年も Talos の脅威の追跡と調査活動の中心をなしています。ロシアによるウクライナ侵攻が始まって以来、ロシアの APT によるサイバースパイ活動、サイバー影響工作、破壊的攻撃への関与が強まっています。ロシアの APT は、昨年のレポートで報告した活動に沿った形で、戦争および NATO とその同盟国によるウクライナへの軍事支援に起因する地政学的な課題への適応を続けています。さらに 2023 年には、法執行機関による世界的な取り組みによって Snake マルウェアが無効化されました。これは、ロシア連邦保安庁(FSB) の攻撃ツール群の中でも最も多用された高度なサイバースパイ活動ツールの 1 つと考えられており、世界中のシステムに対して広く展開されていたマルウェアです。

Gamaredon と Turla が今年も上位の脅威、攻撃対象選定のパターンは異なる

ロシア系 APT グループの Gamaredon と Turla は、ロシアのサイバー脅威に対抗する国際的な取り組みが行われているにもかかわらず、TTP を強化する攻撃手法とツールキットを更新しながら、この領域における上位の脅威であり続けています。

Cisco Talos は、APT の Gamaredon に関連する活動を注意深く追跡しています。Gamaredon は、クリミアを拠点に活動するロシア政府の支援を受けた攻撃グループだと一般的に考えられています。ここ数か月、同グループはウクライナの組織に対するサイバースパイ活動に力を注いでいますが、この領域で活動するロシアの他の APT ほどは攻撃対象を絞らず、世界各地の組織を標的にしています。Turla もまた、ロシア諜報機関の優先事項に沿った長期的なスパイ活動やデータ漏洩を目的とした活動を行っており、米国政府は FSB の 1 部隊と見なしています。Turla は、さまざまな部門を標的にしていることが 2023 年に観測された Gamaredon（図 10）とは対照的に、戦略的に重要な少数の組織に対して、かなり的を絞った活動を展開することで知られています。Turla は、Gamaredon が代理で活動している FSB の部隊とは別の部隊に代わって活動していると一般に考えられています。Turla には、おそらく世界中のもっと広範な組織を侵害する能力がありますが、価値が高いと考える対象に攻撃を限定しています。

Talos のテレメトリを基にすると、Gamaredon と Turla が標的にした部門の数と被害者数は大きく異なっていました（**図 10、図 11**）。

図 10

Gamaredon の標的となった業界

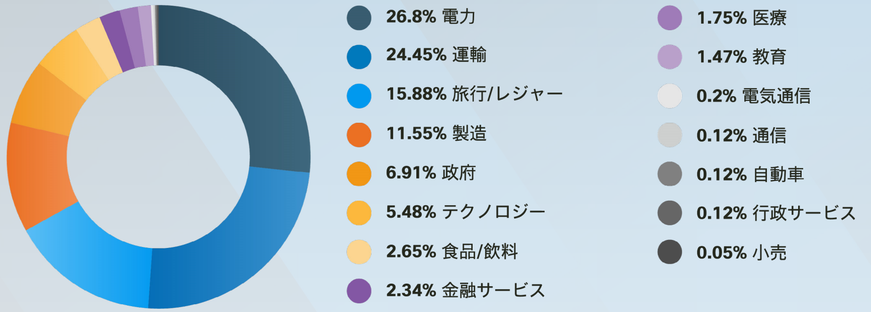
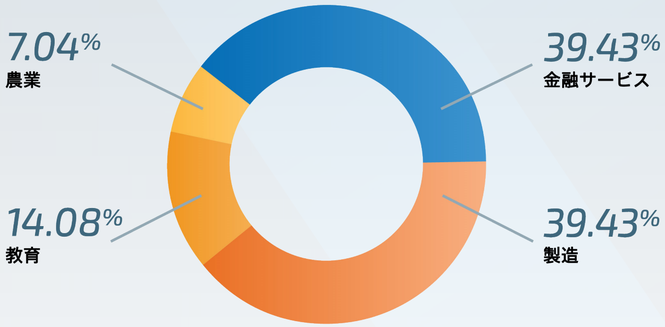


図 11

Turla の標的となった業界



注：割合は四捨五入されているため、合計が 100% にならない場合があります。

Advanced Persistent Threat（APT）：ロシア

図 12

1 年間の Gamaredon の悪意のあるダウンロードの件数

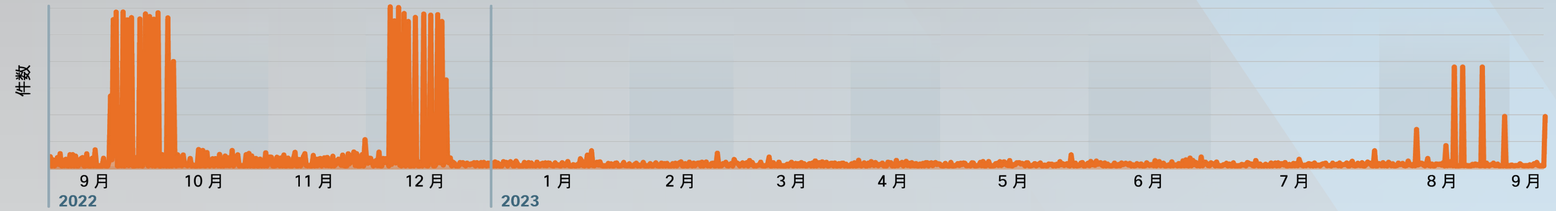
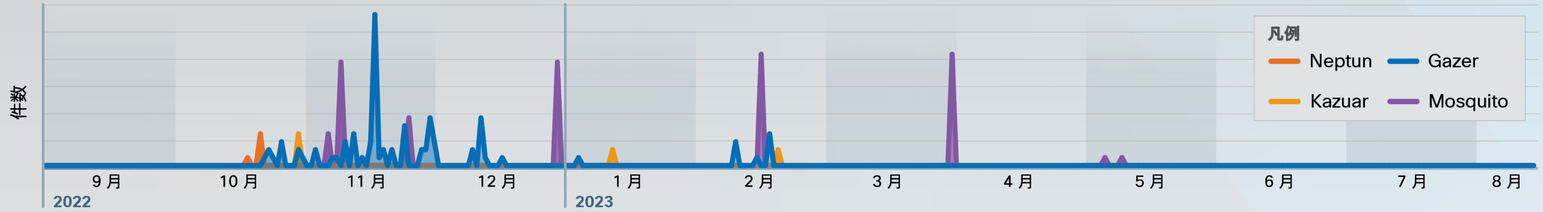


図 13

Turla のマルウェア亜種 Gazer、Kazuar、Mosquito、Neptun の 1 年間の活動



「このデータは、Gamaredon と Turla が今年標的とした部門を浮き彫りにするだけでなく、Snort が防止に役立った攻撃の量もおおむね表しています」

Gamaredon の被害者は北米が最も多く、次いで欧州、中東と続き、西ヨーロッパで被害者数が突出して多くなりました。Gamaredon の攻撃活動の半分以上が電力部門と運輸部門に影響を与えるものでした。これは、ロシアが重要インフラ組織を標的にしている状況と一致しています。その狙いはおそらく、戦略的な組織に最大の混乱を引き起こし、ウクライナの戦争努力を妨害することにあります。

Gamaredon の活動には 2022 年 9 月と 12 月、そして 2023 年 9 月に、はっきりと 3 回の急増が見られました **（図 12）**。これは、特定の標的を対象とした集中的な活動である可能性があります。図 12 に見られるように、2023 年 8 月に Gamaredon の活動が活発化したことは、ウクライナの国家サイバーセキュリティ調整センター（NCCC）のレポートによる同グループの活動レベルと一致しています。

Gamaredon が今年標的にした業種の広さとは対照的に、Turla は同グループの作戦に忠実に、より少ない業種と地域に対して攻撃を行いました。製造業と金融サービス業が同じ割合で最も影響を受け、教育と農業が受けた影響はそれよりも少なくなっています **（図 11）**。このデータは、Gamaredon と Turla が今年標的とした部門を浮き彫りにするだけでなく、Snort が防止に役立った攻撃の量もおおむね表しています。

持続的アクセスに使用されるさまざまなバックドアやインプラントなど、Turla が展開したカスタムマルウェアが、主に 2022 年 9 月から 2023 年 2 月の間に発生した一連の出来事で集中的に確認されました。この期間に活動が活発化した理由は不明ですが、ロシアのウクライナ侵攻を受けて活動頻度が高まったことに起因している可能性があると考えています。この 4 つのマルウェアファミリ（Gazer、Kazuar、Mosquito、Neptun）は、Turla のマルウェアを網羅しているわけではなく、Turla のカスタムマルウェアや改造されたオープンソースマルウェアの豊富な攻撃ツール群の一部であり、常に更新され、より高度なバージョンに置き換えられています。

図 13 に見られるように、Turla のカスタムマルウェアの活動が経時的に変化して集中発生していることは、Turla の活動頻度の傾向を伝え続けており、これは標的の選定と密接に関係している可能性があります。注目すべきは、図 13 にグラフで表示されている Turla のマルウェア活動が（すべて網羅しているわけではありませんが）、2023 年 5 月頃に大幅に減少していることです。これは、米国司法省が Turla の Snake マルウェアを無効化した時期と一致しています。

Turla は 20 年近くにわたって Snake を展開し、世界中に散らばる多数のリレーノードを通じて、標的のシステムからデータを盗み流出させました。Snake の無効化が Turla の現在および将来の活動に及ぼす影響はまだ不明ですが、無効化の結果、マルウェアの活動が減少して Turla のツールキットが変わったことを表している可能性があります。

図 14

ウクライナタスクフォースの調査による上位の脅威

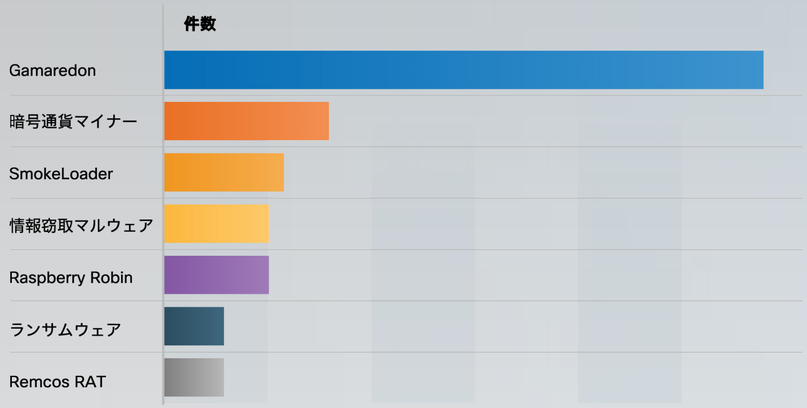
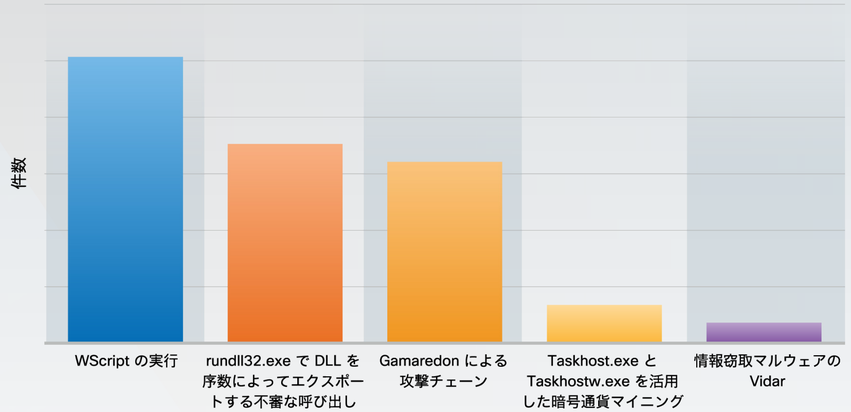


図 15

ウクライナのパートナーに影響を与えた悪意のあるアクティビティのトップ 5



Talos のタスクユニットがウクライナに対する脅威を継続的に監視

Talos によるウクライナへの継続的な支援は、今年も引き続き業務上の取り組みの大きな焦点です。タスクユニットの活動の一環として、ウクライナの重要インフラ部門（政府、電力、金融サービス、医療、運輸などが中心）の約 30 のパートナーのエンドポイントテレメトリにおける不審な活動を監視しています。

これらの組織に対する脅威がすべて APT の活動を示すとは限りませんが、展開されている脅威の量と不安定な地政学的情勢は、重要な資産を守るネットワーク防御担当者に重大なリスクをもたらしています。

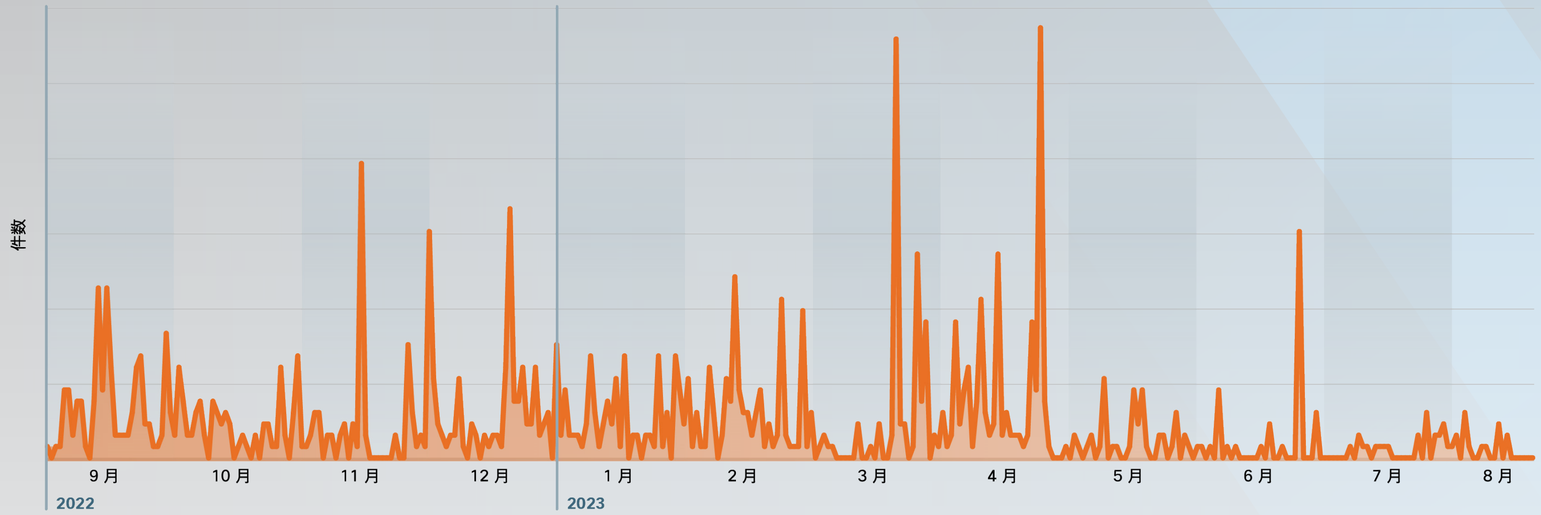
Talos のタスクフォースが対応したウクライナに対する脅威の中で最も多く確認されたのは Gamaredon です **（図 14）**。同グループは以前からウクライナの組織、特に国防、外交、国内治安を担当する組織を主な標的としています。

Gamaredon とその攻撃チェーンの一部は、ウクライナのパートナーに通知される Cisco Secure Endpoint からの脅威ハンティングアラートで常に上位に登場しています（図 15）。たとえば、この図に示すトップ 5 のアクティビティは、LoLBin とこれに関連する Wscript の実行などの手法が一貫して使用されていることを示しています。Wscript は正規の Windows プロセスであり、マルウェアの展開を問題のないアクティビティに見せかけるために使用されることがあります。こうした手口が、攻撃ライフサイクル全体でさまざまな脅威をサポートするために引き続き使用されています。また、暗号通貨マイニングや情報窃取マルウェアなどを展開する金銭目的のサイバー犯罪者が関わっていることの多い活動も、ウクライナのさまざまな業種の組織に影響を与え続けており、ウクライナが直面する脅威が幅広いことを物語っています。

Advanced Persistent Threat（APT）：ロシア

図 16

1 年を通した SmokeLoader マルウェアの活動



「ウクライナのパートナーを守るために Talos が投入し続けているサイバー防御のリソースは、この脅威領域にも間違いなく大きな影響をもたらしており、初期段階で攻撃を緩和することによって重大な混乱を防止しています」

図 14 と図 15 は、Gamaredon の活動が一貫して行われたことを強調しているだけでなく、タスクユニットが今年対応した脅威の多さも示しています。具体的には、ローダー、情報窃取マルウェア、ランサムウェア、暗号通貨マイナー、Raspberry Robin などのマルウェアの脅威による活動です。Raspberry Robin は、昨年の年次レポートでも取り上げた多用されているマルウェアファミリであり、引き続き一貫して企業環境への脅威となっています。たとえば SmokeLoader は、今年タスクユニットが繰り返し対応してきた、さまざまなグループが利用しているダウンローダーです **(図 14)**。通常、SmokeLoader はメールで送り込まれ、感染したマシンにマルウェアをドロップします。このことは 5 月初旬以降、ウクライナのコンピュータ緊急対応チーム（CERT-UA）から一貫して報告されており、脅威環境における SmokeLoader の持続的な使用がさらに浮き彫りになっています。

4 月下旬から 5 月上旬にかけて SmokeLoader の活動が急増したことが確認されており、ウクライナの組織を標的として SmokeLoader が大量に配布されているというウクライナのコンピュータ緊急対応チーム（CERT-UA）の報告と一致しています。

ロシアとウクライナの戦争が始まって以来、タスクユニットは継続的に無数のサイバー脅威に対応してきましたが、2023 年に観測された活動は、Talos が通常この領域で目にすることが予想される高度な攻撃者に関連する脅威よりもはるかに能力面で劣っていました。今年の活動は活発でしたが、ロシアがウクライナや NATO の同盟国に対してこれまで示してきた非常に広範な破壊的サイバー能力を反映してはいません。この背後にある理由は、業界のパートナーや専門家によって議論されてきましたが、おそらく、サイバーセキュリティ業界、米国政府、他国のパートナー、そして自国民を守るというウクライナ自身の強い信念が一体となった取り組みの結果と思われます。ウクライナのパートナーを守るために Talos が投入し続けているサイバー防御のリソースは、この脅威領域にも間違いなく大きな影響をもたらしており、初期段階で攻撃を緩和することによって重大な混乱を防止しています。

Advanced Persistent Threat（APT）：ロシア

Project PowerUp：ウクライナで明かりを灯し続ける活動

Talos は、産業界、政府、ウクライナとの独自の関係を活かして、戦場における GPS ジャミングの影響を受けたウクライナの送電網を安定させるための取り組みの最前線に立ってきました。

GPS 信号の停止による運用障害にウクライナの変電所がいかに耐えられるようにするかという複雑な問題に直面したシスコのハードウェアとソフトウェアのエンジニアは、シスコの商用ネットワークスイッチの 1 つであるシスコの産業用イーサネットスイッチを改造し、停電中はウクライナの送電網設備がホールドオーバー状態になるようにしました。

数か月にわたる開発とさまざまなパートナーとの調整を経て、デバイスがウクライナに届けられ、国内各地の変電所に設置されました。現在も戦闘が続く地域では並大抵のことではありませんでした。今年後半のシスコの年次パーパスレポートで、この活動について紹介する予定です。この事例は、2023 年のロシアの激しいサイバー攻撃からウクライナの重要インフラを守るために、シスコの取り組みがいかに役立ってきたかをさらに証明するものです。

GPS が停止するとウクライナの送電網にどのような影響が出るのか

ウクライナ国内の送電事業で重要な役割を担う多数の高圧変電所では、正確な GPS 時刻情報が幅広く活用されているからです。送配電事業者は複雑な高圧送電網についての予測、対応、診断を行うために GPS 時刻情報を役立てています。GPS 信号が広範囲にわたって妨害されると、正確なタイムスタンプを割り当てられなくなるため、変電所では報告された時刻情報を正確に同期できません。正しく同期されたデータがなければ、システムの異なる部分間で負荷を割り振る作業に影響が及びます。特に需要のピーク時や急激な電圧変化が発生した場合には、停電や故障を避けるために負荷処理が必要です。この妨害は広範囲に及ぶことがあり、そうなれば広い地域で長時間 GPS サービスが使用できなくなります。

Advanced Persistent Threat（APT）：ロシア

図 17

攻撃グループ YoroTrooper の概要

別名	不明
所属	カザフスタン
活動開始時期	2022 年
目標	国家の目標をサポートするためのスパイ活動とデータ窃取
被害状況	特に独立国家共同体（CIS）加盟国を中心とした欧州の政府機関
注目すべき TTP	ソーシャルエンジニアリング、スピアフィッシング、データ漏洩、カスタムツール、コモディティ型マルウェア
マルウェアとツール	YoroTrooper は AveMaria/Warzone RAT、LodaRAT など、さまざまな独自開発のコモディティ型マルウェアファミリを採用

YoroTrooper のメンバーの一部はカザフスタン出身の親ロシア派

今年初め、Cisco Talos は新たな攻撃グループに関する情報を公開しました。Talos が「YoroTrooper」と名付けたこの攻撃グループの少なくとも一部のメンバーはカザフスタン出身だとほぼ確信しています。YoroTrooper は強い動機を持っており、その攻撃能力の低さを、多数の汎用マルウェアファミリを使用して積極的に組織に対する攻撃を仕掛けることで補完しています。同グループは 2022 年以降、アゼルバイジャン、タジキスタン、キルギスタン、その他の独立国家共同体（CIS）加盟国の政府機関やエネルギー部門の被害者に対して、スパイ活動やデータ窃盗を目的とした活動を行っています。

ロシアの同盟国による APT 活動

地域の脅威に対する Talos の調査や監視は、かつてソビエト連邦の一部であった国々による APT 活動まで対象を拡大しています。それらの APT の諜報目標、TTP、被害者像はロシア政府のものとだいたい一致しています。これらの政府間の長期にわたる政治的結びつきを考えれば、協力は不思議ではありません。ただし、ロシア政府の関与を示す直接的な証拠はありません。

Talos は、YoroTrooper が欧州とトルコ政府の戦略的価値が高い組織も標的にしていると考えています **（図 17）**。例を挙げると、欧州連合（EU）の重要な医療機関や世界知的所有権機関（WIPO）など、少なくとも 2 つの国際機関のアカウントを侵害しています。他にも、アゼルバイジャンやトルクメニスタンなど欧州諸国の大使館サイトの侵害に成功しています。

Talos は今年、CERT-UA がベラルーシ政府と関係があるとしている GhostWriter の攻撃活動も監視しています。ウクライナとポーランドの政府機関、軍事組織、民間人に対する GhostWriter の攻撃が数回確認されました。このような活動は、地域の安全保障協力を弱体化させることを目的に反 NATO の主張を煽っていると見られがちですが、情報を盗み出し、持続的なリモートアクセスを得ることを目的としている可能性が非常に高いと Talos は判断しています。CERT-UA によって追跡された最近の活動でも、WinRAR ZIP の解析に関する脆弱性（CVE-2023-38831）の悪用が確認されています。この脆弱性を利用して、攻撃者は JPG や TXT ファイルなどの一般的なファイル形式を装った ZIP アーカイブに悪意のあるコードを隠すことができ、GhostWriter はこれを利用して Cobalt Strike とマルウェアダウンローダーの PicassoLoader を展開しました。

現時点では、YoroTrooper や GhostWriter へのロシアの関与を否定できません。こうした活動と攻撃対象選定のパターンはロシアの戦略的利益と強く合致しているものが多く、ロシアのウクライナ侵攻を背景とした地域の脅威について理解するための鍵になります。

CISCO TALOS

一年の総括

2023

Advanced Persistent Threat（APT）：中東

本セクションのハイライト

- 2023 年 10 月初旬のハマスとイスラエル間の出来事が一因となり、政治的動機に基づく複数のハクティビストグループが、協調性がなく、多くは高度とは言えない攻撃を両陣営に対して開始しました。これと同じようなことが、ロシアとウクライナの戦争が始まった際にも観測されました。
- 中東の複雑な地政学的環境は、今年も変動的な状況が続きました。これが今後のサイバー領域に影響を与えることが予想されます。この地域の長年にわたる敵対国が関係を正常化しようとしている中、数十年来の紛争が新たな暴力を引き起こしているため、中国やイランのような中東に経済的、政治的利害を持つ重要なサイバープレーヤーが、直接的な活動または代理による活動を通じて、結果に影響を与えようと意欲を高める可能性があります。
- 中東を拠点とする APT グループは、この地域の通信会社を標的としており、Talos がこれまで観測してきたこの分野を標的とする高度な攻撃グループの動向と合致しています。この活動において、Talos が HTTPSnoop および PipeSnoop と名付けた新しいインプラントを関連組織に展開する新しい侵入セットの ShroudedSnooper が特定されました。
- イラン政府の支援を受けた APT グループの MuddyWater は、リモートアクセスやマルウェアの展開に不可欠な、一般的に使用されている Syncro 社のツールを例年と比べてあまり使用していません。これは、MuddyWater の既知の TTP に対するサイバーセキュリティ業界の措置に対応したものと思われます。

Advanced Persistent Threat（APT）：中東

この地域の国家の支援を受けたグループによる、北米、欧州、中東、アジアの組織に対する広範なサイバー攻撃が続いています。攻撃の大部分を受けたのは通信会社です。本レポートの他の部分で概説したように、複数の APT に見られる傾向です。この領域での Talos の調査が、新たな攻撃グループの発見につながりました。Talos が ShroudedSnooper と名付けたこの攻撃グループはこの地域の主要な通信事業者を標的としていると思われます。イラン政府の支援を受けた APT グループの MuddyWater が引き続きこの脅威領域における重重要プレーヤーであり、今年の Talos の調査活動の多くは MuddyWater に焦点を当てたものでした。同グループは知的財産の窃取と情報収集という主要な目標を達成するために、同じ手法の多くを使い続けますが、業界の取り組みが、同グループの特定のツールを使用する能力に影響を与えている可能性があります。たとえば 2022 年末に使用されていたリモート管理およびモニタリング（RMM）プラットフォームである Syncro などのツールです。

中東は間違いなく世界で最も複雑な地政学的地域であり、2023 年 10 月にハマスとイスラエルの間で勃発した紛争は、世界的な影響を及ぼす出来事がほぼ前触れなく急速に展開することを思い出させます。この地域の常に変化する地政学的情勢が今後のサイバー活動に影響を与えることは間違いありません。これは、イランなど、地域の既存のプレーヤーが引き続き特定の地政学的目標を達成しようすることに加え、中国のような新たな攻撃主体もその影響力を拡大しようとするためです。

ハマスとイスラエルの紛争でハクティビストグループが多数参入

ハマスが 10 月にイスラエルに仕掛けた奇襲攻撃は、世界的に影響を与えただけでなく、サイバー領域にも影響を及ぼし、紛争の両陣営の攻撃グループを即座に引き込みました。政治的な動機に基づくハクティビストグループとして有名なのは Killnet や Anonymous Sudan のような攻撃グループですが、あまり知られていないグループもいます。脅威領域が瞬く間に多くの異なる攻撃グループで溢れかえったので、当初は協調性がなく、多くは高度とは言えない攻撃が開始されました。複数のハクティビストグループが、イスラエルとハマスの紛争における両陣営への支持をすぐに表明し、脅迫的な政治的メッセージを投稿して追随者に参加を呼びかけ、関心のある標的に対する DDoS 攻撃を担うと主張しました。これは典型的なハクティビストの TTP です。これとほぼ同じことが、ロシアとウクライナの戦争が始まったときに観測されており、サイバー活動がまるで一夜にしてこれらの国々に集中して流入したかのようでした。

このような地政学的に重要な出来事は、外国政府による支援と資金提供を受けている攻撃グループを含め、より高度な攻撃者の参加も招きます。ごく最近ではウクライナでこの状況を目にしており、Gamaredon や Turla など、ロシア政府の支援を受けた高度な組織が戦争の勃発以来、ウクライナの組織を執拗に攻撃しています。同様に、ハマスのイスラエル攻撃を受けて、中東におけるイランのサイバー活動が活発化することが予想されます。イランとイスラエルは長年敵対関係にあり、数十年来の対立がイランのサイバー活動に大きな影響を与えています。イランは、ハマス、ヒズボラ、パレスチナのイスラム聖戦など、反イスラエルの複数の過激派やテロリスト集団の主要な支援者でもあります。いずれも、ごく最近のイスラエルに対する多数の暴力に関与してきました。これらのグループに対するイランの支援とイラン政府がイスラエルに抱く歴史的な敵意からすると、イランが今回の危機の結果に影響を及ぼすために自国のサイバー能力を用いる可能性は十分にあります。外交政策の目標を推進するための不可欠なツールとして、他の国々がサイバー攻撃に依存するのとほぼ同じことです。

「イラン政府の支援を受けた APT グループの MuddyWater が引き続きこの脅威領域における重要プレーヤーであり、今年の Talos の調査活動の多くは MuddyWater に焦点を当てたものでした。同グループは知的財産の窃取と情報収集という主要な目標を達成するために、同じ手法の多くを使い続けますが、業界の取り組みが、同グループの特定のツールを使用する能力に影響を与えている可能性があります」

Advanced Persistent Threat（APT）：中東

サイバー活動の可能性を予感させるこの地域での中国の野望

中国は従来から中東での最大の投資国の 1 つとして重要な経済的役割を担ってきましたが、中国指導部はこの 1 年、地域の紛争調停に関与することで、この地域における政治的存在感の拡大も図りました。3 月、中国政府の仲介により、長年敵対してきたイランとサウジアラビアが国交正常化に合意しました。9 月には、シリアのバッシャール・アサド大統領が 10 年以上にわたる残忍な内戦を経て国際社会に復帰し始めていることを受け、中国とシリアが戦略的パートナーシップを結んだと発表しました。この中国とシリアの協定は、中国政府にも大きな経済的インセンティブをもたらす可能性があり、中国がシリアの復興活動の主要な資金援助者になる可能性があります。中国によるこうした戦略的な動きは、9.11 後の時代に続いて米国がこの地域からほぼ撤退した時期に行われているもので、中国政府はこれを、米国の関与と影響力の低下を利用する好機と見ているようです。

中東における中国の政治的存在感が高まっているため、この地域で中国の APT 活動がより活発になることが予想されます。Talos は、国家の支援を受けた脅威の中でも最も活発かつ持続的な中国の APT が、投資先の地域でのスパイ活動によって財政努力を補い、経済的目標に合致した知的財産を持つ民間部門の組織や政府を標的にしていることを確認しています。今後の活動は中国の APT の確立された TTP と一致したものになる可能性があります。たとえば、中国の戦略計画に不可欠な産業で活動する組織や個人を標的にする、標的のネットワークへの長期的かつ秘密のアクセスを確立する、知的財産と技術を盗む、といったことです。

図 18

OfficeCore 社の LBS System を装う HTTPSnoop の URL

```
'http://+:80/1bsadmin/valve/',0
'http://+:80/1bsadmin/salon/',0
'http://+:80/1bsadmin/disorder/',0
'http://+:80/1bsadmin/cute/',0
'http://+:80/1bs/alpha/',0
'http://+:80/lbs/special/',0
'http://+:80/1bs/blue/',0
'http://+:80/1bs/mystery/',0
'http://+:80/1bswap/army/',0
'http://+:80/1bswap/problem/',0
'http://+:80/1bswap/goose/',0
'http://+:80/1bswap/useful/',0
```

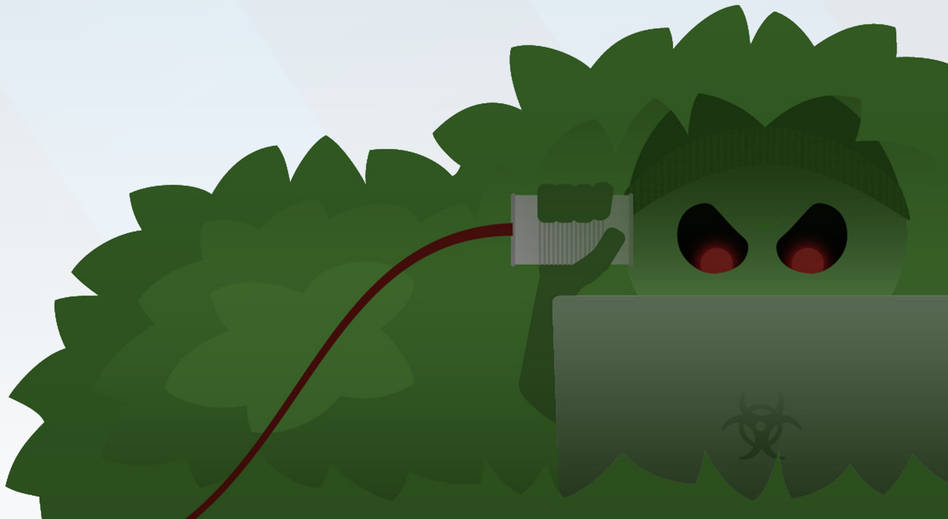
中東における中国の政治的存在感が高まっているため、この地域で中国の APT 活動がより活発になることが予想されます。

地域の攻撃グループの主な標的は引き続き通信分野

2023 年、Talos は新しい侵入セットの ShroudedSnooper を発見しました。中東の通信事業者に対して HTTPSnoop と PipeSnoop という新たなバックドアインプラントを展開するものです。Talos が監視してきた、高度な攻撃グループが通信分野を繰り返し攻撃するという傾向が続いています。今のところ、ShroudedSnooper の活動を特定の国に結びつける十分な証拠はありません。ただし、同グループがこの地域の通信会社で使用されているソフトウェア アプリケーションを一貫して偽装し、地域の複数のプロバイダーに影響を及ぼしていることは、世界中の、おそらく国家の支援を受けている攻撃グループや高度な攻撃グループと非常によく合致しています。

HTTPSnoop と PipeSnoop のインプラントで新たに採用されている手法は、特定の HTTP（S）の URL に対する着信リクエストを待ち受け、感染したエンドポイントで実行するというものです。HTTPSnoop インプラントの中には、特に通信会社向けに販売されている OfficeTrack を装った URL を使用するものもあります。OfficeTrack は、ユーザーによる管理タスクの管理を支援するソフトウェア会社である OfficeCore 社によって開発され、ワークフォースマネジメント ソリューションとして販売されているアプリケーションです。URL の末尾が「lbs」や「LbsAdmin」になっているものがありましたが、これはブランド名が OfficeTrack に変わる前のアプリケーション名（OfficeCore 社の LBS System）を表していると思われます **（図 18）**。

Talos が分析した ShroudedSnooper のインプラントでは、攻撃者はイスラエルの通信事業者を含む通信会社のプロビジョニングサービスを模倣したパターンで構成される URL を複数使用していました。一般的なネットワークトラフィックと間違える可能性が高い URL です。HTTPSnoop の DLL ベースの亜種は通常、無害なアプリケーションやサービスの DLL を悪用して、感染したシステムで起動させます。これは、今年最も用いられた手法として、本レポートの初めのセクションで取り上げたものです。



Advanced Persistent Threat（APT）：中東

業界の取り組みが MuddyWater の活動に影響を与えた可能性

2022 年後半に、イランの支援を受けた APT グループ MuddyWater がリモート管理ツールの Syncro を利用して標的のデバイスを乗っ取っていたことが初めて報告されました。これは 2022 年第 4 四半期（2022 年 10 月～ 12 月）の Talos IR のデータと一致しています。当時、Syncro を使用する攻撃者が増加していて、約 30% のインシデント対応業務で確認されました。

2022 年 12 月、Syncro 社は声明を出し、中東およびアジアの組織を標的としたスピアフィッシング攻撃で MuddyWater が Syncro が展開されていることに懸念を表明しました。同社は、不正ユーザーによる Syncro の利用を制限するために、新規のトライアルアカウントの作成について追加の検証手段を導入し、不正なアカウント情報や利用状況を監視して、これらの新しいポリシーに違反するアカウントを停止しました。

Syncro 社がとったこの迅速な措置が MuddyWater の活動に影響を与えたことは間違いなく、業界が高度な攻撃者の活動の一部を阻止して直接的な効果をもたらし得ることを浮き彫りにしています。2022 年第 4 四半期に Syncro の利用が増えた理由は不明ですが、マネージド サービス プロバイダー（MSP）向けのフル機能を搭載したリモート アクセス プラットフォームとして使用されていること、また企業環境全体で利用できることから、魅力的な選択肢になったと思われます。

「Syncro 社がとったこの迅速な措置が MuddyWater の活動に影響を与えたことは間違いなく、業界が高度な攻撃者の活動の一部を阻止して直接的な効果をもたらし得ることを浮き彫りにしています」

アクセスの維持に利用された Syncro

Talos IR は、ある通信会社に影響を与えたインシデントで「スタッフ昇格」という件名（アラビア語からの翻訳）のフィッシングメールを送信している同社のメールアカウントを特定しました。このメールには、Syncro のインストールに使用された Microsoft Windows インストーラ（MSI）の圧縮ファイルが格納されている OneDrive と OneHub のフィッシングリンクが記載されていました。攻撃者は Syncro を使用して、標的のユーザーのワークステーションへの接続を維持しました。MSI ファイルの分析中に、SyncroRecovery（SyncroLive）や SyncroOvermind など、複数の Syncro サービスもインストールされたことを確認しています。攻撃者の戦術は、Syncro のインストールによる初期アクセスの維持に重点を置いているように見えました。メールへのアクセスに対し MFA が行われないため、フィッシング攻撃が可能になっていました。これは、すべての重要資産において MFA を確実に行う必要があることを浮き彫りにしています。

CISCO TALOS

一年の総括

2023

コモディティ型ローダー

本セクションのハイライト

- Qakbot、Ursnif、Emotet、Trickbot、IcedID などのコモディティ型ローダーは、最も影響力が大きい、広く使用されている脅威であり、活動の重要な部分を実現するために攻撃者が日常的に多用しています。これらのローダーは、情報窃取マルウェア、ランサムウェア、他のマルウェアのダウンローダーとして使用されているので、脅威環境の主役になっており、世界中の組織に無差別に影響を及ぼしています。
- いずれも、以前はバンキング型トロイの木馬として機能するだけでしたが、開発者が近年機能を多様化し、より高度な活動をサポートできるようになっています。IcedID、Ursnif、Qakbot の新バージョンは 2023 年にランサムウェアの攻撃者専用にカスタマイズされたと考えられます。これは、偵察機能が強化され、ウイルス対策による検出を引き起こしそうな機能が削除され、ランサムウェアグループや初期アクセスブローカーによって迅速に採用されていることに基づく判断です。
- Microsoft 社がマクロをデフォルトで無効にしたため、コモディティ型ローダーの攻撃者は、検出されずにマクロを使用する新しい方法を編み出したり、マクロの使用を完全に避けたりするようになりました。Qakbot の攻撃グループは、多種多様なファイルタイプ、スクリプト言語、パッカー、エクスプロイトを使用してローダーを展開しました。Qakbot に比べ頻度は少ないながら、Emotet、IcedID、Ursnif も手法を変えましたが、依然として古い TTP に頼る傾向がありました。
- コモディティ型ローダーの脅威は、たとえそのボットネットを解体したとしても根絶が難しいかもしれません。というのは、開発者が別のマルウェアグループに代わって活動を続けたり、ボットネットを再構築したりすることが知られているからです。さらに、以前に侵害されたインフラが、他の攻撃グループによって悪意のある活動に利用される可能性もあります。

コモディティ型ローダー

攻撃者は、何年もの間一貫してコモディティ型ローダーを多用しており、2023 年も状況は変わりませんでした。これらの脅威の多くはいろいろな地下フォーラムで購入できるので、スキルの低い攻撃者にとっての参入障壁が低くなっています。また、高度にモジュール化されているため、攻撃者は多段階の攻撃を実行できます。2023 年を通して、この領域で最も影響力が大きかった脅威としては、Qakbot、Ursnif、Emotet、Trickbot、IcedID が突出していました。

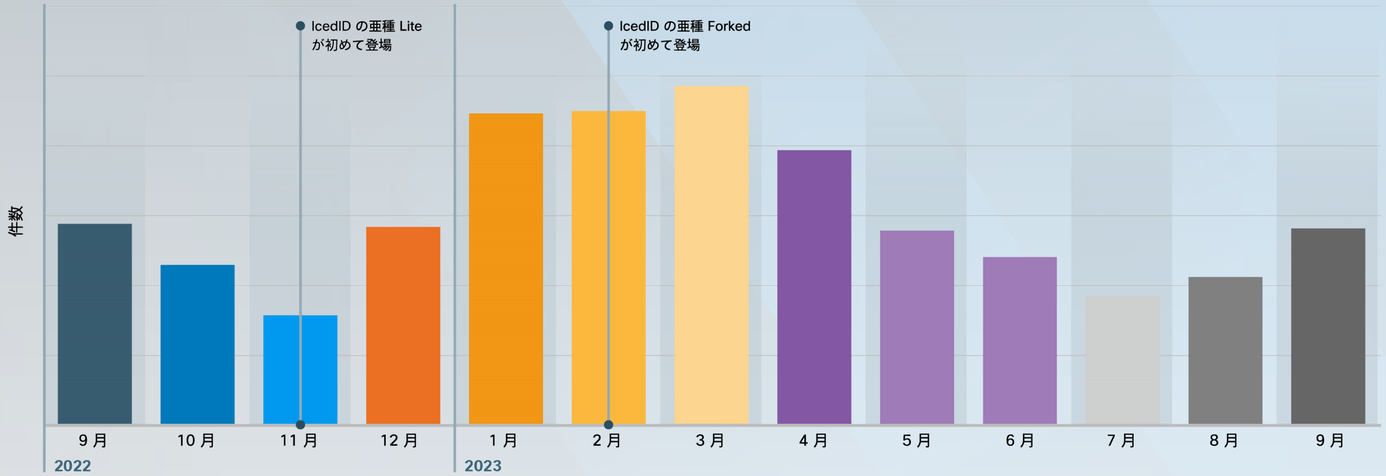
ランサムウェア活動をサポートするためのカスタマイズと考えられるコモディティ型ローダーのアップデート

2023 年後半に、IcedID と Ursnif の最新の亜種および Qakbot の新しい自動化機能が、ランサムウェアの展開をサポートしていることが確認されました。これは、コモディティ型ローダーがランサムウェアの感染チェーンで不可欠な役割を果たしているという傾向に沿っています。これらのアップデートでは、カスタマイズによってマルウェアのドロッパー機能が強化されており、バンキング型トロイの木馬としての本来の用途からさらに離れたことを意味していると思われます。Trickbot と Emotet もランサムウェア攻撃を促進することで知られていますが、同様のアップグレードは 2023 年には行われていません。

2022 年 11 月と 2023 年 2 月に IcedID の開発者は、バンキング機能が削除され、ドロッパーとしてのみ機能するように設計された 2 つの新バージョンをリリースしました。これらのバージョンは「Forked」、「Lite」と名付けられ、2023 年に、ネットワークのアクセス権をランサムウェアグループに販売することで知られる初期アクセスブローカーによって使用されました。元のバージョンも初期アクセスブローカーやランサムウェアグループに使用されていましたが、新バージョンはウイルス対策製品のシグネチャをトリガーする可能性のある機能が削除され、ステルス性能が向上したので、より魅力的なオプションになっていると思われます。2022 年 11 月から 2023 年 2 月にかけて確認された IcedID の活動の増加は、新バージョンのリリースに対応しており、攻撃者がこの脅威の最新機能を試すことに強い関心を持っていたことがうかがえます **(図 19)**。

図 19

新しい亜種のリリースの頃に活発化している IcedID の活動



同様にバンキング型トロイの木馬の機能を削除して改造された Ursnif の最新亜種も、ランサムウェアの展開をサポートすることを意図していると考えられます。この更新されたバージョン（2022 年にリリース）は、活発な活動を見せるランサムウェアグループ Royal によって 2023 年に採用され、更新された Ursnif がランサムウェアグループの活動に取り入れられた最初の例になりました。この新しい亜種を利用していることが確認されているのは Royal だけなので、開発者間に専門的なつながりがあるのかもしれません。Royal は、2022 年 9 月に活動を開始した高度なサイバー犯罪者グループですが、多くのセキュリティ専門家からは、活発な動きを見せていたロシアのランサムウェアグループ Conti が名称変更したものではないかと疑われています。Royal は、過去 2 年間に現れた他のランサムウェアグループの多くが RaaS として活動することを選択したのとは違い、マルウェアとランサムウェアの活動を厳重に管理しています。したがって、Ursnif の新しい亜種と Royal の独占的な提携はおそらく意図的なものであり、開発者間の提携を暗示していると思われます。

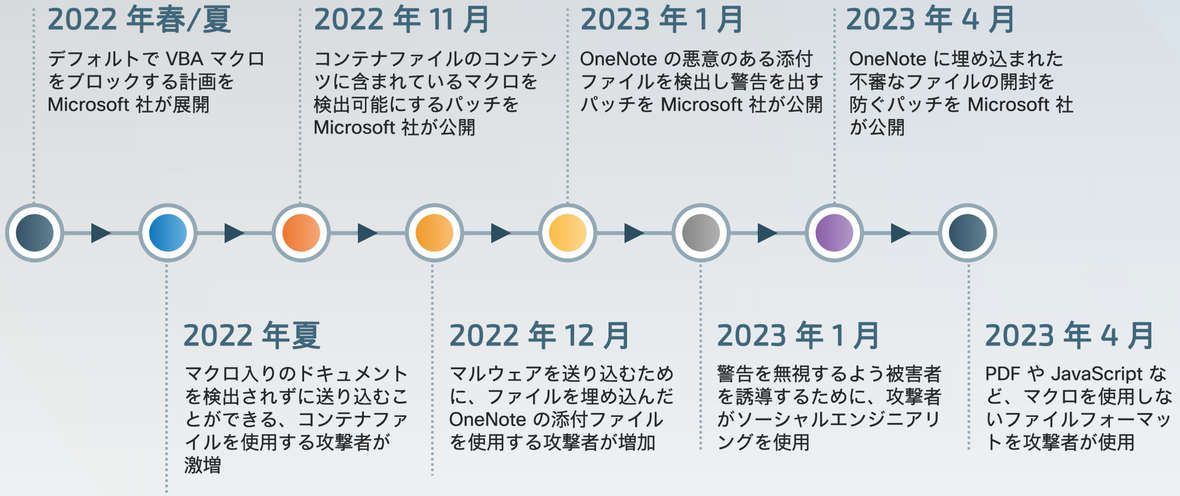
最後に、2022 年後半に Qakbot は、ランサムウェアグループがその展開前に重要な標的を特定しやすくなる最適な機能など、いくつかの新しい自動化機能を展開しました。このアップデートには、初期感染時に顧客の環境を詳細に調べるための偵察コマンドのリストが含まれていました。これらの偵察コマンドの出力には、ドメイングループ、ドメイン名、ドメインコントローラの名前など、ランサムウェアグループにとって非常に有用なデータが列挙されていました。ランサムウェアグループがよく用いる戦術である、Active Directory の乗っ取りを引き起こすラテラルムーブメントに、こういった情報が利用される可能性があります。Qakbot の新しい自動偵察機能は、ランサムウェアグループが検出を回避するためにも役立っている可能性があります。収集したデータを使って詳細な攻撃計画を立て、初期感染から暗号化までの時間を最小限に抑えられるからです。

コモディティ型ローダーの攻撃者がマクロをブロックする新しいセキュリティアップデートに対応し TTP を進化、2022 年中頃に始まった傾向が継続

2023 年に Microsoft 社がマクロをデフォルトでブロックしました。この注目すべき変更により、攻撃者は初期アクセスの手法とマルウェアを送り込む手法を変更しました。変更前は、Microsoft Office の文書を開くとマクロが自動的に実行されていました。マクロは、攻撃者によってかなり悪用されてきました。その狙いは、被害者がフィッシングメールに添付されている悪意のあるファイルをクリックしたときにマルウェアを自動的に実行することです。今は、悪意のある添付ファイルをクリックするとセキュリティの警告が表示されるようになっており、マルウェアをダウンロードする可能性が低くなりました。Microsoft 社によるマクロの無効化は 2023 年を通して影響を与え続けました。検出されずにマクロを使用する方法やマクロの使用を完全に避ける方法を攻撃者が新たに考案したからです。Microsoft 社がセキュリティ機能をアップデートするために新しいパッチを作成してもいたちごっこで、攻撃者は TTP をすぐに変更することができました（**図 20**）。

図 20

セキュリティ機能の変更を受け、攻撃者がコモディティ型ローダーを使用してすぐに TTP を変更



2023 年に Qakbot のアフィリエイトによる展開が確認された偵察コマンドの例

攻撃者は、活動の拡大に必要な情報を収集するために偵察を行います。Talos は、Qakbot のアフィリエイトが一般的な Windows ユーティリティを悪用していることを確認しました。これにより、正当な操作に紛れて偵察コマンドを実行できます。以下は、偵察コマンドが有害な影響をもたらす可能性を示すほんの一部の例です。

netstat -nao : 攻撃に対して特に脆弱なオープンポートのリストと、感染したホストと他のシステム（クラウド環境など）の間のアクティブな接続のリストを取得するために使用されます。目的は、被害者が攻撃者にとって価値のあるデータにアクセスできるかどうかを判断することです。

net localgroup : 管理者アカウント（機密データにアクセスし、システムに変更を加えることができる特権を持つアカウント）を識別するために使用されます。この情報は、攻撃者が攻撃活動でどのアカウントを優先すべきかを知るのに役立ちます。

arp -a : 感染したホストに接続した各 IP アドレスとそれに対応する MAC アドレスの記録である ARP キャッシュを表示するために使用されます。この情報を用いて、攻撃者は 2 つ以上のネットワークデバイスの通信に割り込み、別のデータを盗んだり、送信データを操作したりすることができます。

コモディティ型ローダー

2022 年に始まり 2023 年まで続いている傾向として、Microsoft 社の新しいセキュリティアップデートを受け、コモディティ型ローダーを用いる攻撃者が TTP を繰り返し変更しました。2022 年 11 月、ZIP や LNK などのコンテナファイルに含まれているマクロ入りのコンテンツ（マクロを不正に使用する一般的な方法）を検出してブロックするために、Microsoft 社がパッチを 2 つ公開しました。そのわずか数週間後、添付ファイルに OneNote を用いてマルウェアを展開する、Qakbot、Emotet、IcedID などを使用する攻撃者の急増が確認されました。OneNote を使用してマルウェアを送り込むのは新しい手法ではありませんが、マクロ入りのドキュメントを検出されることなく容易に送り込むことができたため、ウイルス対策製品による検出を回避したいアフィリエイトが好んで使用した方法でした **（図 21）**。

すると 1 月、Microsoft 社は更新プログラムをひそかに公開し、OneNote ファイル内に埋め込まれたマクロ入りのドキュメントはすべてデフォルトでブロックされるようになりました。つまり、マクロが埋め込まれた OneNote の添付ファイルを開くと、セキュリティの警告が表示されるようになったということです。OneNote を使用する攻撃者は依然として見られましたが、それは警告を無視するように被害者を誘導する巧妙なソーシャルエンジニアリングの手法を伴うものでした。IcedID を展開したある攻撃では、攻撃者が DocuSign のおとりを使用して被害者を騙し、リンクが埋め込まれたボタンをクリックさせたことが確認されました。[復号してメッセージを表示する（Decrypt and View Message）] ボタンには、実際には悪意のある HTML アプリケーション（HTA）ファイルが含まれていました **（図 22）**。これを開くと、OneNote のディレクトリに HTA ファイルがドロップされ、実行されるという仕組みでした。

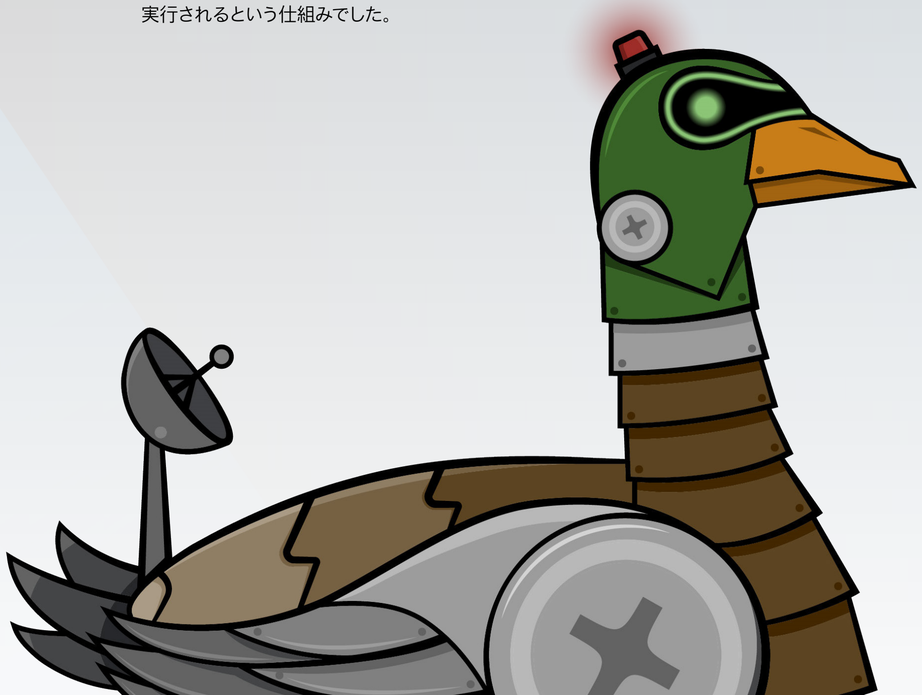
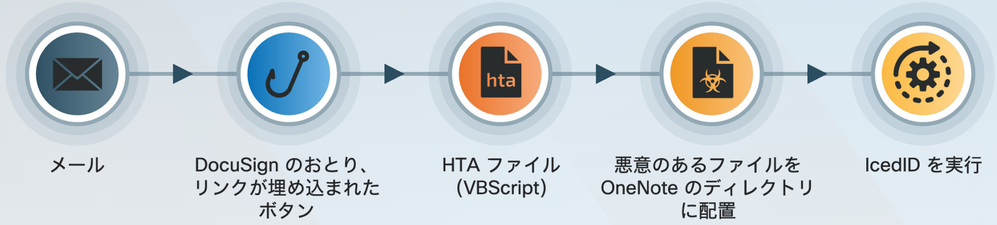


図 21

マクロ入りのファイルが埋め込まれた OneNote を使用してマルウェアを送り込む感染チェーンの例

図 22

セキュリティの警告を無視するように被害者を誘導しようとする感染チェーンの例



コモディティ型ローダー

図 23

マクロを使用しない感染チェーンの例

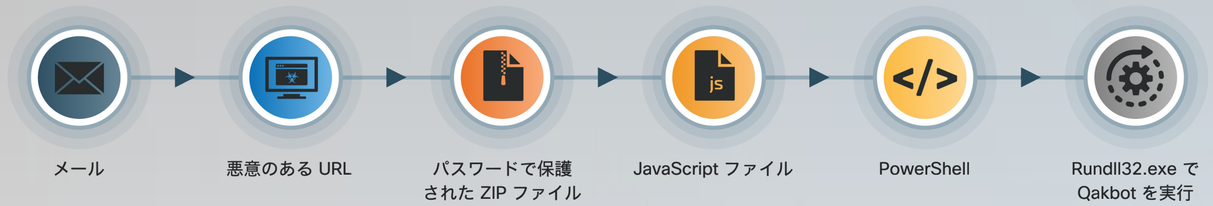


図 24

バイナリパディングを使用した Emotet の感染チェーン

最終的に、2023 年 4 月に Microsoft 社は別の更新プログラムを公開し、OneNote に埋め込まれた潜在的に危険であると見なされる拡張子のファイルをユーザーが開けないようにしました。危険と見なされる添付ファイルを OneNote ユーザーが開くには、デバイス上で実行されているセキュリティ アプリケーションが添付ファイル内の悪意のあるコードを検出できるように、ファイルをデバイスに保存してから開く必要があります。この最新のアップデートにより、コモディティ型ローダーを使用する多くの攻撃者が、マクロの使用を隠ぺいする手口として OneNote を用いることを断念することになりました。その代わりに攻撃者は、LoLBin を使用して実行される JavaScript ファイルなど、マクロに依存せずにマルウェアを実行するファイルタイプに目を向けるようになりました **(図 23)**。

攻撃者は OneNote の他にも、マクロに依存しない、または検出されずにマクロを使用できるマルウェアを展開する手口を試みていました。遅くとも 2022 年 12 月以降は、攻撃者が Google Ads プラットフォームを利用して、Ursnif、IcedID、Trickbot などのマルウェアを展開したことが確認されています。これはマクロの使用を完全に回避できる手口です。一連の攻撃における攻撃チェーンは、ユーザーが Google の検索エンジンでソフトウェアやサービスに検索語を入力することから始まります。Google の検索結果ページが読み込まれると、悪意のある広告は通常、検索結果リストの最初に表示されます。これは、広告が目に留まる可能性を高めるために、攻撃者が検索エンジンの最適化（SEO）を利用しているからです。ユーザーが悪意のある広告をクリックすると、Google Ads サービスの URL が生成され、次に、さまざまな脅威を送り込むダウンロードリンクを含む悪意のある偽ドメインにユーザーを誘導する第 2 の URL が生成されます。Talos は、Microsoft Teams や WhatsApp、1Password のような人気のあるパスワードマネージャなど、正規のソフトウェア製品がこれらのなりすまし攻撃の対象にされたことを確認しています。攻撃者が Google Ads や Google 検索を利用すると攻撃者のおとりが極めて合法的に見えます。検索結果の上位に優先的に表示される有料広告の真正性をユーザーが疑う可能性は低いのです。

2023 年には、セキュリティアップデートの進化を受け、多くのアフィリエイトが新たな TTP を導入しました。一方、コモディティ型ローダーが旧来の手法を使用していることも確認されました。たとえば Emotet、IcedID、Ursnif ですが、いずれも感染チェーンの初期でマクロ入りの Office 文書を使用したことが確認されています。さらに、2020 年に初めて見つかった「RedDawn」テンプレートを使用したフィッシングメールで Emotet が送り込まれたことも Talos は確認しました **(図 24)**。これらの攻撃者は、より高度な攻撃を実行できるかもしれませんが、特にパッチが適用されていない企業のレガシーシステムに対して、古い TTP を使用して今も成功を収めている可能性があります。

世界中のセクターを狙った大規模な無差別攻撃で、上位 5 つのコモディティ型ローダーが同様に展開

2023 年には、5 つのコモディティ型ローダーのすべてが、北米と欧州を中心に世界中の企業に影響を与えたことが確認されました **(図 25)**。標的の地理的分布は必ずしも、グループ間で攻撃対象地域を調整していることを意味しているわけではありません。というのは、この脅威はサービスとしてのマルウェア（MaaS）として販売されているからです。そのため、攻撃対象選定に見られるパターンは、攻撃を実行するどのグループでも同じかもしれませんが、異なる可能性もあります。

Talos が主に観測したのは、無差別に脆弱な標的を侵害しようとする大量のスパム攻撃です。初期感染後に、もっと狙いを絞ったラテラルムーブメントを行うことを意図している可能性があります。攻撃者は通常、標的とする地域に合わせてフィッシングのおとりをカスタマイズします。たとえば 2023 年には、Ursnif が主に米国とイタリアの企業に対して、標的とする国の言語を使用した大量のスパム攻撃を無差別に展開したことが確認されました。

コモディティ型ローダーは、個人の金融データを狙うのではなく、主に企業に対して展開されることが確認されています。これは、マルウェアがバンキング型トロイの木馬として使用される頻度が低くなるにつれて生じた変化です。このことは Talos が確認したフィッシングのおとりにも反映されています。たとえば 3 月下旬には、四半期ごとに税金を納める米国企業を狙った Emotet の増加が見られました。このおとりでは「IRS 納税申告書 W-9」といった件名で内国歳入庁（IRS）に関連したテーマが使用されました。昨年も 2022 年 11 月の会計四半期末に同じ手口が用いられたことが確認されています。W-9 納税申告書は通常、企業や金融機関から従業員に配布されます。

図 25

コモディティ型ローダーの影響を受けた地域を示す世界地図（最大から最小まで）

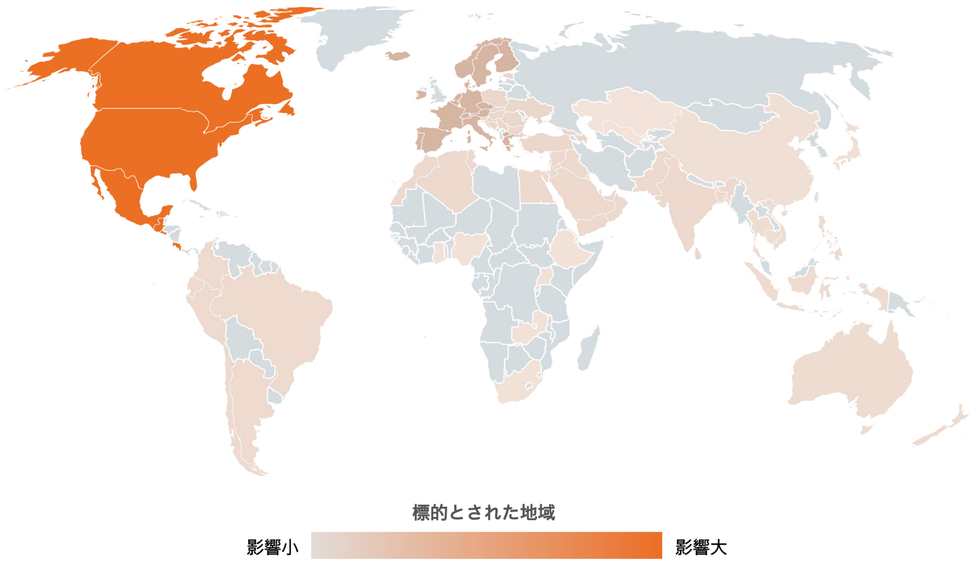
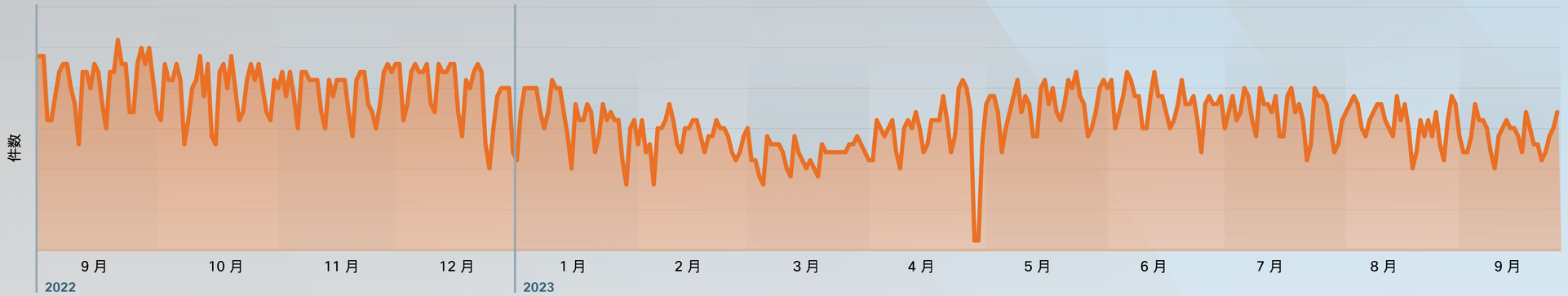


図 26

Trickbot の活動の経時変化



コモディティ型ローダーの脅威がボットネット解体後も長く続く可能性

2023 年 8 月、世界の法執行機関による大規模な活動により、多用されていたコモディティ型ローダーの Qakbot が解体されましたが、ボットネットのインフラを解体したからといって、サイバー犯罪者が活動を停止するとは限りません。Emotet など他のローダーに関連する同様のシナリオでも見てきたように、Qakbot は今後、数か月の休止期間を経て再び出現する可能性があります。この脅威について監視し報告することが一層必要になっています。注目すべきは、Qakbot の背後にいる攻撃者が世界的な取り締まりの間に逮捕されなかったことです。Talos の最新の調査結果では、同じ攻撃者が今も活動している徴候が見られます（ただし、送り込んでいるのは別の脅威です）。つまり、Qakbot のボットネットを再構築したか、名称を変更した可能性があります。

他のマルウェア開発者も、ボットネット解体後もサイバー脅威環境で活動を続けていることが確認されています。たとえば Trickbot は 2022 年 2 月にインフラを解体しましたが、米国と英国が 2023 年 2 月と 9 月に開発者を制裁しており、Trickbot がサイバー脅威環境で今も活動していることが示唆されています。他の種類のマルウェアを作成することや、Emotet や Conti など長年関係を築いてきた他のグループに協力することを開発者が選択した可能性があります。2022 年の一連のリークにより、Trickbot と Conti の開発者間に緊密で専門的なつながりがあることが明らかになり、2021 年には Trickbot がインフラの一部を Emotet のボットネットの再構築を支援するために貸与していました。

たとえ攻撃者がサイバー犯罪活動を停止することを選択した場合でも、Qakbot に感染したデバイスでゾンビの活動が観測される可能性があります。これは Trickbot で見られたことで、2022 年 2 月に Trickbot のインフラが解体されたにもかかわらず、Talos のテレメトリでは 2023 年を通してその活動が認められました。これは、まだ修復されていない古い感染が残っているか、攻撃者が前に侵害したインフラを利用しているからだと考えられます。過去 1 年間の Trickbot の活動を見ると、同じ中央値近辺で推移しており、このボットネットが現在もある程度の規模で活動しているものの、開発者はボットネットの拡大に積極的に関与していないという Talos の見解を裏付けています **（図 26）**。新しい攻撃が実行されたり、新たなインフラ（IP や C2 サーバー）が導入されたりすれば、上記のチャートにもっと著しい急上昇や不規則なパターンとして表れる可能性があります。

その一方で、Qakbot や Trickbot のような以前は活発だったボットネットに取って代わる新しいコモディティ型ローダーが常に登場しています。たとえば、IcedID が Qakbot の穴を埋めたと考えるのも論理的には妥当かもしれません。2021 年に Emotet が解体された後、IcedID がアフィリエイトを招き入れたという歴史的な前例があります。さらに、Qakbot と IcedID が同じ攻撃で同時に展開された例が数多くあるので、多くの Qakbot のアフィリエイトが IcedID をよく知っている可能性があります。最後に、最近の高度な IcedID のアップデートを見ると、開発者が高品質の製品を維持する能力も意欲もあることがわかります。