REPORT

フォーティネット グローバル脅威レポート

FortiGuard Labs による 2023 年上半期レポート

FORTINET

目次

概要

脅威環境や組織の攻撃対象領域は常に変化しています。そして、サイバー犯罪者は、自らの手法をすばやく設計し、適応する能力を進化させることで、この進化する環境を悪用し、業種や地域を問わず、あらゆる規模の企業に重大なリスクをもたらし続けています。

2023 年前半の活動を検証したところ、サイバー犯罪組織や国家が支援するサイバー攻撃グループが新しいテクノロジーを迅速に採用していることがわかりました。注目すべきは、一般企業とほとんど変わらず明確に定義された責任、成果物、目的を持って活動している攻撃者もいるということです。このような組織構造が過去のエクスプロイト* やその組織を支援する国家から提供される潤沢な資金と結び付くことで、新しい生成 AI などの最先端テクノロジーの実験や採用が可能になり、結果として、攻撃を容易にし、より複雑化させて検知を困難なものにしています。

特にサイバーセキュリティの領域においては、攻撃者の高度化が急速に進んでおり、脅威の頻度も複雑さも大幅に上昇しています。フォーティネットの AI を活用したグローバルな検知機能によって、複雑なランサムウェアキャンペーン、大規模なデータ侵害、MITRE ATT&CK** 戦術の大きな変化などが観察されたことからもわかるように、さまざまな業種での高度な標的型攻撃が増加しています。

* エクスプロイト攻撃とは、ソフトウェアやアプリケーション、OS などの脆弱性やバグ、不具合などを悪用したツールを利用して、非倫理的な攻撃を行うことを指します。特定の脆弱性を悪用するプログラムがエクスプロイトです。エクスプロイトは OS やアプリケーションなどさまざまなまだ対策されていない脆弱性を見つけ、それを悪用します。詳細：https://www.fortinet.com/jp/resources/cyberglossary/exploit-attack

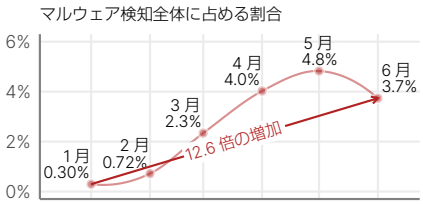
** サイバー攻撃の目的や具体的な使用技術が体系的にまとめられたデータベース

2023 年上半期のハイライト

APT グループ

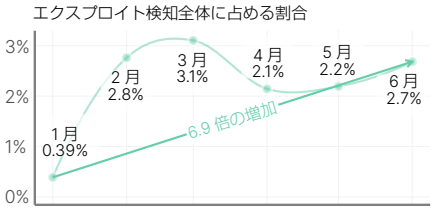
MITRE が特定した 138 の APT グループのうち 41（30%）の活動が検知されました。これらの攻撃は、集中型であるだけでなく計画的でもあり、目まぐるしい「波」となって発生するため、分類されたすべての APT グループの 3 分の 1 が活発に活動しているのは懸念すべきことです。

ランサムウェア



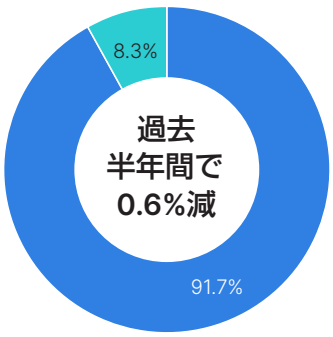
ランサムウェアの活動の乱高下が続き、2023 年上半期の終了時に開始時の 13 倍を記録しました。ランサムウェアの検知に成功している組織が以前より減少したことは（22% から 13% へ）、ランサムウェアもさらに高度化し、標的型になっていることを再認識させるものです。

ICS / OT 攻撃



産業用制御システム（ICS）やオペレーショナルテクノロジー（OT）を標的にする攻撃は、大量に発生したわけではないものの、2023 年上半期に増加傾向を示しました。半数の組織で ICS / OT のエクスプロイトが確認され、エネルギーと公益事業が標的の上位になりました。

レッドゾーンへの突入



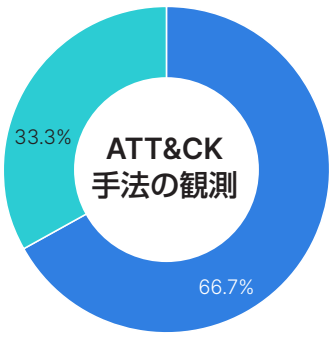
2023 年上半期の攻撃者に標的にされたエンドポイント脆弱性の割合は、前期と比べると比較的安定していました（約 8%）。

エクスプロイトまでの時間

327 倍

フォーティネットの分析によると、機械学習を用いた悪用可能性のスコアリング手法である EPSS（Exploit Prediction Scoring System）で特定された、エクスプロイトの可能性が最も高い上位の脆弱性が 1 週間以内に攻撃される可能性は、レーダーで検知される他の脆弱性の 327 倍です。

ATT&CK 手法の観測



フォーティネットの検知テクノロジーにより、2023 年上半期に既知の MITRE ATT&CK 手法の 3 分の 2 の活動が観測されました。

2023 年上半期には、APT（Advanced Persistent Threat：高度な持続的脅威）グループの活発な活動、ランサムウェアの頻度と複雑さの上昇、ボットネット活動の増加、攻撃者が使用する MITRE ATT&CK 手法の変化などが確認されました。

しかしながら、脅威環境が変化しているとは言え、防衛側にとって悪いニュースばかりではありません。本レポートでは、脆弱性についても詳しく解説し、パッチの適用や修復の優先度の判断についてのアドバイスも提供します。また、我々が目にする脅威の多くは馴染みのものであるため、攻撃者に対する効果的な防御を可能にする戦略を実装する機会はたくさんあります。最後に、脅威インテリジェンスを活用した組織の保護を始めとする、今すぐ実行できるいくつかの手順も説明します。

分類されたすべての APT グループの 3 分の 1 の活動を 2023 年上半期に確認

分析するこれらのトレンドの背後にいる攻撃者に注目することには十分な価値があります。MITRE は、ATT&CK フレームワークをサポートする取り組みの一環として、138 のサイバー脅威グループを追跡しています [1]。これらのグループの集団的活動を監視することは、脅威環境のマッピングと分析に不可欠な要素です。2023 年 1 月～ 6 月にかけて、これらのグループのうち 41 のグループ（30%）の活動を観測し、その中でも最も活動が活発だったのは、マルウェア遺伝子コード分析に基づくと、Turla、StrongPity、Winnti、OceanLotus、WildNeutron であることがわかりました。

Turla は恐らくは、現存する脅威グループの中で最も能力の高いグループの 1 つです。20 年近く前から、さまざまな別名（Snake、Venomous Bear、Blur Python など）で活動を続けてきました。Turla はこれまでに、45 件以上の有名な攻撃に関与したとされており、世界中の公的機関、メディア、エネルギー部門の組織、大使館などを攻撃しました。多くの組織に対する攻撃を成功させ、監視体制が厳しい環境にあっても長年にわたって検知を逃れてきたことに加えて、ロシアとウクライナの紛争が激化していることを考慮すれば、このグループの活動が活発化したことに驚きはありません。

しかしながら、悪いニュースばかりではありません。APT グループの活動の過去 6 ヵ月間の影響がすべての組織のごく一部に限定されていることから、少なくとも当面は、APT 活動が引き続き高度な標的型の攻撃であることを示しています。自らのサイバー兵器をスプレー攻撃に浪費することは恐らくないため、これは納得できることです。

ランサムウェア活動の乱高下が継続

ランサムウェアは数十年前から存在しますが、RaaS（Ransomware-as-a-Service：サービスとしてのランサムウェア）の普及に伴い、最近では、高度で複雑なマルウェアで攻撃者がネットワークに侵入するようになりました [2]。また、ランサムウェアの活動が依然として活発であることから、世界中のビジネスリーダーが、脅威に対する懸念を強めています。フォーティネットが最近実施した調査によると、78% のリーダーが、自社に攻撃への備えがあると回答しましたが、半数が攻撃を受けていたことがわかりました [3]。

ランサムウェア活動に減速の兆しはなく、マルウェア検知全体に占めるランサムウェアの割合が、2023 年上半期の終わりには、2023 年初頭の 13 倍を記録しました。ところが、影響を受けた組織の数は、乱高下の下限にとどまっています。5 年前には、約 4 分の 1（22%）の組織のネットワークでランサムウェアの活動が検知されましたが、2023 年上半期には、その割合が 13% に下落しました。この明らかな活動の減少は残念ながら、ランサムウェア活動の沈静化を示すものではなく、ランサムウェア攻撃が集中型になったことを示すものであり、ランサムウェアグループがビジネスモデルを進化させ、素早く適応できる高度なプレイブックを使用した標的型の攻撃を実行するようになったということです。

2023 年上半期にフォーティネットのテレメトリで観測された、最も拡散したマルウェアファミリーについての情報を下図に示します。クリプトマイナー、インフォスティーラー、ランサムウェア、RAT（リモートアクセスのトロイの木馬）のカテゴリごとの上位のファミリーを記載します。

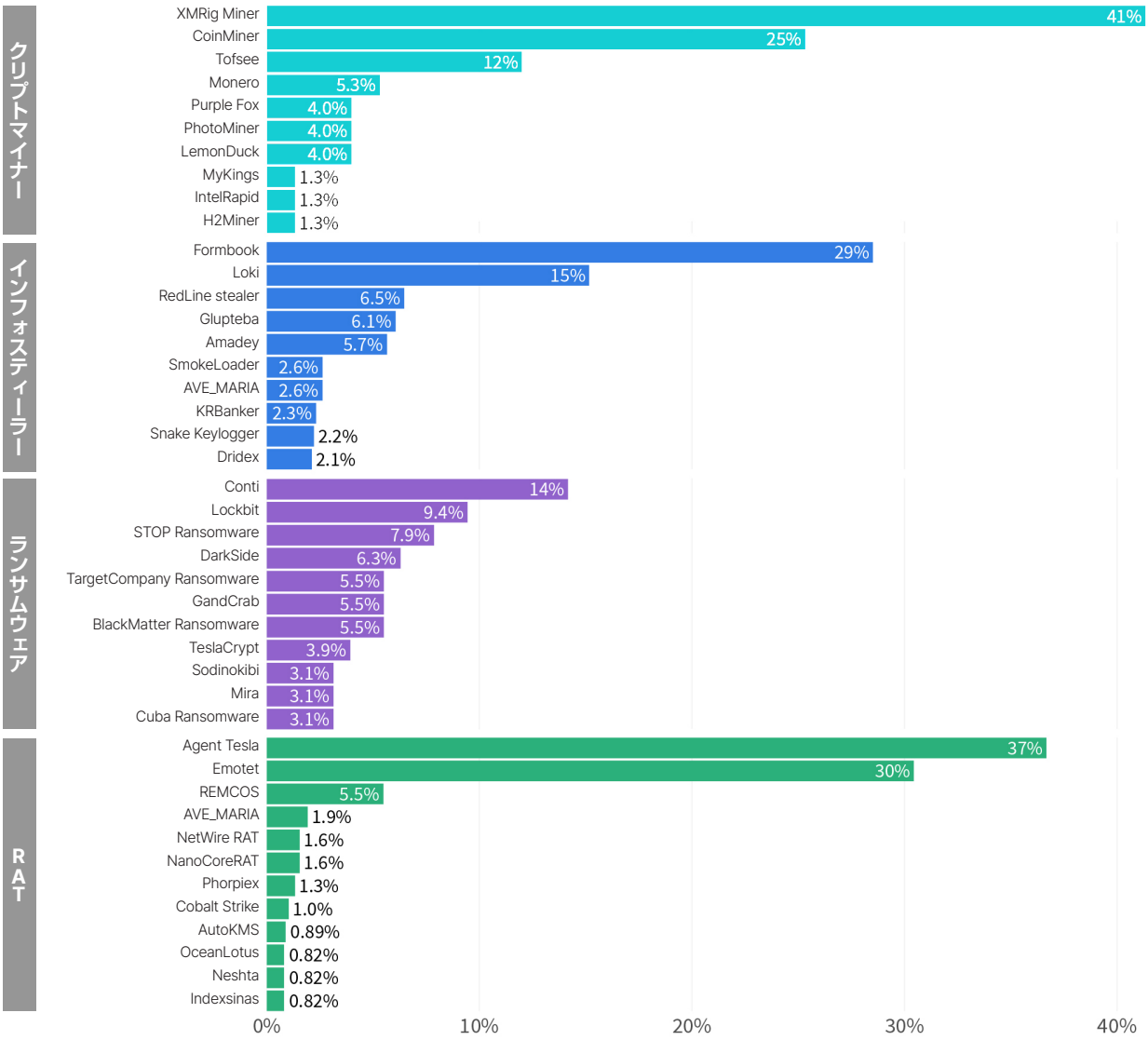


図 1：タイプ別の上位のマルウェアファミリー

ワイパーは減速しつつある（今のところは ...）

図に記載されていないランサムウェアのカテゴリの 1 つが、ワイパー型マルウェアです [4]。ワイパーという名前は、この破壊的な攻撃手法が感染システムからデータを「ワイプ（消去）」するためです。2022 年初めにワイパーの使用が急増しましたが、その大きな要因となったのが、ロシアとウクライナの紛争です [5]。その増加は 2022 年末まで継続しましたが、2023 年前半になると減速しました。

ワイパーは、主に紛争時に国家が支援する攻撃者によって使用される場合が多く、サイバー犯罪者がこのタイプのマルウェアを使用して、テクノロジー、製造、政府、電気通信、医療など、特定の分野の組織を標的にすることもあります。

5 年間の脅威トレンドを振り返る

セキュリティの管理者の多くが、サイバーセキュリティについてのあらゆる出来事は悪化の一途をたどると考えているようです。

果たしてそれは事実なのか、あるいは思い過ごしなのでしょうか？ 時には一歩引いて長期的なトレンドを検証することが重要であり、そうすることで、脅威の現状についての必要とされる視点が生まれることもあります。エクスプロイト、マルウェア、ボットネットに関する 5 年間のトレンドを振り返ってみましょう。

エクスプロイト	マルウェア	ボットネット
10,042 検知された一意のエクスプロイトの数 ■ 過去 5 年間で 68% 増	**44,886** 一意の亜種の数 ■ 過去 5 年間で 172% 増	**330** 検知された一意のボットネットの数 ■ 過去 5 年間で 27% 増
54 組織あたりのエクスプロイト検知件数 ■ 過去 5 年間で 75%	**7,063** 異なるファミリーの数 ■ 過去 5 年間で 135% 増	**4.3** センサーあたりの活動中のボットネットの数 ■ 過去 5 年間で 126% 増
69% 深刻なエクスプロイトを経験した組織の割合 ■ 過去 5 年間で 10% 減	**18** 10 社に 1 社以上の割合で拡散したマルウェアファミリー ■ 過去 5 年間で 100% 増	**83** 平均感染日数 ■ 過去 5 年間で 1,085% 増

エクスプロイト亜種の増加

一意のエクスプロイトの検知数が、過去 5 年間で 68% 増加しました。このことは一方で、悪意のある攻撃を検知する方法が以前より増えていることを示しています。さらには、攻撃者がエクスプロイトを加速させ、多様化させていることも示しています。しかしながら、これと同時に、組織あたりのエクスプロイトの試行は 75% 減少し、重大なエクスプロイトは 10% 減少しました。

このエクスプロイトの試行の減少は、良いことのように思えるかもしれませんが、攻撃者が標的型の攻撃を実行するようになったことを示すもう 1 つの兆候です。サイバー兵器も、過度に使用されれば、いずれは検知される可能性が高くなり、時間の経過と共にそのペイロードが役に立たなくなって効力を失うことになるでしょう。

組織的サイバー犯罪によるマルウェア活動の増加

マルウェアファミリーと亜種は過去 5 年間で爆発的に増加し、それぞれ 135% と 175% 増加しました。さらに注目すべきは、グローバル組織の少なくとも 10%（重要な拡散のしきい値）に侵入したマルウェアファミリーの数が倍増したことです。これは間違いなく、サイバー犯罪グループや国家が支援するグループの増加と現在活動しているグループによる攻撃の拡大の結果です。

このような攻撃者の標的を選択する能力、精度、破壊力の増大に伴って、脅威が次第に激化していることから、防御側は、攻撃者との果てしない戦いを余儀なくされています。攻撃者は、ここ数年の最先端の重要な技術的進歩を活用することで、急速な進歩を遂げ、高い能力を身に付け、多様な攻撃を可能にし、検知を逃れるようになっています。

ボットネットの永続化

最近のマルウェアの多くは、コマンド & コントロール（C2）通信のためのボットネットを確立します。マルウェアファミリーと亜種の増加を考えれば、ボットネット活動も増加するのは当然のことでしょう。今日、活動中のボットネットの数は増加し（27%）、組織のボットネット感染の発生率も増加しています（126%）。

しかしながら、ボットネットのトレンドの本当の要因は、「活動日数」（ボットネット活動の最初の検知から最後のセンサーの「ヒット」までの日数）の合計の大幅な増加です。これは、ボットネット通信を検知してブロックしてから、ボットネットの侵入の試行が失敗して進路を変えるまでの平均日数を測定したものです。言い方を変えれば、このタイプの活動を検知したセンサーが活動を「認識して除去する」平均時間ということになります。過去 6 ヵ月の平均は、183 日（測定した最終日）のうちの 83 日で、全期間のほぼ半分でした。これは、2018 年初めの測定から 1,000 倍以上の増加であり、ボットネットの永続化の能力がこの 5 年で大幅に向上したことを示しています。「ボットネット兵器ベルト」に装着できる脆弱性やエクスプロイトが全体として増加し、短期間でボットネットが適応して自動的に侵害し、制御できるデバイスの範囲が拡大していることから、これは大きな懸念事項と言えます。

レッドゾーンを理解する

グローバル脅威レポートに 2022 年下半期から追加されたレッドゾーンは、攻撃者による特定の脆弱性のエクスプロイトの可能性がどの程度高いか（または低いか）を理解するためのものです [6]。

エンドポイントに存在する CVE（Common Vulnerabilities and Exposure：共通脆弱性識別子）と攻撃者に標的にされる CVE との関係には、組織の脆弱性管理の手法や攻撃者によるツールの開発などの複数の要因が影響しますが、セキュリティリーダーによるパッチ適用の優先順位付けの判断に利用できる、攻撃対象領域の状態の貴重なスナップショットを提供してくれます。

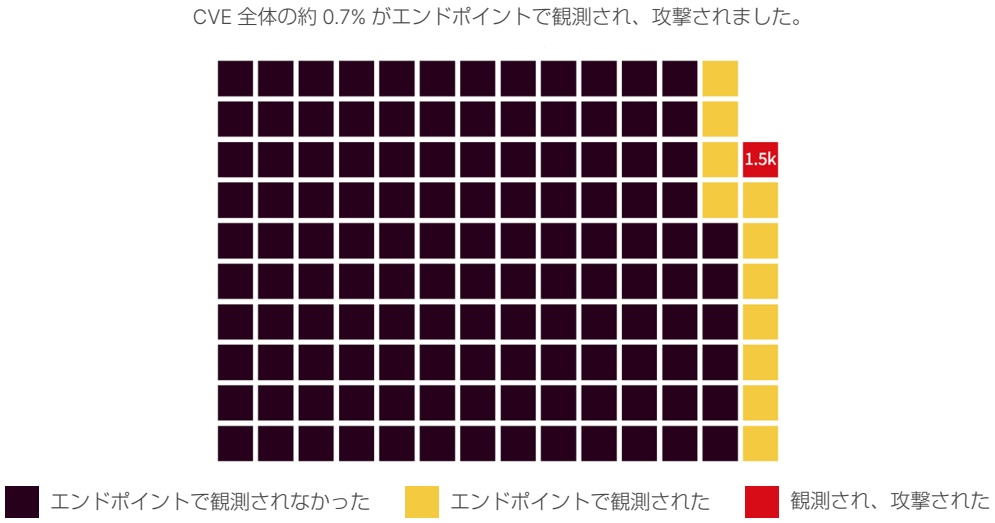


図 2：エンドポイントにおける存在と攻撃別のすべての CVE

レッドゾーンは 2022 年下半期に 9% 前後で推移しましたが、これは、観測された 16,500 以上のうち、約 1,500 の CVE が攻撃されたことを意味します。ところが、攻撃された CVE のこの割合が 2023 年上半期に 8.3% に低下しました。興味深いことに、攻撃で観測された CVE がほぼ同じだった一方で、エンドポイントで観測された CVE の割合は増加しました。これは必ずしも、新たな脆弱性との戦いで組織が優位な方向に進んでいることを示すものではありませんが、少なくとも、攻撃される脆弱性の割合が以前と比べると少し減少しているようです。

また、攻撃された脆弱性の割合はプラットフォームによって大きく異なり、以下に示すように 11% もの差があります。プラットフォーム間でのもう 1 つの大きな違いは、黄色で示した、エンドポイントで観測されたすべての CVE の割合です。Microsoft と Adobe で関連する脆弱性の半数以上が観測されたのに対し、Apple のプラットフォームでは 12%、Linux では 20% でした。注意点として、これらのグラフはすべてのプラットフォームを正規化したものであり、例えば、Adobe の 1 つの四角と Linux の 1 つの四角では、表す脆弱性の絶対数が異なります。

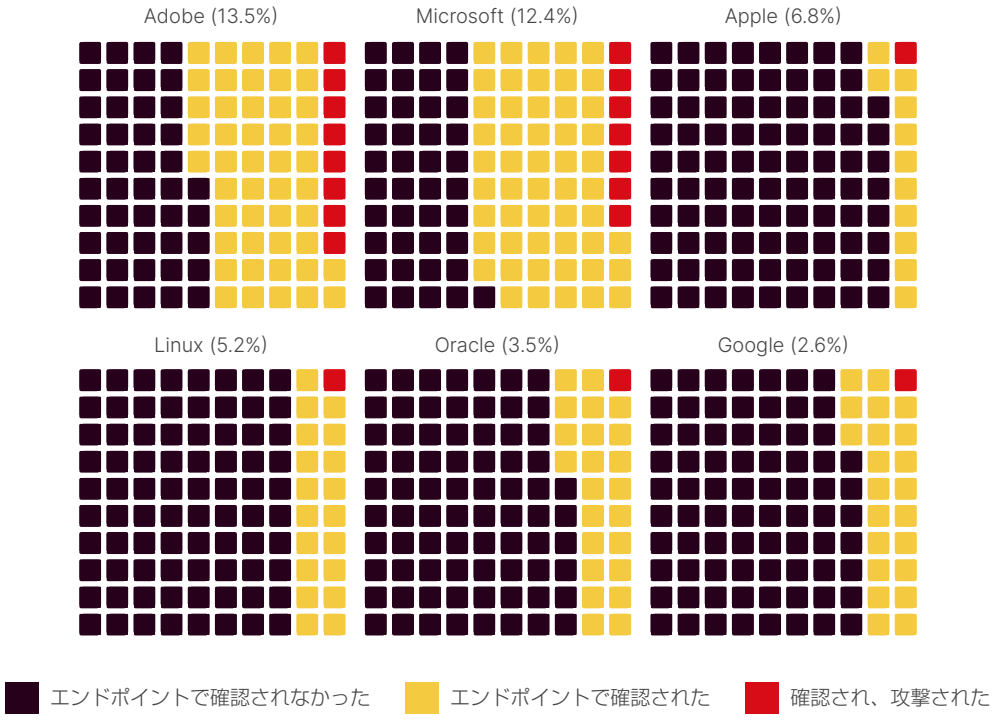


図 3：エンドポイントにおける存在と攻撃別の複数のプラットフォームの CVE

確実に言えるのは、組織は公開された脆弱性をすぐに修正することに苦労しており、サイバー犯罪者はその現実をすばやく悪用しているということです。そのため、パッチを適用する脆弱性の優先度を判断するための適切な戦略が不可欠です。優先度を判断する過程でそれぞれのプラットフォームを考慮する必要がありますが、それは、近い将来に攻撃の標的になる可能性のある未解決の脆弱性の表面的な予測に過ぎません。

防御側には幸いにも、EPSS（Exploit Prediction Scoring System：エクスプロイト予測スコアリングシステム）というさらに強力なツールがあります。次のセクションでは、この EPSS について説明します [7]。

エクスプロイトの予測からアウトブレイクまで

フォーティネットは、EPSS を中心メンバーとして当初から支援し、エクスプロイト活動データの提供を続けています。EPSS（Exploit Prediction Scoring System：エクスプロイト予測スコアリングシステム）は、多くのデータソースを活用して、脆弱性が悪用される可能性を予測するもので、フォーティネットもメンバーとして参加している FIRST.org の SIG（Special Interest Group）が主導して ESPP を運用しています。

多くの脆弱性管理チームが EPSS を利用して修復作業の優先度を判断していますが、EPSS は、脆弱性の最初の公開から実際のエクスプロイトの発生までの経過を追跡するインテリジェンス活動にも役立ちます。ここで紹介する後者のユースケースでは、EPSS データを脅威インテリジェンスのプロセスに組み込むことで、早期警戒システムとして活用します。

以下に、その例を紹介します。5 月 31 日、MOVEit Transfer Web アプリケーションに SQL インジェクションの脆弱性が存在し、認証されていない攻撃者がデータベースエンジンで使用されている要素を変更したり削除したりできる可能性があることがわかりました [8]。サイバーセキュリティコミュニティはただちに、この脆弱性を注視すべき脆弱性の 1 つと認識し、FortiGuard Labs は、この脆弱性を周知するための脅威シグナルとエクスプロイト活動を監視するための IPS シグネチャを公開しました [9]。

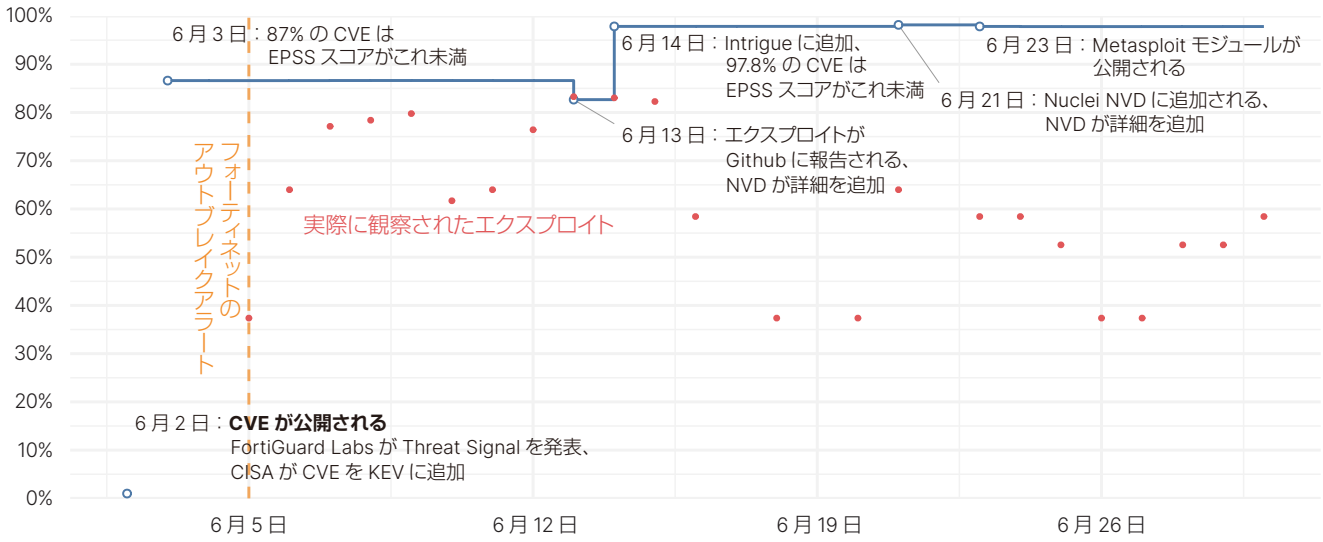


図 4：EPSS の進化と MOVEit 脆弱性のエクスプロイト

CVE が公開された段階で、30 日以内にエクスプロイトの可能性が非常に高いことを EPSS で予測することができました。そして、結果として、程なくしてそれが現実になりました。フォーティネットのセンサーは、脆弱性が最初に特定されてからわずか 5 日後の 6 月 5 日に攻撃者による MOVEit の脆弱性のエクスプロイトの試行を記録し、その日のうちにシグネチャを公開しました。EPSS はこの例では、アナリストが予測したことを独自に検証し、新たな脅威の活動が急増する前に対策を講じるのに役立ちました。

MOVEit の例から、いくつかの興味深い疑問が生まれます。脆弱性の最初の発表からエクスプロイトまでの時間は一般的にどれ位なのでしょうか？ EPSS スコアが高い CVE はスコアが低い CVE より早く悪用されるのでしょうか？ そうであれば、EPSS を使用して特定の脆弱性のエクスプロイトまでの平均時間を予測できるのでしょうか？

これらの疑問の答えを見つけるため、フォーティネットのセンサーでエクスプロイトが検知された 11,000 以上の公開された脆弱性に関する 6 年間のデータを分析しました。CVE ごとに、公開から最初のエクスプロイトの観察までの時間と対応する EPSS スコアを割り出しました。その分析結果を下図に示します。

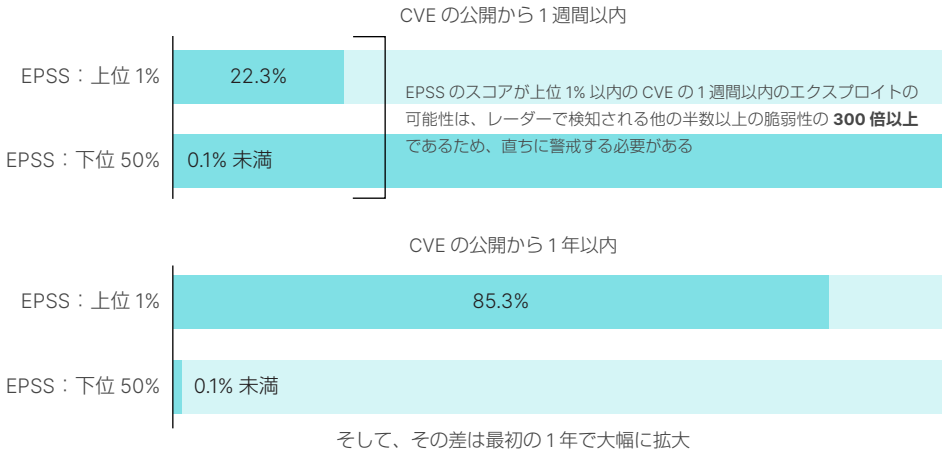


図 5：EPSS スコアが異なる脆弱性のエクスプロイトの割合

簡単に言えば、どの脆弱性のエクスプロイトの可能性があり、そのエクスプロイトがどれほど早く発生するかを予測する場合、EPSS が極めて有効であることがわかりました。公開から 7 日以内に、EPSS スコアが最も高い脆弱性（上位 1%）の 22% でエクスプロイトの活動が確認されたのに対し、EPSS スコアが下位の半分の脆弱性についてはわずか 0.07% でした。1 年が経過した段階で、上位の EPSS CVE の 85% はエクスプロイトが記録されましたが、下位の半分はほとんど攻撃者に無視されたままです。

つまり、EPSS のスコアが上位 1% 以内の CVE の 1 週間以内のエクスプロイトの可能性は、レーダーで検知される他のほとんどの脆弱性の 300 倍以上であるため、直ちに警戒する必要があるということです。これから警戒を始める場合は、EPSS スコアを毎日取得し、スコアに従ってパッチの優先度を判断することをお勧めします [10]。

グローバル ATT&CK ヒートマップ

フォーティネットは、1,000 万以上のセンサーのグローバルネットワークを活用したデータ処理を約 6 ヵ月間にわたって継続した後に、最もよく観測されるハッシュのリストを作成しました。フォーティネットの最先端のセンサーは、機械学習（ML）手法を採用して、未加工データを強力なデータセットに変換することで、ネットワークトラフィックに存在する潜在的な脅威の調査を支援します。フォーティネットは、検知した不正ペイロードをフォーティネットの製品とソリューションのポートフォリオを使用して分析し、その根底にある目的を示すわずかな挙動を観察して特定しています。このプロセスで生成された実用的なインテリジェンスは、世界中のサイバーセキュリティの防御側にとって極めて重要であり、レッドチームによる対象を絞り込んだ調査や効果的な脅威ハンティング活動を可能にします。

MITRE を参考にすることで、攻撃者の活動を理解できるようになります。ATT&CK は、わかりやすく実用的であるため、防御側が攻撃側の行動を体系的かつ反復可能な方法で分類し、最終的にはセキュリティチームが潜在的な攻撃を確実に特定し、組織のリスクを正確に評価するのに役立ちます。

ただし、本レポートは「パイの一部」に過ぎず、セキュリティソリューションが異なれば、特定の手法を検知する機能や役割も異なる点に注意する必要があります。本レポートの分析は、サンドボックスソリューションである FortiSandbox と EDR（エンドポイントの脅威検知とレスポンス）ソリューションである FortiEDR のデータに基づくものです。

最初に、データを検証します。これらの手法を攻撃能力と考えるとわかりやすいでしょう。

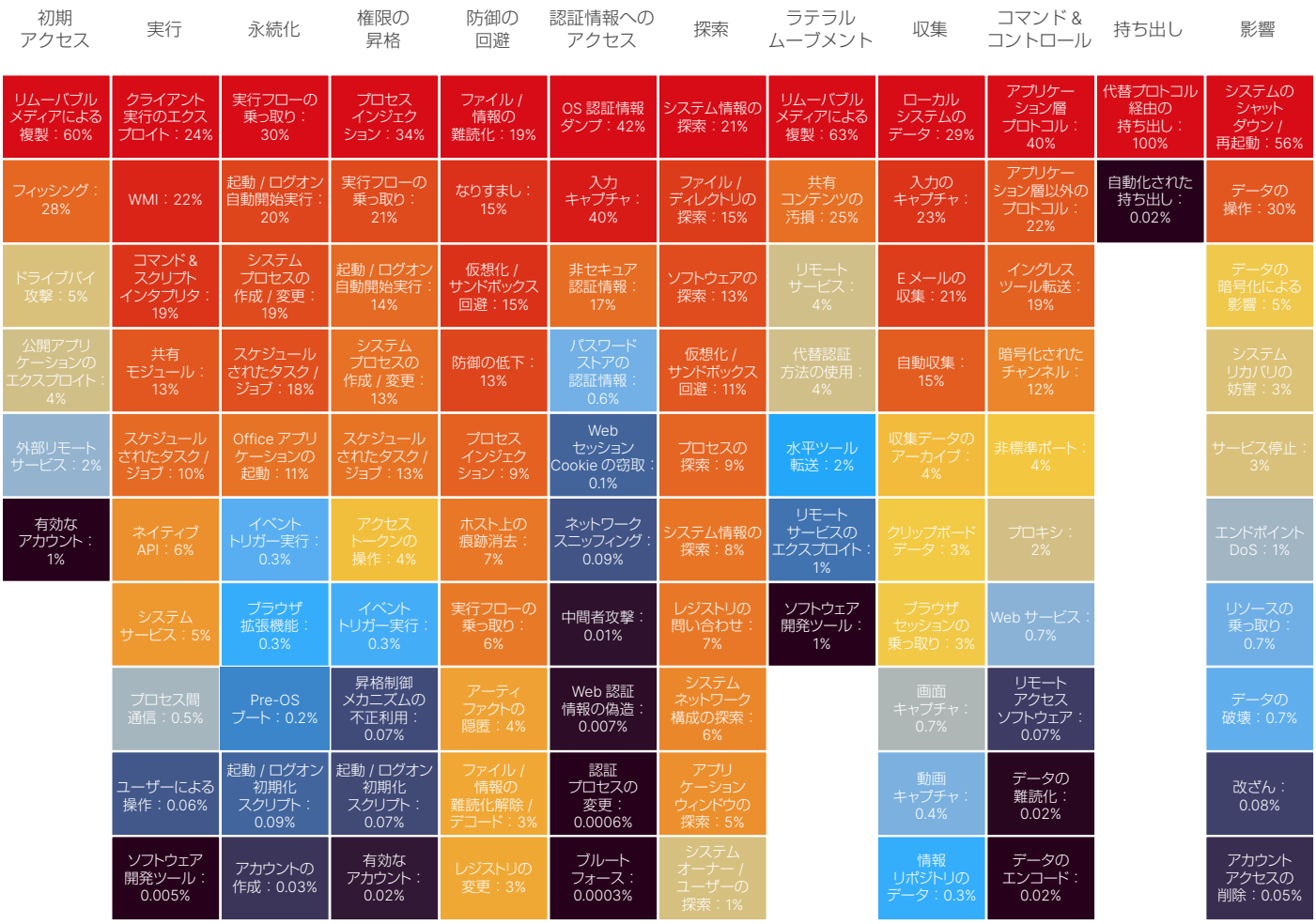


図 6：戦術別のクラウドデータにおける ATT&CK 手法

図 6 でわかるように、データから得られた検知結果により、ATT&CK フレームワーク全体が可視化されます。上の方の列は、それぞれの戦術で検知された 10 位までの手法が何かを示しています。見やすさを考慮して、親である手法の下の列にそのカテゴリのサブ手法を記載しました。これらの手法が過去 6 ヵ月間にどのように展開されたのかを検証し、それらに対抗する方法を考えてみましょう。

初期アクセスフェーズで最も多く確認された手法は、リムーバブルメディアによる複製です [11]。企業ネットワークへの侵入口の首位ではないものの、分析した不正ペイロードの大半は、この方法で拡散する可能性があります。前回のレポートで解説した Raspberry Robin が採用したことで、この手法の利用が急増しました [12]。それ以降も、このワームが他でも多く利用されていることを Microsoft が発見し、Raspberry Robin は、最大のマルウェア配布プラットフォームの 1 つになるまでに成長しました。FortiGuard Labs は、このワームがこれほど広く拡散したのは、主に .LNK ファイルをフォルダに見せかけるという単純な戦術によるものと考えており、ほとんどの個人はこれを開いてしまう可能性があります。このマルウェアファミリーは、米国の CISA（Cybersecurity and Infrastructure Security Agency）によって、現存する最も活発なドロッパーの 1 つに指定されており、IcedID、TrueBot、Bumblebee マルウェアの配布に使用されています [13]。

実行フェーズで我々が注目したのは、ユーザー実行のエクスプロイトの急増です [14]。このトレンドは、ユーザーが不用意にペイロードを開始したり、マクロを有効にしたりすることを前提にする攻撃が減少していることを示しています。その一例が、最近のいくつかのブログ記事で増加しているとして解説した Follina などの Microsoft Word で悪用される脆弱性です [15]。FortiEDR で阻止した脅威にも、このトレンドが確認されました。多くの場合、コードの実行にあたってユーザーとのやり取りを必要とすることは少なくなりました。この手法から組織を保護する 1 つの方法は、脆弱性に定期的にパッチを適用することで攻撃対象領域を縮小することです。

永続化フェーズでは、DLL サイドローディングのインスタンスが引き続き多く観察されました（実行フローの乗っ取りの下）[16]。3CX は、この手法を採用して防御回避と永続化の両方を達成した例で、最近のブログ記事でこれについて分析しています[17]。この手法が特に厄介なのは、アプリケーション制御やソフトウェア実行のその他の制限などの保護対策を攻撃者が回避できてしまうためです。この手法から組織のネットワークを保護するには、大前提として、ソフトウェアが DLL サイドローディングに対して脆弱でないことを確認することであり、これは、意図しないコードが実行されないようにする方法がこれ以外にほとんどないからです。ネットワークに存在する不正ペイロードは最終的には検知されますが、メモリに読み込まれて初めて検知されます。

防御回避の上位 3 つの手法がファイル / 情報の難読化、なりすまし、仮想化 / サンドボックス回避であることに大きな驚きはありません[18、19、20]。マルウェアに固有の部分でも、API コールからメモリ内の文字列までのさまざまな形で難読化が使用されています。サンドボックスソリューションがオンプレミスや SaaS（Software-as-a-Service：サービスとしてのソフトウェア）として広く導入されていることを考えると、これらの手法の習得が、あらゆる攻撃者に不可欠になっています。

認証情報アクセスの列では、OS 認証情報のダンプと入力キャプチャが上位に入りました[21、22]。Mimikatz のリリース以来、複数の攻撃者が Mimikatz を関連する機能を利用したことが確認されています。さらには、Cobalt Strike、Metasploit、Sliver などのさまざまなポストエクスプロイトフレームワークへの統合（および、PowerShell によるリフレクション型のロードの能力）により、ファイルレス攻撃においても有用なツールとなっています。

探索とラテラルムーブメントのフェーズは相互依存関係にあり、すなわち、資産の探索が増加すれば、侵害した環境でのラテラルムーブメントも増加します。これに対する最も効果的な防御策の 1 つは、ネットワークトラフィックを適切に可視化し、制御することであり、それは、これらのフェーズではさまざまな手法が発生し、適切な制御で検知できるためです。

収集から影響までのいずれのフェーズであっても、ほとんど変わりありません。攻撃者は同じ手法で機密データを収集してまとめ、コマンド & コントロールチャネルとは異なるプロトコルでそれを持ち出します。約 22% の攻撃は、C2 サーバーとの通信に UDP や ICMP などのアプリケーション層以外を使用します。接続の確立と維持が複雑でエラーを訂正する方法がないために、一般的ではない選択ではあるものの、これらのプロトコルは厳しく監視されていないため、この手法が検知されずに利用されている可能性があります。

エンドポイントテレメトリから得られる、手法に関する実用的なインテリジェンス

FortiEDR のデータに注目することで、攻撃やサイバー犯罪者が使用する初期アクセスの手法を別の視点から理解できます。多くの場合、EDR 機能を使用する組織は何らか形のサンドボックスも使用しているため、EDR ツールで阻止される脅威は、恐らくは「従来型の」サンドボックステクノロジーをくぐり抜けた脅威です（深層防御の必要性を示す良い例です）。これらの脅威の動作を理解することで、防御側は、脅威ハンティング活動に役立つ、詳細で絞り込まれたインテリジェンスを利用できるようになります。

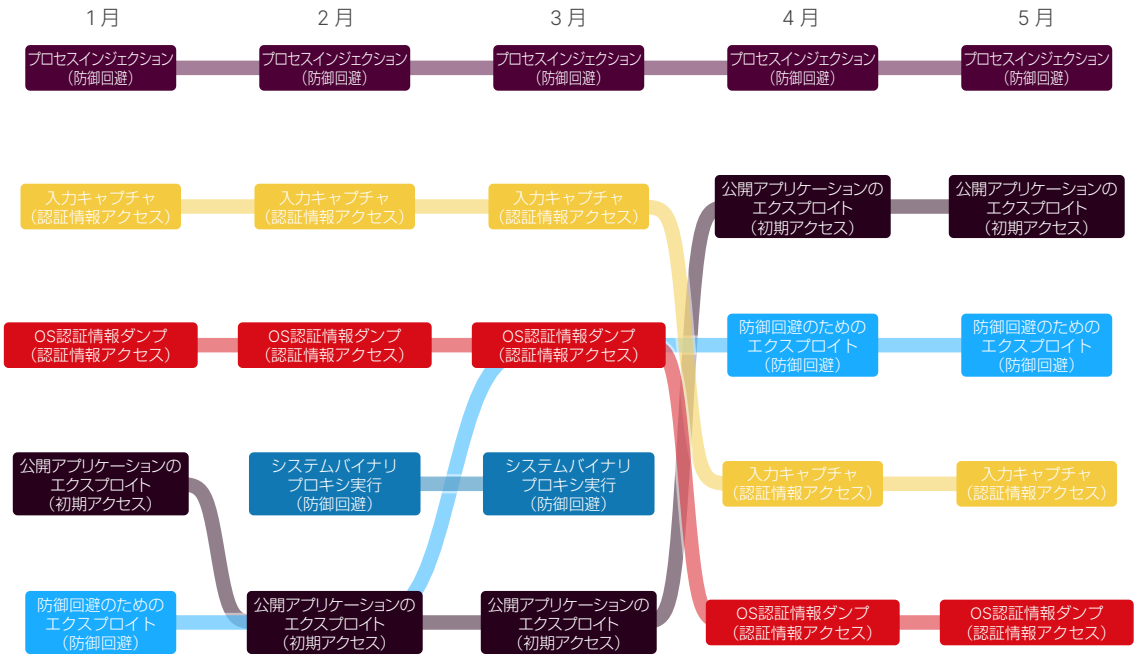


図 7：月別の FortiEDR で検知された上位の ATT&CK 手法

上記は、月ごとの最も活発だった 5 つの手法です。組織のマシンの内部である手法が実行されると、サンドボックステクノロジーが阻止したのと同じ手法が他のイベントでも使用されるようになります。2023 年上半期に確認された最も活発なテクノロジーは以下の通りです。

- プロセスインジェクション
- 入力キャプチャ
- OS 認証情報ダンプ
- 公開アプリケーションのエクスプロイト
- 防御回避のためのエクスプロイト

プロセスインジェクションが、いずれの月も首位になりました[23]。攻撃者は間違いなく、12 の潜在的なタイプがすでに分類されているこの手法を防御回避と権限昇格の両方の目的で使用し、悪用しています。

2 番目と 3 番目に多く使用された手法は、いずれの月も認証情報アクセスと入力キャプチャでした。攻撃者はこれらの手法を使用して、ユーザーの入力を傍受して認証情報を取得しようとしたり、メモリ内の認証情報を探してデータを収集しようとしたりします。通常のシステムとのやり取りでは、ユーザーがさまざまなエンドポイントから認証ポータルやシステムプロンプトウィンドウなどの認証情報を入力します。多くの場合、この入力をキャプチャする目的で採用された、API による認証情報の不正取得などのメカニズムをユーザーが見分けることはできません。

最後に、防御回避と初期アクセスの両方に対するエクスプロイトが最終的に最も使用された手法であり、実際に観察された活動のほぼすべてでこれらの手法が確認されました。攻撃者は、ソフトウェアの脆弱性を競って悪用し、システムで有利な立場を確立することで、さらに有害な行動を実行しようとしています。CVE の数はここ数年で指数関数的に増加し（今年は CVE が 30,000 に達する見込みで、2021 年に報告された 20,000 の 50% 増）、攻撃者が自らの道具箱に追加する脆弱性に事欠くことはありません。LLM（Large Language Model：大規模言語モデル、大規模データセットを高速で処理することで侵入する脅威や既存の脆弱性を迅速に特定する目的で使用される）の登場と相まって、攻撃しやすい標的のエクスプロイトがかつてないほど容易になっており、今後もサイバー攻撃者が真っ先に目をつける武器となることが予想されます。

進化する脅威から保護する

サイバー犯罪者が利益を上げる機会を逃すことは決してなく、最近では、RaaS グループなどの組織化されたサイバー犯罪が急増したことで、これまで以上に手っ取り早く報酬を得られるようになりました。攻撃者は、新しい脆弱性や高度な攻撃手法を常に探して悪用し、ネットワークに侵入します。しかしながら幸いにも、過去数ヵ月間に攻撃者が使用した戦術のほとんどは我々にとって馴染みのあるものであり、これは、防御側が攻撃を事前に阻止する機会がこれまで以上に増えているということを意味します。

ただし、攻撃者は自らの活動を進化させ続けているため、組織内のサイバー防御戦略を評価して強化することで、潜在的な脅威に先行することが極めて重要です。そこで、脅威インテリジェンスの活用と共有から適切なテクノロジーの実装までの、企業のネットワークとデータを保護するために今すぐ実行できるいくつかの手順を紹介します。

脅威インテリジェンスを共有し、活用する

かつてない勢いで高度化し、増大するサイバー脅威に対抗するため、脅威インテリジェンスの共有と活用を実践することが、あらゆる組織の防衛戦略に不可欠な要素になりました。フォーティネットは、脅威インテリジェンスの共有を推進する活動に積極的に参加しています。

フォーティネットは、競合するサイバーセキュリティベンダー間での脅威インテリジェンスの共有を可能にする目的で 2014 年に設立された Cyber Threat Alliance（CTA）の創設メンバーです[24]。CTA は現在、世界規模でのサイバー犯罪との戦いを優位に進める上で不可欠な組織となるまでに成長しました。しかしながら、信頼と機密性の確立、データ標準化の保証、大量の情報の管理など、効果的な情報共有を複雑にしている障害は枚挙に暇がありません。CTA は、これらの課題の解決に積極的に取り組み、世界中のサイバー脅威インテリジェンス（CTI）の精鋭チームの連携によるサイバー脅威に関するグローバルな視点の大幅な強化を成し遂げました。

攻撃フローを理解し、侵害のパターンと指標を特定する

サイバー攻撃が高度化し、頻度も被害も増大しているため、攻撃者についてできるだけ知ることが極めて重要です。最初の侵入口からポストエクスプロイトの活動までの攻撃フローを理解することが、効果的なサイバーセキュリティ戦略の策定に不可欠です。

攻撃フローとは、攻撃者が標的システムに侵入して目的を達成するまでの一連の手順のことで、偵察、初期アクセス、権限昇格、ラテラルムーブメント、データの持ち出し、永続化などのさまざまな段階が含まれます。それぞれのフェーズを理解することで、脆弱性の特定、適切なセキュリティ対策の実装、サイバー脅威への効果的なレスポンスが可能になります。

攻撃フローを理解することは、いくつかの理由から極めて重要です。第一に、攻撃のステップとそれらの関係、さらには結果を視覚的に理解できます。各フェーズでの攻撃者の TTP（Tactics, Techniques and Procedures：戦術、手法、手順）を研究することで、セキュリティチームがパターンや IOC（Indicators of Compromise：侵害指標）を特定できるようになり、進行中の攻撃の特定とタイムリーなアクションの実行が可能になります。

攻撃フローを理解することは、より効果的なリソースの配分にも役立ちます。初期アクセスや権限昇格などの攻撃の最も脆弱なフェーズに注目することで、セキュリティ対策と投資の優先度を判断し、サイバーセキュリティ態勢を最大限まで引き上げることができます。

最後に、攻撃フローを理解することで、インシデントレスポンスの機能を強化できます。攻撃のさまざまな段階と潜在的な活動をマッピングすることで、セキュリティチームがそれぞれの段階に合わせたプレイブックとレスポンス計画を開発でき、サイバー攻撃の進行中の迅速かつ効果的なレスポンスが可能になります。

フォーティネットは、攻撃フローを完全に理解することのメリットを十分に理解し、MITRE Engenuity の CTID（Center for Threat-Informed Defense）ATTACK Flow プロジェクトにリサーチスポンサーとして参加しています [25]。脅威インテリジェンスのこのような進歩によって、プロファイルに基づく攻撃の特定とレスポンスが可能になり、攻撃の経済性を防御側にとって有利な方向に変えることができるはずです。

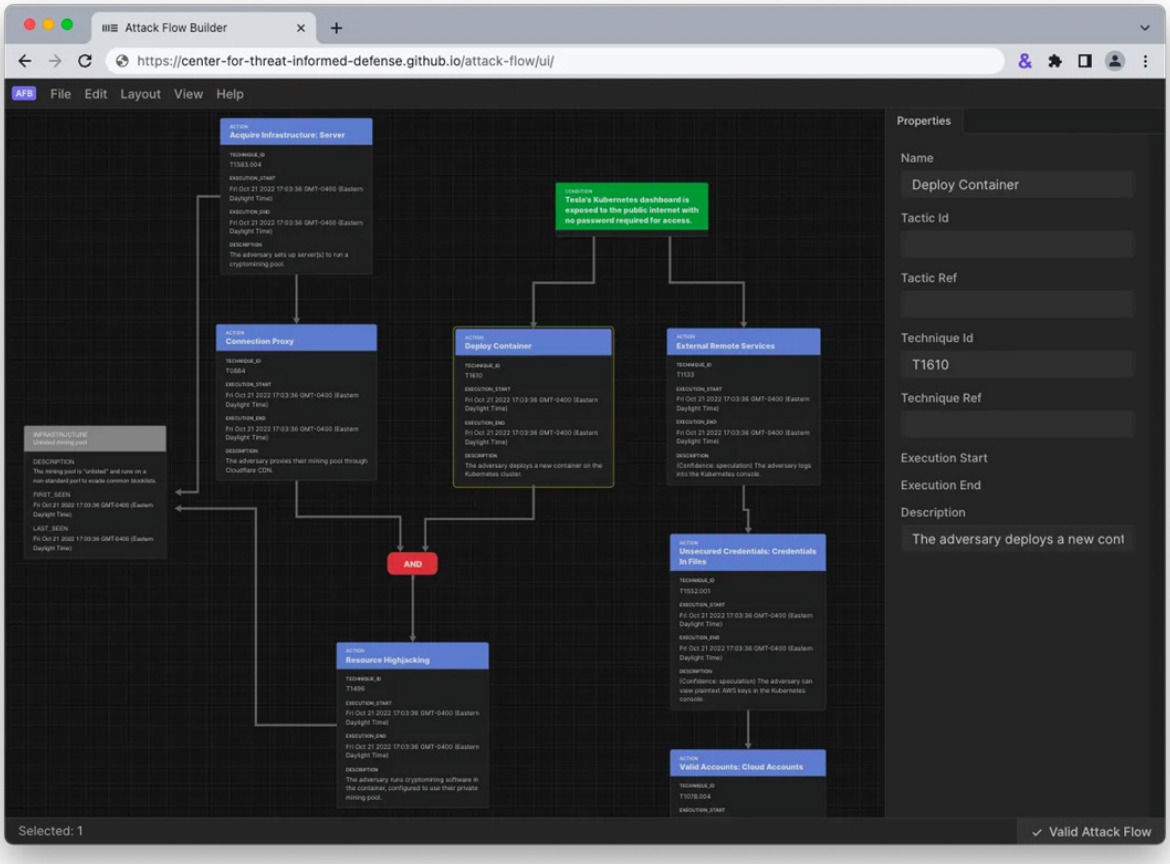


図 8：MITRE ATT&CK Flow Builder - フローの例

フォーティネットは、2 名のリサーチャーが発表した Wintapix ドライバーについての調査を始めとして、フォーティネットのレポートへの標準の採用も開始しています [26]。

テクノロジーとプロセスを強化する

新しいセキュリティテクノロジーの実装や現在のスタックの再評価の好機と言える今、どのようなツールを選択する場合も、AI、ML、DL（深層学習）、高度な分析を活用できることを確認する必要があります。これらの能力を活用することが、組織で生成される膨大な量のデータを処理し、脅威やその他のリスクを示す可能性のある危険なトラフィックや異常なトラフィックを特定するために不可欠になっています。

攻撃者に先行しようとするならば、現在のプロセスを検証し、調整する必要があり、これには、セキュリティチームの役割と責任の再定義、プレイブックの作成や更新、机上演習によるチームの能力に対するプレッシャーテスト、解決する必要があるプロセスギャップの特定などが含まれます。

多くの組織が、自社のセキュリティ担当者を補完する目的で信頼できるベンダーを利用するようになりました。FortiGuard の AI を活用したセキュリティサービスは、NGFW（次世代ファイアウォール）、ネットワークのテレメトリと分析、EDR、XDR（拡張検知とレスポンス）、DRP（デジタルリスク保護）、SIEM（セキュリティ情報 / イベント管理）、インラインサンドボックス、デセプション、SOAR（セキュリティオーケストレーション、自動化、レスポンス）などのさまざまな強力なツールに対応しています。これらのソリューションは、高度な脅威の検知と防御の機能を提供することで、攻撃対象領域全体のセキュリティインシデントの迅速な検知とレスポンスを支援します。

まとめと総論

我々が本レポートを楽しみながら作成したのと同様に、皆様も本レポートを楽しみながらお読みいただけたことを願っています。サイバーセキュリティは時として非常に複雑に見えますが、この分野では常に、高い志と熱意を持つ人たちが、セキュリティ態勢を強化する革新的で合理的なアプローチをコミュニティに提供しようと努力を続けています。サイバー犯罪や国家が支援する脅威との闘いに終わりはありませんが、我々は、セキュリティ業界として万全の体制でそれに立ち向かい、闘い続けます。

サイバー戦争においては、脅威インテリジェンスを共有する官民のパートナーシップの強化が極めて重要です。脅威インテリジェンスは、包括的なプレイブックを通じて直ちに実行できるものでなければなりませんが、共有、ツール、レポートについては、標準化されてなければ役に立たない場合もあるでしょう。脅威インテリジェンスの共有は、摩擦がなく、タイムリーで効果的なレスポンスを可能にする重要な要素であり、今日、攻撃の経済性を変えるために防御者が利用できるさまざまなツール、知識、サポートがあり、いずれも攻撃者に対抗する強力な手段となるはずです。

[1] 「MITRE ATT&CK Matrix for Enterprise」、MITRE、2015 ～ 2023 年（英語）：https://attack.mitre.org/

[2] 「2022 年下半期 フォーティネット グローバル脅威レポート：CISO 向けの重要で実用的なインテリジェンス」、Douglas Jose Pereira dos Santos、フォーティネット、2023 年 3 月 3 日（英語）：https://www.fortinet.com/blog/ciso-collective/threat-report-2h-2022-ciso-insights

[3] 「2023 年ランサムウェアグローバル調査レポート」、フォーティネット、2023 年 3 月：https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ja_jp/report-2023-ransomware-global-research.pdf

[4] 「ワイパー型マルウェアの年」、Geri Revay、フォーティネット、2023 年 1 月 24 日：https://www.fortinet.com/jp/blog/threat-research/the-year-of-the-wiper

[5] 「ワイパーの最新情報」、Derek Manky、フォーティネット、2023 年 3 月 23 日：https://www.fortinet.com/jp/blog/threat-research/intel-on-wiper-malware

[6] 「2022 年下半期 フォーティネット グローバル脅威レポート：CISO 向けの重要で実用的なインテリジェンス」、Douglas Jose Pereira dos Santos、フォーティネット、2023 年 3 月 3 日（英語）：https://www.fortinet.com/blog/ciso-collective/threat-report-2h-2022-ciso-insights

[7] 「Exploit Prediction Scoring System」、FIRST.org、2015 ～ 2023 年（英語）：https://www.first.org/epss/

[8] 「ゼロデイ攻撃に悪用される MOVEit Transfer の重大な脆弱性（CVE-2023-34362）」、James Slaughter、Fred Gutierrez、Shunichi Imano、フォーティネット、2023 年 6 月 8 日：https://www.fortinet.com/jp/blog/threat-research/moveit-transfer-critical-vulnerability-cve-2023-34362-exploited-as-a-0-day

[9] 「Threat Signal Report: MOVEit Transfer Critical Vulnerability (CVE-2023-34362)」、FortiGuard Labs、2023 年 6 月 2 日（英語）：https://www.fortiguard.com/threat-signal-report/5174

[10] 「EPSS API」、FIRST.org、2015 ～ 2023 年（英語）：https://www.first.org/epss/api

[11] 「Replication Through Removable Media」、MITRE ATT&CK、2017 年 5 月 31 日（英語）：https://attack.mitre.org/techniques/T1091/

[12] 「IPS Threat Encyclopedia: Raspberry.Robin.Worm」、FortiGuard Labs、2022 年 7 月 14 日（英語）：https://www.fortiguard.com/encyclopedia/ips/51814

[13] 「Increased Truebot Activity Infects U.S. and Canada-Based Networks」、Cybersecurity and Infrastructure Security Agency、2023 年 7 月 6 日（英語）：https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-187a

[14] 「Exploitation for Client Execution」、MITRE ATT&CK、2018 年 4 月 18 日（英語）：https://attack.mitre.org/techniques/T1203/

[15] Follina についてのフォーティネットのブログ記事、2023 年 7 月 27 日確認（英語）：https://www.fortinet.com/blog/search?q=follina

[16] 「Hijack Execution Flow: DLL Side-Loading」、MITRE ATT&CK、2020 年 3 月 13 日（英語）：https://attack.mitre.org/techniques/T1574/002/

[17] 「改ざんされた 3CX デスクトップアプリ（CVE-2023-29059）」、FortiGuard Labs、フォーティネット、2023 年 3 月 30 日：https://www.fortinet.com/jp/blog/threat-research/3cx-desktop-app-compromised

[18] 「Obfuscated Files or Information」、MITRE ATT&CK、2017 年 5 月 31 日（英語）：https://attack.mitre.org/techniques/T1027/

[19] 「Masquerading」、MITRE ATT&CK、2017 年 5 月 31 日（英語）：https://attack.mitre.org/techniques/T1036/

[20] 「Virtualization/Sandbox Evasion」、MITRE ATT&CK、2019 年 4 月 17 日（英語）：https://attack.mitre.org/techniques/T1497/

[21] 「OS Credential Dumping」、MITRE ATT&CK、2017 年 5 月 31 日（英語）：https://attack.mitre.org/techniques/T1003/

[22] 「Input Capture」、MITRE ATT&CK、2017 年 5 月 31 日（英語）：https://attack.mitre.org/techniques/T1056/

[23] 「Process Injection」、MITRE ATT&CK、2017 年 5 月 31 日（英語）：https://attack.mitre.org/techniques/T1055/

[24] 「Partnering to Disrupt Cybercrime,」、Derek Manky、フォーティネット、2023 年 2 月 14 日（英語）：https://www.fortinet.com/blog/business-and-technology/partnering-to-disrupt-cybercrime

[25] 「MITRE Attack Flow の貴重なコンテキストが CISO のリスク管理を改善」、Douglas Jose Pereira dos Santos、2022 年 11 月 3 日：https://www.fortinet.com/jp/blog/threat-research/mitre-attack-flow-gives-cisos-better-risk-management

[26] 「WINTAPIX：中東諸国を標的にした新型カーネルドライバー」、Geri Revay and Hossein Jazi、フォーティネット、2023 年 5 月 22 日：https://www.fortinet.com/jp/blog/threat-research/wintapix-kernal-driver-middle-east-countries

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

TR-23H1-202309-R1