
cisco
Talos
2022 年版
一年の
総括

cisco | Talos

2022 年版一年の総括

はじめに

第 1 号となる、Cisco Talos の『一年の総括』をお読みくださりありがとうございます。
本レポートは、さまざまなデータと専門知識を交えながら一年間の成果を網羅的に紹介しようという、シスコ社内のかつてない取り組みから生まれたものです。

シスコはグローバルに展開する大規模セキュリティ組織として、データに基づいて調査を行っています。しかしデータは有益である一方で、ときに問題を引き起こします。有益なデータは、エンドポイント検出やインシデント対応業務、ネットワークトラフィック、メールコーパス、サンドボックスやハニーポットなどさまざまなソースから得られます。世界中のお客様からはさらに多くの有益なデータをご提供いただいています。一方で問題は、利用できるテレメトリが非常に多く、業務によっては緊急を要するために、一歩下がって全体像を把握するのが難しい場合があることです。モネの絵を理解しようとして顔を近づけすぎてしまうのに似ています。

これに着想を得て作成したのが Cisco Talos の『一年の総括』です。シスコのあらゆる部署にいる各分野のエキスパートから知見を得たいと考え、リバースエンジニア、検出のスペシャリスト、データサイエンティスト、翻訳担当者、マネージド ハンティング プロバイダー、インシデント対応担当者、脅威インテリジェンスアナリストなどの多様な人材に、以下の重要な質問を投げかけました。

1. 2022 年にシスコが対応した主なセキュリティイベントは何ですか。それらの現状と影響も教えてください。
2. 脅威環境には主にどのような傾向が見られますか。また、何が変わると思いますか。
3. 2022 年に確認された重大な脅威は何ですか。それらの現状も教えてください。

本レポートでは、これらの質問に対する社内エキスパートの回答と一年間のデータに基づいて説明を進めます。今後数週間で、本レポートのさまざまな側面を取り上げていきます。具体的には、ウクライナにおけるシスコの取り組み、大損害を与える Log4j の脆弱性、攻撃フレームワークや標的マシンのネイティブソフトウェアが攻撃者に利用されている現状、ランサムウェア環境の変化、コモディティ型のローダーとトロイの木馬による絶え間ない脅威を紹介し、シスコが最も懸念している Advanced Persistent Threat（APT）のいくつかについて概要を説明します。レポート全体に共通する重要なテーマは明らかです。攻撃者は地政学的な状況の変化、法執行機関の措置、防御側の取り組みに適応しようとしています。防御側はレジリエンスを保つために、こうした行動の変化を追い、対応をとる必要があります。

データに基づいているこのレポートをお読みいただければ、シスコやセキュリティコミュニティが成し遂げた注目すべき成果や残された課題について理解を深めることができます。この一年の総括レポートは今後も発表していく予定です。年とともに移り変わっていく脅威環境を把握するのに役立つデータや解説を提供していきます。このレポートを通じて、研究者や執筆者が得た知見を読者の皆様が獲得でき、脅威を阻止し続けていくために必要な情報やコンテキストをセキュリティコミュニティが得られれば幸いです。

cisco | Talos

2022 年版一年の総括

目次

cisco | Talos

2022 年版**一年の総括**

ウクライナ

図 1. ロシアとウクライナの戦争開始以降、ウクライナの重要インフラと政府機関パートナーに対してシスコが行っている支援

ウクライナ

Talos によるウクライナへの継続的なサポートは、今年の運営上の取り組みの大きな焦点となっています。ウクライナの人々とインフラをサイバー攻撃から守るという核となる使命に突き動かされ、Talos はロシアの攻撃者と戦時のサイバー脅威環境に関する知識の強化にも取り組んできました。将来同様の危機が発生した場合は、これらの情報を分析、防御、戦略の参考にして危機に対処し、さらに充実させることができます。このセクションでは、2022 年のウクライナ関連の業務を振り返り、脅威環境と攻撃者の行動に関して戦略的に重要なポイントをいくつか紹介します。根拠として、シスコのテレメトリ、Cisco Talos インシデント対応チーム（CTIR）のデータ、現在も活動を続けている Talos 内部のウクライナタスクフォースのケーススタディを使用します。

タスクフォースが Talos のウクライナ支援を推進し、将来の危機対応のモデルとして機能

2 月にロシアがウクライナに侵攻したのを受け、Cisco Talos はすぐにウクライナの人々やパートナーの支援に動き出し、数週間から数か月の間に幅広い取り組みを開始しました。この取り組みは、かつてない範囲とペースで行われました。ウクライナにおけるカバレッジを迅速に拡大し、ウクライナの新しいエンドポイントでシスコのセキュリティ製品を導入および管理し、一部の従業員に、この取り組みを支える監視能力と検出能力の強化にあたらせたのです。この業務の多くは、継続的で包括的な戦時の取り組みの一環として現在も続けられており、ウクライナの人々を守り、ウクライナの組織のレジリエンスを高めています。

この業務に従事するにあたり、Talos はウクライナタスクフォースを内部で編成しました。これは、サイバー空間に重大かつ持続的な影響をもたらすであろう将来の世界的な出来事に、どう対応できるかを示すモデルになっています **（図 1）**。

図 2. ウクライナに対する主なサイバー攻撃

このタスクフォースは Talos に所属する約 45 人の有志で構成されており、メンバーには脅威ハンター、マルウェアのリバースエンジニア、インシデント対応担当者、データサイエンティストなどがいます。これらのエキスパートは、ウクライナを拠点とするさまざまな重要インフラ業界のお客様約 30 社の環境を監視し、必要不可欠な支援を提供しながら情報収集にあたりました。収集した情報は、攻撃者や戦時のサイバー脅威環境に関する知識強化に役立てています。このセクションは、タスクフォースで得られた知見を参考に作成されています。

ウクライナの脅威環境に見られる多様な攻撃者と脅威

2 月の戦争開始以降、かつてないほど多くの攻撃者が確認されています。さまざまな動機を持ち、スキルレベルが異なる攻撃者が同じ脅威環境に集まっているのです。ウクライナとその支持者にとって、この程度の活動状況はある意味で見慣れたものです。ウクライナは遅くとも 2014 年以降、あらゆる種類の高度なサイバー攻撃から自国を守り続けているからです **(図 2)**。この直近の紛争に多様な攻撃者が関わっているために、お客様、パートナー、防御側はさまざまな課題に直面しており、攻撃者の戦術、手法、手順（TTP）の継続的な変化、新たな脅威や進化する脅威、活動主体のグループを特定することの難しさへの対応を余儀なくされています。これらの多様な攻撃者は今年一年を通じて活発に活動を続けてきました。

サイバー犯罪者、ワイパーマルウェア、APT が脅威環境にすばやく参入

常に攻撃機会をうかがっていることで知られるサイバー犯罪者が、この脅威環境の中心となっています。戦争が始まって以降、人道支援や各種の募金活動など、紛争関連の話題に便乗したメール攻撃が確認されています **(図 3)**。これらのメールのほとんどは詐欺目的のものですが、リモートアクセス型トロイの木馬（RAT）などのさまざまな脅威を配布したものもあります。新型コロナウイルスの感染拡大のような世界的な出来事や危機が起きると、今回と同じような事態が発生するのが常です。社会的関心の高まりを受け、サイバー犯罪者が話題に便乗して自らの利益のために利用し、自らの適応力の高さを強調しようとするわけです。

ロシアの組織を攻撃するためのサイバーツールだと称してマルウェアを配布し、親ウクライナ派の人々を食い物にしようとするサイバー犯罪者も確認されています。たとえば「disBalancer」という攻撃者が、ロシアのプロパガンダ用 Web サイトを攻撃するためとして、分散型サービス拒否（DDoS）ツールと称する「Liberator」を Telegram 上で配布していることが確認されました **(図 4)**。実際にダウンロードされるファイルは情報窃取マルウェアです。何の疑いもなく実行すると、ログイン情報をダンプして暗号通貨関連の情報を盗むように設計されたマルウェアに感染します。

国家の支援を受けた攻撃者やその他の高度な攻撃者も、この戦争の間、活発に活動を続けてきました。たとえばロシア政府の支援を受けた Advanced Persistent Threat（APT）グループである Gamaredon がその代表格です。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したが、こうした活動は 2 月のロシアによる侵攻以降、増加する一方です。9 月には、Gamaredon による新たな攻撃が確認されました。これは、目的のファイルを盗み出し、追加のペイロードを展開できるカスタムの情報窃取マルウェアをウクライナのユーザーに感染させるものです。ロシア政府の支援を受けていると思われる攻撃者が、GoMet というオープンソースバックドアの改変版を、ウクライナのソフトウェア企業に対して展開している事例も確認されました。標的企業のソフトウェアがウクライナの政府機関に広く利用されていることと、このマルウェアが永続アクセスの確立を意図したものであったことから、サプライチェーン攻撃を試みた可能性があります。

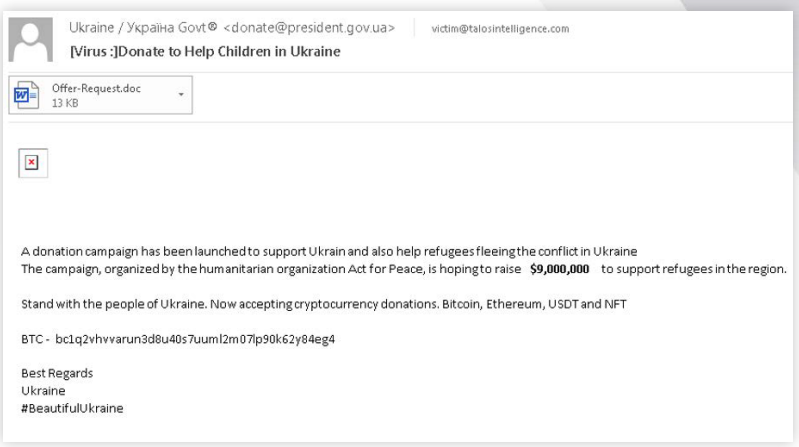


図 3. ウクライナ難民への人道支援要請を装ったスパムメールのメッセージ

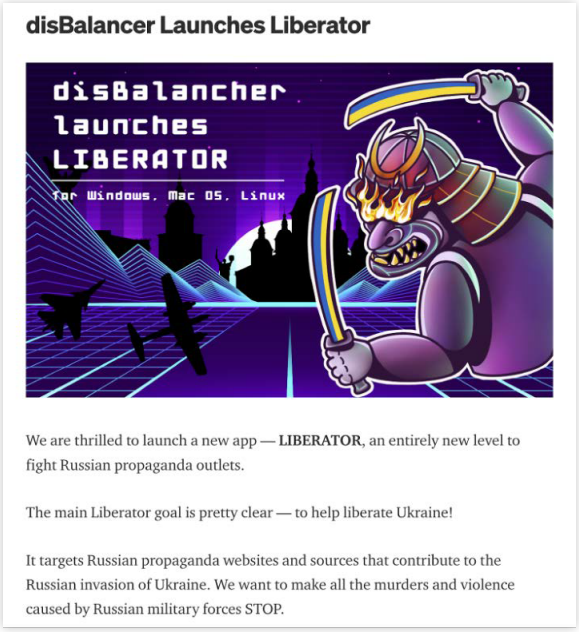


図 4. disBalancer による「Liberator」の広告のスクリーンショット

戦争が進むにつれ、明確な政治目的に突き動かされた新たなグループが出現しており、変わりやすい脅威環境と、地政学的な出来事によるサイバー環境への継続的な影響を浮かび上がらせています。

他にも、高度な攻撃者が戦争を都合よく利用する事例が見られます。多くの場合、話題に便乗した罠を仕掛けて標的にマルウェアを配布する手法がとられています。2 月のロシアによる侵攻と同時期に、中国を拠点とする Mustang Panda という攻撃グループがヨーロッパの組織や機関に対してフィッシング攻撃を仕掛け始めました。攻撃対象にはロシアの組織も含まれています。フィッシングメールでは、ウクライナ戦争と北大西洋条約機構（NATO）諸国への影響に関する欧州連合（EU）の公式報告書を装ったものや、ウクライナ政府の「公式」報告書に見せかけた偽ファイルが配布されています。いずれも、侵害したマシンにマルウェアをダウンロードするものです。

他にも、数えきれないほどの脅威を確認または分析してきました。これらは特定の攻撃者によるものではありませんが、現在の脅威環境に居座る攻撃者とマルウェアの多様さを浮き彫りにしています。ロシアによるウクライナ侵攻の前、そして侵攻直後から、攻撃者はウクライナの組織を標的にした各種マルウェア（破壊的なワイパーマルウェアなど）を展開するようになりました。具体的には、WhisperGate、HermeticWiper、CaddyWiper、DoubleZero、Cyclops Blink などです。Talos の分析と米国政府の報告によると、これらの脅威の一部は、国家の支援を受けた攻撃者によって展開されたと考えられます。より最近では、Talos 内部のウクライナタスクフォースが、ウクライナのシスコパートナーに影響を及ぼすさまざまな脅威を確認しています。これらは、IcedID コモディティ型ローダーや Sality マルウェアなどのよく見られる脅威から、WannaCry ランサムウェア、破壊的な Industroyer2 マルウェア、GrimPlant バックドア、GraphSteel 情報窃取マルウェアなどのより高度な標的型脅威にいたるまで、多岐にわたります。

ロシアとつながりのある攻撃者が NATO 諸国を標的に

戦争が進むにつれ、明確な政治目的に突き動かされた新たなグループが出現しており、変わりやすい脅威環境と、地政学的な出来事によるサイバー環境への継続的な影響を浮かび上がらせています。そのような攻撃グループの一例として Killnet が挙げられます。Killnet は、新ロシア派の利益にかなう分散型サービス拒否（DDoS）攻撃を仕掛けるハクティビスト集団です。2022 年 2 月、つまり戦争が始まった頃から活動しており、西側諸国に度重なる攻撃を行ってメディアの注目を集めています。米国のいくつかの州と主要空港も攻撃対象になりました。

Killnet は、ロシアの組織を標的とするハクティビスト集団「アノニマス」に対抗して、ウクライナ政府の 20 以上の Web サイトに最初の DDoS 攻撃を仕掛けました。さらに、その後の数か月間にわたって、ポーランド、ノルウェー、リトアニア、イタリア、ルーマニア、エストニア、日本などの親ウクライナ諸国の Web サイトを次々と狙うようになりました。たとえばリトアニアには、ロシアへの物品輸送を禁止したことへの対抗措置として攻撃を仕掛けています。これらの DDoS 攻撃では、概して複数のサービスとオペレーションに影響を与えるさまざまな政府系 Web サイトが狙われています。防衛省や、運輸、銀行、警察関連などの Web サイトがその例です。

これまではネットワークを中断させる目的で攻撃を行ってきた Killnet ですが、将来的に攻撃力の強化を目論んでいる可能性を示す兆候がいくつかあります。報道によると、Killnet は今年初めに、自分たちの代わりに攻撃を仕掛けるランサムウェアグループのメンバーを募ろうとしたとされています。Killnet がより破壊度の高い攻撃を仕掛けるために同志を育成しているか、闇市場から人材を調達している可能性がうかがえます。また、Killnet は今年初めに Mirai ボットネットを利用して攻撃能力を高めたと伝えられており、マルウェアによる攻撃力の強化に対する関心の高さがいっそう色濃く表れています。

Killnet の攻撃活動は高度ではなく、カスタムツールもマルウェアも利用していません。標的が DDoS 攻撃から短時間で復旧できる場合が多いことから、Killnet は標的に最大限の損害を与えたりネットワークを中断させたりすることよりも、自らの大義についてメディアの注目を集めることに重点を置いていると考えられます。Killnet の分散型の構造、熱烈なロシアナショナリズム、標的の知名度の高さを踏まえると、親ウクライナまたは反ロシアと認識されている国や組織は今後数か月の現実的な攻撃対象になるでしょう。

テレメトリからわかる、戦争開始以降の主要な脅威と活動の傾向

1 月から 9 月までのエンドポイントテレメトリを精査したところ、紛争が始まってからの脅威の傾向について、独自の知見が得られました。これらの知見は動作保護（BP）のデータを根拠としています。BP は、シスコが作成するルールに基づいて、悪意のあるアクティビティを検出してブロックする Cisco Secure Endpoint 内のエンジンです。このデータから、ウクライナのお客様組織とパートナー全体で実行頻度の高い上位 10 個の BP シグネチャのリストを導き出しました **(図 5)**。

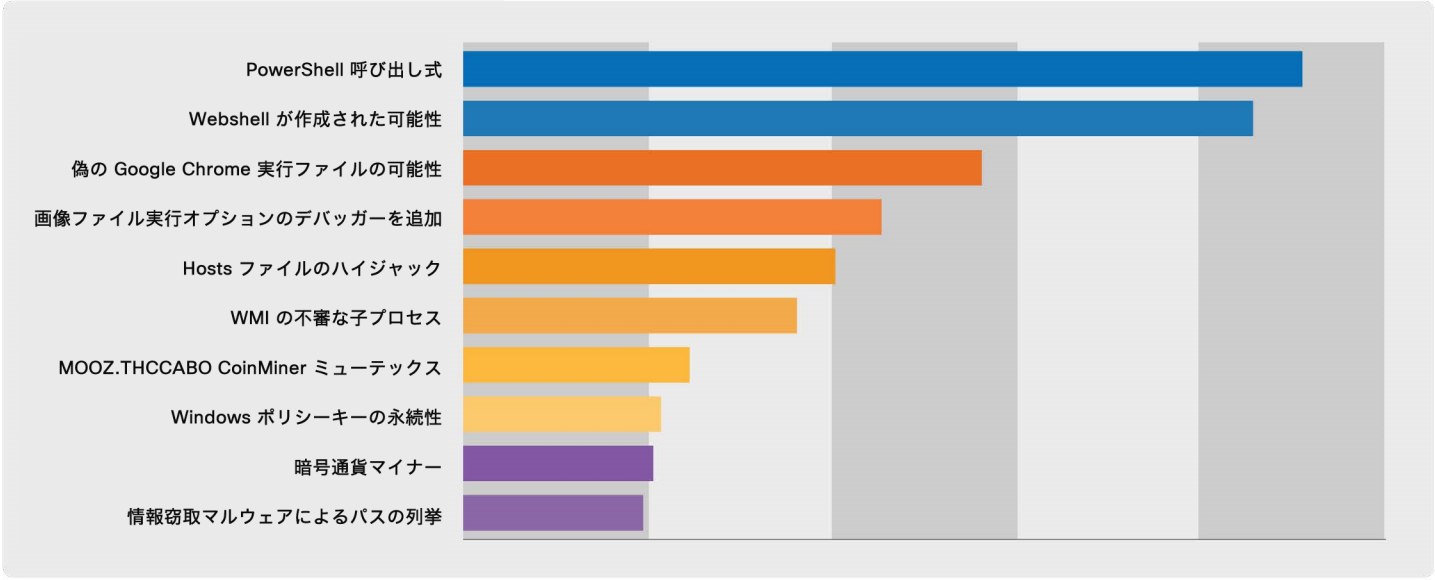


図 5. Cisco Secure Endpoint を導入しているウクライナのお客様全体で特に実行頻度が高い Cisco Secure Endpoint の動作保護ルール

このデータで示しているのは一意のエンドポイントではなく合計の数であることを踏まえると、数日または数週間のうちに 1 つ以上のエンドポイントが同じ BP を実行している可能性はあります。それでもこのグラフから、今回の戦争で広く用いられてきたいくつかのユーティリティ（PowerShell、WMI）、手法（Windows ポリシーキーを使用した永続性の確保、偽の Google Chrome 実行ファイル）、マルウェア（情報窃取マルウェア、暗号通貨マイナー）が明らかになります。BP が実行された原因の上位に挙がっている「WebShell が作成された可能性」では、攻撃者が Web UI を使用して標的マシンを制御できるようになる恐れがあります。これには HTTP/HTTPS ポート経由でアクセス可能な標的マシンを利用します。つまり、影響を受けるエンドポイントはサーバーであり、個人ユーザーのデスクトップやラップトップではありません。実行頻度が多い上位 2 つの BP である「WebShell が作成された可能性」と「PowerShell 呼び出し式」はそれぞれ、アラート発出の合計日数においても 1 位と 2 位でした。これらの手法の広まりは、経時的に確認された頻度からもわかるということです。

エクスプロイト防止（BP と同様、Cisco Secure Endpoint 検出エンジンの 1 つ）のデータの結果を確認すると、「rundll32 を用いた署名付きバイナリプロキシの実行」シグネチャの検出件数が 5 月から着実に増えていることがわかります **（図 6）**。

このアクティビティは、MITRE ATT&CK の手法「System Binary Proxy Execution: Rundll32」（T1218.011）と完全に同じものです。攻撃者はこの手法で、悪意のあるコードのプロキシ実行に「rundll32.exe」を悪用することで防御を回避します。これによりセキュリティツールの起動を回避しやすくなるのは、許可リストや通常の管理操作の誤検出を理由に「rundll32.exe」プロセスの実行をツールで監視していない場合があるからです。また、rundll32 は通常、DLL ペイロードの実行にも関連しています。興味深いことに、シスコのテレメトリによれば、この手法も世界中のあらゆるお客様への攻撃においてますます一般的になりつつあります **（図 7）**。MITRE によると、さまざまな攻撃者がこの手法を使用することが知られており、その中にはロシアとつながりのある Gamaredon、APT28、APT29 といったグループも含まれています。

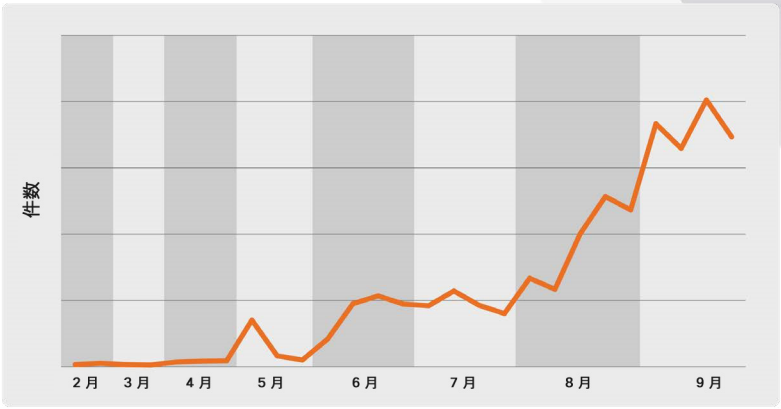


図 6. ウクライナのお客様における rundll32 検出件数

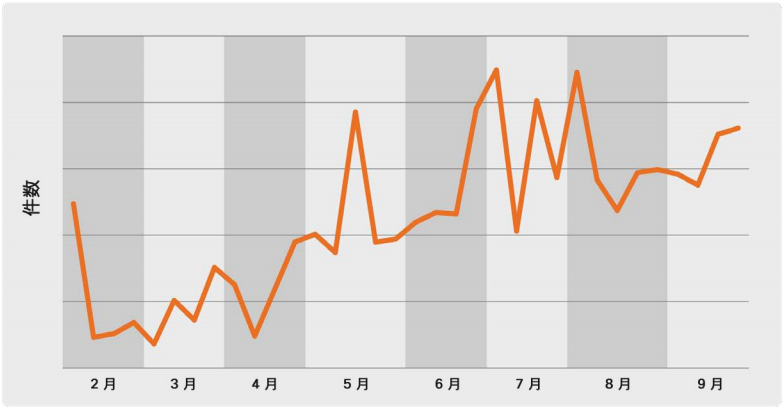


図 7. シスコのすべてのお客様における rundll32 検出件数

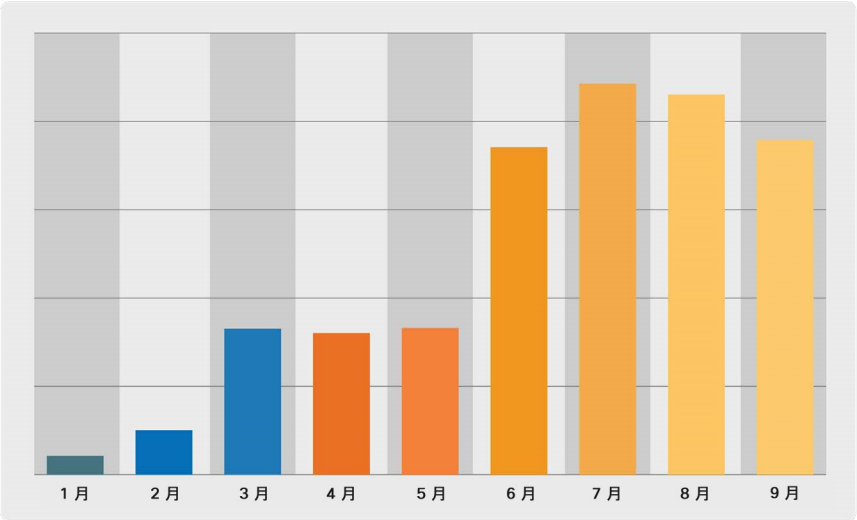


図 8. ウクライナのお客様における動作保護アラートの合計件数 (3 月と 6 月に増加)

39.175.68[.]100	192.241.221[.]160
207.249.96[.]145	128.14.225[.]243
128.1.42[.]231	117.208.234[.]11
45.83.192[.]134	152.32.200[.]79
103.178.237[.]134	143.244.135[.]246
85.198.141[.]6	61.52.46[.]172
31.43.190[.]200	167.172.69[.]26
206.189.37[.]136	152.32.153[.]235
185.218.200[.]1	178.128.103[.]166

図 9. ウクライナの組織を標的とする攻撃者の IP (カスタム検出の結果より)

このデータをより広い視点で見てみると、戦争の開始以降、ウクライナの組織全体で BP の検出件数が徐々に増加していたこともわかります **(図 8)**。3 月から 5 月にかけてのアクティビティは安定していましたが、6 月に急激に増加し、現在まで一貫して多い状態が続いています。

ネイティブのカスタム検出システムで攻撃者 IP を新たに検出

戦争が始まり、ウクライナの人々を守るための取り組みを活発化させ始めたとき、シスコは不審なアクティビティや標的型攻撃の可能性を特定しやすくする新しいカスタム検出システムをいくつか開発しました。そのうちの 1 つは、ウクライナの組織を標的としている一意の IP アドレスを検出できるようにするものです。IP は、シスコのデータサイエンティストによる設定に従って、特定のターゲットしきい値を超えるとフラグが付けられます。その後、これらの IP が悪意のあるものとして手動で確定されると、残りの IOC がブロックされます。

図 9 は、この検出システムを基に特定した攻撃者の IP アドレスのうち、それまで報告されていなかったもののリストです。すべての IP がシスコのセキュリティ製品でブロックされています。

Talos IR で確認された戦争初期の脅威件数の減少は、攻撃者がロシアとウクライナの標的に狙いを定めたことを示唆

先ほどのテレメトリは、ウクライナの組織を狙った脅威活動が活発な状況がこの数か月間続いていることを示していました。これに加えて、Cisco Talos インシデント対応チーム (CTIR) のデータからも、戦争開始以降、攻撃者がロシアとウクライナの攻撃環境に集中していることがわかります。インシデント対応担当者が確認したところ、シスコのお客様に影響を与える脅威は 2022 年前半に減少しました。ランサムウェア、情報窃取マルウェア、コモディティ型マルウェア、既知の脆弱性のエクスプロイトといった脅威が、戦争初期に当たる 2 月から 6 月に著しく減少したのです。CTIR が確認した脅威の件数がほぼ通常の数に戻ったのは 7 月頃でした。

この減少の直接的な原因は特定できませんが、ロシアとウクライナの戦争がおそらく重要な要因であったと Talos では判断しています。従来であればさまざまな地域と業界の組織を標的にしていたであろう大勢の攻撃者が、親ロシア派または親ウクライナ派のサイバー活動に関心を向けた可能性があります。本レポートで詳しく述べてきたように、こうした判断は、この地域で見られる攻撃者の多様さや活動の高まりによって裏付けられています。ロシアの侵攻と残酷な戦術は、親ロシア派と親ウクライナ派のどちらからも強い反応を呼んできました。これは紛争初期のサイバー環境に表れており、この時期には、ロシアとウクライナの戦いに大勢の攻撃者が参入している状況が確認されました。ロシア派もウクライナ派もいました。関心を持つ攻撃者がこのように急増したことは、複雑な地政学的環境によって攻撃者の行動がどのような影響を受け得るのかを示しています。

今回の戦争は、攻撃者の関心を従来の標的から遠ざけただけではありません。さまざまな脅威グループ内での対立や仲間割れも引き起こし、これが早期の衰退につながった可能性もあります。Conti がロシア支持を公言した後、反発したアフィリエイト（実行役）の 1 人が、活動上重要な情報を含む同グループのプレイブックを流出させました。8 月と 9 月に頻発した分散型サービス拒否（DDoS）攻撃は、いくつかのランサムウェアグループに活動とセキュリティの面で課題を突き付けました。これについては本レポートで後ほど詳しく説明しますが、攻撃を受けたグループの関心が従来の活動からさらに遠ざかる可能性があります。

将来的に戦場で軍事的な停戦が実現したとしても、サイバー脅威活動が活発化する可能性はなくならないでしょう。

まとめ

ウクライナおよび親ウクライナ派の政府組織と民間組織に対する脅威が活発な状況は、戦争が終結するまで続くと考えられます。シスコのテレメトリ、タスクフォースの調査結果、脅威ハンティングの検出結果からは、ウクライナの組織に対する脅威活動が下火になっているという兆候は認められません。これらの組織に降りかかる脅威の種類はおそらく変わり続けるでしょう。一方で、ロシアの攻撃者が 2014 年以降、ウクライナの組織にワイパーマルウェアを好んで展開し、成功したことを踏まえると、より破壊度の高い攻撃が起こる可能性は特に高いと考えられます。ロシアはウクライナの一部を占領および併合するという目標にこだわり、ロシア政府は市民や重要インフラ機関に対して、甚大な影響を与える軍事攻撃を実行する意向を一貫して示しています。ロシアのサイバー攻撃者も同様に、戦争の趨勢に影響を与えるために必要であれば、積極的に平然と攻撃を仕掛けるでしょう。さらに、将来的に戦場で軍事的な停戦が実現したとしても、サイバー脅威活動が活発化する可能性はなくならないと考えられます。

cisco | Talos

2022 年版一年の総括

Log4j

Log4j

2021 年 12 月、Apache ソフトウェアでよく使用される Log4j ライブラリに影響する悪名高い脆弱性が発見されたことを受け、Talos は、関連する脅威を軽減するために数か月に及ぶ継続的な取り組みを開始しました。非常に多くの組織が Log4j を使用しているため、アタックサーフェス（攻撃対象領域）が大きくなっており、攻撃者が脆弱なシステムに侵入する経路の候補が多数生まれています。さらに、Log4j ライブラリはたいてい他のシステムに組み込まれているため、自組織のインフラに Log4j の脆弱性が存在するのか、存在するとすればどこにどの程度の脆弱性が存在するのかを判断することは困難です。高度な攻撃を行う APT をはじめとして、あらゆるスキルレベルの攻撃者が、Log4j を使用する脆弱なシステムをエクスプロイトし続けています。Log4j の一連の脆弱性（CVE-2021-44228、CVE-2021-45046、CVE-2021-45105）に伴う特有の課題は、これらが組織とサイバーセキュリティ プロバイダーにとって今後も長期的な課題であり続けることを示唆しています。このセクションでは Talos のテレメトリを基に、2022 年における Log4j 関連の活動傾向について、最新情報を紹介します。今年特に影響が大きかった脅威の 1 つを取り上げ、以前からある脆弱性の頻繁なエクスプロイトが未だに広く見られる問題であることを再確認します。

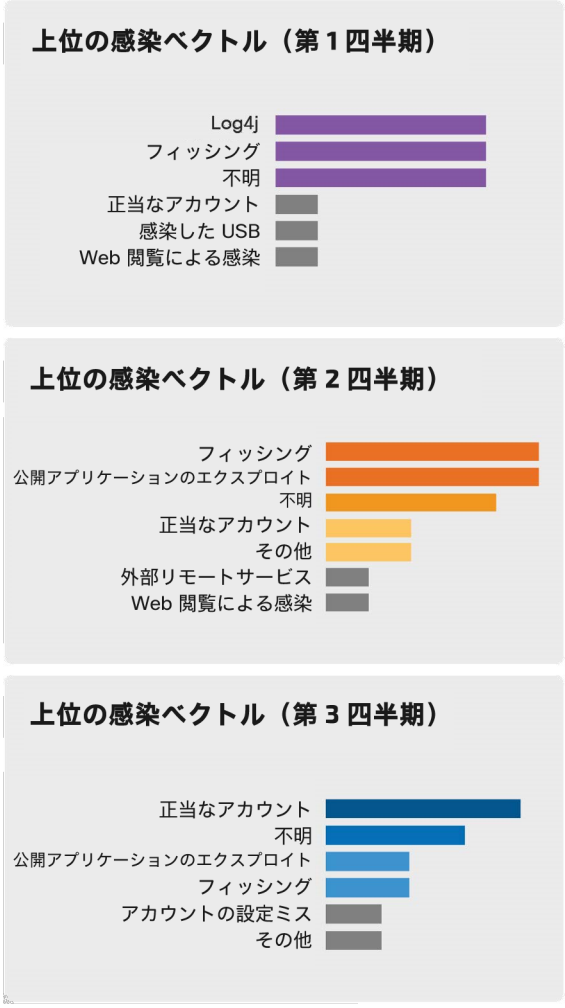


図 10. 上位の感染ベクトル（Talos IR データより）

Log4j のエクスプロイトの試みは一貫して多い状態

Log4j の脆弱性が発見されてから約 1 年経ちますが、Talos の複数のデータセットによると、攻撃者はこのセキュリティ上の欠陥を頻繁にエクスプロイトし続けています。この欠陥の発見からひと月も経たない 1 月中旬、脆弱性のある Log4j バージョンを実行している VMware Horizon サーバーへの大規模なエクスプロイトの試みが早速確認されました。複数の業界の組織が標的になったことから、無差別攻撃だったことがわかります。こうしたアクティビティはまず Cisco Secure Endpoint データとハニーポットテレメトリで確認されました。その後すぐに、さまざまな暗号通貨マイナーや追加のマルウェアの展開、PowerShell リバースシェルの使用、システム情報検出のための VMware コマンドの発行などといった、エクスプロイト後の一連の行動がいくつも確認されています。

関連する脅威アクティビティの件数は急速に伸び、脆弱なシステムを探してエクスプロイトしようとする攻撃者も多様化しました **(図 10)**。Cisco Talos インシデント対応チーム（CTIR）のデータによると、2022 年第 1 四半期には、シスコのお客様に影響を与えた脅威の 2 位に Log4j のエクスプロイトの試みがランクインしています。ランサムウェアに次ぎ、Log4j のエクスプロイトは主要な脅威の代表格であり続けました。2022 年の上半期を通じては、公開アプリケーションのエクスプロイトがフィッシングと並んで最も多い感染ベクトルだったことが CTIR の調査結果で判明しており、インシデント対応業務における Log4j の存在が際立っています。第 3 四半期に対応したインシデントの約 15% で、設定ミスのある公開アプリケーションの特定やエクスプロイトが行われていました。外部 Web サ

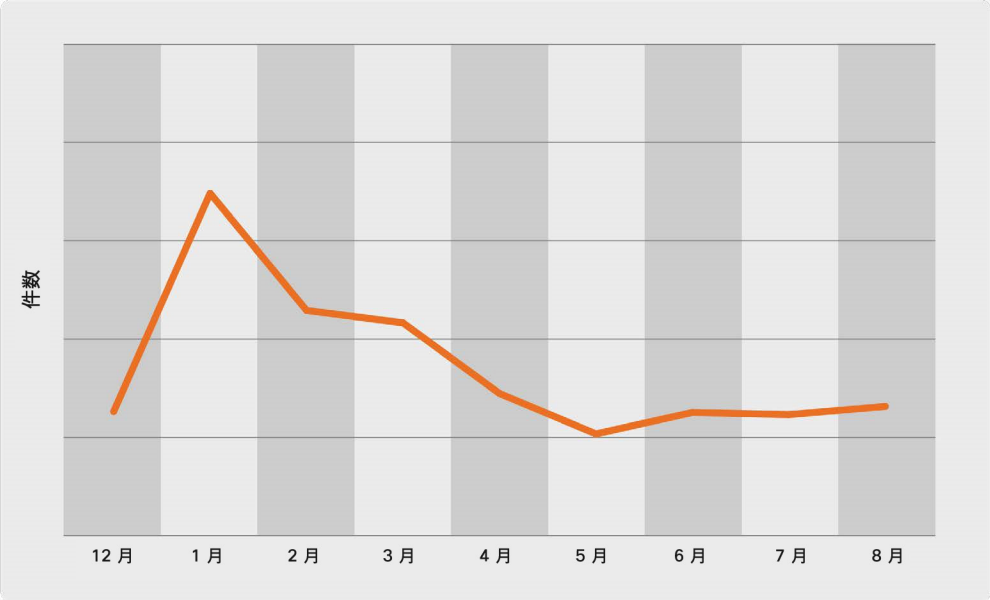


図 11. Log4j のエクスプロイトの試みであると特定された悪意のあるネットワークトラフィックに関するアラートの合計件数

イトに対して Structured Query Language（SQL）インジェクション攻撃を実行する、VMware Horizon の脆弱なバージョンで Log4Shell をエクスプロイトする、設定ミスのあるサーバーや公開されているサーバーを狙うといった手口によるものです。

CTIR データに加えて Snort テレメトリ（悪意のあるネットワークトラフィックをシグネチャによって特定するもの）からも、Log4j 関連の脅威アクティビティが年間を通じて多かったことが明確にわかります。Log4j の脆弱性をエクスプロイトしようとする試みを検出する 44 個の Snort ID（SID）を精査したところ、これらの SID に関するアラートの件数が 1 月に約 40% 急増したことが確認されました。その後、4 月からは横ばいになっていますが、アラートの件数は依然として数千万に上っています **（図 11）**。

このデータは、Log4j を使用する脆弱なシステムを探すことに攻撃者が関心を持ち続けている状況を明らかにしているだけでなく、Snort が防止に貢献した攻撃の件数も大いに表しています。SID は、ユーザーや組織によってルールの事前設定が変更されない限り、悪意のあるアクティビティを検出した時点で必ずそのネットワークトラフィックをドロップします。このデータセットにある SID はすべて、Java Naming and Directory Interface（JNDI）である Log4j の「ルックアップ」機能に含まれるリモートコード実行の脆弱性をエクスプロイトしようとする試みを検出するルールです。これは、「Log4Shell」の脆弱性（CVE-2021-44228）と直接関係があります。検出件数が多い上位 5 つの SID は、58722、58723、58742、58737、58726 でした。これらの SID の検出件数は全体の 95% を占め、月に数百万から数千万に上りました。

ランサムウェア攻撃者は常に攻撃機会をうかがっていることで広く知られていますが、Log4j の欠陥から収益を得ようと試みたのも早く、現在も試行を続けています。

スキルや動機が異なる攻撃者が活動に Log4j を利用

Log4j 関連の活動が急増した要因は、2022 年を通じて、初歩的なサイバー犯罪者から高度な攻撃を行う APT まで、さまざまな攻撃者がいたことでした。CTIR の対応業務での一例を挙げると、中国政府の支援を受けていると思われる Deep Panda が Log4j をエクスプロイトして標的のシステムにカスタムのバックドアを仕掛けている事例が確認されました。別のブログで詳しく述べたように、北朝鮮政府の支援を受けた Lazarus グループも活動において Log4j を標的としています。これらの調査結果は、Log4j の脆弱性のエクスプロイトを試みている数多くの高度な攻撃者（イランのイスラム革命防衛隊 (IRGC)、中国とつながりのある APT41 など）に関する他の報告と合致します。

暗号通貨マイニンググループは新たに見つかった脆弱性をよく悪用します。Log4j も同様で、いち早く脆弱性を探してエクスプロイトするようになりました。この中には、独立した攻撃者や、8220 マイニンググループのように長く活動している有名な攻撃者集団も含まれています。ランサムウェア攻撃者は常に攻撃機会をうかがっていることで広く知られていますが、Log4j の欠陥から収益を得ようと試みたのも早く、現在も試行を続けています。Talos は今年の第 2 四半期にこの証拠をつかみました。ランサムウェアグループ Conti のアフィリエイトが脆弱な VMware Horizon サーバーで Log4j をエクスプロイトしている事例を CTIR が確認しています。2021 年 12 月（脆弱性が公表された直後）以降の攻撃活動に Log4j が利用されてきたという、これまでの報告と合致する事例でした。セキュリティ上の欠陥が新たに発見、公開された場合、攻撃者がそれをいかに早くからエクスプロイトし始め、初期の頻繁な試みの後も長く継続するのかが、この事例からわかります。

まとめ

Log4j のエクスプロイトの試みという脅威は、2023 年以降も組織にとって課題であり続けると考えられます。サイバー攻撃者は戦術、手法、手順（TTP）が効果的であるうちは同じ TTP を再利用すると言われており、Log4j も例外ではないでしょう。Log4j は今なお、非常にエクスプロイトしやすい感染ベクトルであり、攻撃者は脆弱なシステムを可能な限り悪用し続けようとすることが予想されます。攻撃者の適応力が高いとは言え、既知の脆弱性をまだエクスプロイトできるのであれば、新しい手法の開発リソースを増やす理由はほとんどありません。

このことは、最もエクスプロイトされた脆弱性に関する CISA の年次調査結果によって裏付けられています。CISA の 2022 年の報告によると、以前からある周知のソフトウェア脆弱性がエクスプロイトされ続けていることがわかりました。これらの脆弱性の一部は、2020 年以前にも繰り返しエクスプロイトされていたものです。以前からある脆弱性がエクスプロイトされるということは、適切なタイミングでソフトウェアにパッチを適用していない組織や、ベンダーサポートが終了したソフトウェアを使用している組織はリスクにさらされ続けるということです。

Log4j は組織の環境に普及しているため、パッチの適用には困難が伴います。非常に広く使用されているライブラリであるため、大規模なシステムに深く組み込まれている場合があります。この場合、特定の環境内のどこにソフトウェア脆弱性があるのかをすべて確認することは難しくなります。さらに、Log4j には統一されたパッチ適用システムがありません。つまり、重要なセキュリティアップグレードも含め、ソフトウェアの更新が定期的または自動的に実行されることはありません。先ほど取り上げたように、2022 年に CTIR が対応した Log4j のエクスプロイト件数の多さは、攻撃者がパッチ未適用の脆弱な公開アプリケーションを狙うという手法に頼っている現状をはっきりと示しています。攻撃者の巧みな標的設定、組織におけるパッチ適用の課題、Log4j の普及度、既知の脆弱性をエクスプロイトするという攻撃者のこれまでの傾向を踏まえると、Log4j は 2023 年も脅威であり続けるでしょう。

cisco | Talos

2022 年版**一年の総括**

全般的な脅威環境

2022 年における全般的な脅威環境の確認

ウクライナへの継続的な支援と Log4j の脆弱性への対応は、2022 年における特に広範で影響の大きい取り組みでしたが、Talos は他にも数多くの脅威に対応しました。セキュリティコミュニティが攻撃者とマルウェアの増加に直面していたことが背景にあります。Talos は 1 月に、2022 年の脅威環境を変化させる、または特徴づけるであろう新たな傾向をいくつか特定しました。最終的に、その多くが今年の重大な出来事として顕在化しています。このセクションでは、Talos 全体で収集されたテレメトリセットを基に、2022 年を通じた全般的な脅威環境と主な傾向を概観します。Cisco Secure Malware Analytics の侵入兆候、Snort と ClamAV のアラート、Cisco Secure Endpoint の動作保護 (BP)、CTIR の対応業務のケーススタディなどを紹介します。

デュアルユースツール：環境内で検出を回避しながら密かに攻撃を仕掛ける手段に

APT、ランサムウェア運営者、サイバー犯罪グループなどの攻撃者は、攻撃ライフサイクル全体にわたってさまざまな操作をサポートするために攻撃フレームワークを活用しています。これらのフレームワークは攻めのセキュリティ対策を行うチームによって正当な目的で使用されているため、デュアルユースツールと呼ばれます。また、これらのツールは匿名化によって保護を強化しています。非常に多様な攻撃者の間でこれらのデュアルユースツールの利用が確認されており、そうした攻撃で見られる TTP も実にさまざまであるため、サイバーセキュリティの専門家は往々にして、ツールを使用したグループを特定しづらくなっています。

Cobalt Strike は依然として、サイバー攻撃者が好んで使用するツールです。正規のネットワーク防御ツールおよび脅威エミュレーション ソフトウェアであり、偵察、エクスプロイト後の活動、さまざまな攻撃シミュレーションなど豊富な機能を備えているため、攻撃者にとって非常に便利なツールとなっています。6 月初旬に、Cobalt Strike のダウンロード試行を検出する Snort ID (SID) 53658 と、Cobalt Strike の名前付きパイプの使用に対する Cisco Secure Malware Analytics の侵入兆候の検出が増加しました（それぞれ**図 12 と 13** を参照）。これは、1 月以降、CTIR の対応業務で Cobalt Strike の検出件数が 10% 増加したことと合致します。

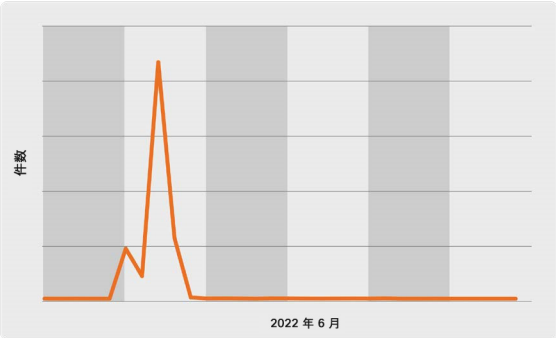


図 12. Cobalt Strike に関する Snort SID 53658 の検出件数

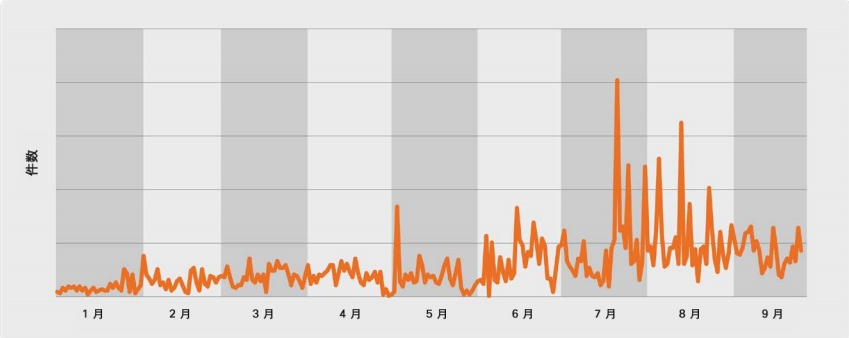


図 13. Cobalt Strike の名前付きパイプの使用についてアラートを出す侵入兆候の数

8 月には、今後他の攻撃で使用される可能性のある Cobalt Strike ビーコンを配布する攻撃が確認されました。確認されたペイロードは Cobalt Strike ビーコンの流出版であり、プロセスインジェクションを実行（任意のバイナリをターゲットプロセスに挿入）するコマンドを含んでいました。Cobalt Strike のソースコードは 2020 年後半に流出しました。現在出回っているクラックバージョンと改変版の数の多さは、攻撃活動における Cobalt Strike の成功を物語っています。これは、マルウェア攻撃の実行者が普及度の高いフレームワークの流出版を引き続き攻撃に取り入れようとしていることの表れでもあります。

Talos とセキュリティコミュニティは Cobalt Strike への対応を長年続けており、より優れた堅牢な検出機能を継続的に開発しています。こうした開発に合わせる形で攻撃者が Sliver や Brute Ratel などの攻撃フレームワークも利用するようになった可能性があると Talos は見ています。

今年に入って、オープンソースのレッドチーミング フレームワークである Sliver に関するアクティビティがエンドポイントテレメトリで確認され始めました。3 月に CTIR で対応した事例でも、同じ動きが見られました。Conti によるランサムウェア攻撃で初期アクセスを確立するために Log4j のエクスプロイトが行われましたが、これをサポートするのに Sliver が使用されたのです。

以下のケーススタディは、Sliver を取り入れた Conti のアフィリエイトに CTIR で対応したときのものです。攻撃者が正規のリモート管理ツールも使用していることがわかります。

攻撃者はパッチ未適用の脆弱な VMware Horizon サーバーで Log4j をエクスプロイトすることにより、初期アクセスを取得しました。CTIR は、悪意のある Windows インストーラファイル（「setup.msi」）のダウンロードとサイレント実行を試みる後続の PowerShell コマンドを確認しました。このコマンドが実行され、正規のリモート管理ツールである Atera Agent のインストールが開始されました。Atera Agent が提供する接続オプションにより、このランサムウェアのアフィリエイトは AnyDesk や Splashtop などの多数のリモートアクセスツールを使用して永続性を確保できます。AnyDesk のインストールには PowerShell が使用され、「C:\Program Files (x86)\AnyDeskMSI\AnyDeskMSI.exe --service」が実行されました。その後、攻撃者は PowerShell コマンドを使用して、VMware の実行ファイルを装ったペイロードのダウンロードと実行を試みました。このファイルは Sliver インプラントと特定されました。実行後、このサンプルは C2 に接続し、追加のコマンドを受信するまで鳴りを潜めていたようです。

当時、Conti が Sliver インプラントを攻撃に利用していたという報告例はなかったため、インシデント対応業務における Sliver の存在は注目に値しました。それ以来、Sliver は Cobalt Strike の代替として公に報告され、さまざまな攻撃者のツールキットに採用されています。Talos は 6 月、Avos というランサムウェアグループのアフィリエイトが、VMware Horizon ユニファイドアクセスゲートウェイにおける Log4j の脆弱性を悪用して足掛かりを築き、エクスプロイト後の活動で Cobalt Strike と Sliver を使用している事例を確認しました。

Cobalt Strike

- 正規のネットワーク防御ツールおよび脅威エミュレーション ソフトウェアであり、偵察、エクスプロイト後の活動、さまざまな攻撃パッケージなど豊富な機能を備えているため、攻撃者にとって非常に便利なツールとなっています。
- ビーコンは Cobalt Strike のペイロードであり、攻撃を生成して、HTTP、HTTPS、または DNS 経由でアウトバウンドトラフィックを作成します。Cobalt Strike ビーコンは、Metasploit フレームワークの一部である Meterpreter と同等のものとみなすことができ、侵入テスト担当者や攻めのセキュリティ対策の研究者がサービスを提供するときに使用します。

Brute Ratel

- 2020 年に攻撃シミュレーションツールとしてリリースされた、高度な正規のレッドチーミングツールです。リリース以来、攻撃ライフサイクルのさまざまなステージを円滑に進める目的で攻撃者に利用されてきました。
- Brute Ratel は特に、Endpoint Detection and Response（EDR、エンドポイントにおける検出と対応）とウイルス対策（AV）による検出を回避するように設計されています。

Sliver

- セキュリティテストの実行に使用できる、オープンソースのレッドチーミング フレームワークおよび攻撃シミュレーションツールです。Sliver のインプラントは、非対称暗号化キーでバイナリごとに動的にコンパイルされ、数多くのプロトコル（mTLS、HTTP、DNS）で C2 をサポートします。
- Sliver インプラントは、MacOS、Windows、Linux でサポートされています。Sliver は、ステージ型とステージレス型のペイロード、動的なコード生成、名前付きパイプを使用した横展開、メモリ内の .NET アセンブリの実行など、多様な機能を備えています。

Sliver に加えて、敵対的攻撃シミュレーションツールである Brute Ratel（BRc4）も攻撃者にますます利用されるようになっています。Brute Ratel は実際に攻撃のサポートによく利用されており、9 月下旬にクラッキングされ、現在は複数のハッキングフォーラムやコミュニティで無料で共有されていることから、特に懸念されています。これは、Qakbot 攻撃の実行者が Brute Ratel を使用した初の報告例であるという Talos の見解とも一致します。6 月と 9 月の 2 回、エンドポイントテレメトリで確認された一連のアクティビティから、Qakbot で最終的に Brute Ratel をドロップする攻撃チェーンが明らかになりました。脅威環境において Brute Ratel が台頭するのと並行して、Qakbot 攻撃の実行者が最近になって Brute Ratel を導入しており、クラックバージョンも利用可能になっています。このツールをポストエクスプロイトキットとして攻撃活動に取り入れる攻撃者は、今後さらに増えるものと考えられます。

「Manjusaka」と「Alchimist」という 2 つの新しい攻撃フレームワークも確認されました。実装方法は異なりますが、どちらのフレームワークも同じ設計理念に沿っており、事実上同じ機能群を備えています。このため、開発者は異なるものの要件リストは同じで、それらの要件に従って作成されたと考えられます。どちらもスタンドアロンの GoLang ベースの実行ファイルとして動作するように設計および実装されており、比較的簡単に配布できます。これらのフレームワークを使用すれば、初心者であっても攻撃を実行できます。Alchimist はすでに実際に使用されています。本レポートの執筆時点では、Manjusaka が広く展開されている状況を確認していませんが、Manjusaka は世界中の攻撃者に採用される可能性があります。

図 14. 第 3 四半期 (2022 年 7 月~ 9 月) の CTIR の対応業務で確認されたさまざまなツール

Talos では他のデュアルユースツールも確認しています。7 月から 9 月にかけて、攻撃ライフサイクルの複数のステージで攻撃をサポートするために公開ツールやスクリプトが使用されている事例が目立ちました。こうしたツールやスクリプトは GitHub リポジトリやサードパーティの Web サイトでホストされています。第 3 四半期の CTIR の対応業務だけでも、公開ツールの利用の 50% 以上がログイン情報へのアクセスと収集を狙ったものでした。公開ツールが果たす役割が浮き彫りとなっており、この攻撃ステージにおいて攻撃者の目的を推進する可能性があります **(図 14)**。攻撃者の目的遂行を支援する攻撃的なセキュリティツールやレッドチーミングツールは CTIR の対応業務でよく確認されます。しかし、これらの存在感が高まっているということは、攻撃者が監視の目をかいくぐりながら目的を達成するために、より柔軟な選択肢を常に見極めているということであり、その適応力の高さを示しています。

企業が環境内でデュアルユースツールを効果的に監視できるように、ツールの動向を追跡することが重要です。サイバーセキュリティ コミュニティが検出機能を強化し続ける中、攻撃者はより新しいデュアルユースツールに適応し、攻撃の中でそれらのツールを試し続けるでしょう。

年間を通じて使用された LoLBin

2022 年を通じて企業の環境に影響を与え続けた脅威に目を向けると、環境寄生型バイナリ (LoLBin) の利用とその関連手法が、攻撃ライフサイクルのさまざまなフェーズをサポートする目的で引き続き活用されています。LoLBin はオペレーティングシステムに事前にインストールされており、ファイルレスマルウェアや正規のクラウドサービスと組み合わせる形で攻撃に悪用されることがよくあります。攻撃者の狙いは、組織内でできるだけ検出を回避することです。これらのツールは正規の管理機能の一部として組織で使用されているため、防御側は異常な挙動がないかを監視しているときに、LoLBin を利用した攻撃を見逃してしまう可能性があります。

サイバー攻撃者は TTP が効果的であるうちは同じ TTP を再利用すると言われており、LoLBin も例外ではありません。Talos が 2019 年に LoLBin のハンティングに関する記事を公開して以来、攻撃者は自らの活動をサポートする目的で、攻撃のあらゆるステージで正規のユーティリティを利用し続けています。2022 年における Cisco Secure Endpoint の動作保護(BP) デー

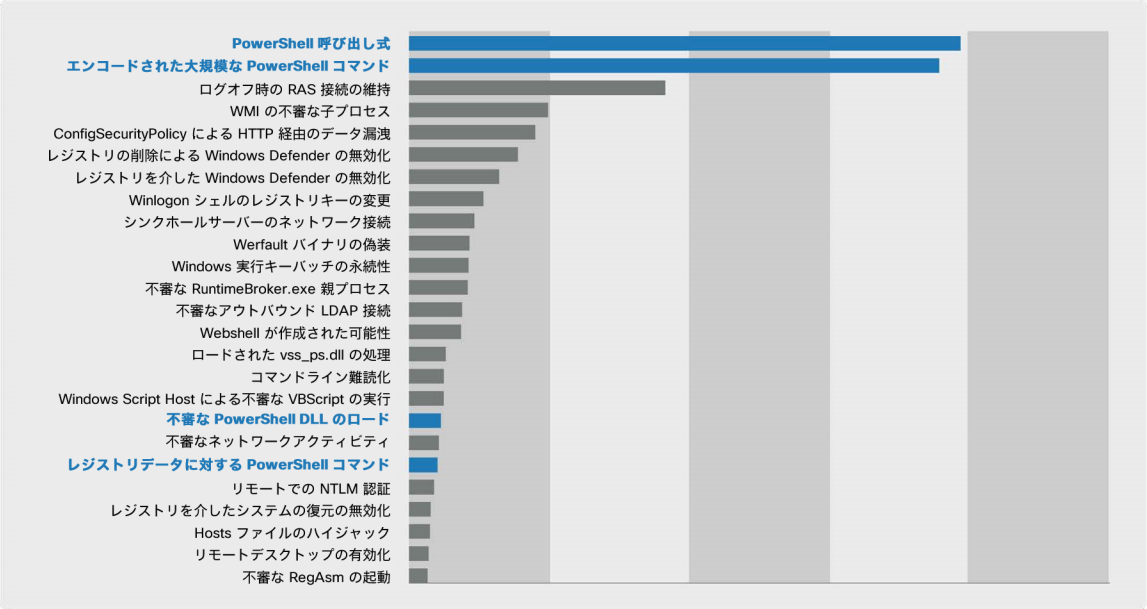


図 15. アラートが多かった動作保護シグネチャの上位 25 個 (2022 年 1 月~ 9 月)

タを確認すると、アラートが多かった BP シグネチャの上位 25 個のうち 4 個は PowerShell 関連のものであり、攻撃者が PowerShell の悪用可能性に目を付け、利用し続けている状況が浮き彫りになっています **(図 15)**。PowerShell の悪意のある使用は広まっており、ChromeLoader のようなアドウェアのインストール、暗号通貨マイナーのダウンロード、Elasticsearch といったソフトウェアの脆弱性のエクスプロイトなど、さまざまな攻撃活動をサポートする目的で利用されています。

Microsoft の PsExec も攻撃者に頻繁に悪用されるネイティブユーティリティです。プログラムやプロセスをリモートで実行する機能を備える PsExec は、第 3 四半期（7 月から 9 月）に CTIR の対応業務で確認されたランサムウェア攻撃の 75% で、ランサムウェアの実行に重要な役割を果たしました。

Black Basta によるランサムウェア攻撃では、悪用頻度の高い別の LoLBin である「vssadmin.exe」が確認されました。これは、ボリュームシャドウコピーのバックアップを使用してローカルのシャドウコピーを削除するという、ランサムウェア攻撃者に一般的な手法が使われていることを示すものです。その直後、PsExec によって悪意のあるランサムウェア DLL の起動と、VSSadmin を使用したローカルバックアップの削除が行われ、影響を受けたエンドポイントで拡張子が「.basta」のファイルが確認されるようになりました。

正当な目的で使用されたと思われるものから判断が難しいものまで、LoLBin が防御側にもたらす特有の課題を考えると、LoLBin は今後もさまざまな攻撃者の間で好んで利用されると予想されます。

古いとされていた手法が新しくなって復活：USB 攻撃が 2022 年に増加

再認識させられるのは新たな脅威の出現や攻撃者の TTP の進化だけではありません。攻撃者は、旧式でパッチが適用されていない企業のレガシーシステムに今なお効果がある手法を今後も利用し続けるでしょう。そうした旧来の手法が機能しなくなった場合にのみ、適応していくと思われます。1 月以降、CTIR が対応した業務で、リムーバブル USB ドライブによって組織にマルウェアを感染させた事例が増加し続けています。Sality、PlugX などの複数のマルウェアファミリがこの手法で配布されていました。Windows システムを標的とするマルウェアであり、リムーバブルドライブ経由で拡散することがわかっています。USB ドライブは攻撃の初期アクセスを確立する目的で長年利用されてきましたが、今回見られた動きは USB 関連の脅威が和らいでいないことの表れであり、USB からの感染を防ぐ重要性を強調し続ける必要があることが明確になっています。

こうした動きは、Cisco Secure Malware Analytics で、USB などの外部ドライブに関連するさまざまな挙動全般の検出件数が増加したことも合致しています。たとえば実行ファイルを USB ドライブに書き込む挙動や、検出を回避するために USB ドライブ上のファイルの隠し属性を設定する挙動で検出件数が増加しました（それぞれ**図 16 と 17** を参照）。**図 17** に見られる 7 月の急増は説明できませんが、USB を利用した脅威の年間件数が、USB の使用に関連する挙動全般の増加に寄与しているようです。これについては以下で詳しく取り上げます。

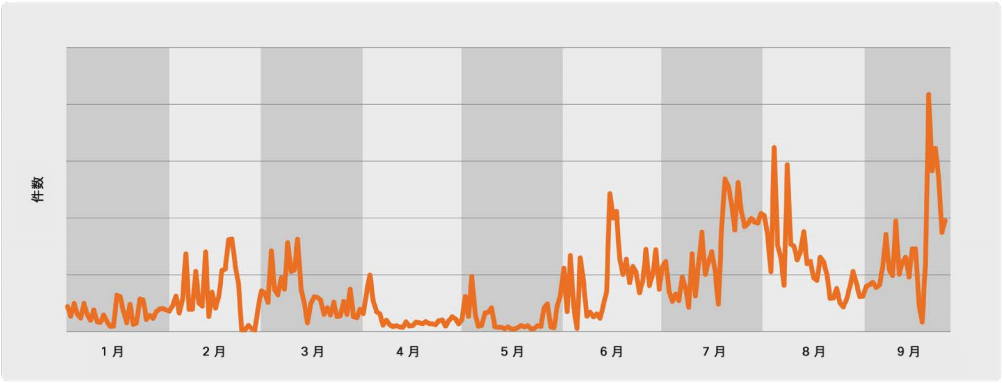


図 16. 実行ファイルが USB に書き込まれたという侵入兆候の件数

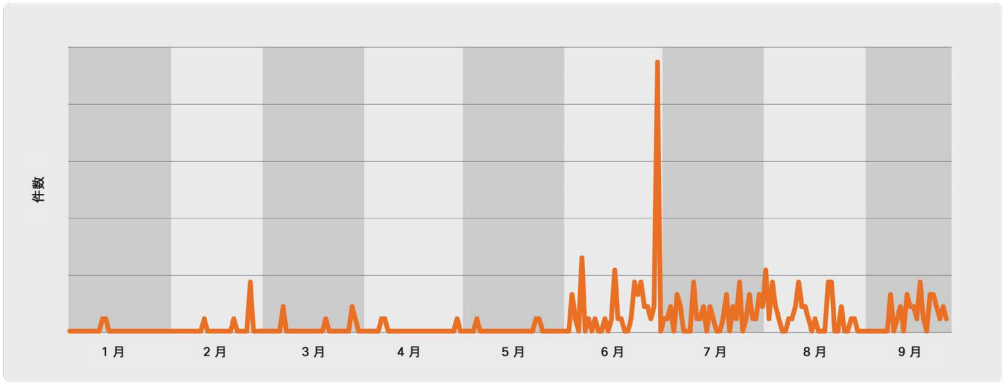


図 17. USB 上のファイルの隠し属性が設定されたという侵入兆候の件数

Talos では Raspberry Robin というマルウェアに関連する継続的な活動を追跡してきました。Raspberry Robin は多数の LoLBin を利用し、USB デバイスなどの外部ドライブを介して自己拡散できるワームのような機能を備えています。Windows の正規のインストーラである「msiexec. exe」に関連するコマンドライン アクティビティの特徴的なパターンとして、難読化されたコマンドライン引数を明らかにするアクティビティがエンドポイントテレメトリで確認されました。これらのコマンドライン引数は、感染した外部ドライブの名前を取得していると思われ、「USB」、「USB DISK」、「USB Drive」を含む値を持っていました。Raspberry Robin は最初の感染後、侵害された QNAP ネットワーク アタッチト ストレージ（NAS）デバイスから「msiexec. exe」によってペイロードをダウンロードし、Windows の正規のユーティリティである「rundll32.exe」を使用してそのコードを実行し、The Onion Router（Tor）接続を介して C2 チャネルを確立します **（図 18）**。

自動ハンティングルールに基づく Talos の脅威ハンティングテレメトリではこのアクティビティが継続的に確認されています。ただし**図 19** に見られるように、Raspberry Robin 関連のアクティビティを検出する自動ハンティング件数は 4 月に急増し、数か月にわたって一貫して多い状態が続きました。

この脅威の分析を続けたところ、Microsoft のユーザーアクセス制御（UAC）機能をバイパスする試みも確認されました。侵害したデバイスを高度な権限または管理者レベルの権限で操作するために、サイバー攻撃者は UAC を頻繁に悪用します。Raspberry Robin は、システムバイナリの使用、Tor ベースのコマンドアンドコントロール（C2）、侵害した QNAP アカウントの悪用によって検出を回避しようとします。攻撃者の最終的な目的は依然としてわからない部分が多いものの、Raspberry Robin は世界中のお客様のエンドポイントで大量に確認され続けています。

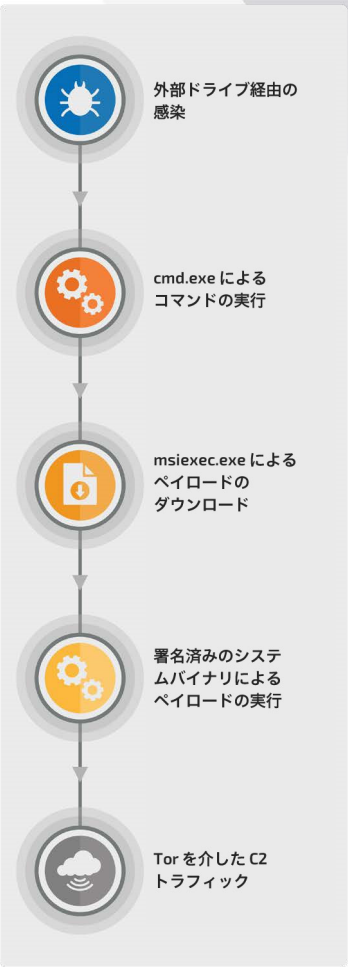


図 18. Raspberry Robin の実行チェーン

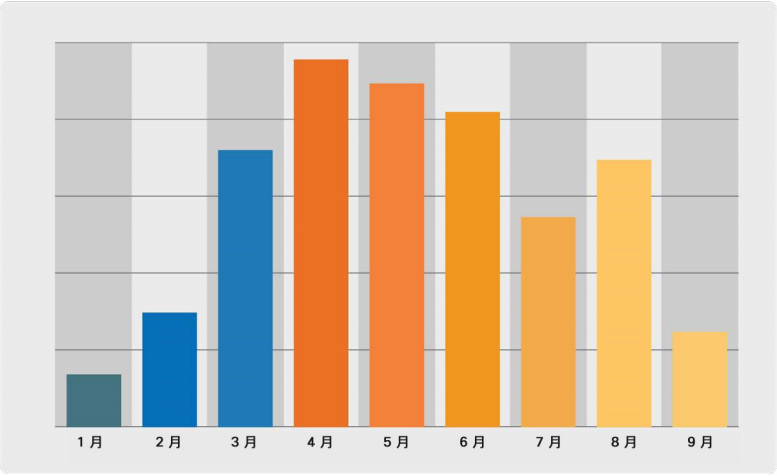


図 19. 経時的な自動ハンティングで特定された Rasperry Robin 関連のアクティビティ

USB を攻撃に利用するという傾向は、CTIR の対応業務とエンドポイントテレメトリ以外でも継続的に確認されています。2022 年にいくつかの APT グループが攻撃作戦とマルウェアを、USB ドライブを利用する形に変更していることがわかりました。たとえばパキスタンとのつながりが疑われる Transparent Tribe は USB モジュールを取り入れており、北朝鮮を拠点とする Lazarus グループ は USB ドライブからファイルやフォルダをコピーするために USB ダンプを実行しています。

さらに 2022 年 1 月、米連邦捜査局 (FBI) は、米国保健福祉省の名を騙った郵便物で新型コロナ関連の情報を格納したとする悪意のある USB ドライブが送られてくる件について、組織に警告を発しました。USB がユーザーのマシンに接続されると、自身をキーボードとして登録し、自動化されたキーストロークをマシンに送信して悪意のある PowerShell コマンドを実行します。この PowerShell コマンドによってマルウェアがダウンロードされ実行される仕組みです。一部の事例では、侵害されたネットワークにランサムウェアが展開されました。

まとめ

セキュリティコミュニティは不正なデュアルユースツールと LoLBin の追跡や検出に役立つプレイブックとガイダンスを公開し続けています。このため攻撃者は、分析を妨害するために TTP を変え、更新せざるを得ないと感じるようになるでしょう。実際、セキュリティチームにあまりなじみのない比較的新しい攻撃フレームワーク (Sliver や Brute Ratel など) が攻撃に利用されるようになってきています。さらに、普及度の高いレッドチーミングツールのクラックバージョンや流出版が今後も攻撃に取り入れられ、配布ライセンスに伴う高額なコストを回避しつつ、それらのバージョンを利用する攻撃者の数がさらに増えていく可能性があります。

組織は、通常の使用パターンと異なる操作 (サービスの変更やファイルの実行など) を実行可能なツールのコマンドライン呼び出しを監視することによって、レジリエンスを高め、先述のデュアルユースツールや LoLBin を攻撃者に悪用されるリスクを軽減できるようになります。また、Windows サービスに関連する実行ファイルなどへの変更がレジストリに反映されていないかを監視すれば、攻撃者が永続性を確保しようとするリスクを最小限に抑えられます。

さらに、2022 年に USB 攻撃が復活したことから、比較的古い攻撃ベクトルに対する企業の関心の薄れを利用するために、攻撃者が戦術を適応させるであろうことがわかりました。正当な業務のために USB などのリムーバブルドライブを使用する可能性があるすべての組織で、環境内での USB の使用を制限し、できれば使用禁止にすることを推奨します。また、既知および未知の USB を企業システムや個人デバイスに接続することに伴うリスクについて、ユーザーの意識向上トレーニングを設けることをおすすめします。

cisco | Talos

2022 年版一年の総括

ランサムウェアの脅威環境

ランサムウェアのアフィリエイトはもはやサイロ化されておらず、複数のグループにまたがって活動しています。こうした状況では、スキルセットの特異性が高い攻撃者ほど、複数の攻撃作戦や組織に加担する機会が多くなっています。

ランサムウェアの脅威環境

新たな RaaS（サービスとしてのランサムウェア）グループの出現、既存グループの名称変更や活動停止により、ランサムウェアの脅威環境は進化しています。2022 年に入った頃、Talos は、ランサムウェアの脅威に対抗するために打ち出された米国政府一丸の取り組みがもたらし得る影響を注視し続けていました。この取り組みでは、財務省、司法省、国務省をはじめとする行政機関により、ランサムウェア攻撃者の能力を削ぐことを目的とした計画が定められました。同じ頃、世界中の法執行機関と民間部門でも同様のランサムウェア対策が講じられましたが、この取り締まりはロシアによるウクライナ戦争を背景に開始され、脅威環境の大きな変化を促してきました。とはいえ、ランサムウェアの脅威は今なお広く見られます。2022 年は特に教育分野が狙われ、全業種の中でトップでした。

Talos では十数の RaaS グループの動向を追跡しており、ランサムウェアのデータリークサイトに被害者情報が投稿されると監視を行っています **(図 20)**。なお、投稿日時を記載していないグループもあったため、**図 20** のリストは 1 月から 10 月のすべての投稿を反映していない可能性があります。Talos の調査結果によると、今年最も活発に活動した RaaS グループは LockBit で、ダーク Web における被害者情報の投稿総数の 20% 以上を占めています。これに Hive と Black Basta が続きました。LockBit に関する調査結果は、今年 Talos が同グループの活動全般について追跡して把握した内容とかみ合っています。後で詳しく述べるように、LockBit は妨害行為の増加に直面する中、新機能やアップデートを発表し続けています。

これらの調査結果は、ランサムウェア攻撃者の民主化の進行という傾向を裏付けるものでもあります。Talos は遅くとも 2022 年第 1 四半期には、CTIR の対応業務中に見られるこの傾向を取り上げていました。シスコのマルウェア分析プラットフォーム、Cisco Secure Malware Analytics、社内のダーク Web 監視活動といった複数のテレメトリソースにおいて、民主化が進行している様子が見て取れます。数多くのランサムウェアグループが出現しており、一部の少数のグループが圧倒的な存在感を誇っていた過去数年間とは全体的な変化が見られるのです。ランサムウェアのアフィリエイトはもはやサイロ化されておらず、複数のグループにまたがって活動しています。こうした状況では、スキルセットの特異性が高い攻撃者ほど、複数の攻撃作戦や組織に加担する機会が多くなっています。RaaS 環境におけるこのような多様化は、初期アクセスを確立するための TTP の違いにも表れています。注目されている脆弱性を利用する手法から、フォーラムで初期アクセスブローカー（IAB）を介してアクセス手段を購入する手法までさまざまです。

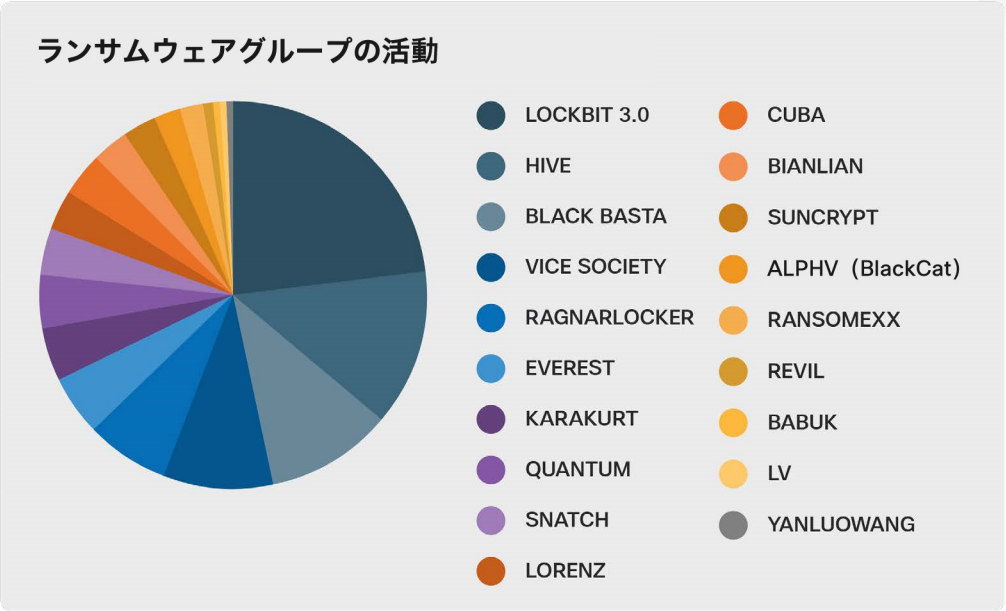


図 20. 1 月~ 10 月における、ランサムウェアのデータリークサイトへの投稿件数 (Talos の追跡調査より)

2022 年全体で見ると、Hive は CTIR の対応業務のいくつかの事例で確認された主要なランサムウェアファミリであり、これに Vice Society と Conti が続きました。ところが、2022 年になって数か月が経つと Conti は活動停止を発表し、6 月までにインフラの大半をオフラインにしました。これについては後で詳しく説明します。Conti の活動停止からほどなくして、Conti が名称変更したものと思われる Black Basta という比較的新しいファミリが現れました。Black Basta の登場は遅く、2022 年に入ってからのことですが、データリークサイトへの投稿件数 **(図 20)** が証明しているとおり、同グループは短期間で驚くほどに活動を活発化させました。

2022 年のインシデント対応事例全体に占める割合という観点でランサムウェアを見てみましょう **(図 21)**。第 4 四半期のデータが一部揃っていないという前提で、誤検出を除くと、これまでの CTIR の対応業務で確認された脅威の 20% 強をランサムウェアが占めていることがわかります。CTIR でのランサムウェアの確認件数は、第 1 四半期に最も多く、第 2 四半期には減少し、第 3 四半期の終わりまでに再び増加しました。これは、先に述べた傾向 (2 月から 6 月にかけて、ランサムウェアなど CTIR が確認した脅威の件数が減少) に沿ったデータであり、ウクライナ戦争の開始以降、攻撃者がロシアとウクライナに集中的に攻撃を仕掛けていた可能性を示唆しています。

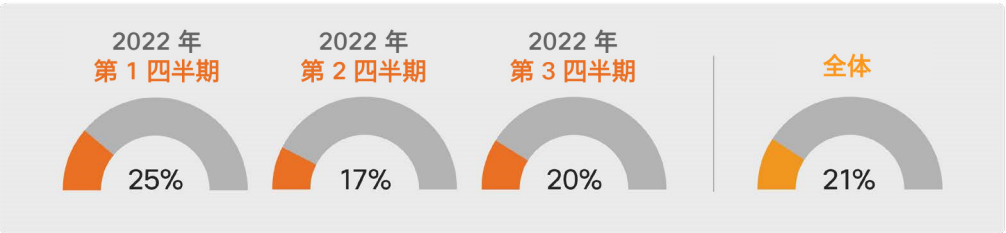


図 21. 2022 年のインシデント対応事例に占めるランサムウェアの割合

2022 年に最も狙われたのは教育分野

国の重要インフラ分野に含まれる教育分野は、1 月以降の CTIR の対応業務においてランサムウェア攻撃の影響を最も受けています。一般に、教育分野が狙われるのは珍しいことではありません。ただ今年の状況は、ランサムウェアグループの標的が教育分野に偏っているという現在の傾向の一端を示すものであり、米国サイバーセキュリティ インフラストラクチャ セキュリティ庁（CISA）の報告と一致しています。ランサムウェアのアフィリエイトは今後も教育機関を高価値の標的とみなし続けるでしょう。特に、ダウンタイムを許容しがたい新学期などに狙われる可能性があります。さらに、学資援助や学生ローンといった大学の中核的なサービスを混乱させることで、一刻も早く通常の業務に戻るために被害者が身代金を支払うように仕向けることも考えられます。

Vice Society ランサムウェアが教育機関に影響を及ぼした事例を分析したところ、感染したホストから他のシステムに対して Remote Desktop Protocol (RDP) のアウトバウンド接続が何度も試行されていたことが明らかになりました。これは、ラテラルムーブメントが試行されたことを示唆しています。Talos はリモートアクセス ソフトウェア ツールである AnyDesk と TeamViewer の 2 つを特定し、50 以上のシステムが TeamViewer にアクセスしていることを確認しました。また、Windows Defender のファイアウォールに例外が追加され、SYSTEM アカウントによる「AnyDesk.exe」の実行が可能になっていました。おそらく PsExec の実行がトリガーとなり、続いてランサムウェアが展開され、侵害されたユーザーの Windows ローミングプロファイルに書き込まれていたものと思われます。

今年に入ってからの CTIR の対応業務で見ると、最も狙われた分野は教育でしたが、その次に影響が大きかったのは地方政府および地方自治体でした **(図 22)**。

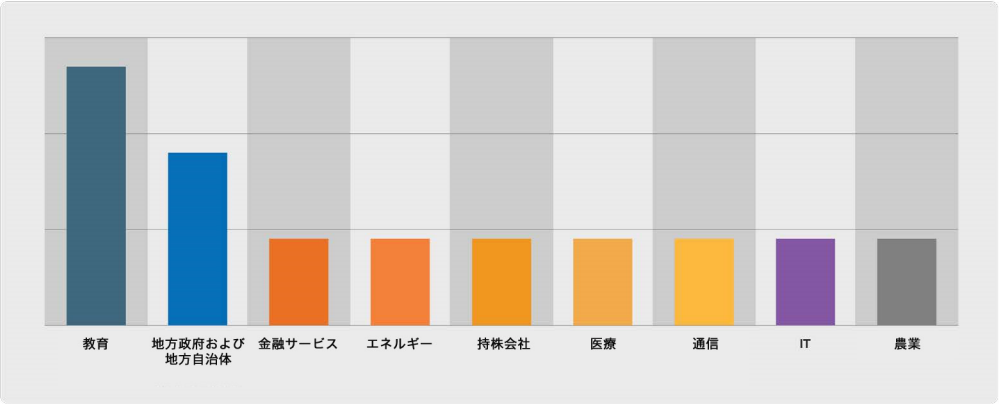


図 22. 2022 年 1 月から 9 月に CTIR で確認されたランサムウェアインシデントの分野別件数

ランサムウェアグループがロシアとウクライナの戦争に加担

先ほどウクライナのセクションで述べたように、ウクライナで戦争が勃発したのを受け、多くの攻撃者がどちらの陣営につくかを決め、親ロシア派または親ウクライナ派を攻撃の標的にするようになりました。Talos はこうした状況の初期兆候を確認していました。ランサムウェアグループをはじめとするサイバー犯罪者が、ロシア政府への支持または反対の声明を出し始めたのです。ウクライナ侵攻が始まったときには、予想し得なかった攻撃者が次々と現れ、不特定多数の人による攻撃が組織にとって現実の脅威となりました。一般に公開されている報告によると、ダーク Web フォーラムの管理者はロシア政府の行動に明確に反対し、ロシアから接続するユーザーを締め出す旨を発表しました。

RaaS グループの Conti は戦争開始時に最も声高に立場を主張していたグループの 1 つであり、ロシアによるウクライナ侵攻を妨害しようとする者は誰であっても攻撃すると警告しました。Conti のこうした主張や、類似のグループが行った主張がきっかけとなり、多くのランサムウェア コミュニティ メンバーの間で内部対立や仲間割れが起きました。Conti メンバーがロシアによるウクライナ侵攻への支持を公表したところ、Conti とつながりのある人物が同グループへの報復として、マルウェアのソースコードやアフィリエイト間の内部チャットといった、同グループに関する情報を流出させました。Conti では 2021 年以降、一連のプレイブックの形で TTP が流出し続けています。流出元は、反発を抱いたアフィリエイトだと言われています。Talos はこれらの流出情報を入手でき、Conti 運営者どうしで交わされた内部メッセージ、組織内のさまざまな役割、アフィリエイトの新規採用プロセスなど、興味深い活動情報が明らかになりました。一般に公開されている報告から、Conti が自らの決断による影響に対処し続けていることが確認できます。そのような一連の動きの例として、以前は Conti の元メンバーによって運用されていた Cobalt Strike サーバーに反ロシア的なメッセージが大量に送り付けられました。

ロシアがウクライナに侵攻した後、注目度の高いサイバー犯罪グループや新興のサイバー犯罪グループがいずれかの国の側につきました。 あらゆるレベルのサイバー犯罪組織に侵攻の影響が及んだことがわかります。Conti に続き、Stormous ランサムウェアグループや CoomingProject といった、あまり知られていないランサムウェア攻撃者もロシアへの支持を公言し、ウクライナとその同盟国に政治的動機による攻撃を仕掛けることを主張し始めました。

ウクライナ侵攻が始まったときには、予想し得なかった攻撃者が次々と現れ、不特定多数の人による攻撃が組織にとって現実の脅威となりました。

RaaS コミュニティ内部での摩擦が脅威環境の進化を助長

ランサムウェア環境は絶えず変化しており、地政学的環境の変化、防御側の対策、法執行機関の取り組みに適応し続けています。2022 年には変化の範囲が広がり、激しさも増しました。こうした状況を背景に、名称変更、活動停止、新たな戦略的協力関係の構築を行うグループが出てきています。

Talos はランサムウェア環境の変化を継続的に追跡するにあたり、ダーク Web フォーラムを常に注視し、運営面の変化と、特定のグループに対する RaaS メンバーの不信感の高まりを明らかにしています。往々にして、状況が変わればランサムウェア環境に影響が波及し、RaaS グループが人材を呼び込んで採用しながら既存のメンバーを維持する方法も変わってきます。このような状況下では、一般に公開された情報を基に RaaS グループを監視するのが難しくなる可能性があります。

2022 年 5 月に先述の情報流出が起きた後、Conti はまず活動停止を発表し、データの暴露と被害者との身代金支払いの交渉に使用していた Tor サーバーなど、インフラの大半を 6 月までにオフラインにしました。このとき、シスコのテレメトリで Conti の検出件数が全体的に減少しました。**図 23** に示すように、Cisco Secure Malware Analytics（SMA）の侵入兆候データセットで特に顕著です。

Conti の活動停止の影響が出始めた今年半ばには、Conti が名称変更したものと思われる「Black Basta」というグループが現れました。一般に公開されている報告によると、2 つのファミリが類似しているという根拠は、身代金支払い用の Web サイトとリーク用 Web サイト、一部のメンバーのコミュニケーションスタイルが似ていることです。Talos は Black Basta に関する SMA の侵入兆候を作成し、この脅威が台頭する様子をとらえました。5 月下旬に、Black Basta によるレジストリ変更が検出され始めました **(図 24)**。Black Basta の身代金要求メッセージ画像がドロップされる直前、壁紙を表示するように被害者のデスクトップが変更されますが、その場合にアラートが出るようになっています。

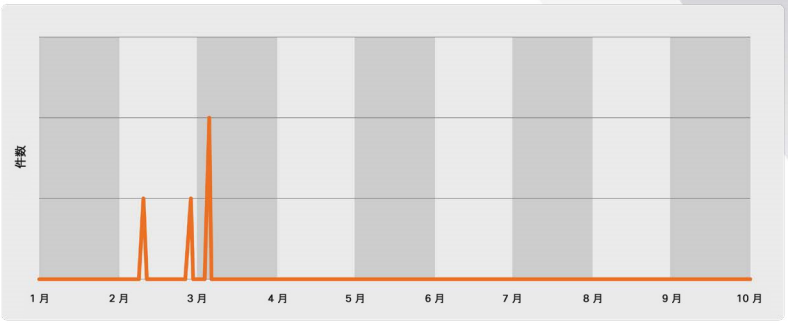


図 23. Conti ランサムウェアに関する侵入兆候の検出件数

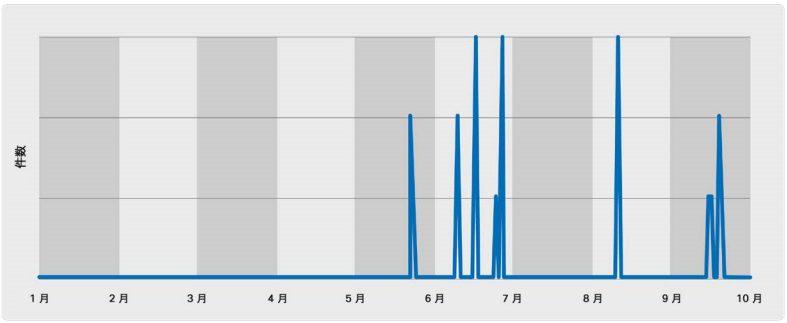


図 24. Black Basta によるレジストリ変更に関する侵入兆候の検出件数

流出情報の公開に関して今年コミュニティでよく話題になったと思われるのが、「LockBitBlack」という LockBit 3.0 ランサムウェア暗号化ツールの流出したビルダーが公開されたことです。ビルダーを流出させたと明言している人物は LockBit の開発者とされており、LockBit によれば、その人物は同グループの支払い体系に不満があると主張していました。Talos は、流出したビルダーを分析し、そのビルダーから生成した新しい 2 つの Snort ルール（60622、60623）によるアラートを確認しました。その結果、このビルダーは、独自のランサムウェア攻撃に必要な実行ファイル（暗号化ツール、復号ツール、復号ツールを起動するための専用ツールなど）を誰もが構築できる仕様になっていることがわかりました。このビルダーには暗号化ツールのカスタマイズに使用できる構成ファイルが含まれており、標的ごとに身代金要求メッセージを変更する、構成オプションを変更する、終了するプロセスとサービスを決定する、暗号化ツールのデータ送信先となる C2 サーバーを指定するなどの調整を行えます。攻撃者は構成ファイルを変更することで、自分のニーズに合うようにカスタマイズしたり、作成された身代金要求メッセージを編集して自分の C2 インフラへのリンクを記載したりできます。

8 月には、ALPHV（別名 BlackCat）や LockBit などいくつかの有名なランサムウェアグループの公開データリークサイトが DDoS 攻撃を受けている疑いがあることが確認されました。この手のサイトは通常、Tor の隠しサービスでホストされています。二重恐喝と呼ばれる戦術では、身代金の要求が通らなかった場合に RaaS のアフィリエイトが被害者の情報を掲載する先としてリークサイトが利用されます。その後すぐに、少なくとも他の 7 つの RaaS リークサイトがアクセスできなくなり、断続的にオフラインになっている状態が確認されるようになりました。いくつかの RaaS リークサイトは数週間にわたって断続的なサービス停止に追い込まれました。これらの RaaS グループが新しい被害者情報を投稿できないよう妨害することで、RaaS 運営者とアフィリエイトの間に混乱あるいは内部対立を引き起こすことを狙った共同での活動だったと考えられます。誰が攻撃を仕掛けていて、動機が何なのかは依然不明です。ただ、内部対立を起こさせたり、望まない注目を浴びさせたりするために敵対者が混乱をもたらした可能性があることから、影響を受けた一部のグループの間で緊張が走ったと考えられます。

流出した LockBit 3.0 ビルダーは今後、防御者や研究者に課題をもたらす可能性があります。LockBit による攻撃が疑われる場合の犯人特定が難しくなるからです。複数のグループがすでにこのビルダーを攻撃に取り入れ始めました。たとえば「BI00dy Gang」という新しいランサムウェアグループが、流出した LockBit 3.0 ビルダーを最近の攻撃で使っています。Conti のプレイブックの流出でもそうだったように、スキルがあまり高くない攻撃者がランサムウェアを独自開発せずに、他のランサムウェアグループの流出したビルダーやソースコードを使用することで時間とリソースを節約できるようになる可能性があります。

クロスプラットフォームのランサムウェアによって適応力を向上

現在、ランサムウェア亜種のアジャイル開発を推進するために Rust や GoLang などのクロスプラットフォームのプログラミング言語を使用するランサムウェア運営者が増えており、研究者による分析やリバースエンジニアリングが難しくなる可能性があります。

攻撃者が身代金の額を決定する方法、減額交渉に応じる姿勢、営業戦術、被害者に支払いを迫る手法を見抜くことができました。

2022 年 4 月、FBI は ALPHV ランサムウェアグループに関連する IOC を公開しました。ALPHV は、プログラミング言語 Rust を使用してランサムウェアを商品化した最初のグループとして知られる特異な存在です。Rust を活用することで、ランサムウェアを Windows OS と Linux OS の両方に対して使用できるため、ALPHV のアフィリエイトは標的ごとに最初の感染ベクトルを調整できます。

3 月下旬には、Hive 運営者が VMware ESXi Linux 暗号化ツールを Rust に切り替える更新を行い、被害者との交渉をセキュリティ研究者に監視されにくくするための新機能を追加していることが確認されました。3 月から Hive と被害者との間で交わされたチャットのログを入手して確認したところ、Hive 運営者は暗号化ツールも Rust で記述されたものに更新して使い始め、他の復号ツールは役に立たないことを被害者にほのめかしていました。なお、韓国の国民大学校の研究者が Hive ランサムウェアに感染したファイルの復号方法を説明する論文を公開しましたが、上述のチャットはその論文よりも前のものです。約 1 か月後に、韓国インターネット振興院（KISA）が回復ツールをリリースしています。このような更新を重ねていることから、Hive の開発者がセキュリティ研究者に何度も痛い目に遭わされ、政府の取り締まりを受けても活動を続けていくつもりであることがわかります。

ダーク Web からもわかる RaaS の状況

Talos はダーク Web とアンダーグラウンドのサイバー犯罪フォーラムを継続的に分析する中で、ランサムウェアグループの流出したコンポーネントを入手しています。こうして得た知見は、入手したコードと TTP を基に検出機能と防御用プレイブックを作成してお客様へのサポートを改善したり、これらの活動に関わるランサムウェアのアフィリエイトをより詳細に追跡したりすることにつながっています。

Talos は一般に公開されている情報の調査を通じて、ランサムウェアグループ Conti および Hive の運営者とその被害者との間で交わされた 4 か月間のチャットログ（40 回を超す会話）を入手し、分析しました。このチャットログは、攻撃者と被害者の間のコミュニケーションスタイルと身代金交渉における微妙な違いを浮き彫りにしています。これらのチャットを分析することで、攻撃者が身代金の額を決定する方法、減額交渉に応じる姿勢、営業戦術、被害者に支払いを迫る手法といった、攻撃活動の詳しい実態を見抜くことができました。

また、Talos はランサムウェア運営者のインフラを見つけやすくする手法を特定し、これまで謎に包まれていた複数のランサムウェアグループ（DarkAngels、Snatch、Quantum、Nokoyawa など）のインフラを発見しました。ランサムウェア運営者は自分たちの活動を隠すためにダーク Web でのみ行動するのが一般的で、被害者とやり取りするポータルには、Tor ネットワーク上で特定の URL を使用しないとアクセスできません。ランサムウェア運営者らは Tor を使用して活動を隠してはいるものの、使用されているインフラの一部がわかる構成ミスを Talos の調査で特定することができ、グループの活動やリソースに対する理解が深まりました。

2021 年末から 2022 年初めにかけて、XSS や Exploit といった人気のダーク Web フォーラムはランサムウェア関連の販売行為と会話に対する制限を厳しくし、ランサムウェア関連の会話を行ったメンバーの出入りを禁止すると脅していました。ランサムウェアの広告やサービスを削除することさえありました。一方、RAMP（Russian Anonymous Marketplace）などのように、ランサムウェア関連の売買活動を歓迎すると明言するフォーラムもありました。しかし 2022 年の後半には、RAMP までもが管理者の交代に伴ってコンテンツを制限するようになりました。Talos のロシア語翻訳担当者の指摘によれば、ロシアのハッカーコミュニティにおける RAMP の評判は、現在の管理者になってから悪化しているとのことです。汎用チャットルームに参加している人数は 1 桁台で非常に閑散としており、RAMP の管理者かモデレータの発言が大半という状況だと言います。一方で XSS には 4 万人近くのメンバーがいます。今でもランサムウェア関連の会話は厳しく制限されていますが、参加状況に RAMP ほどの大きな変化はありません。

まとめ

Talos は今年、ロシアとウクライナの戦争と進化し続ける RaaS コミュニティを背景に進行した、ランサムウェアファミリと攻撃者の増加に直面しました。こうした変化が加速したのは遅くとも 2021 年半ばだと言えるでしょう。この時期に、Colonial Pipeline 社に DarkSide のランサムウェア攻撃が仕掛けられ、これを受けて法執行機関が REvil のテイクダウン措置を行ったことで、いくつかのランサムウェアグループの協力関係がなくなりました。今年に話を戻すと、ランサムウェア環境はかつてないほど変わりやすくなっているように見えます。法執行機関や民間部門が次々に妨害措置を講じるようになったこと、仲間割れやグループ内に潜む脅威の存在、競争市場でランサムウェアの開発者や運営者が最大の利益を求めて手を組む相手を変え続けるといった状況に、さまざまなグループが適応しようとしていることが背景にあります。

この 1 年でわかったように、組織が強い警戒感を持ってランサムウェアの脅威に対する検出機能と軽減策を生み出し続けている現状を踏まえると、こうした流れは 2023 年も続く可能性が高いでしょう。CTIR の第 3 四半期のデータに見られた傾向として、ランサムウェアの感染前と感染後の対応件数が同じであり、両者を合わせると同四半期の 40% 近くを占めました。この結果は注目に値し、ランサムウェアコミュニティにおける専門化とアウトソーシングの進行を表している可能性があります。さらに、防御側の検出手法が進化し、最終的なペイロードがドロップされる前の不審な挙動を警告することに重点を置くようになったことも示しています。

しかし、圧倒的な勢いを誇るランサムウェアグループがいなくなったことで、脅威インテリジェンスのアナリストは課題を突き付けられています。前掲の図 20 からわかるように、Talos が積極的に監視しているデータリークサイトへの投稿の 75% は、少なくとも 8 つのグループによるものです。攻撃者が複数の RaaS グループにまたがって活動している現状では、新しいグループが出現すると犯人の特定が難しくなります。

2023 年の 1 つの傾向になりそうな状況として Talos が確認しているのは、LockBit などのグループが恐喝手段を増やし始めていることです。たとえば身代金要求に応じなければ被害者の組織に対して DDoS 攻撃を仕掛けると脅しています。防御側はランサムウェア感染前の TTP に関連する挙動を検出し続けています。このため、検出を回避しながら金銭的な支払いを受ける手段として、ランサムウェアグループが独創的で進化を続ける恐喝戦術に頼ってランサムウェア展開前に恐喝を行うようになる可能性があります。

cisco | Talos

2022 年版一年の総括

コモディティ型ローダー

2022 年に特に活発に展開された上位 4 つのコモディティ型ローダーは、Qakbot、Emotet、IcedID、Trickbot でした。

コモディティ型ローダー

コモディティ型ローダー（第 2 段階のマルウェアを展開する商用のトロイの木馬）は常に存在する脅威であり、すべての業界に世界的な影響を与え続けています。そのため Talos は、コモディティ型ローダーのマルウェアファミリとそれらがお客様のネットワークにもたらす脅威を定期的に追跡しています。このセクションでは、2022 年に Talos がコモディティ型ローダーを調査した結果について、複数のデータソースを十分吟味しながら考察していきます。

ネットワークとエンドポイントの複数のテレメトリセットを分析したところ、2022 年に特に活発に展開された上位 4 つのコモディティ型ローダーは、Qakbot、Emotet、IcedID、Trickbot でした **(図 25)**。これらの 4 つの脅威は元々、組織を侵害して金銭的利益を得るためのバンキング型トロイの木馬として開発されたものです。時代とともに銀行業界のセキュリティ管理の強化に適応していった結果、マルチフェーズの攻撃チェーンを利用したり、戦術、手法、手順（TTP）を進化させたり、別のマルウェアを展開したりと、はるかに高度な脅威に発展しました。このような進化は脅威環境に影響を与え続けています。世界中の法執行機関が注目してリソースを投入しており、組織とネットワーク防御者は技術の変化を常に注視せざるを得なくなっています。これらの脅威の検出と阻止に最大限の努力が注がれているにもかかわらず、マルウェア攻撃の実行者は TTP を調整して、標的のセキュリティ環境の変化に対応し続けています。こうした動きはマルウェアの進化過程にも表れています。現在、マルウェアは主にモジュール機能を備えたローダーとして動作するようになっており、サイバー犯罪者はこれを多様なセキュリティ環境に合わせて柔軟かつ迅速に適応させることができます。また、これらのローダーをさまざまなオープンソースツールや新たに開発されたマルウェアと組み合わせて使えるという柔軟性もあります。

全体的な傾向の 1 つとして、攻撃の実行者は ISO、ZIP、LNK 形式のファイルを使用して Qakbot、Emotet、IcedID を配布する場合が多いことが確認されました。おそらくは、マクロが有効化されたドキュメントをブロックする Microsoft の取り組みを回避するのが目的でしょう。別の傾向として、Qakbot、Emotet、IcedID の攻撃の実行者が被害者の環境で見つけた環境寄生型バイナリ（LoLBin）を使用して、悪意のあるペイロードのダウンロードと起動を行っていることが確認されました。Qakbot や Emotet のアフィリエイトが組織内でできるだけ検出を回避できるように、さまざまな LoLBin を試して攻撃手順を高度化させているケースもありました。

地政学的環境もサイバー犯罪者の活動に影響を与えてきました。ウクライナでの戦争を機に仲間割れや内部の人間による情報流出が起こり、国際的な法執行機関の取り組みで犯罪者のボットネットを解体してきた結果、多くのサイバー犯罪組織が分裂しました。こうした変化は、Talos で収集したデータに反映されています。たとえば傾向に関する重要な調査結果のいずれにも入っておらず目立つのが Trickbot ですが、Trickbot の開発者は Conti ランサムウェアグループに参加したと思われます。Conti では今年、リーダー層がロシア支持を宣言したことへの報復として、内部の人間によるデータ流出が起きていました。テレメトリで Trickbot 関連のアクティビティが検出されてはいますが、Trickbot 攻撃の実行者は 2022 年初

めから活動を停止しているため、このアクティビティの多くは以前の感染済みのエンドポイントを検出した可能性が高いと思われます。同様に Emotet はまだ活動してはいますが、2021 年 1 月初めに法執行機関にボットネットを解体される前と比べると、活動の勢いは著しく弱まっています。Qakbot や IcedID などの他のマルウェアが普及し、その穴を埋めている状況です。

コモディティ型ローダー

	Qakbot	IcedID	Emotet	Trickbot
別名	Quackbot、Qbot、Pinkslipbot	BokBot	Geodo、Heodo	なし
所属	ユーラシア大陸のサイバー犯罪者によって開発されたと思われるコモディティ型マルウェア	不明	ロシア系サイバー犯罪グループである Mummy Spider によって開発されたコモディティ型マルウェア	ロシア系サイバー犯罪グループである Wizard Spider によって開発されたコモディティ型マルウェア
活動開始時期	2007 年	2014 年	2017 年	2016 年

目標

- 初期アクセスを取得し、永続性を確保して、さらなる侵入活動を容易にする。
- 次の段階のマルウェア（ランサムウェアなど）を展開する。

被害者に関する考察

- 世界中ですべての業界を標的とする。
- ロシアとウクライナの戦争開始以降、Trickbot は、ロシア国民を狙ったと思われる攻撃には報復すると脅している。

注目すべき TTP

- フィッシング、マルスパム、ソーシャルエンジニアリング、脆弱性のエクスプロイト、データ（財務データやログイン情報など）の窃取、ワームのような伝播。
- モジュール性が高いため、多様な攻撃を実行できる。

マルウェアとツール

- マルウェアの亜種は他のさまざまなマルウェアファミリを展開する場合もあれば、それらによって展開される場合もある。互いに展開し合う場合もある。
- 攻撃ライフサイクルのさまざまなステージで商用ツール（Cobalt Strike など）や LoLBin を使用する。

図 25. コモディティ型ローダーの脅威マトリックス

Qakbot

Qakbot（別名 Qbot、Quackbot、Pinkslipbot）は、世界中のサイバー犯罪者の間で特に幅広く使用され、積極的な開発が進められている脅威の 1 つです。Qakbot は元々、バンキング型トロイの木馬として 2007 年に発見されましたが、それから機能が継続的に更新され、現在はアフィリエイトがボットネットの形成、第 2 段階のペイロードの配布、データの窃取を Qakbot で行ったり、Qakbot を各種モジュールと連携させて使用したりできるようになっています。

2022 年において Qakbot は、Talos のエンドポイントテレメトリで特に活発に展開されていることが確認されたコモディティ型ローダーの 1 つでした。それまでの年と同様に、Qakbot のアフィリエイトは悪意のあるリンクや添付ファイルを含むフィッシングメールを最初の感染ベクトルとして使用するなど、見慣れた TTP を使用し続けています。一方で、攻撃の実行者は防御側のセキュリティ検出プロトコルに敏感に対応しており、状況に応じて戦術を変更すると言われています。今年、これまで確認されていたツールと TTP（ソーシャルエンジニアリングの手口、リンク、添付ファイルなど）をアフィリエイトが多様化させていることがわかりました。おそらく検出を回避するのが目的でしょう。さらに、Qakbot が Black Basta ランサムウェアや正規のレッドチーミングツールである Brute Ratel などの新しいペイロードを取り入れている事例が今年初めて確認されました。

お客様に影響を与えたコモディティ型ローダーの中で特に活発に展開された Qakbot

Cisco Secure Endpoint のテレメトリを確認したところ、2022 年 1 月下旬以降、Qakbot 関連のアクティビティが次第に増加し、5 月から 6 月頃と 8 月から 9 月頃に急増したことがわかりました **（図 26）**。Qakbot 関連のアクティビティの増加は、同マルウェアが復活し広く展開されたことに関係しています。この背景には、競合するボットネット（Emotet や Trickbot などのメールで拡散されるボットネット）が法執行機関やテクノロジー企業からの度重なる妨害に遭っていたという事情があります。

Qakbot 関連の検出件数の約 90% が 2 つの Snort SID（58280、58279）によるものです。どちらの SID も、Qakbot のボットネットから SquirrelWaffle をダウンロードする試みを検出するものです。ボットネットはその後、Qakbot ペイロードの展開を円滑化するために使用される可能性があります。SquirrelWaffle はマルウェアローダーであり、侵害したシステムに対する攻撃の最初の足掛かりを築くと言われています。

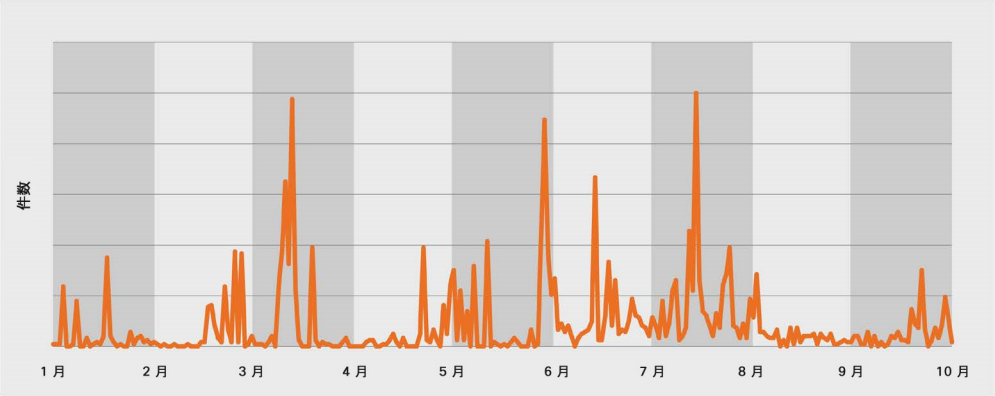


図 26. Cisco Secure Malware Analytics による Qakbot ミューテックスの検出件数

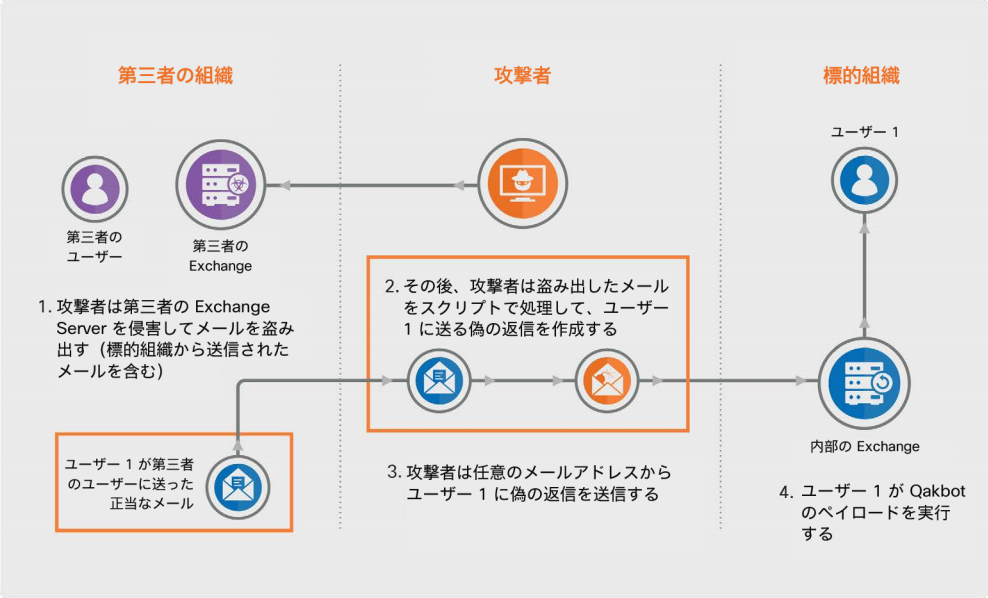


図 27. 外部スレッドの乗っ取り

Qakbot が外部スレッドの乗っ取りを開始

遅くとも 2022 年 3 月以降、アフィリエイトは外部スレッドを乗っ取ることで Qakbot を配布しています。この手法では、標的組織と信頼できる第三者の間でやり取りされたメールスレッドを侵害して利用し、その第三者からの返信を装ってフィッシングメールを送信します **(図 27)**。そのため、よく知らない送信者からの新しいメールに比べて、被害者の信頼を得る可能性が高くなります。さらに、スレッドを乗っ取る場合、標的組織内部のメールアカウントを侵害する必要がないため、検出されるリスクが下がります。CTIR で対応した Qakbot 関連の事例の 1 つでは、2021 年の ProxyLogon を悪用した攻撃中に収集された数か月前から数年前のメールスレッドが利用されたという判断を下しました。ProxyLogon は CVE-2021-26855 で追跡されている脆弱性であり、この脆弱性を持つ Microsoft Exchange Server が標的になりました。

アフィリエイトが使用するファイルの変化：XLSB ファイルから、LNK ファイルを含む ISO ファイルへ

Talos は、Qakbot のアフィリエイトが乗っ取ったメールスレッドを使用して、ISO ファイルが格納された ZIP ファイルを配布している事例を確認しました。この ISO ファイルには、マルウェアの実行に必要な LNK ショートカットファイルなどのファイルが含まれていました。この事例では、「mshta.exe」を使用してリモートの Microsoft HTML アプリケーション（HTA）ファイルを実行します。すると、Windows エラー報告プロセスである「wermgr.exe」に Qakbot を挿入するドロッパー DLL がダウンロードされます **(図 28a)**。また、Qakbot を展開する攻撃者は乗っ取ったメールスレッドで ZIP ファイルを配布していますが、「mshta.exe」を使用する手法から、Windows スクリプトホストである「wscript.exe」を使用して初期のステージを実行する手法に切り替えました。このプロセスによってドロッパー DLL が起動し、最終的に Qakbot が「wermgr.exe」に挿入されます。

Qakbot はこれまで XLSB ファイルを使用していましたが、現在は LNK ファイルを使用しています。Microsoft 社が 2022 年半ばに、ダウンロードされたコンテンツについてはドキュメントのマクロをデフォルトでブロックすると発表したことが理由だと思われます。

マクロは、Web からダウンロードされたファイルにフラグを付ける「Mark of the Web」（MOTW）属性に基づいてブロックされます。ただし、LNK ファイルを配布する場合、MOTW 属性が付けられるのは添付ファイルのみです。ZIP や ISO などのファイルの場合も同様です。添付ファイルの中身には MOTW 属性が付かないため、攻撃の実行者はマクロが有効なドキュメントを検出されずに配布できます。さらに、添付ファイルに LNK ファイルや DLL などが含まれている場合は、添付ファイル自体がペイロードのダウンロードを開始する可能性があります。これらは Qakbot の新手の TTP ではありませんが、状況を見ながら散発的に使用されていることから、Qakbot の攻撃者が標的の変化し続けるセキュリティ環境に合わせて TTP を適応させている可能性がうかがえます。

検出回避が目的と思われる LoLBin の利用

Talos は、Qakbot 攻撃の実行者が Qakbot DLL のダウンロードと起動の両方で、使用するファイルを「rundll32.exe」から「regsvr32.exe」に切り替えていることを確認しました。「rundll32.exe」を使用した場合、既知の PowerShell 関数名を含むコマンドラインパラメータがあるために、容易に検出され、ブロックされていました。「regsvr32.exe」に切り替えたことで、そのコマンドラインパラメータが XML 形式の Windows ActiveX コントロールファイル（OCX）に代わったため、PowerShell の検出を回避できていました。また、アフィリエイトが Windows のコマンドラインツール「curl.exe」の使用をやめて Microsoft の計算アプリケーション「calc.exe」を使用することで攻撃の実行手段を高度化させていることも確認されました。「calc.exe」が DLL サイドローディング攻撃に対して脆弱であることが理由と思われます。「calc.exe」は System32 ディレクトリからオリジナルの DLL をロードする代わりに、現在のフォルダから DLL をロードします。そのため、Qakbot 攻撃の実行者は正規のアプリケーションを使用して悪意のある DLL をロードでき、操作の正当性がさらに高まります。

新しい高度なオープンソースツールを導入し続ける攻撃者

2022 年 6 月に初めて見られた動きとして、Qakbot 攻撃の実行者がランサムウェアの Black Basta と正規のレッドチーミングツールである Brute Ratel を感染チェーンに取り入れていました。過去に使用が確認されたレッドチーミングツールの Cobalt Strike やハッキン

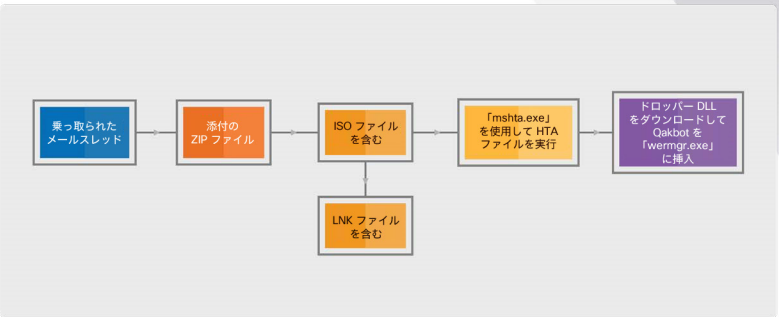


図 28a. LNK ファイルと「mshta.exe」を使用した Qakbot 感染チェーン

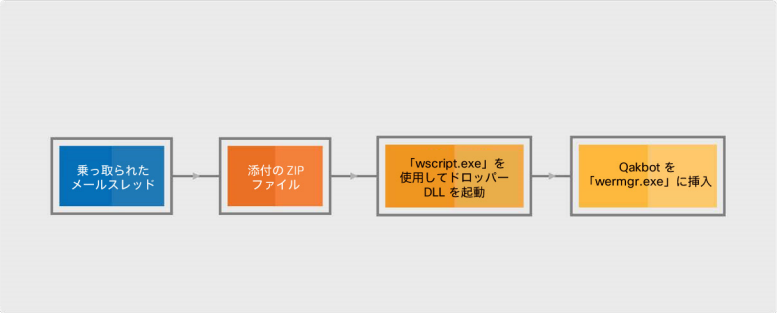


図 28b.「wscript.exe」を使用した Qakbot 感染チェーン

グツールの DarkVNC などと併用された形です。比較的新しい種類のランサムウェアである Black Basta を Qakbot 攻撃の実行者が展開したことから、他の攻撃者と引き続き協力していく意向があること、さらには、他の攻撃者も活動に Qakbot を導入する価値を認めていることが明確にわかります。Emotet や Trickbot といった他のモジュール式の脅威を展開する攻撃者も同様の行動をとっており、メールでボットネットを拡散する攻撃者と他のランサムウェアグループの間で協力している様子が確認されています。Qakbot 攻撃の実行者が Brute Ratel を使用していることから、Brute Ratel の注目度が高まっている様子がうかがえます。Qakbot を使用する攻撃者は、攻撃の効果を維持するために新しい脅威や手法を活動に取り入れ続けています。さらに言えば、こうした Brute Ratel 導入の動きは、Qakbot の開発者がマルウェアの感染チェーン全体を検出されにくい形に改良し続けているという Talos の過去の判断を補強するものです。

Emotet

Emotet は 2014 年に初めて発見されたモジュール式のトロイの木馬であり、この数年で最も猛威を振るったマルウェア脅威の 1 つになっています。元々はバンキング型トロイの木馬として開発されましたが、現在では、攻撃者が新しい環境で最初の足掛かりを得た後、他のマルウェアを起動する目的でよく使用されます。2021 年初めに国際的な法執行機関が Emotet の活動を封じ込めるテイクダウン措置を実施したと発表し、ボットネットを停止に追い込んでいました。2021 年 11 月、Emotet は復活し、Trickbot のインフラを使用してボットネットを再構築し始めました。Emotet の現在の攻撃活動は、2021 年のテイクダウンの前に見られた勢いをまだ取り戻していませんが、再び深刻な脅威となり、拡大し続けています。

Emotet の現在の攻撃活動は、2021 年のテイクダウンの前に見られた勢いをまだ取り戻していませんが、再び深刻な脅威となり、拡大し続けています。

Emotet の活動は 2021 年の停止措置から完全には回復していない模様

Emotet の活動には以前から、散発的で急激に活発化する、数週間から数か月にわたる休止期間がある、といった特徴が見られます。休止期間中はスパムは拡散されませんが、ボットネットは運用されていることが一般的です。そのため、感染済みのシステムは引き続き侵入に利用できます。2022 年の Emotet の活動でもこのような動きの緩急があり、数週間の休止期間を挟みながら急激に活動を活発化させるというパターンが数回見られました。

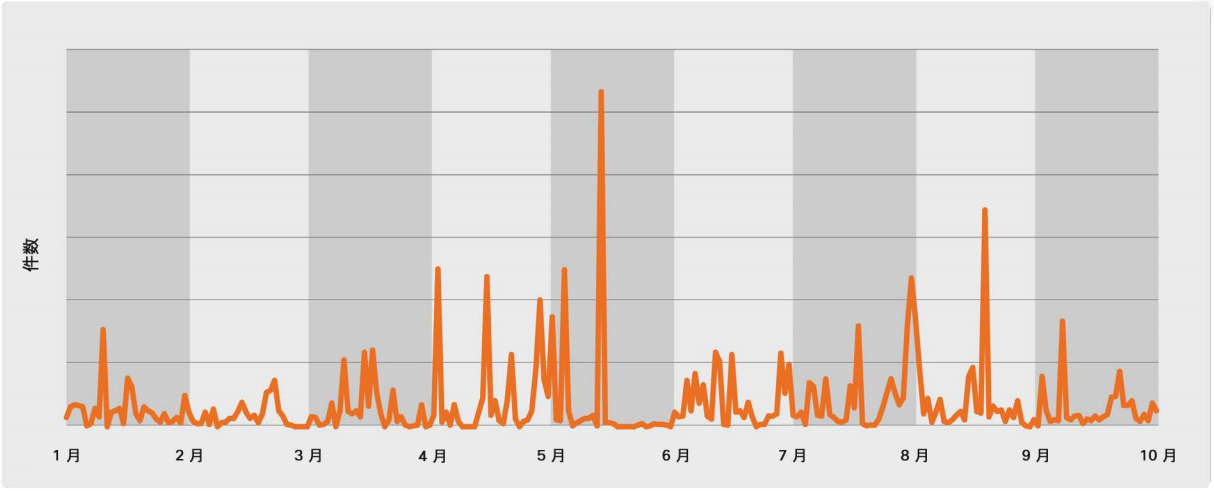


図 29. Cisco Secure Malware Analytics による Emotet ミューテックスの検出件数

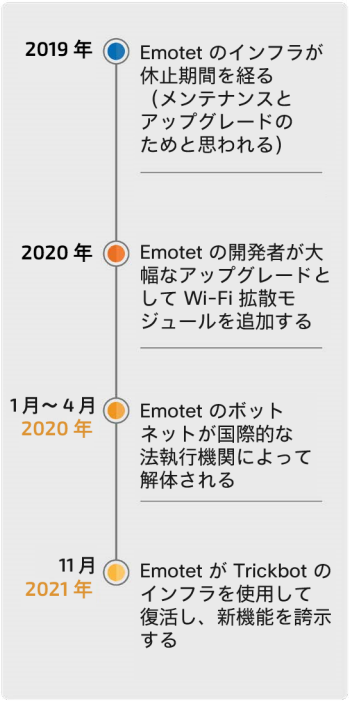


図 30. Emotet の活動のタイムライン

これは、Cisco Secure Malware Analytics によるミューテックスの検出件数の推移を表した**図 29** にも反映されています。

Emotet によるエクスプロイトの試みを検出する 26 個の Snort SID のうち、検出件数の 99% を占めた最多の SID（48402）のトリガーは、感染したホストによる Emotet ボットネットとのアウトバウンド C2 接続の試行であることがわかりました。このアクティビティの少なくとも一部は、Emotet のボットネットがフル稼働していた時期に Emotet に感染したデバイスが、法執行機関に解体された Emotet の古いインフラに現在も接続を試みていることによるものだと思われます **(図 30)**。

活動を隠すために PowerShell から移行

2022 年に確認された Emotet の活動の大半で PowerShell が使用された一方で、PowerShell に対する防御側の徹底的な監視に対応するために別の戦術を試す攻撃者もいました。一例として、ある攻撃作戦では、PowerShell ではなく Windows のダウンロードおよびデータ転送のユーティリティである「curl.exe」を使用して Emotet がダウンロードされました。ペイロードのダウンロードと起動の両方に、「regsvr32.exe」などの他の LoLBin も使用されました。OCX ファイルパラメータを指定して「regsvr32.exe」を実行すると、HTTP を介して実行ファイルがダウンロードされ、実行されます。先ほど述べたとおり、Qakbot もこの戦術を同じように使用しています。

ペイロードの起動に LNK ファイルや Excel ファイルを使用

2022 年も、以前から Emotet に関連があるとされてきた多くの TTP が使用されました。最初の感染ベクトルとしてフィッシングを利用したりソーシャルエンジニアリングを行ったりして、ユーザーがリンクや添付ファイルをクリックするよう仕向ける手口がその例です。一方で Emotet は Qakbot などのマルウェアファミリと同様に、2022 年になって LNK ファイルを取り入れた新しい

感染チェーンを採用し、使用する添付ファイルも Microsoft Word ファイルから、マクロが埋め込まれた Microsoft Excel ファイルに切り替えています。Emotet が短い休止期間を経て 2021 年 11 月に復活したときには、2 つの独立したボットネット（エポック）を使用してスパムメッセージを配布しています。スパムメッセージには、パスワードで保護された ZIP アーカイブ、Word ドキュメント、VBA マクロが埋め込まれた Excel スプレッドシートが添付されていました。2022 年には、これらのエポックがそれぞれ別の方法で Emotet を展開していたことが確認されています。一方が送信していたのは、マクロが埋め込まれた XLS ファイルを添付したフィッシングメッセージで、もう一方は、悪意のあるリンクまたは添付ファイル（パスワードで保護された ZIP ファイル、マクロが埋め込まれていない Excel ドキュメント、LNK ファイルのいずれか）を含むメールを送信していました。

IcedID

IcedID（別名 BokBot）は元々、金融データの窃取を目的として 2017 年に開発されたモジュール式のコモディティ型ローダーです。その後、機能が拡張し、ランサムウェアなど後続のペイロードの配布も可能になっています。IcedID は米国の金融サービス機関を主な標的としており、ブラウザフッキング、ログイン情報の窃取、Adversary-in-the-Middle（AiTM）プロキシの確立、仮想ネットワーク コンピューティング（VNC）モジュールを使用したリモート制御の確立など、悪意のある機能を豊富に備えています。

新たな TTP を導入して IcedID を展開し、さらなる難読化を図る攻撃者

2022 年より前に IcedID のアフィリエイトに最もよく見られた手法は、パスワードで保護された ZIP ファイルを添付したフィッシングメールを送信することでした。この ZIP ファイルには、マクロが埋め込まれた Word ドキュメントが格納されており、そのマクロを実行すると IcedID のペイロードが起動されました。2022 年には、アフィリエイトがフィッシング攻撃の際にさまざまな TTP で IcedID を展開していることが確認されました。LNK と DLL を含む ZIP ファイルが格納された ISO ファイルをメールに添付した事例もあれば、ZIP ファイルを使わずに、LNK と DLL が格納された ISO ファイルをメールに添付した事例もありました。しまいには、JavaScript と DLL を含む HTML を添付したメールも確認されました。いずれの事例でも、DLL の読み込みと実行には「rundll32.exe」が使用されました。多くの事例で IcedID の実行ファイルはデジタル署名されていました。セキュリティ アプリケーションによる検出を回避するために正当性を装ったものと思われます。

多くの事例で IcedID の実行ファイルはデジタル署名されていました。セキュリティ アプリケーションによる検出を回避するために正当性を装ったものと思われます。

IcedID の展開中に検出回避手段を使用した攻撃事例も確認されました。ある事例では、LNK ファイルではなく、VBA マクロが埋め込まれた Word ドキュメントがフィッシングメールに含まれていました。この悪意のある VBA マクロは、実行中に「rundll32.exe」をコピーして別の名前を付けました。「rundll32.exe」に一致するパターンを特定することで悪意のあるアクティビティを検出するセキュリティ アプリケーションによる監視から逃れるのが狙いでした。別の事例では、IcedID インストーラのスクリプトが、文字どう

しの間にキャレット記号を挿入することで難読化されていました。これもパターンの一致を回避しようとしたものです。

```
cmd.exe /c "start 73gLujjt.png && start r^un^dl^l3^2 TYnvUcnF.d^l^l, #1"
```

IcedID の代わりに Bumblebee が採用されている可能性が浮上

IcedID は最初に発見されて以降、活動の軸が変わってきました。かつては主にバンキング型トロイの木馬として機能していましたが、現在は、他のマルウェアのドロッパーとして利用されることの方が多くなっています。2021 年 1 月にボットネットが解体された Emotet の穴を IcedID が埋める立場にあるかと思われましたが、2022 年においては、IcedID は Qakbot などの他のコモディティ型ローダーほど活発に使用されていません。3 月頃、Bumblebee という新種のローダーが初めて確認され、数人のセキュリティ研究者が、このローダーが IcedID に取って代わりつつあると考えました。その根拠は、確認された攻撃事例で Bumblebee をドロップしたのが、過去に IcedID を使用したことが判明している攻撃者だったことです。現時点では、IcedID の代わりとして Bumblebee が使用されているのかどうかは判断できませんが、シスコのテレメトリでは、Bumblebee が初めて確認された 3 月から 4 月にかけて、Snort ルールに基づく IcedID の検出件数は確かに急減しています **(図 31)**。ただし執筆時点では、CTIR の対応業務で Bumblebee を確認した事例はまだなく、2022 年を通じてテレメトリで検出された Bumblebee 関連のイベントは IcedID に比べてはるかに少ないことは述べておきたいと思います。

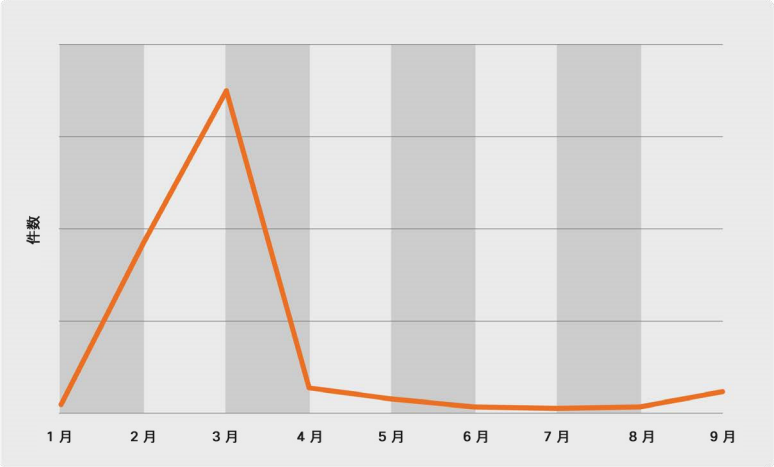


図 31. IcedID を追跡する Snort アクティビティ

ウクライナの組織を狙った IcedID の使用：ロシアの対ウクライナ戦争の支援が目的か

Talos 内部のウクライナタスクフォースは、ウクライナを拠点とするさまざまな重要インフラ業界（エネルギーおよび公益事業、銀行、医療、運輸、防衛など）のお客様約 40 社を狙う、日々の脅威活動を監視しています。2022 年 4 月、

エネルギー業界や政府部門に属する複数のお客様の環境で IcedID が確認されました。ちょうど同じ頃、ロシアとウクライナの戦争を受け、Conti（活発に活動する親ロシア派のランサムウェアグループ）がウクライナの組織に仕掛けた複数の攻撃作戦において IcedID を展開したことが一般公開の報告からわかりました。ある事例では、侵害されたエンドポイントにある「rundll32.exe」か「regsvr32.exe」を使用して悪意のある DLL を実行するスケジュール済みタスクが作成されたことを Cisco Secure Endpoint で検出しました。これがきっかけとなり、システムに IcedID が展開されているなど、他にも複数の挙動を Cisco Secure Endpoint で検出できました。IcedID が展開された別の事例では、悪意のあるファイルが使用されたと考えられます。見つかったファイルの名前はエンドポイントによって違っていましたが、そのうちの 1 つはロシア語の名前でした。さらに、そのファイルはコマンドアンドコントロール（C2）に HTTP トラフィックを使用し、IcedID に関連する後続のファイルをダウンロードするようになっていました。これらの出来事の関連を示すものはありませんが、それらはすべて、ウクライナに対するロシアの戦争遂行を支援する動きであると思われます。

Trickbot

Trickbot は元々はバンキング型トロイの木馬として 2016 年に発見されましたが、何年間もの機能拡張によって他のマルウェアをドロップできるようになり、ランサムウェア攻撃の収益性を大幅に高めています。また、継続的な更新によってボットネットの拡大、機能の強化、多様なモジュールとの連携も実現してきました。こうしたモジュール性により、攻撃者は標的の環境に合わせて手法を調整できるようになりました。

活動が大きく停滞してもなお懸念される Trickbot

2021 年末の時点で、Trickbot はサイバー犯罪者の間で特に広く使用されたマルウェアの 1 つでした。2021 年 10 月に初めて発見された Diavol ランサムウェアと Trickbot の関連を FBI が公式に認めたように、Trickbot は勢力拡大の兆しさえ見せていました **(図 32)**。しかし不可解なことに、2021 年 12 月から 2022 年 2 月にかけて Trickbot の活動は急速に停滞し始めました。その後、わずかな進展は何度か確認されましたが、Trickbot 攻撃の実行者がボットネットを放棄したという見方が強くなっています。これについてはいくつかの説が出回っており、Trickbot 攻撃の実行者が、長年にわたって緊密な関係にある前述のランサムウェアグループ Conti に移籍したという説や、Emotet などメールで拡散される別のボットネットに切り替えたという説があります。正確な原因はわかりませんが、国際的な法執行機関による妨害措置や競合のサイバー犯罪グループといった外部要因によって攻撃の中止を余儀なくされた可能性は低いと見られます。

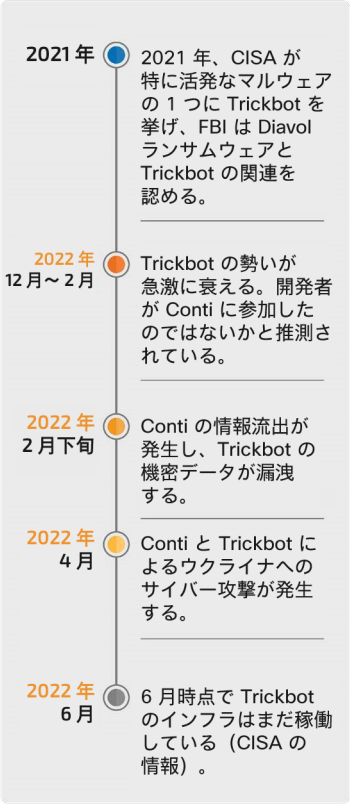


図 32. Trickbot の活動のタイムライン

これまでの傾向として Trickbot は大幅な停滞や長期の活動停止を経ては復活してきたため、Talos は引き続き同グループの活動を注視しています。

Trickbot が初期のメンバーにあまり使用されなくなったと考える人もいますが、シスコのエンドポイントテレメトリでは今でも Trickbot のボットネットのアクティビティが確認されています。また CISA は、同グループのインフラが 2022 年 7 月の時点でまだ稼働中であることを確認しています。Trickbot の活動停止に関する報告が多数公表されていますが、これらを踏まえると、シスコのテレメトリで今年検出された Trickbot のアクティビティの少なくとも一部は説明できると思われます。

まず、ボットネットが解体されたからといって、過去に感染したシステムが自動的に修復されるわけではありません。これらのシステムが現在も感染したまま、すでに無効になっている Trickbot の C2 サーバーに接続を試行し続けている可能性があります。この場合、Snort などの検出システムがトリガーされます。Trickbot によるエクスプロイトの試みを検出する 75 個の Snort ID（SID）のうち、検出件数で 95% 以上を占めた上位の SID は、50714、57893、54212 であることがわかりました。1 つ目の SID は Trickbot の自己署名証明書を検出した場合にトリガーされ、残りの 2 つの SID は、Trickbot に感染したデバイスが Trickbot の C2 にビーコンを送信した場合にトリガーされます。これらの挙動は長期にわたって検出されていますが、必ずしも、Trickbot 関連の目立った事象が起きているわけでも、C2 サーバーからの何らかの応答や接続の確立が確認されているわけでもありません。

また、シスコのマルウェア分析サンドボックスである Cisco Secure Malware Analytics を使用すると、出回っているサンプルを自動で収集できるだけでなく、マルウェアのサンプルを手動でアップロードできます。研究者がこのツールで古い Trickbot サンプルを分析しているために Trickbot の検出件数に影響が出ているという可能性が考えられます。

最後に、他の攻撃者が自分の活動のために、過去に Trickbot に感染したデバイスと Trickbot の古いインフラを利用している可能性もあります。この場合、テレメトリで Trickbot として検出されます。たとえば一部のセキュリティ研究者が述べているように、Trickbot が Conti に移籍したか Emotet を採用したのだとすれば、それらのマルウェアファミリを使用する攻撃者が Trickbot の古いインフラを使用している可能性はあります。また、Trickbot の侵害を受けたシステムへのアクセス権をサイバー犯罪者が購入して攻撃に利用したことが知られています。

これまでの傾向として Trickbot は大幅な停滞や長期の活動停止を経ては復活してきたため、Talos は引き続き同グループの活動を注視しています。さらに、同グループを活動停止に追いやる外部要因があったとは見られないことから、今後どこかの時点で再び Trickbot に投資し始める可能性があります。

自動ハンティングを使用した指標の追跡

Talos 内のチームの 1 つは、Secure Endpoint Premier のお客様向けに「ハンティング」という自動探索機能を開発しています。このハンティング機能は、Qakbot、Emotet、IcedID、Trickbot などの各種マルウェアに関連があるとされている挙動がないか探します。この機能を使えば、

お客様の環境に潜む未知の脅威や、対策が講じられていない進行中の脅威を特定しやすくなります。探索対象として指定されている特定の挙動が検出されると、その都度、レポートが作成されます。シスコの一部のお客様に関するものではありますが、このレポート結果も、2022 年における脅威活動の分析に使用できるデータセットになります。

2022 年には、Qakbot の挙動を探索する自動ハンティング機能を新たに 2 つ作成し、「curl.exe」コマンドと「rundll32.exe」による「DllInstall」関数の呼び出しを検出できるようにしました。これは「wermgr.exe」への Qakbot の挿入を可能にする挙動です。Emotet の挙動に関するハンティング機能も新たに 1 つ作成し、「powershell.exe」の呼び出しを伴わない Invoke-Expression（IEX）コマンドレットの実行を検出できるようにしました。2022 年より前に作成されたハンティング機能からもレポートが生成されました。これらの機能で検出されたのは、Emotet が Microsoft Office 製品を利用して「regsvr32.exe」経由で悪意のあるファイルを実行する挙動と、IcedID が「rundll32.exe」を使用して不審な DLL を実行し、DLL の関数を名前ではなく序数で呼び出す挙動です。

まとめ

Qakbot、Emotet、IcedID を使用するアフィリエイトの TTP は、今後も標的のセキュリティ環境の影響を受け続けるでしょう。これらのグループは活動開始以降、継続的にマルウェアを進化させてきました。今では、さまざまな方法での柔軟な利用を可能にするモジュールなどの新しい機能を備え、金融データの窃取という当初意図した機能以外のタスクも実行できるマルウェアになっています。こうした動きが終わる気配はありません。注目される点として、CTIR のデータによればコモディティ型マルウェアは、第 2 四半期に確認された脅威の 20% を占め、1 年以上にわたって最多であったランサムウェアを押しのけて最大の脅威となりました。

また、コモディティ型ローダーが金銭目的のサイバー犯罪者にとって成功を確実にするツールであること、ボットネットの中断やセキュリティソリューションに屈しない力を示してきたことを踏まえると、全体として見れば、これらの脅威はしばらく猛威を振るい続けるでしょう。さらに、新しいマルウェアファミリが絶えずリリースされている現状は、サイバー犯罪者の間でこの手のマルウェアの需要があることを示しています。

最後に、Trickbot が世界的な影響力を持っており、同マルウェアの侵害を受けたネットワークへのアクセス権がサイバー犯罪者に販売されていることから、Trickbot のボットネットは今後も稼働し続けると考えられます。こうした動きが見られるからといって、Trickbot が開発者に積極的に使用されているとは限りませんが、依然として深刻な脅威となり得るものとして、今後も注意深く追跡していきます。

cisco | Talos

2022 年版一年の総括

Advanced Persistent Threat (APT)

今年確認された大半の APT 活動で、カスタマイズされたマルウェアを取り入れたり、既知のマルウェアの新しい亜種を展開したりする傾向が強く見られました。

Advanced Persistent Threat（APT）

2022 年に地政学的環境はいっそう複雑化し、緊張が高まりました。そのせいで脅威環境に変化が生じたことについては、他のセクションですでに説明したとおりです。Advanced Persistent Threat（APT）グループも、こうした地政学的な課題に適応しました。国家の支援を受けたグループや、国家とつながりのあるグループの適応が特に顕著であり、ロシアの APT グループがウクライナでの戦争に反応したことはその最たる例です。さらに Talos は、イラン、中国、北朝鮮、インド亜大陸諸国を起源とする複数のグループが関係するサイバー攻撃をいくつか確認しました。これらのグループは、スパイ行為、知的財産の窃取、破壊的なマルウェアの使用など、さまざまな活動に関与していました。今年確認された大半の APT 活動で、カスタマイズされたマルウェアを取り入れたり、既知のマルウェアの新しい亜種を展開したりする傾向が強く見られました。さらに、APT グループは依然として Log4j ユーティリティなどの広く知られた脆弱性をエクスプロイトし、パッチ適用ルールが不十分な組織を侵害しています。

標的に対して持続的に高度な攻撃を仕掛けるところから名前が付いた APT グループは、その名のとおりネットワークから根絶するのが非常に難しいとされています。ネットワークに侵入した後、複数のアクセス手段を確立する場合が多いからです。さらに、これらのグループは防御側の動きにも適応し続けており、継続的にツールを更新し、活動の高度化を図りながら目的を遂行していることが Talos の調査でわかっています。

注目に値する興味深い傾向として、今年は Cisco Talos インシデント対応チーム（CTIR）の業務で通常よりも多くの APT 事例が確認されました。たとえばイラン政府の支援を受けた MuddyWater グループや、中国政府とつながりのある複数の APT グループの事例です。これらの対応事例を通して、APT グループの活動を詳細に分析し、その実態について全般的な理解を深めることができました。

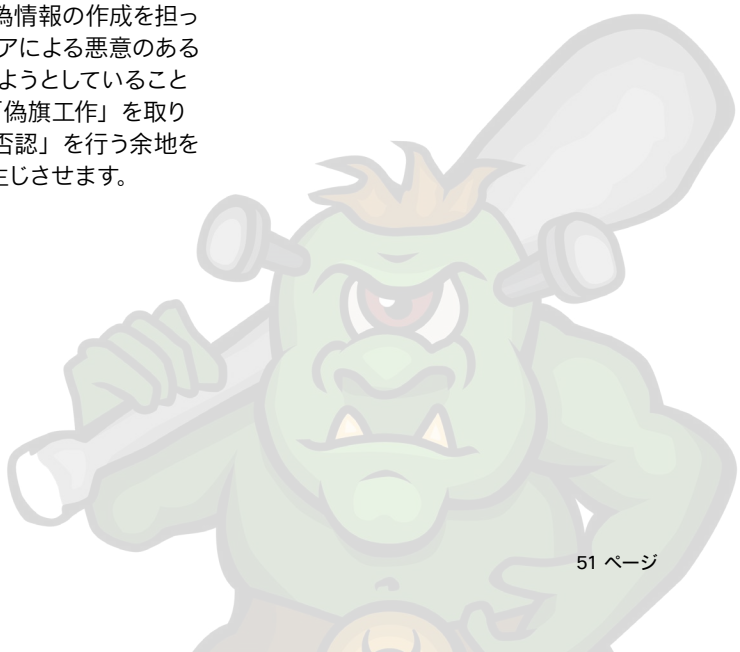
ロシア

2022 年に Talos が確認した中で特に活発に活動した APT グループのいくつかは、ロシアとのつながりがあるか、ロシア政府の支援を受けていました。戦争終結までウクライナの組織を支援することを掲げている Talos にとって、これらのグループは特に注視すべき存在になっています。ロシア政府は、国内の政治的安全保障の確保、情報環境の統制、地域および国際社会における目標の推進など、国家としての利益を勝ち取るために、さまざまなサイバー攻撃を支援し続けています。Talos は、サイバー空間でのスパイ活動や影響力工作、破壊的な攻撃に関与する数多くの APT を追跡していますが、ロシアによる 2 月のウクライナ侵攻の直前、そして侵攻と同時に APT のこうした活動が激化しました。このセクションでは、今年確認されたロシアの APT グループについて Talos の見解を示します。ロシア政府の暗黙の了解を得て同国内で活動していると思われるさまざまなサイバー犯罪者やランサムウェアグループについては、ここでは考えません。

破壊的な攻撃に関与した攻撃者がさらにサイバー空間での影響力工作を実行

Talos の見解では、ロシアによるウクライナでの軍事行動に先駆けて、国家の支援を受けていると思われる攻撃者がウクライナのコンピュータネットワークを中断させる攻撃に関与した後、その攻撃についてウクライナ軍に濡れ衣を着せる影響力工作を行ったと考えられます。「WhisperGate」と名付けられたこの破壊的な攻撃には、2017 年にウクライナをはじめ世界各地の組織に影響を与えたワイパーマルウェア NotPetya と似ている部分があります。NotPetya と同様、WhisperGate のペイロードはマルウェアの実行ファイルであり、マスターブートレコード（MBR）全体を消去して身代金要求メッセージを残すように設計されていました。しかし、上書きされた MBR が復元できなかったことから、ランサムウェア攻撃や恐喝が最終目的でないことは明らかでした。この攻撃の黒幕はおそらく何か月間も被害者のネットワークにアクセスしていたと考えられます。CERT-UA によると、サプライチェーンや Log4j と OctoberCMS の脆弱性が悪用された可能性があります。盗み出したログイン情報を攻撃者が使用したというのが Talos の見解です。被害を受けたウクライナの組織はその後、HermeticWiper、CaddyWiper、DoubleZero、CyclopsBlink など少なくとも 4 つのワイパーファミリに立て続けに感染しました。高度な技術を持ち、計画的かつ持続的に攻撃を仕掛ける必要があったと見られますが、これは国家の支援を受けた攻撃者の特徴です。

とりわけ、WhisperGate 攻撃の特徴は、Fancy Bear という APT グループ（別名 APT28、Tsar Team、STRONTIUM）が過去に関与していたとされる攻撃と類似しているようでした。Fancy Bear は、ロシア軍参謀本部情報総局（GRU）の一部隊だと考えられています。WhisperGate は破壊的な影響を与えるだけではありません。Talos は、Fancy Bear との関連を持つ攻撃者がもっともらしい理屈をつけて、ウクライナの一般市民にデマ攻撃を仕掛けたと思われる事例を確認しました。国家規模のランサムウェア攻撃に見せかけたこの WhisperGate 攻撃では、ロシアによる過去のデマ攻撃に関連すると思われる証拠が見つかっています。WhisperGate の偽の身代金要求メッセージに攻撃者の連絡先として記載されていたメールアドレスが、過去のデマ攻撃で使用されたものだったのです。このメールアドレスを追跡したところ、すでに知られている 1 人のロシア系プロパガンディストが浮上しました。その人物は Fancy Bear による過去のデマ攻撃に関与したと見られており、今回の WhisperGate 攻撃では、使用する偽情報の作成を担っていました。Talos の調査結果から、APT 攻撃者がロシアによる悪意のあるサイバー活動の犯人特定を難しくするために話を捏造しようとしていることがわかります。WhisperGate のような破壊的な攻撃に「偽旗工作」を取り入れるといった戦術は、ロシア政府に「もっともらしい否認」を行う余地を与え、さらには標的となった国家や組織の間に対立を生じさせます。



攻撃者の素性

Gamaredon

別名

Primitive Bear、Armageddon、Shuckworm、Winterflouder、BlueAlpha、BlueOtso、IronTiden、SectorC08、Callisto、Trident Ursa

所属

ロシア

活動開始時期

2013 年

目標

スパイ活動、データ窃取、長期アクセスの確立

被害者に関する考察

ウクライナの組織（特に、政府機関、重要インフラ、およびウクライナの防衛、安全保障、法執行機関に関連する組織）を頻繁に狙う。二次的な活動として、ヨーロッパをはじめとする世界各地のさまざまな組織（政府機関、軍事組織、人道組織、非営利組織など）を標的とする。

注目すべき TTP

ソーシャルエンジニアリングの手法、スピアフィッシング、侵害されたドメインとダイナミック DNS、長期アクセス、データ窃取、スクリプトベースのカスタムマルウェア。

マルウェアとツール

Gamaredon のみが使用する独自開発の各種カスタムインプラント（スクリプトベースのカスタムマルウェア、情報窃取マルウェア、バックドアなど）を採用している。注目すべきマルウェアファミリとして、GammaLoad、GammaSteel、Gidome、Powerpunch、Pterodo がある。

図 33. 攻撃グループ Gamaredon の素性

執拗なサイバースパイ活動でロシアの軍事行動を支援

ロシア政府の支援を受けた APT はウクライナに対するサイバースパイ活動に長らく関与してきましたが、ロシアによる 2 月のウクライナ侵攻が近づくにつれてスパイ技術の重要性はよりいっそう際立つようになりました。準備段階における軍事目的（ウクライナ政府の指揮統制の不安定化、情報環境の支配、侵攻部隊の支援、サービス停止を狙うサイバー攻撃の経路の整備など）の遂行を支援するために永続アクセスを利用して情報収集作戦を行った可能性が非常に高いと思われます。Talos は、ウクライナの標的に対するサイバースパイ活動に関与しているいくつかの APT グループを監視しました。監視対象は Gamaredon や Turla などです。

Cisco Talos は、Gamaredon という APT グループに関連する活動を注意深く追跡しています。Gamaredon グループは、クリミアで活動するロシア政府の支援を受けた攻撃者集団だと一般的に考えられています **(図 33)**。Gamaredon はこれまで、ロシア政府の戦略的利益を支援するために、ウクライナの政治や軍事などに関連する政府機関や民間機関を主な標的にしてきました。

今年の初めに Gamaredon の攻撃者は、ウクライナ政府の関係者を情報窃取マルウェアに感染させることを目的とした大規模なスピアフィッシング攻撃を開始し、悪意のあるドキュメント（不正ドキュメント）を添付したメールを送り付けました。この不正ドキュメントは、悪意のある VBS マクロを含むリモートテンプレートを取得するよう設計されていました。ユーザーがこのドキュメントを実行すると、マクロによって RAR アーカイブがダウンロードされます。この中には、ロシアによるウクライナ侵攻に関連したファイル名の Windows ショートカット（LNK）が格納されていました **(図 34)**。LNK を開くと、一連の PowerShell スクリプトによってリモートの Gamaredon のインフラからペイロードが取得されます。複数のステージからなるこの感染プロセスで最終的に配布されるのは、被害者のエンドポイントを検索して機密データを盗み出すカスタムの情報窃取マルウェアです。このマルウェアは、攻撃者の指示があれば、悪意のあるペイロードを追加で配布することもできます。これらの攻撃の犠牲者、インフラ、TTP、悪意のあるサンプルに関する Talos の分析結果は CERT-UA の報告と一致しており、CERT-UA も同様の活動を Gamaredon によるものと判断しています。

LNK ファイル名	翻訳
Розвідувальне зведення від 08 серпня 2022 року щодо різких змін в оперативної обстановці.lnk	作戦環境の急激な変化に関する機密情報の概要（2022 年 8 月 8 日）.lnk
Щодо надання пропозицій до наради Про стан протидії злочинності на території проведення ООС.lnk	OOC 領域における犯罪対策の現状に関する会議への提案について .lnk（Talos 注：OOC は「統合運用部隊」の略）
Інформація щодо злочинів, пов'язаних зі збройним конфліктом, вчинених стосовно дітей та у сфері охорони дитинства станом на 10.08.2022.lnk	子どもに対する武力紛争関連犯罪および幼少期の保護の分野に関する情報（2022 年 8 月 10 日現在）.lnk
Щодо порушення кримінального провадження (ЄРДР 2201605000000123 від 09.08.2022 ч.1 ст.111).lnk	刑事訴訟手続きの開始について（2022 年 8 月 9 日付、ERDR 2201605000000123、第 1 部、第 111 条）.lnk

図 34. スピアフィッシングメールで見られた Gamaredon の LNK ファイル名（地政学的なテーマを利用）

攻撃者の素性

Turla

別名

Venomous Bear、Waterbug、Snake、Uroburos、WhiteBear、Iron Hunter、ITG12、KRYPTON

所属

ロシアが起源。ロシアの FSB に属していると考えるセキュリティ研究者もいる。

活動開始時期

2004 年

目標

ロシア政府の諜報活動における目的遂行を支援する、長期的かつ執拗なサイバースパイ活動

被害者に関する考察

主に NATO 提携国や旧ソ連諸国の重要な軍事組織、政府機関、外交機関、および民間組織に標的型攻撃を仕掛けている。ロシアの諜報活動における目的に沿う地政学的な出来事が発生すれば、標的は変わる可能性がある。

注目すべき TTP

Turla はサイバースパイ活動とデータの窃取を行うために、水飲み場型攻撃、ソーシャルエンジニアリングの手法を利用したスピアフィッシングメールの送信、カスタムマルウェアの展開、既知の脆弱性のエクスプロイトを採用している。防御の回避を得意としており、カスタムの復号ルーチンや、一般的でない暗号化方式の改変などの手法を使用する。

マルウェアとツール

Turla はさまざまなカスタムマルウェア、オープンソースマルウェアの改変版、公開ツールを採用している。注目すべきカスタムツールとして、Tiny Turla、Uroburos、Mosquito などがある。

図 35. 攻撃グループ Turla の素性

Turla グループに関連があるとされているサイバー攻撃の痕跡からも、ロシアの APT 活動の活発さがわかります **（図 35）**。Turla の脅威活動を Talos 内部で総合的に調査したところ、同グループは依然として、NATO 提携国や旧ソ連諸国の軍事組織、政府機関、外交機関、および民間組織に標的を絞った攻撃活動に関与していることがわかりました。アクセス権の取得とデータの窃取を行うために、水飲み場型攻撃、スピアフィッシング攻撃、ソーシャルエンジニアリングの手法、既知の脆弱性のエクスプロイト、カスタムのバックドア（Crutch や Gazer など）を使用し続けています。また、Turla 攻撃の実行者は、コマンドアンドコントロール（C2）インフラとして使用するために衛星通信をハイジャックしていました。この手口については昨年の報告でも取り上げています。

Gamaredon や Turla など、ロシアのいくつかの APT グループは今後も世界中でサイバースパイ活動を続けると予想されますが、ウクライナでの戦争が進行するにつれて、同国と NATO 提携国を狙った活動の比重がますます大きくなっていくでしょう。これらの APT グループは引き続き、ロシアの戦争遂行を支援するための軍事的価値のある機密情報や、ロシアの影響力工作や戦略的目的に役立つ可能性のある政治的な機密情報を収集すると思われます。当然ながら、ロシアの戦略的利益が変化するにつれて、これらのグループの作戦の優先順位も変化すると予想できます。また、戦場で軍事的な停戦が実現したとしても、こうした活動は続くでしょう。

イラン

Talos では 2022 年に、イラン政府の支援を受けた APT に関する重要な動きをいくつか突き止めました。そこからわかったのは、これらのグループが依然としてイランの政治、経済、国家安全保障における目的を遂行するためのサイバースパイ活動に積極的に関与しているということです。イラン政府の支援を受けたグループは知的財産の窃取と情報収集を主な目的として、広範囲に及ぶサイバー攻撃を北米、ヨーロッパ、中東、アジアの組織に仕掛け続けています。しかし Talos の見解では、イランの APT はランサムウェアや他の破壊的なマルウェアを展開するための技術的手法は変えていません。また、7 月にアルバニア政府を攻撃して損害を負わせた事例からうかがえるように、公共サービスや重要インフラを中断させることを厭わない姿勢を見せています。

イラン政府が支援する APT は地域集中型グループの集合体か

MuddyWater という APT はイランの情報安全保障省（MOIS）に所属する攻撃グループであり、2022 年は特に活発に活動しました。永続アクセスを使用して、世界各地のエネルギー会社、通信会社、防衛産業基盤、政府、地方自治体を狙っています **(図 36)**。今年の初めに Talos は MuddyWater の複数の攻撃を総合的に調査しました。その結果、同グループは複数の独立したチームの集合体であり、それぞれのチームが異なる戦術で特定の地域の標的を狙っている可能性が高いという結論にいたりました。この結論は、MuddyWater が 1 つの攻撃グループとして活動しているという一般的な見方に反するものです。

攻撃者の素性

MuddyWater

別名

Static Kitten、MERCURY、Seedworm、TEMP.Zagros、Earth Vetala

所属

イランの情報安全保障省（MOIS）

活動開始時期

2017 年

目標

イランの国家安全保障と経済における目的遂行を支援するスパイ活動、知的財産の窃取。業務停止を引き起こすランサムウェア攻撃

被害者に関する考察

MuddyWater は中東、アジア、北米、アフリカ、ヨーロッパの重要な標的を主に狙っている。公的組織と民間組織の両方にサイバー攻撃を仕掛けており、標的とする分野は通信、石油およびガス、情報技術、学界、政府、地方自治体、NGO など多様である。

注目すべき TTP

MuddyWater はスピアフィッシングメールを使用して、悪意のある追加のコンポーネントを含む ZIP ファイルを配布する。既知の脆弱性をエクスプロイトしたりオープンソースツールを使用したりすることで、機密データにアクセスしてデータを盗み出し、ラテラルムーブメントを行って後続のマルウェアを展開する。また、DLL サイドローディングによって正規のプログラムに偽装してマルウェアを実行させたり、PowerShell スクリプトを難読化して C2 関連の関数を隠したりする。

マルウェアとツール

MuddyWater は POWERSTATS、Small Sieve、Mori バックドア、PowGoop ローダー、リモートアクセス型トロイの木馬の Canopy/SloughRAT など、複数のマルウェア脅威のほか、PowerShell、VBScript、JavaScript などの公開ツール、環境寄生型バイナリ（LoLBin）を使用する。追加で使用するポストエクスプロイトツールとリモートアクセスツールとして、Mimikatz、ConnectWise、Remoteutilities がある。

図 36. 攻撃グループ MuddyWater の素性

2021 年から 2022 年までの MuddyWater の活動を総合的に調査したところ、中東、パキスタン、アルメニア、トルコ、アラビア半島の組織に対する攻撃で、特有の TTP と共通の TTP の両方が確認されました。特定の地域を標的とする過去の攻撃でのみ使用されていたアーティファクト（不正ドキュメント、感染トークン、ダウンローダー、各種の永続アクセスツールなど）が、その後、他の地域を標的とする別の攻撃で再利用され、他の手法と併用されるというパターンが見つかっています。また、攻撃対象地域を移すたびに、これまで使用したことがない新しい TTP を少なくとも 1 つ導入していたことがわかりました **(図 37)**。

これらの調査結果は、特定の国や地域への攻撃を担う複数のグループで MuddyWater が構成されているという Talos の見解を強力に裏付けるものです。各グループは、独立した TTP、ツール、マルウェアを開発しているように見えますが、他の地域での攻撃で効果が証明されている TTP、ツール、マルウェアがあれば、それらを MuddyWater の別のチームから借用しています。

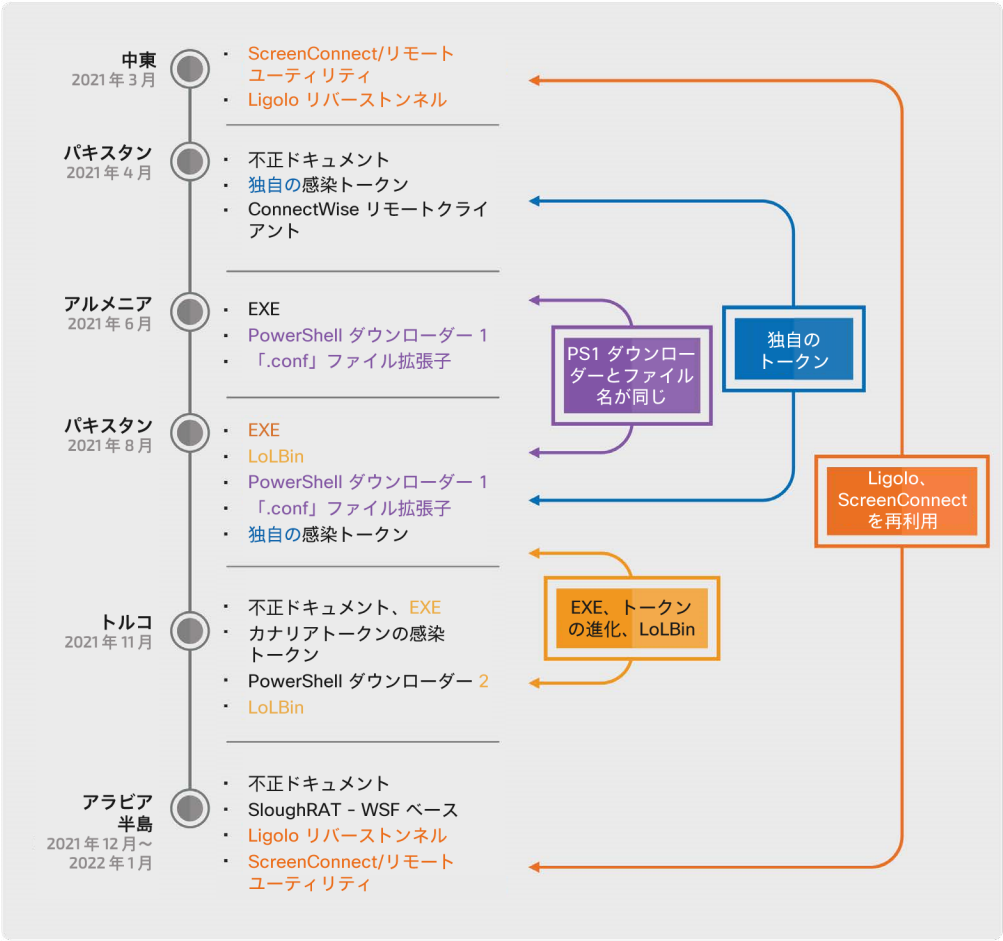


図 37. MuddyWater 攻撃と TTP の重複

MuddyWater は 2022 年もこれまでと同様に、標的への初期アクセスを取得する手法としてフィッシングメール、リンクが埋め込まれた PDF、不正に細工した Microsoft Office ドキュメントを採用しました。

MuddyWater がサイバースパイ活動に利用する手法はさまざま

2022 年、MuddyWater は最初の感染と情報収集にさまざまな手法を使用しました。Talos の調査結果に基づけば、同グループがかねてより備えていた、攻撃ライフサイクルを最新化する能力が今年も見られた形と言えます。同グループはこれまでと同様に、標的への初期アクセスを取得する方法としてフィッシングメール、リンクが埋め込まれた PDF、悪意のある Microsoft Office ドキュメントを採用しました。たとえば今年初めに Talos が報告した MuddyWater の事例では、トルコ保健省やトルコ内務省の実際の文書に見せかけた悪意のある PDF と Microsoft Excel（XLS）ファイルを使用して、トルコ政府機関への侵入を試みています。この PDF ファイルにはリンクが埋め込まれており、それをクリックすると、悪意のあるマクロを含む XLS ファイルがダウンロードされるようになっていました。他の亜種では、悪意のある URL をクリックすると Windows の実行ファイルが配布される仕組みがとられていました。どちらの場合でも、攻撃の最後の段階で VBS または PowerShell ベースのスクリプトが実行され、最終的なペイロードが取得されています。

MuddyWater は今年、SloughRAT（別名 Canopy）という新しいインプラントを導入しました。CTIR の調査結果によると、悪意のある Excel ファイルを含むフィッシングメールが中東諸国の標的に送り付けられています。Excel ファイルの悪意のあるマクロを受信者が実行すると、2 つのスクリプトがドロップされます。その 1 つが SloughRAT（Windows スクリプトファイル（WSF）をベースとしたリモートアクセス型トロイの木馬）でした。SloughRAT は、感染したエンドポイントの IP アドレス、ユーザー名、システム名などのシステム情報を収集します。そして、C2 サーバーからコマンドを受信し、そのコマンドを実行してネットワークから収集したすべてのデータを HTTP POST リクエストによって別の MuddyWater サーバーに送信します。また、攻撃の制御性をさらに高めるために、Ligolo というオープンソースのリバーストンネリングツールを展開していることも確認されました。

この APT はスパイ活動の中で追跡用トークンも採用しています。トルコを標的とした前述の攻撃では、MuddyWater の攻撃者がカナリアトークン（canarytokens[.]com）を使用しました。これは、ドキュメント、Web ページ、メールなどのオブジェクトに埋め込まれたトークンを追跡するサービスであり、オブジェクトを受信者が開いたタイミングで送信者にアラートを発信します。不正ドキュメント（フィッシングメールでトルコの標的に配布されたもの）に含まれていた VBA マクロの一部は、スクリプトをドロップするだけでなく、canarytokens[.]com に HTTP リクエストを送信し、標的に感染させたタイミングで MuddyWater にアラートを発信していました。

MuddyWater は、標的の環境への永続アクセスを確立する方法を巧妙化させています。CTIR が緊急で対応した事例では、中東を拠点とする通信会社のネットワークで MuddyWater の活動が確認されました。悪意のあるファイルを添付したフィッシングメールを同社の従業員に送信することで最初の足掛かりを築き、多数のバックドアとポストエクスプロイトツール（Mimikatz など）、正規のリモートアクセスプログラム（ConnectWise、Remote Utilities など）をドロップしています。修復を行ったにもかかわらず、同社は今年初めに再び侵害を受けました。Talos

は、サーバーインフラに MuddyWater のバックドアが追加されており、リモートサービスと攻撃ツールの実行に Impacket が使用されていることを確認しました。密かにアクセスする手段を多様化することに MuddyWater は長けているようです。

中国

2022 年、中国とつながりのある APT グループがさまざまな業界の組織を標的にしました。その大部分は、中国政府の外交政策および国内政策の目標と関わりのある組織です。Talos のインテリジェンスに基づく調査結果は、中国による悪意のあるサイバー活動の目的は主要な産業や重要インフラから知的財産と機密データを盗むことであるという米国政府の報告と一致しています。一般的に言って、最も狙われているのは、中国の 5 か年計画で国家の優先領域とされている業界です。これに関連して、中国の APT グループは国益が絡む可能性のある業界の中でも特に、通信会社、ソフトウェアプロバイダー、マネージドサービス プロバイダー、医療機関、公衆衛生機関、防衛関連企業、政府機関、非営利団体へのアクセスを試みたり実際にアクセスを成功させたりしていることが Talos の調査でわかりました。これらのグループの目的は、情報収集とデータ窃取を行うために企業ネットワークへの永続アクセスを維持することであったと思われます。

Talos は、地域や世界で新たに生じた地政学的事象に中国の APT が適応した過程も追跡しました。ロシアとウクライナの戦争の前後には、ヨーロッパの組織を標的としたスパイ活動を確認し、すでに知られている中国の APT グループの仕業だと特定しています。今年の後半には、中国、米国、台湾の間で緊張が高まる中で、台湾政府の複数の Web サイトに対する DDoS 攻撃と同時期に起きた APT 活動を監視しました。

ロシアとウクライナの戦争に乗じてヨーロッパの組織を狙う Mustang Panda

今年の初め、Mustang Panda という中国の APT グループがロシアとウクライナの戦争に便乗し、ロシアを含むヨーロッパの組織を狙った広範なスパイ活動を展開しました。同グループは 2022 年 1 月頃から、EU の政治活動に関する内容のファイルを添付したフィッシングメールをヨーロッパの標的に送信し始めました。ギリシャへの国家援助に関する欧州委員会の報告書や、のちには、EU の 2022 年の人権に関する優先事項を扱った添付ファイルで誘い込む事例が確認されています。2 月にロシアのウクライナ侵攻が始まると、同グループは便乗する話題を変えて、ウクライナおよびベラルーシとのロシア国境沿いの軍事活動に関する文書を添付するようになりました。いずれの場合でも、メールは複数のステージからなる感染チェーンを実行する第 1 段階であり、永続アクセスの確立に主に使用されるツールとマルウェアのダウンロードを目的としていました。こうしたスパイ活動は、Talos が把握している同グループの特徴に合致するものです **(図 38)**。

攻撃者の素性

Mustang Panda

別名

RedDelta、Bronze President、TA416

所属

中国

活動開始時期

2012 年

目標

スパイ活動

被害者に関する考察

Mustang Panda の被害者は世界各地に見られる。同グループは、米国、ヨーロッパ、台湾、香港、チベット、ミャンマー、モンゴル、ベトナム、アフガニスタン、パキスタン、インドなどさまざまな国と地域の政府、NGO、宗教組織、シンクタンク、通信会社、インターネット サービス プロバイダー、活動家グループを標的としている。

注目すべき TTP

Mustang Panda は通常、ソーシャルエンジニアリングの手法を用いたフィッシングメールを送信して初期アクセスを取得する。添付ファイルは正当な政府または組織からの公式文書を装ったものであることが多い。PlugX RAT を最初に展開することで、追加のマルウェアのダウンロードとインストールが可能になる。

マルウェアとツール

Mustang Panda はカスタムマルウェアだけでなく、一般的に利用可能な攻撃フレームワーク（Cobalt Strike、Meterpreter など）も使用している。また、DLL ベースのローダー、カスタムステージャ、リバースシェルを開発し、PlugX（Korplug）や Poison Ivy などのカスタムインプラントや、NBTScan などのオープンソースツールを展開している。

図 38. 攻撃グループ Mustang Panda の素性

こうした活動状況から、主に米国とアジアの組織を狙ってきた Mustang Panda の従来の方針が変化していることがわかりますが、時事問題に便乗して標的を侵害するという姿勢は相変わらずです。同グループは、コロナ禍、国際的な首脳会議、各種の政治トピックといったさまざまな時事問題や課題に便乗することが知られています。

ペイロードの配布手段としては、Mustang Panda はローダーを使用し続けています。手法は進化しており、これまでに不正ドキュメント、ショートカットファイル、悪意のあるアーカイブなどが使われてきました。これらのローダーを使用して 3 つのコンポーネントを取得し、感染システムに展開します。そのコンポーネントとは、本物の EU 報告書（おとりとして注意を削ぐための PDF）、無害な実行ファイル（悪意のある DLL ローダーをロードするために使用）、DLL ローダー（最終的な DLL ペイロードの復号化、ロード、アクティブ化に使用）です。ほとんどの事例で、最終的に展開された悪意のあるペイロードは PlugX というリモートアクセス型トロイの木馬でした。PlugX はエクスプロイト後に使用される RAT であり、Mustang Panda をはじめ、中国とつながりのある APT との関連が広く認識されています。PlugX の一般的な機能としては、システムとプロセスの列挙、ファイルの管理と変更、キーロギング、スクリーンショットのキャプチャ、リモートシェルの実行などがあります。また、Mustang Panda は複数のバリエーションの感染チェーンによって、PlugX、カスタムステージャ、Meterpreter ベースのシェル、カスタムリバースシェルを展開していることが知られています。これらの感染チェーンは、悪意のある各種コンポーネントの展開に使用される LNK ファイルと不正ドキュメントで構成されています。

中国とつながりのある APT が従来の標的も狙い、既知の欠陥をエクスプロイト

ロシアとウクライナの戦争によって脆弱な立場に置かれている被害者層につけこむチャンスが新たに生まれた一方で、中国の APT は、これまで標的にしてきたとされるアジアの組織などにも容赦ない攻撃を続けています。たとえば台湾政府、香港の活動家、モンゴルやチベットの NGO、日本、ミャンマーのほか、アフガニスタンとインドの通信会社などが狙われています。

2022 年に Mustang Panda が従来の標的を狙っていることを Talos が確認した事例では、同グループがアジアの標的に対してカスタムの中間ステージャを展開していました。その最終的な目的は、感染エンドポイントに追加のマルウェアをダウンロードすることでした。2 月には、同グループの攻撃者が東南アジア諸国連合（ASEAN）首脳会議の文書に見せかけたアーカイブファイルを東南アジアのユーザーに送り付けています。ユーザーが添付の実行ファイルをクリックすると、悪意のある DLL インプラントがロードされ、シェルコードを復号化することがわかりました。このシェルコードはステージャとして機能し、攻撃者が管理する C2 から悪意のあるアーティファクトを追加でダウンロードします。

中国の APT グループによるサイバー攻撃では、広く知られている脆弱性のエクスプロイトが引き続き最初の感染につながっています。たとえば中国とつながりのある別のサイバースパイグループである Deep Panda は、Log4j ロギングユーティリティの欠陥をエクスプロイトしようとしたことが CTIR のデータからわかっています。同グループは、医療機関のネットワークに設置したカスタムバックドアを使用して永続性を確保することに成功しました。初期アクセスの足掛かりを築いた後、PowerShell スクリプトを使用して、Deep Panda とつながりのある C2 サーバーからファイルをダウンロードして実行した痕跡が見つかっています。

北朝鮮

Talos は、北朝鮮政府とつながっているサイバー攻撃者が活発に活動していることを確認しました。Lazarus グループはそうした攻撃グループの 1 つであり、新しいマルウェアを標的に展開していることが確認されています **(図 39)**。同グループはスパイ活動、知的財産などのデータの窃取、ネットワークの中断を目的とした悪意のあるサイバー活動を行うことによって、北朝鮮の政治および国家安全保障における目的遂行を支援し続けています。政府、医療、防衛産業、メディア、重要インフラといったさまざまな分野の組織を狙っているほか、仮想通貨取引所などの金融機関を主な標的とした金銭窃取も広い範囲で行っています。米国インテリジェンス コミュニティ（USIC）の年次脅威評価によると、Lazarus による世界各地での金銭窃取で数億ドルの損失が生じた可能性があり、盗まれた金はおそらく北朝鮮の軍事研究開発（核計画、ミサイル計画など）の支援に回っているとのことです。

攻撃者の素性

Lazarus グループ

別名

Hidden Cobra、APT38

所属

北朝鮮

活動開始時期

2010 年

目標

国家の目的（政治および国家安全保障、軍事研究開発、国際制裁の回避など）の遂行を支援するスパイ活動、データ窃取、ネットワークの中断を目的とした攻撃、金銭窃取

被害者に関する考察

世界各地のさまざまな組織（政府、防衛、金融、メディア、重要インフラに関わる組織など）を標的とする。

注目すべき TTP

既知の脆弱性のエクスプロイト、ソーシャルエンジニアリングの手法、スピアフィッシング、データ窃取、カスタムマルウェア、擬似ランサムウェア/ワイパー

マルウェアとツール

Lazarus のみが使用する独自開発の各種カスタムマルウェアファミリ（RAT、ワイパー、バックドア、DDoS ボットネット）を採用している。注目すべき脅威として、WannaCry、MagicRAT、TigerRAT、YamaBot、VSingle、CRAT などがある。

図 39. 攻撃グループ Lazarus グループの素性

Talos が確認した事例では、内部偵察とデータ窃取を行うために、新しいリモートアクセス型トロイの木馬（Talos が MagicRAT と命名）と他のカスタムインプラントを Lazarus グループが展開していました。

Lazarus が Log4j をエクスプロイトして新旧のインプラントを配布

2022 年の 2 月から 7 月にかけて、外部公開されている VMware Horizon サーバーの欠陥を Lazarus グループの攻撃者がエクスプロイトして、企業のネットワークに侵入する最初の足掛かりを得ました。Log4Shell の脆弱性を利用して、カナダ、米国、日本のエネルギー会社を狙ったのです。Talos が確認した事例では、内部偵察とデータ窃取を行うために、新しいリモートアクセス型トロイの木馬（Talos が MagicRAT と命名）と他のカスタムインプラントを Lazarus グループが展開していました。

Lazarus グループの新しい MagicRAT は C++ で記述されており、最近では Qt フレームワークを使用してプログラムされています。Qt ソフトウェアは GUI を開発するためのものですが、MagicRAT に GUI は搭載されていません。MagicRAT の機能は他の RAT ファミリと比べると標準的ですが、Qt フレームワークを取り入れている点は独特だと言えます。コードの複雑性を高めることで、リバースエンジニアリングの難易度を上げているからです。また、Qt でプログラミングされたマルウェアのサンプルはあまり知られていないため、機械学習やヒューリスティック分析による検出の信頼性もおそらく低くなります。

MagicRAT の機能はリモートアクセス型トロイの木馬としてはかなり単純で、システム情報を Lazarus グループに提供し、リモートシェルを使用して任意のコマンドの実行、ファイルの窃取や削除、RAT の自己削除を行います。ただし、永続性を確保すると C2 インフラから追加のペイロードを起動できることも Talos の調査でわかりました。たとえば軽量ポートスキャナや TigerRAT というリモートアクセス型トロイの木馬（Lazarus グループが使用する別の RAT）が起動されます。Talos は今年、TigerRAT の亜種に 2 つの新機能が備わっていることを確認しました。それが、USB ダンプ機能と（準備段階の）Web カメラキャプチャです。これらの機能は、システム情報の収集、任意のコマンドの実行、スクリーンキャプチャ、キーロギング、Socks によるトンネリング、ファイル管理、自己削除といった従来の機能を補完するものです。

Lazarus の攻撃者は他にも、VSingle や YamaBot RAT などの既知のカスタムマルウェアファミリを配布し続けています。この点は過去の活動と変わりません。カナダ、米国、日本のエネルギー会社を狙った Lazarus 攻撃について先ほど触れましたが、このときの一連の活動では、VSingle インプラントが YamaBot のローダーとして機能していることが確認されました。YamaBot は標準の RAT 機能として、ファイルとディレクトリの列挙、プロセス情報の C2 への送信、リモートロケーションからのファイルのダウンロード、任意のコマンドの実行、自己アンインストールを備えています。

攻撃者の素性

Transparent Tribe

別名

APT36、Mythic Leopard、COPPER FIELDSTONE

所属

パキスタン

活動開始時期

2016 年

目標

スパイ活動、知的財産の窃取

被害者に関する考察

Transparent Tribe は通常、中央アジア、南アジア、東アジアのみを標的とし、アフガニスタンとインドの軍事および政府に関わる組織や職員などに攻撃を仕掛けている。また、パキスタンを拠点とする活動家にスパイ行為を働いてきた。防衛産業や教育業界（大学や学生など）にも被害をもたらしている。

注目すべき TTP

Transparent Tribe は最初の感染の手段として、悪意のある VBA マクロを含む不正ドキュメントや、リモートインフラへのリンクを含む不正ドキュメントを使用することが多い。多くの場合、スピアフィッシングメールで送信する文書には、地域の問題に関連する地政学的な話題を含める。また、標的をさらにおびき寄せるために、ハニートラップ型のステージャを Google ドライブのフォルダに配置して使用したり、標的に関係のありそうな名前のドメインを登録したりする。

マルウェアとツール

Transparent Tribe は CrimsonRAT や ObliqueRAT などのカスタムマルウェアと、.NET ベースの追加のインプラントを展開する。

図 40. 攻撃グループ Transparent Tribe の素性

その他の注目すべき APT 活動

2022 年、Cisco Talos は、南アジア地域で活動する攻撃者による重大なサイバー脅威活動を確認し、その中で特に、インドの組織を主な標的とする多数の APT 攻撃を追跡しました。インドを狙ったサイバー攻撃の大半は、パキスタン政府とつながっている攻撃グループによって仕掛けられているようです。両国は長年敵対関係にあります。領土紛争、反政府活動、中国の影響についての地政学的懸念が残り続ける中、サイバー空間で、注目を集める対立がますます繰り広げられるようになっています。パキスタンとつながりのある APT は、インドの重要インフラ、軍関係者、安全保障分野および政治分野のシンクタンク、通信会社、教育機関を標的にしています。こうした活動の動機はスパイ活動であることが一般的です。

パキスタンとつながりのある APT が複数の業界にスパイ活動を展開、今年は教育業界が主な標的に

この地域で確認された悪意のあるサイバー活動の多くは、Transparent Tribe というパキスタンとつながりのあるグループによるものです。Talos は遅くとも 2016 年から同グループの活動を注視してきました。グループの主な標的は、アフガニスタンとインドの政府機関、軍事組織、その関連組織であり、これには準政府組織のほか、シンクタンク、大学、防衛産業基盤に属する個人が含まれます **(図 40)**。

Transparent Tribe はこれまで標的にしてこなかった対象にまで攻撃を広げようとしていると見られ、インド亜大陸の学生や教育機関を狙うようになりました。今年初めの攻撃で同グループは、悪意のある VBA マクロを含む不正ドキュメントをスピアフィッシングメールによってインドの大学生に配布しました。マクロが実行されると、埋め込まれていたアーカイブファイルが抽出されます。さらにこのアーカイブファイルには、Transparent Tribe が好んで使用する CrimsonRAT というマルウェアが含まれています。CrimsonRAT には、エンドポイントでスパイ活動を行い、Transparent Tribe によって運用されている C2 インフラに情報を送り返すための機能が多数搭載されています。使用された不正ドキュメントの多くは、攻撃者が登録したドメインでホストされていました。それらのドメインは「studentsportal[.]live」や「studentsportal[.]website」など、本物の教育関連サイトを装っています。同グループは「cloud-drive[.]store」などのメディア関連のドメインや、女性の写真

Transparent Tribe は、永続アクセスを維持するために CrimsonRAT や ObliqueRAT といった知名度の高いインプラントを多数使用し続けています。これらのツールの高い効果を今でも認めている証拠です。

を含む Google ドライブのフォルダを埋め込んだ Web サイトも使用しています。これらの戦術と偽装手段は、Transparent Tribe による過去の攻撃で確認されたファイル共有ドメインとハニートラップベースの攻撃から変わっていません。パキスタンを拠点とする SideCopy という APT グループも同様の手口を使用しており、Talos では同グループの追跡を行っています。

教育業界を攻撃したことは、政府関係の職員や組織を普段狙っている Transparent Tribe の方針から外れています。しかしその目的は、インド政府を支援している最高機関から重要かつ非公開の研究情報を盗み出すことだった可能性があると Talos は考えています。これは、パキスタンの戦略的利益とも一致する目的です。Transparent Tribe が署名付きの RAT を攻撃で使用し続けていることから、長期的なアクセスとスパイ活動が今なお同グループの目的である可能性が非常に高いと言えます。

Transparent Tribe が知名度の高い RAT の展開を続けながら、新しいカスタムマルウェアを導入

Transparent Tribe は、永続アクセスを維持するために CrimsonRAT や ObliqueRAT といった知名度の高いインプラントを多数使用し続けています。これらのツールの高い効果を今でも認めている証拠です。2022 年に Talos が調査した攻撃の大半で、同グループは受信者に不正ドキュメントを配布していました。受信者がそのドキュメントを実行すると CrimsonRAT が展開されます。CrimsonRAT は遅くとも 2020 年から同グループが好んで使用している .NET ベースのインプラントです。CrimsonRAT は感染マシンの情報を収集するための機能を多数備えています。システム上のファイル、フォルダ、ドライブや、エンドポイントで実行中のプロセスの ID と名前、ファイルのメタデータと内容を、すべて C2 の指定どおりにリスト化する機能などがその例です。CrimsonRAT はキーロガーとスクリーンショットからも情報を盗み出しました。Transparent Tribe は、2020 年に Talos が発見した C/C++ ベースのインプラントである ObliqueRAT も使い続けています。主にはインド政府関係者を狙った攻撃で、特に秘匿性が優先される場合に、このマルウェアを使用していると思われます。

APT グループ Bitter が ZxxZ という新しいツールを使用し始めました。Talos が特定したこのツールは、同グループの技術が巧妙化していることを示しています。

Transparent Tribe は今年、新しいカスタムマルウェアも導入しました。同グループがより多くの標的を侵害するためにツールの多様化を図っていることがうかがえます。この新しいマルウェアは、簡単かつ迅速に展開できるダウンローダー、ドロッパー、軽量の RAT で構成されています。インド政府職員を狙った攻撃事例では、いくつかの感染チェーンで .NET ベースの軽量インプラントが確認されました。CrimsonRAT や ObliqueRAT と比べると機能は限られていたものの、感染デバイスを監視および制御する機能は十分に備えていました。

知名度の低い APT「Bitter」が存在感を高め、新しいインプラントで南アジア諸国の政府を攻撃

Talos は、知名度の高いグループによる攻撃を明らかにしただけではありません。あまり知られていない Bitter という南アジアの攻撃グループ（別名 T-APT-17）の活動も確認し、新しいマルウェアを開発しながら数多くの重要な標的を攻撃してきたグループの実態を解明しました。2021 年 8 月から今年まで続いている攻撃で、同 APT グループは、南アジア諸国および東アジア諸国の政府や、エネルギー業界およびエンジニアリング業界の組織を標的にしています。スパイ活動が主な目的と見られ、ソーシャルエンジニアリング、脆弱性のエクスプロイト、RAT の展開を長らく行ってきたという経緯があります。

今年、Bitter の攻撃者は新しいツールを使用し始めました。ZxxZ インプラントという Talos が特定したこのツールは、同グループの攻撃チェーンの技術が巧妙化していることを示しています。ある攻撃事例では、同グループがバングラデシュの政府機関の職員におとり文書を配布しました。警察部隊の高官も標的になっています。不正ドキュメントの多くは悪意のある RTF ドキュメントまたは Excel スプレッドシートで、Microsoft の既知の脆弱性をエクスプロイトするように設計されたシェルコードを含んでいます。被害者が不正ドキュメントを開くと、正規のプログラムを装ったトロイの木馬である ZxxZ が Bitter のホスティングサーバーからダウンロードされ、被害者のエンドポイントで実行されます。この新しいインプラントはリモートファイルを実行する機能を備えており、BitterRAT、Artra ダウンローダー、SlideRAT、AndroRAT などの他の悪意ある Bitter ツールを展開できます。Bitter はあまり知られていないため、Talos がこのインプラントを発見したことで、サイバーセキュリティ コミュニティの間で同グループの活動や急速に進化するマルウェア群についての理解が深まるでしょう。

南アジアとつながりのあるグループの間で見られるコードの共通性

今年の初めに Talos が公表した調査は、ある珍しい傾向を示唆していました。それは、南アジアで活動する複数の APT グループが、別のグループによって記述された VBA コードをおそらく意図せずに流用しているということです。Donot Team（別名 APT-C-35）は中国の組織やパキスタンの政府機関および軍事組織を以前から標的としてきた APT グループですが、同グループに関連する悪意のあるアーティファクトの VBA コードを確認したところ、パキスタンを拠点とする Transparent Tribe の VBA コードとの類似性があるという驚くべき証拠が見つかりました。両グループ間で意図

的または直接的にコードが共有された可能性は低いと思われます。それぞれの標的が正反対であることを踏まえれば、なおさら考えにくいでしょう。しかし、これらの APT グループが、他のグループによる攻撃で成果を挙げていると判断したコードを利用して開発を行うために、公開ライブラリに頼った可能性はあります。また、犯人特定の判断を誤らせるために、他方のグループの攻撃で使用されている TTP やマルウェアを採用した可能性もあります。

まとめ

脅威の高まりの中で、公的機関および民間機関を狙った APT 攻撃のリスクは存在し続けています。サイバーセキュリティ コミュニティは今年、ロシアとウクライナの戦争による影響、ランサムウェアや他のモジュール式脅威の拡散、サイバー犯罪グループの急増を追跡することに注力してきました。しかしその一方で、国家とつながりのある APT グループや政府の支援を受けた APT グループは 2022 年の地政学的環境の大きな変化に対応して活動を継続し、拡大させてきました。脅威グループは、自国の利益に合致するとされる目的の達成に今なお力を注いでいます。APT 攻撃全般では、スパイ活動、知的財産と金銭の窃取、ネットワークの中断などの動機が最もよく見られました。こうした事象のリスクは 2023 年になっても残り続けると Talos は考えています。

このセクションで取り上げた APT グループの大半で、新たにカスタマイズされたマルウェアやツールを取り入れたり、既知のマルウェアの亜種を展開したりする傾向が強く見られました。国家とつながりのある攻撃グループは、リモートアクセス ソフトウェアやポストエクスプロイト フレームワークなどのオープンソースツールを取り入れながら APT マルウェアを多様化させ、感染チェーンを巧妙化させています。こうした状況から、これらのグループがセキュリティ システムによる検出やブロックを受けたり TTP を広く暴露されたりしても活動を断念していないことがわかります。APT グループならではの巧妙さがあるため、防御側は攻撃のリスクを常に想定しておかなければなりません。それでも、セキュリティ対策を強化すれば APT の活動による影響を軽減できます。ネットワークのセグメント化、多要素認証の導入、正当なビジネス機能がないツール（リモートアクセス ソフトウェアなど）に対するユーザーアクセスの制限など多層のセキュリティ対策を講じ、パッチ適用やエンドユーザー教育といった賢明な組織ポリシーを組み合わせることが、APT 攻撃を阻止するための最適なアプローチとなります。

最後に、地政学的状況を注視し続けることで APT の目的と標的を把握しやすくなると Talos は考えています。ロシア、イラン、中国、北朝鮮、インド亜大陸諸国の事例でわかるように、防衛、経済、国境、制裁、外交など国益に関わる動向が APT の攻撃活動に影響したり、攻撃の原動力になったりする傾向にあります。これらの国の目的と野望を詳しく追っていけば、防御側の取り組みの方向性を定めやすくなります。

まとめ

企業や個人に降りかかる脅威は 2022 年においても依然深刻である一方で、攻撃者が活動する地政学的環境は著しく複雑さを増しています。攻撃者はツールやインフラを更新したり、自らの要求を企業にのませる手段を新たに生み出したり、新しいエクスプロイト手法を考案したりすることによって、脅威環境を変化させました。しかし今度は、現在の複雑な地政学的環境によって攻撃者自身が変化を強いられる状況になっています。

こうした推移は、本レポートのすべてのセクションに表れています。ウクライナでの戦争の影響は、ロシアを拠点とする APT がウクライナを標的にするようになったことにとどまりませんでした。東ヨーロッパのランサムウェア環境でグループが分裂したりいずれかの陣営についたりして、大きな混乱が起きています。優勢なグループからなる寡占状態だったランサムウェア環境は、法執行機関からの注目の高まりや、グループの仲間割れ、内部の人間による情報流出を背景に、さまざまな攻撃者が入り乱れる空間に変わりました。同様に、法執行機関が Emotet や Trickbot などのかつての主要なコモディティ型ローダーに禁止同然の措置を行っているため、Qakbot などの他のファミリが活動拡大の余地を見出し、セキュリティ研究者の検出手法を常に把握しながら、必要に応じて戦術、手法、手順（TTP）を更新しています。これに関連して、セキュリティコミュニティが Cobalt Strike を検出および追跡する機能を大幅に改善する中、2022 年には新しい攻撃フレームワークの利用が爆発的に増加しました。この状況により、防御側はより多くの困難に直面する可能性があります。その一方、非常に巧妙な国家の支援を受けるグループには十分なリソースがあり、自らとつながりのある政府の地政学的目的が変化する中で、その遂行を支援する攻撃を仕掛け続けています。

こうした変化は防御側にとってどのような意味を持つのでしょうか。第一に、主要な攻撃者が柔軟性と適応力を備えていることから、攻撃の背景がこれまで以上に重要になります。脅威活動の動機となる地政学的な動向を把握し、徹底的な攻撃者追跡方法と脅威インテリジェンスプロセスを整備して、こうした抜け目ない攻撃者の行動の進化を文書化することが防御側に求められます。第二に、攻撃者は検出機能に合わせて行動とツールを変えるため、防御側は強固なセキュリティエコシステムの構築について考えるとともに、セキュリティ製品をアンインストールしにくくし、完全な状態で展開する必要があります。第三に、企業が直面している脅威の多さを考慮すると、セキュリティアラートには、脅威に関する重要な背景情報（重大度の評価など）や修復のための推奨事項を提供し、アラート疲れを起こさないような設計が求められます。最後に、攻撃がますます巧妙化する中で企業がレジリエンスを高めていくためには、侵害について「起こるかどうかではなく、いつ起きるか」を考える癖をつけなければなりません。そして、インシデント対応計画の作成やさまざまな脅威シナリオの実験を行いながら、ネットワークに侵入された後の攻撃をより困難にするための方法を考える必要があります。

2022 年の状況は数々の重大な課題を露呈させていますが、防御側の決意と能力を示してもいます。Cisco Talos がウクライナで行ってきた業務では、防御者が善のために共通の使命を持って協力するとどれだけの力を発揮できるかが示されました。Talos は今後も、お客様、パートナー、コミュニティを脅かす攻撃者と戦い続けます。2023 年は可能な限り多くの攻撃者を阻止していきます。

