フォーティネット
グローバル脅威レポート

FortiGuard Labs による 2022 年上半期レポート

目次

概説とハイライト

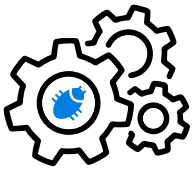
昨今の未曾有の時代は終わることなく、また半年が過ぎました。しかしながら、このような時代であっても、我々が目にするエクスプロイト、攻撃対象、攻撃の種類が変わるわけではありません。次々と登場する脅威からの保護に役立てていただくため、本レポートでは、FortiGuard Labs が監視する世界中に存在するセンサーを活用して、2022 年上半期のサイバー脅威環境を振り返ります。以下にその概要を紹介します。

ランサムウェアの検知数

フォーティネットのプラットフォームではこの半年間に 10,666 件のランサムウェア亜種が検知されましたが、その前の半年間はわずか 5,400 件でした。これは、半年間でランサムウェア亜種が**ほぼ倍増**したことを意味します。

ワイパー型マルウェアの増加

2022 年上半期は、ロシアとウクライナの戦争が続く中で、ワイパー型マルウェア（データ削除を目的とするマルウェア）が急増しました。しかしながら、これらのワイパー型マルウェアは特定の場所だけでなく世界中に拡散し、サイバー犯罪に国境がないことを証明しています。

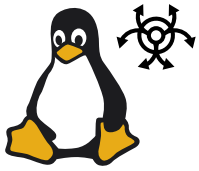


OT の脆弱性

エアギャップで隔離された環境から相互接続された世界へと移行した今日、OT（オペレーショナルテクノロジー）製品がこれまで以上に標的にされ、リスクが上昇することになりました。どの OT ベンダーで最も多くの脆弱性が見つかったのでしょうか。

Log4j の長引く影響

Apache サーバーに存在するこの脆弱性は、2021 年暮れに見つかり、これを標的にするエクスプロイトは当初の予想ほどではないようにも思えますが、大きな脅威でなくなったわけではありません。APT41 などのサイバースパイ集団が 2022 年上半期にこの脆弱性を悪用して米国政府のシステムにアクセスしたことは、「終息」とはほど遠いことを示しています。一般的な傾向として、このようなユビキタス性の高い脆弱性は、公開された概念実証エクスプロイトで簡単に悪用できるため、長年にわたって継続しています。



拡散方法の主流である HTML、JavaScript、Linux

HTML と JavaScript が 2022 年上半期に他を引き離しましたが、Link ファイルも上位に入りました。最近の Linux ベースのマルウェア攻撃の多くは、暗号化に関連するものですが、攻撃者は、ステージング、自動認証攻撃、特定された脆弱性を悪用した後の永続化などにも Linux を利用しています。

2022 年上半期に上位を占めた脅威

本レポートで紹介する調査結果は、世界中の本番環境で毎日観測される数千億件の脅威イベントを収集しているさまざまなセンサーから取得された、FortiGuard Labs の脅威インテリジェンスに基づくものです。第三者機関の調査によれば、フォーティネットはセキュリティデバイスの出荷数では業界最多の実績を有しています。最初に、2022 年上半期に首位に躍り出た（あるいは急上昇した）脅威を検証します。

ゼロデイの隆盛

2022 年も過去最高を記録しそうな勢いでゼロデイ脆弱性が見つかっています。2022 年 1 ～ 6 月に、重要インフラストラクチャの分野にソフトウェアを提供しているベンダーを含む多数のベンダー製品に、72 件のゼロデイが見つかりました。2020 年初めから 2022 年 6 月まで、フォーティネットが半年ごとに発表してきたゼロデイの平均数は一貫して増加し続けており、ゼロデイ活動を追跡している他の企業も同様のトレンドを報告しています。Google の Project Zero が報告するゼロデイの件数も、前年比で着実に増加しています。

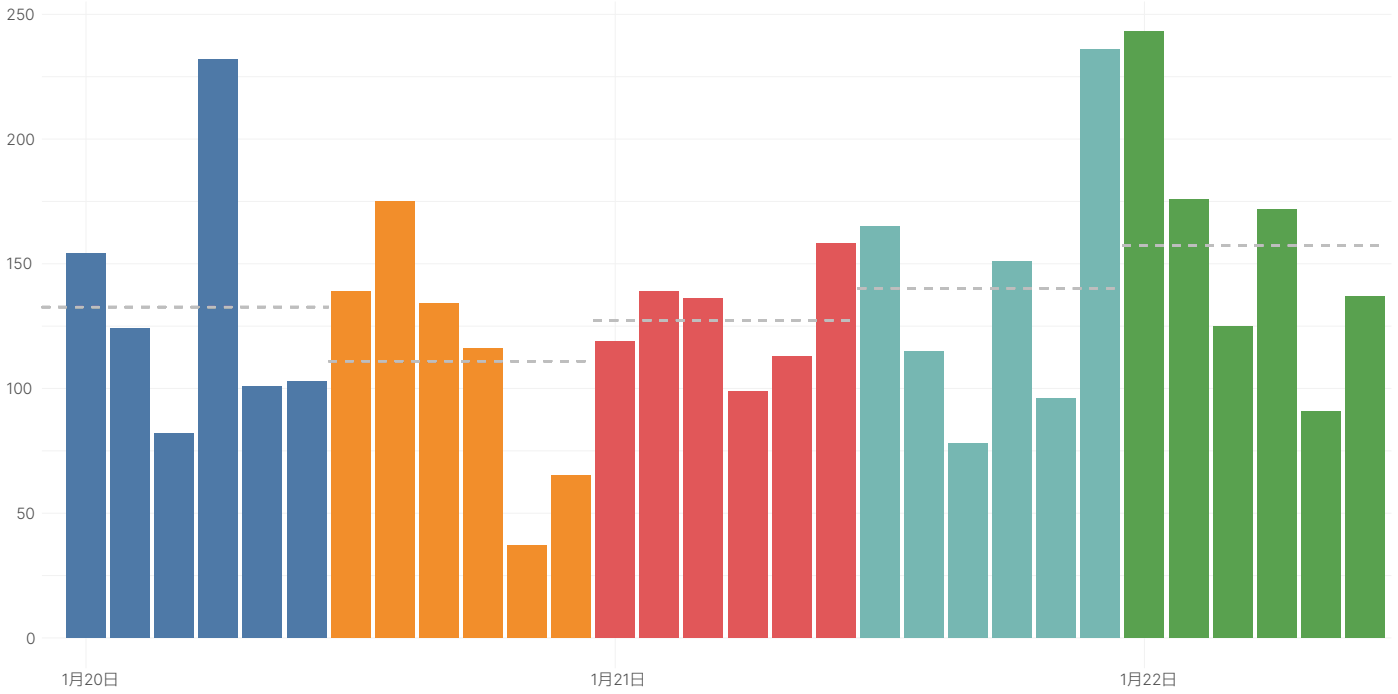


図 1：Google の Project Zero が公開した月別のゼロデイ件数

セキュリティ研究者が検知する能力が向上したこと、また、攻撃者が検知されていない脆弱性を見つけようとしていることが、この増加の原因であると考えるセキュリティ研究者もいます。Google が 2021 年に特定したゼロデイの多くは、過去の脆弱性と類似しており、一般的でよく知られた脆弱性クラスに分類されるものでした。3 分の 2 以上の脆弱性がメモリの破壊に関連しており、残りは主にロジックや設計の脆弱性に起因するものでした。

しかしながら、ゼロデイの定義が「パッチの提供前に攻撃者がすでに悪用した、あるいは少なくとも知っている脆弱性」ということを考えれば、これは組織にとって厄介なトレンドです。特に広く利用されている製品のゼロデイ脆弱性は、攻撃者に企業ネットワークを侵害する手段を与えるだけでなく、脆弱性が見つかるまで数ヵ月も隠れたままである場合もあります。

2022 年上半期も、このような脆弱性がいくつか見つかりました。その 1 つである、Microsoft のサポート診断ツールに見つかったリモートコード実行の脆弱性である MSDT Follina（CVE-2022-30190）を悪用すると、攻撃者が Office 文書経由でシステムを簡単に侵害することができます。セキュリティ研究者の報告によると、国家が支援する集団を含む複数の犯罪者が、データ窃盗攻撃でこの脆弱性を悪用し、Qakbot などのランサムウェアを標的のネットワークにドロップしました。

Microsoft Windows の CLFS（共通ログファイルシステム）ドライバーの CVE-2022-24521 も、2022 年上半期の重大な重大なゼロデイ脆弱性です。Microsoft は 4 月に、米国国家安全保障局（NSA）の研究者から報告された脆弱性の修正を公開しました。2022 年上半期に注目されたもう 1 つのゼロデイである CVE-2022-26134 は、Atlassian の Confluence Server と Data Center テクノロジーに存在する、認証されていない第三者によるコード実行の脆弱性です。攻撃者はこの脆弱性を悪用して、Web シェル、ランサムウェア、クリプトマイナーを脆弱なシステムにドロップしました。また、Microsoft の LSA（ローカルセキュリティ機関）機能のスプーフィング脆弱性である CVE-2022-26925 を悪用すると、ドメインコントローラに自らを強制的に認証させることができます。

2022 年上半期に見つかった 72 件のゼロデイのうち 24 件は、Siemens の PADS Standard/Plus ビューア設計フローテクノロジーのメモリ破損の脆弱性で、そのうち 5 件は深刻度が「Critical（緊急）」、4 件は「Important（重要）」です。FortiGuard ゼロデイプログラムが重要なのは、犯罪者が何らかの損害を与える前にゼロデイを見つけようとするからです。

ネットワークに対するゼロデイ脆弱性攻撃を防止するためにできることはほとんどありません。適切な可視化、デバイスのインストルメンテーション、ゼロトラストアクセス、インシデントへの迅速なレスポンスに重点的に取り組む必要があります。ゼロデイ攻撃の対策の 1 つとして、デバイスにエクスプロイト対策テクノロジーを導入する方法がありますが、FortiClient を利用することでこれを実装できます。

エクスプロイト（IPS）

米国の CISA（Cybersecurity and Infrastructure Security Agency）の KEV（既知の悪用された脆弱性）リソースは、脆弱性の悪用リスクを知る重要な手掛かりとなるものですが、重要システムへの初期アクセスの手段として悪用されることが多いことから、脆弱性を認識するだけでなく、脆弱性を減災する計画を策定し、実行することの重要性を強調するものでもあります。エクスプロイトは、犯罪者が何を探り、何に注目しているのかを教えてくれます。したがって、常に現状を理解して二次ダウンロードやラテラルムーブメントを防止し、きめ細かいセグメンテーションを実装することが非常に重要です。

FortiGuard IPS（侵入防御システム）センサーが捕捉した IPS トリガーに注目してエクスプロイト活動を見つけることで、犯罪者がどのように脆弱性を見つけ、標的を攻撃し、不正インフラストラクチャを構築するかについての比類ない可視性が提供されます。業界で広く利用されている MITRE ATT&CK フレームワークに置き換えると、これらの検知は、偵察、リソース開発、初期アクセスの手法に相当します。フォーティネットが第 1 四半期に発表した FortiRecon を利用することで、CISO が組織の外部からの視点で自社の脆弱性やブランドの評判を理解し、問題を警告できるようになります。

2022 年上半期の 20 位までのエクスプロイトを以下に紹介します。

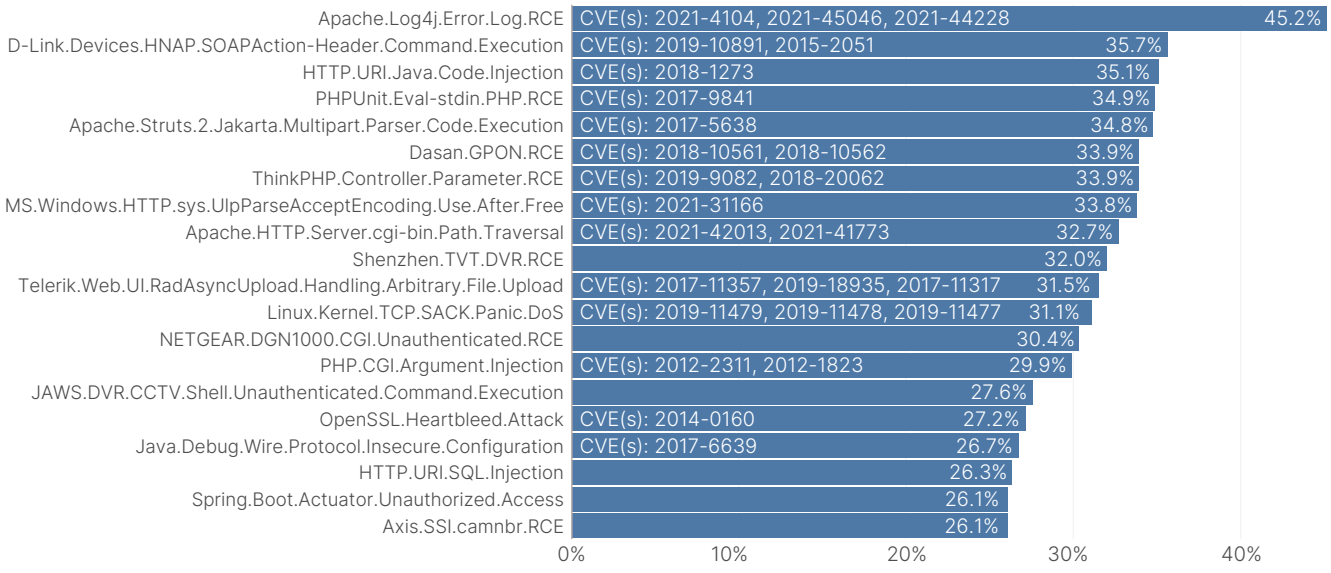


図 2：2022 年上半期の上位の IPS 検知

Log4j については聞き飽きたかもしれませんが、警戒を緩めるべきではないでしょう。米国国土安全保障省の Cyber Safety Review Board は、2021 年の Log4j の最初のイベントについてのレビューで「Log4j のイベントは終息していない」と述べています。Log4j は、システムの奥深い場所に今も存在し、フォーティネットの短期間のレビュー対象期間だけでも、新たな侵害、新たな脅威アクター、新たな事実が確認されました。2022 年の Apache Log4j の脆弱性を標的にしたエクスプロイト活動の多くが VMWare Horizon システムに関連するものであったことから、US-CERT が警告を発表することになりました。

エクスプロイトの件数は当初の予想より少なかったものの、この脆弱性を悪用したいくつもの攻撃が今年の上半期に確認されています。2022 年 3 月には、USAHerds（米国の動物の健康情報管理システム）の脆弱性を悪用した APT41 によるサイバースパイ攻撃で、米国政府の複数のシステムへのアクセスが可能になりました。USAHerds は、米国の畜産農家が家畜の病気の追跡に利用するツールです。医療は Log4j 脆弱性の影響がいかに長期的なものであるかを示すもう 1 つの業種であり、今後も変わることはないでしょう。この脆弱性は多くの基幹システムで見つかっているため、他の部分を中断することなくシステムをアップデートするのは極めて困難です。サイバー犯罪者は、手に入れたいデータや達成したい行動への足掛かりになるものであれば、何でも利用します。Log4j は今後も長期にわたり、本レポートの「上位」のチャートに登場することになるでしょう。これは、脆弱性の評価に加えてアクティブとバーチャルのパッチ適用が極めて重要であることを示す好例です。

エンドポイントの脆弱性

このセクションでは、エンドポイントでの活動を理解し、特定のデバイスに関するより多くの情報、可視性、制御につながる実用的インテリジェンスを提示します。

エンドポイントとは、何を指す言葉なのでしょうか？ ネットワークに接続されたデバイスやアプリケーションはすべて、エンドポイントと見なされます。フォーティネットのエンドポイントデータでは、主にワークステーションについて報告されます。そこで、エンドポイントの脆弱性とその保護についてのトレンドに注目すると、あるネットワークに存在し、動作しているアプリケーション、プログラム、デバイスがかなり複雑に絡み合っていることがわかります。

エンドポイントで最も標的になった脆弱性のベンダーを調べる前に、このサンプルでは、FIRST の ESPP（Exploit Prediction Scoring System）が公表している 18 万件強の CVE のうち、約 1 万 5,300 件の CVE が検知されている点に注目する必要があるでしょう。フォーティネットは、「ソフトウェアの脆弱性が実際に悪用される可能性を推定する、データドリブンの取り組み」である FIRST EPSS に積極的に参加しています。

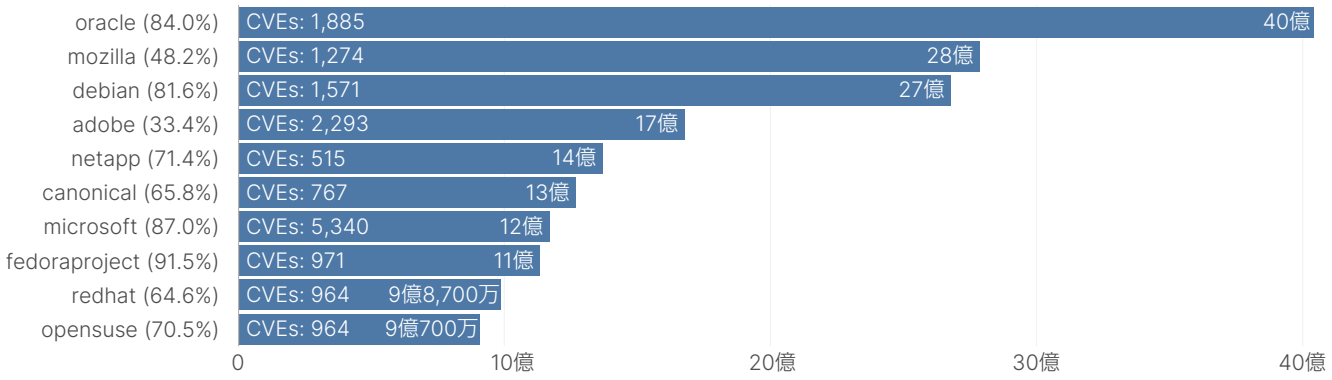


図 3：2022 年上半期のベンダー別のエンドポイント脆弱性件数

前述したように、このように目に見えるものはすべての活動の一部に過ぎません。エンドポイントの脆弱性の検知数が上位 3 つのプラットフォームは、Oracle（その多くは JRE と JDK に関連するもので、MySQL も若干あり）、Mozilla、Debian です。ベンダーごとのデバイスでの検知率についても、括弧内に記載しました。これらのベンダーの多くに存在するエンドポイントの脆弱性により、主として不正ユーザーによるシステムへのアクセスが可能になります。

新しい IPS データを目にしたときに誰もが最初に「これは大きな問題なのか」と疑問を感じ、新しい脆弱性情報を見るたびに、同じ質問を繰り返すことになります。そして、犯罪者が脆弱なシステムへの侵入に成功したときに、この疑問の答えを知ることになります。

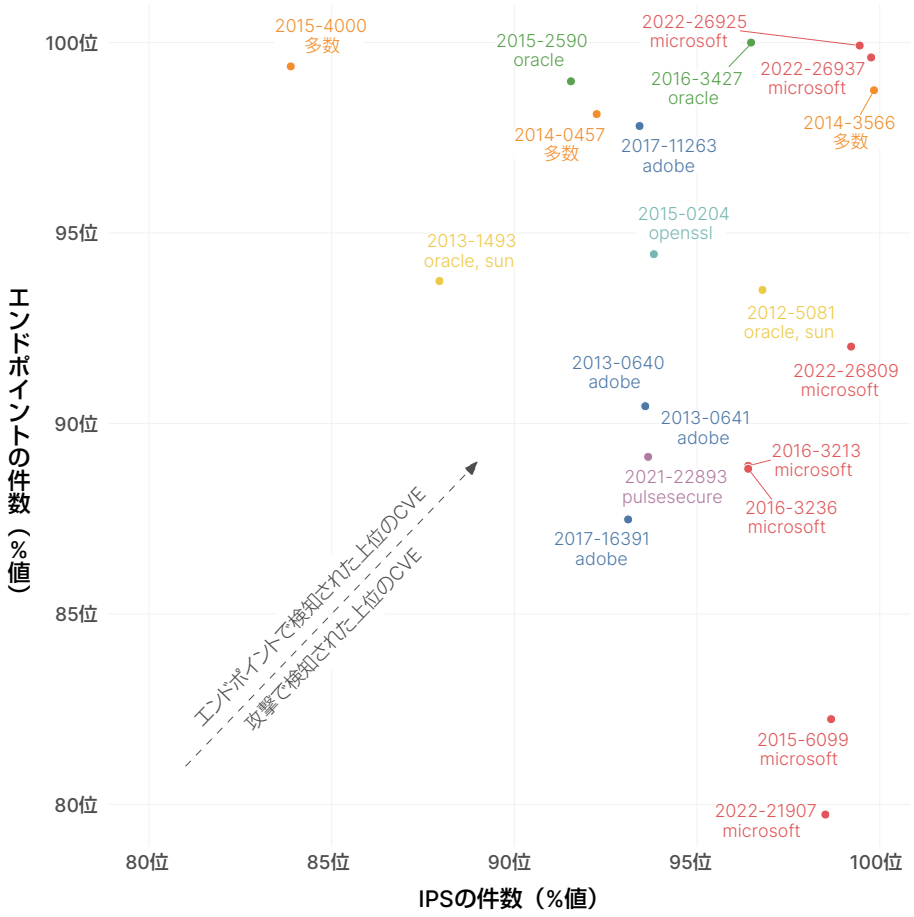


図 4：IPS 活動とエンドポイント検知による CVE の比較

ここで、エンドポイントと脆弱性についての論点を明確にしておきましょう。すべてのエクスプロイトが脆弱性に関連するわけではなく（CVE が割り当てられていないことを意味します）、すべての脆弱性に PoC エクスプロイトが公開されているわけでもありません。脆弱性 ID は、測定した件数をまとめる方法です。ただし、これはそれほど単純な話ではありません。1 つの脆弱性 ID を複数の CVE にマッピングできる場合もあり、これは、複数のソリューションに関連する脆弱性の異なる実装を捕捉するための包括的な語として脆弱性 ID が作成されるためです。しかしながら、以下のグラフで IPS の上位に入っているものであれば、高い確率で IPS の上位にあるものと何らかの関連性があるはずです。これが重要である理由を探ってみることにしましょう。

上図で、エンドポイントと IPS の両方のデータが示され、CVE が両方のデータセットにマッピングされているのがわかります。これは何を意味するのでしょうか。多くのエンドポイントにこれらの脆弱性が存在し、多くの攻撃者が悪用しようとしていることから、今後数ヵ月間に検知されることになる攻撃の概要を知ることができます。

右上にある、スプーフィング脆弱性である CVE 2022-26925 は、X 軸と Y 軸のどちらも他の CVE より上にあり、その近くにリモートコード実行の脆弱性である CVE 2022-26937 が見つかります。CVE 2014-3566 は、「POOD」と呼ばれる SSLv3 の有名な脆弱性です。犯罪者の次の手口を確実に予測するのは不可能ですが（水晶玉があれば別ですが）、犯罪者の目がどこを向いているのかを知る手掛かりにはなるはずです。エンドポイントテクノロジーは、攻撃の初期段階で感染したエンドポイントの減災と効果的な修復に役立ちます。エンドポイントの脆弱性は、多くの利益を手に入れる場所に移動するために、組織のインフラストラクチャへの早期アクセスを手に入れる手段として悪用されます。だからこそ、エンドポイント、ネットワーク、クラウドの脅威インテリジェンスを連携させた多段階型の攻撃の防止とレスポンスが極めて有効であり、ファブリックメッシュのアーキテクチャ設計が重要になります。

OT の脆弱性

OT（オペレーショナルテクノロジー）製品は、多額の金銭や政治的な利益を得ようとする多くの攻撃で標的にされています。フォーティネットは 2022 年 5 月に、Siemens の製品に 24 件のゼロデイを発見し、報告しました。これらのゼロデイが、OT: ICEFALL が今年初めに発表した、OT デバイスに影響する 10 の異なるベンダーにおける 56 件の脆弱性に加わることになります。

多くの OT デバイス（物理デバイスの監視と制御を支援するハードウェアとソフトウェア）は、設計にあたってセキュリティが考慮されているとは言えません。すなわち、ほとんどの OT デバイスは、信頼されているアクセスがデフォルトで有効になっている、（エアギャップが存在する）セキュアネットワークまたはプライベートネットワークで動作することを前提に設計されています。設計者は、システムを効率的に動作させたいと考えるため、新しいハードウェアやソフトウェアのリリースにあたって多くの場合にこの前提を採用します。ところが、設計プロセスは多くの場合に機能指向で、セキュリティが欠如しています。このような設計によって発生する脆弱性が悪用され、実際に攻撃された例があまりに多く、どのネットワークも安全だと断言することはできません。したがって、特に脆弱性やゼロデイに注目する場合には、常に OT を考慮することが極めて重要です。

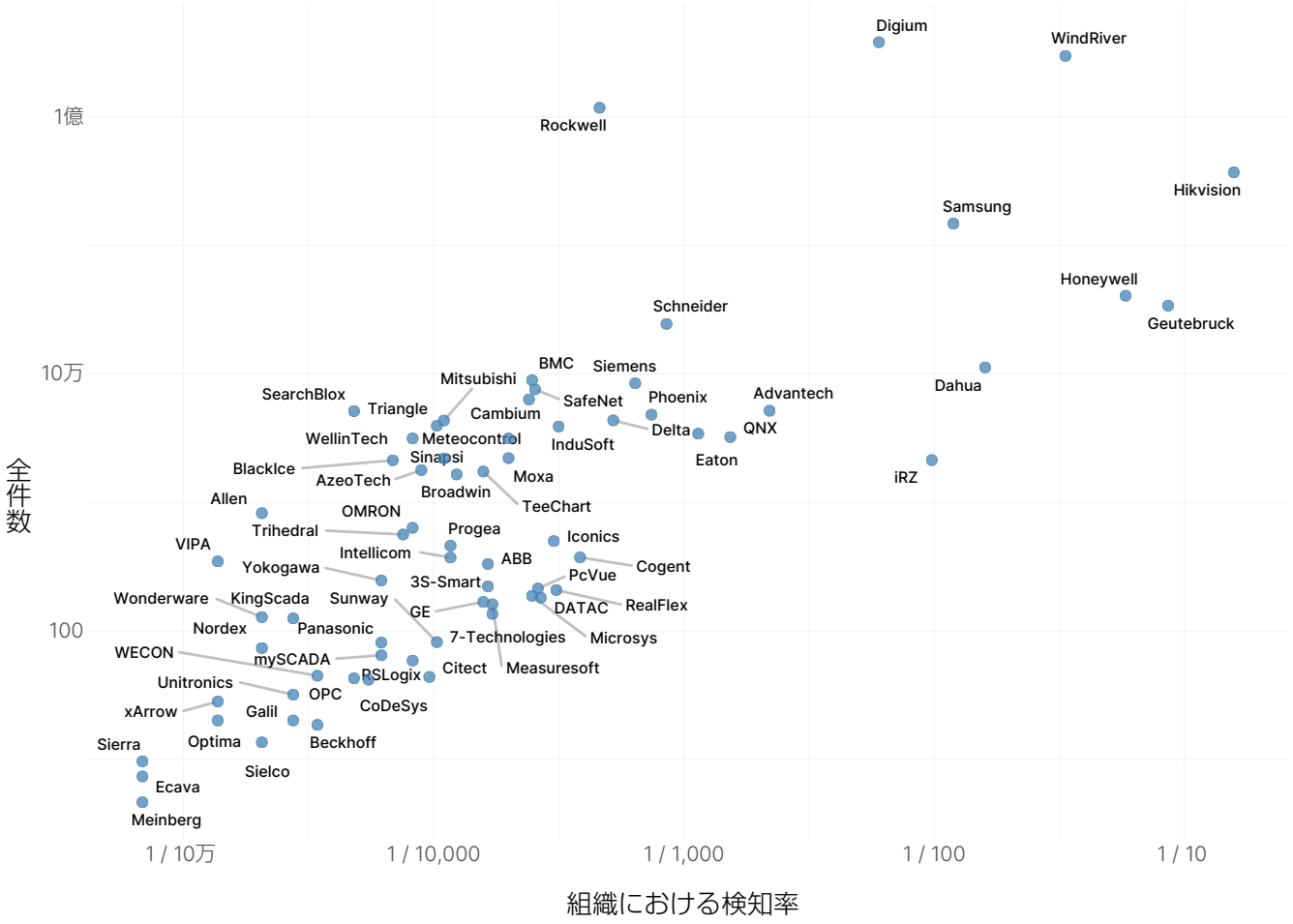


図 5：2022 年上半期の OT を標的にしたエクスプロイトの拡散と件数

上図を見ると、OT デバイスで見つかった脆弱性が数多く攻撃されていることがわかります。多くのベンダー名が接近していますが、Hikvision や Geutebruck のように離れた場所にあるものもあります。この図からご自分の組織で使用している OT を見つけることで、OT 固有のプロトコルや脆弱性とパッチの適用の両方の観点からセキュリティを強化する必要な領域を知ることができます。

マルウェア配信のメカニズム

悪用できる脆弱性を見つけた犯罪者は、次のステップとして多くの場合にマルウェアを送り込み、あらゆる標的に辿り着こうとします。マルウェアのシステムへの配信方法やベクトルはいくつもあって、その多くは検知されず、基本的には使用するプラットフォームに合わせてハッカーが選択します。そこで、過去半年間に最も多く観察されたマルウェア配信のメカニズムに注目することにします。

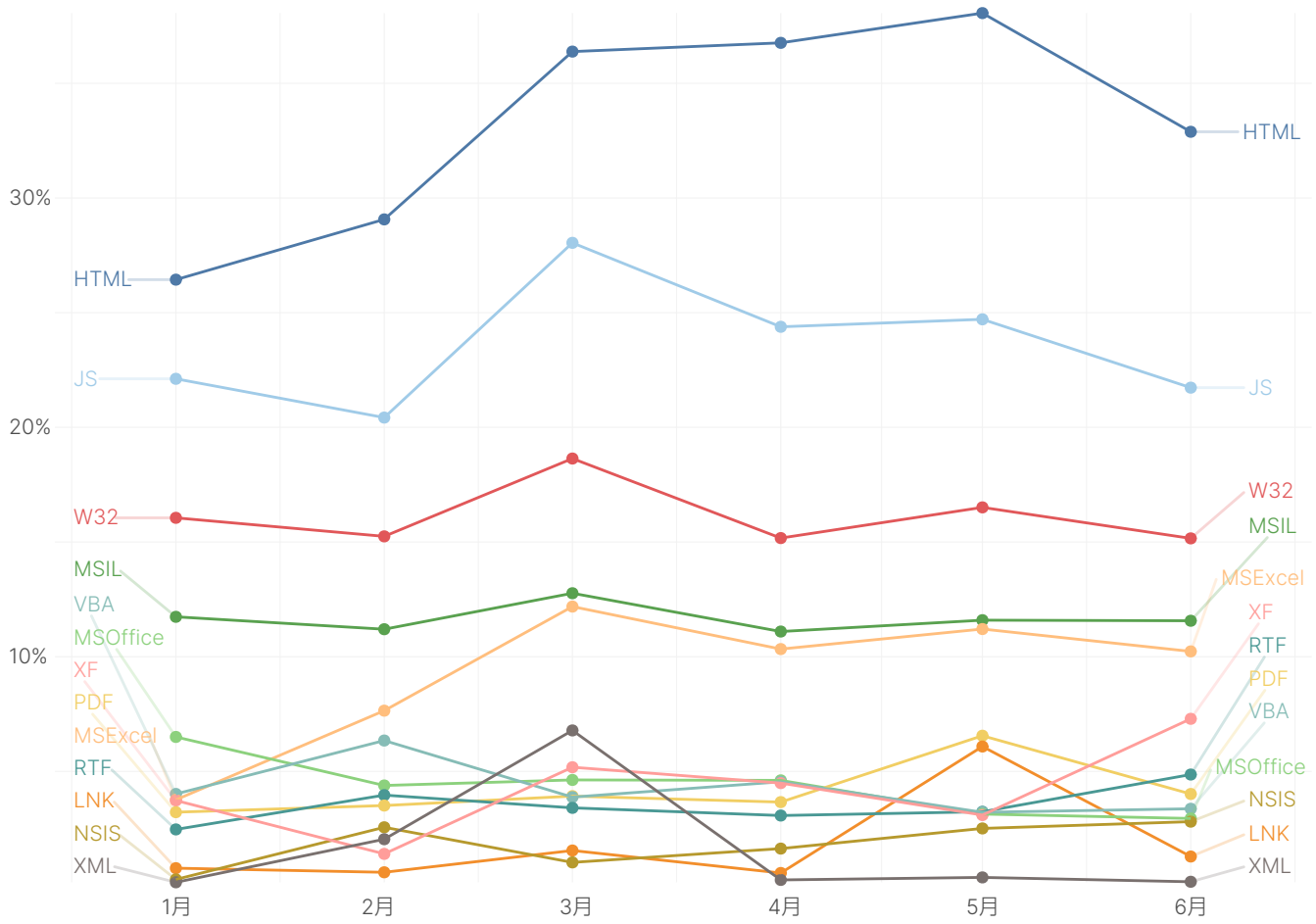


図 6：2022 年上半期のマルウェア配信のメカニズムの月別検知

HTML はマルウェア配信の最も一般的な方法であり、JS と 10% 近い差があります。これは、特段の驚きではありません。ただし、XML は例外で、3 月に若干増加したものの、4 月に大幅に減少しています。マルウェア開発者は通常、1 つのマルウェア配信プラットフォームを専門に使用するため、これは想定内のことです。

それでは、どのようなプラットフォームがマルウェア配信に利用されているかを理解できたところで、それぞれのプラットフォームで上位の亜種に注目してみましょう。

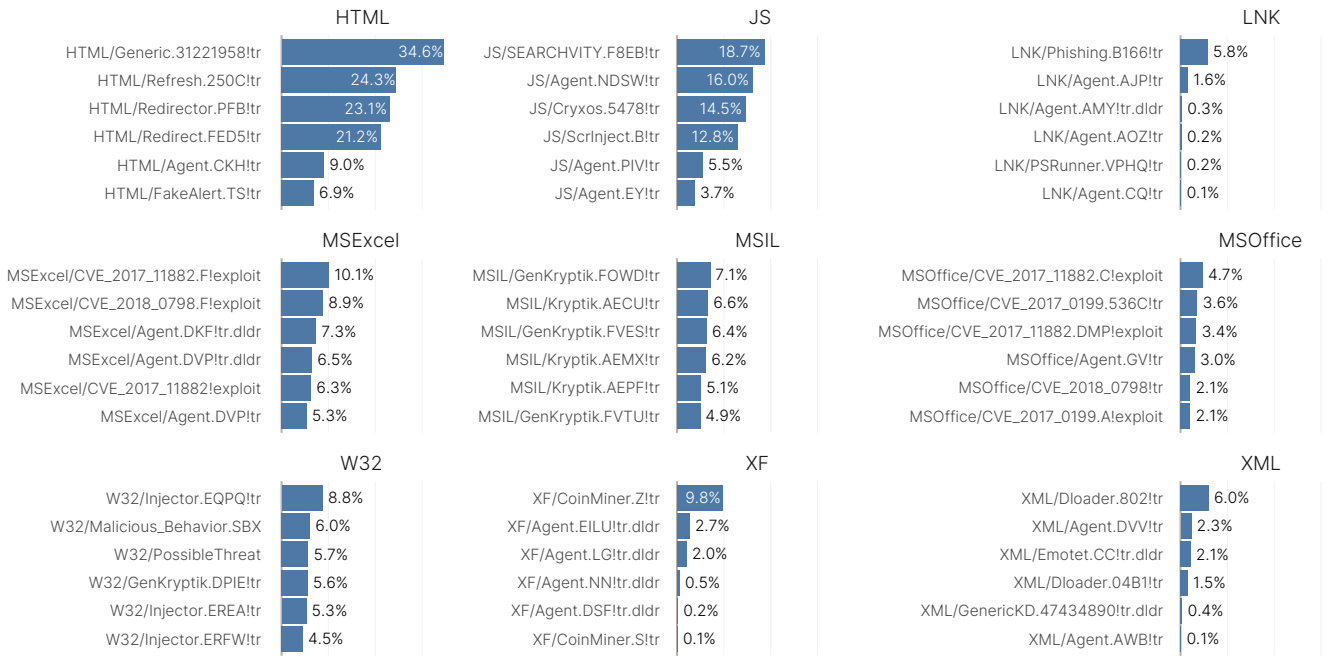


図 7：2022 年上半期の主要プラットフォーム別の上位のマルウェア亜種

HTML と JS が他を引き離していますが、LNK も上位に入りました。拡張子が LNK のマルウェアを展開する不正フレームワークが登場し、このタイプの攻撃を簡単に実行できるようになりました。LNK は、参照先である他のアプリケーション、フォルダー、またはファイルを開く、シェル項目です。eXcelForumla（XF）は、Excel スプレッドシートの感染によって動作する、Excel 数式ウイルスです。この例では、FortiGuard Labs が CoinMiner を「ユーザーに知られることなく活動を実行する」トロイの木馬として特定しました。具体的には、リモートアクセス接続の確立、キーボード入力のキャプチャ、システム情報の収集、ファイルのダウンロードやアップロード、感染したシステムへの他のマルウェアのドロップ、DoS（サービス拒否）攻撃の実行、プロセスの実行と終了などの活動を一般的に実行します。

このデータに登場しないプラットフォームの 1 つが Linux です。件数が多くなければ影響がないことを意味するわけではなく、最近の Linux ベースのマルウェア攻撃のほとんどは、クリプトマイニングに関連するものです。さらには、このタイプの送付のメカニズムを利用する攻撃者は、攻撃のステージング、認証攻撃の自動化、特定した脆弱性のエクスプロイトの後の攻撃の持続などにこのメカニズムを利用することが多いようです。そこで、Linux プラットフォームで最も多く検知された脅威について見てみましょう。

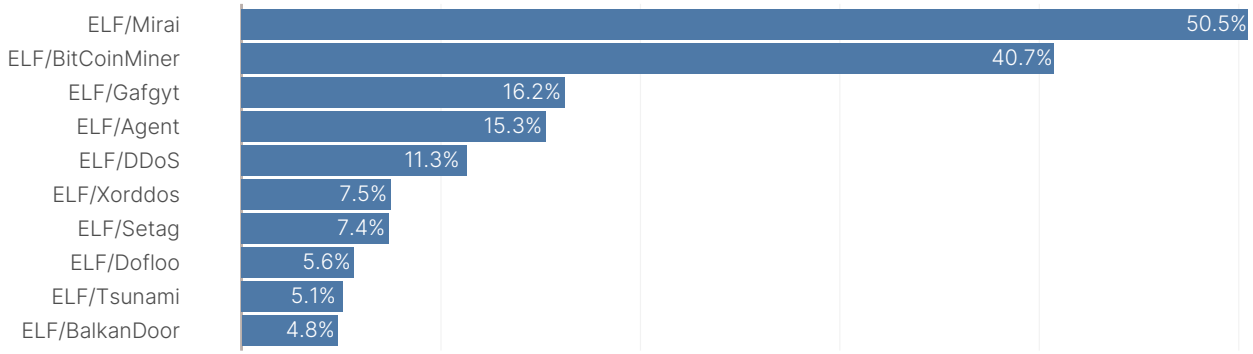


図 8：2022 年上半期に最も多く検知された ELF マルウェア

Linux の活動の全体的な件数と Linux ベースのマルウェア攻撃についてわかっていることを比べてみれば、Mirai が首位であることに驚きはありません。このボットネットは、初めて登場したのが 2016 年であったにもかかわらず、6 年後の今も多く利用され、悪用され、更新され続けています。最近のトレンドを反映するように、BitCoinMiner が次に検知数の多い ELF となり、エージェント、DDoS、Tsunami などの比較的件数が少ない脅威がこれに続きます。ただし、件数が少なければ必ずしも影響が少ないことを意味するわけではありません。そこで、他の ELF の検知数にも注目し、Linux のエクスプロイトについてのこれ以外の情報も探ってみることにしましょう。

ELF 検知数では Miner のサンプルが圧倒的に多数であることがわかりますが、AvosLocker、Hive、Vigorf などのランサムウェアサンプルも Linux を利用しています。AvosLocker は、ダークウェブで RaaS（Ransomeware-as-a-Service：サービスとしてのランサムウェア）として販売され、広く拡散しているランサムウェアプログラムです。AvosLocker は 2021 年 7 月に初めて特定されましたが、犯罪者がマルウェアを操作して標的を決定できるため、企業や組織がこれに対処するのは困難です。2022 年 3 月には同じくランサムウェア亜種である Vigorf が急増し、6 月には Stealthworker の件数が Hive（ランサムウェア）と Miner マルウェアの両方を上回り、2019 年に見つかった、総当たり攻撃を仕掛ける Golang ベースのマルウェアも、非常に少数ではあるものの引き続き検知されています。

戦術と手法：TTP

いずれかのシステムがマルウェアに感染した場合に、SOC チームがほぼリアルタイムで検知し、対応することができれば、感染したシステムを隔離することができます。そのためには、一般的には不正である機能を認識する必要がありますが、AvosLocker は、検知の回避能力が極めて高い「セーフモード」で動作することがわかっているため、認識するのが困難な可能性があります。

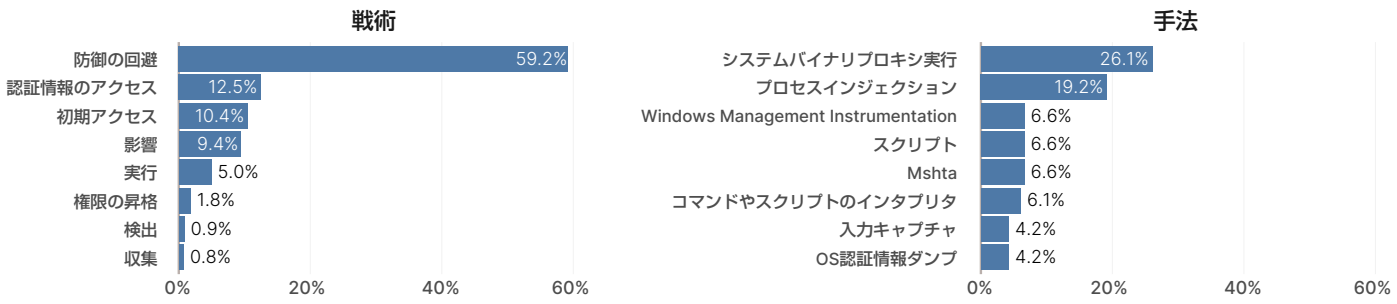


図 9：2022 上半期の EDR データで上位のマルウェアの戦術と手法

過去半年間の EDR テレメトリで 8 位までの戦術と手法に注目すると、マルウェア開発者が最も多く採用した戦術が防御の回避であることがわかります。また、システムバイナリプロキシ実行を使用して防御を回避する可能性が最も高いこともわかります。悪意の隠蔽はマルウェア開発者の必修科目の 1 つであるため、防御を回避するためのコマンドを隠蔽する目的で正規の証明書を使用し、マルウェアではないように見せかけるのは理にかなったことです。プロセスインジェクションは、防御を回避するためにプロセスにコードを挿入するもので、過去半年間で 2 番目に多く確認された手法です。

フォーティネットのさまざまなソリューションから送信されるデータも含む、FortiSandbox Cloud で活性化したマルウェアサンプルに注目することで、それぞれの手法の地域差も知ることができます。

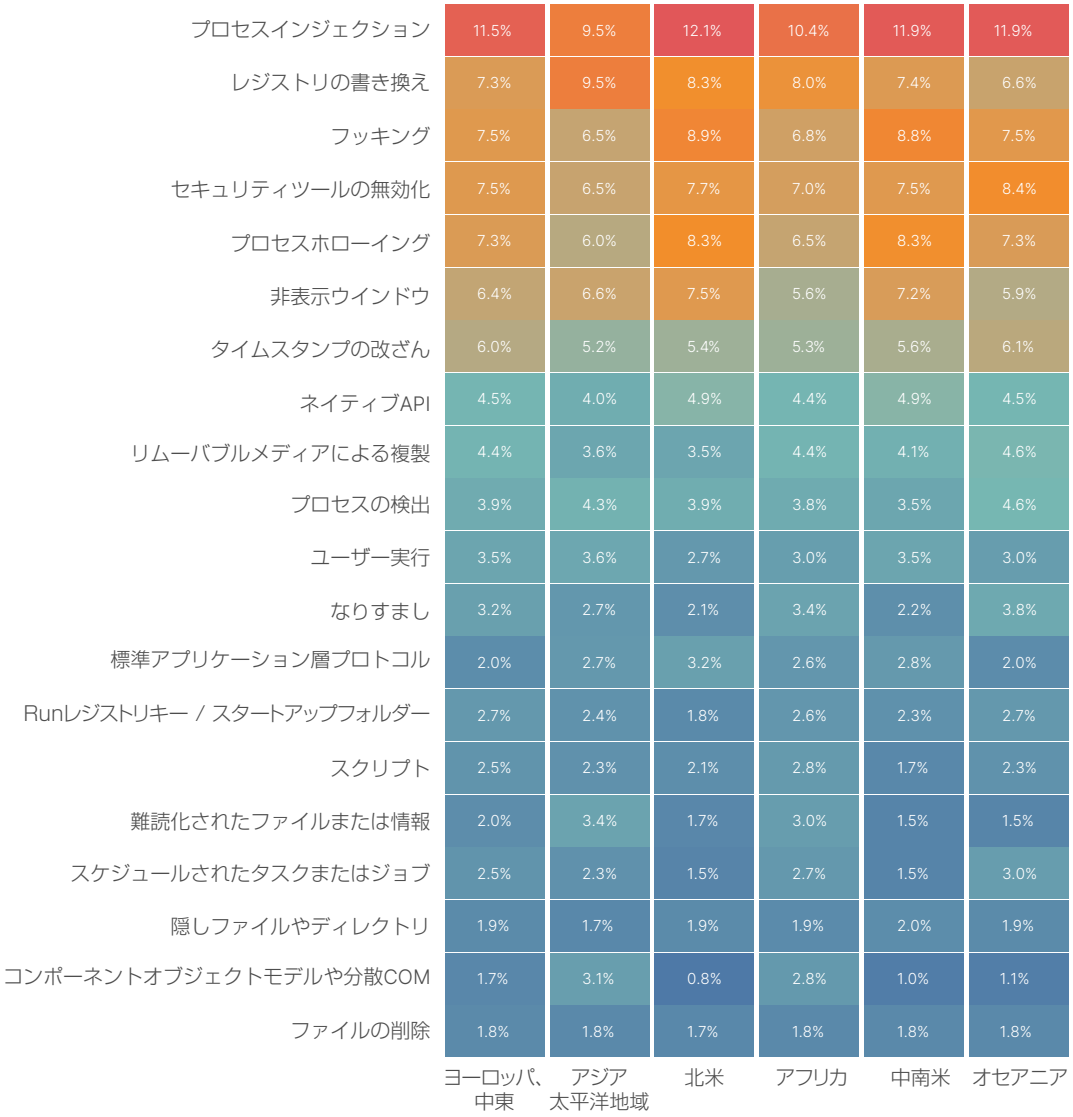


図 10：2022 年上半期の FortiSandbox Cloud データでの地域別の手法の検知

プロセスインジェクションによる防御の回避は、どの地域においても 1 度は最も多く検知された手法になったことがあります。このヒートマップに注目すると、ご自分の地域にとって最も影響が大きいものが何かを確認できます。

脅威、戦術、手法、さらには新たに見つかる脆弱性に対処することは、大海に乗り出すようなもので、海底に届くことも、次の船といつすれ違うかもわからないように感じるかもしれません。しかし、周囲の環境を知っておくことで、次の嵐の到来への備えを強固なものにすることができます。

ランサムウェアについてのまとめ

ランサムウェアが拡散しているという実感はありますが、それを数値化するのが困難な場合もあります。話題に上る機会が増えただけなのでしょうか、あるいは、本当に件数が増えたのでしょうか。

もちろん、後者が正解です。

フォーティネットのプラットフォームでこの半年間に 10,666 件のランサムウェア亜種が記録されましたが、その前の半年間はわずか 5,400 件でした。亜種が半年でほぼ**倍増**したことになります。

その理由は何でしょうか。

その大きな要因の 1 つが、RaaS（Ransomware-as-a-Service）です。RaaS のダークウェブでの売買が増加しており、プラグアンドプレイで利用できるランサムウェアのサブスクリプションモデルサービスがさまざまなテクノロジーを利用して構築されています。このため、サイバー犯罪の初心者でも、個人あるいは企業や組織を攻撃して手っ取り早く金銭を手に入れることができます。番組をストリーミングしたり、食べ物を注文したり、お気に入りの場所に行ったりするのと同じように、RaaS をサブスクリプションすることで、犯罪者が手軽にランサムウェアやその他の不正ソフトウェアを入手するようになっています。

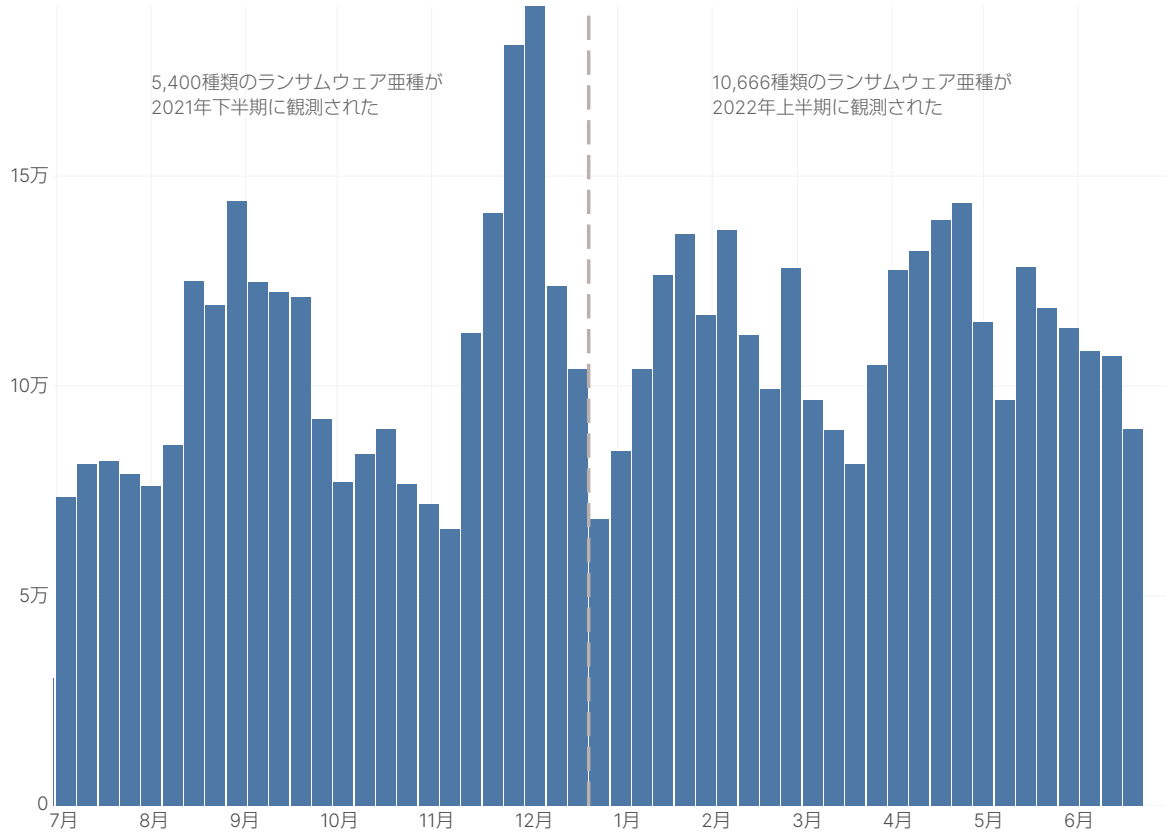
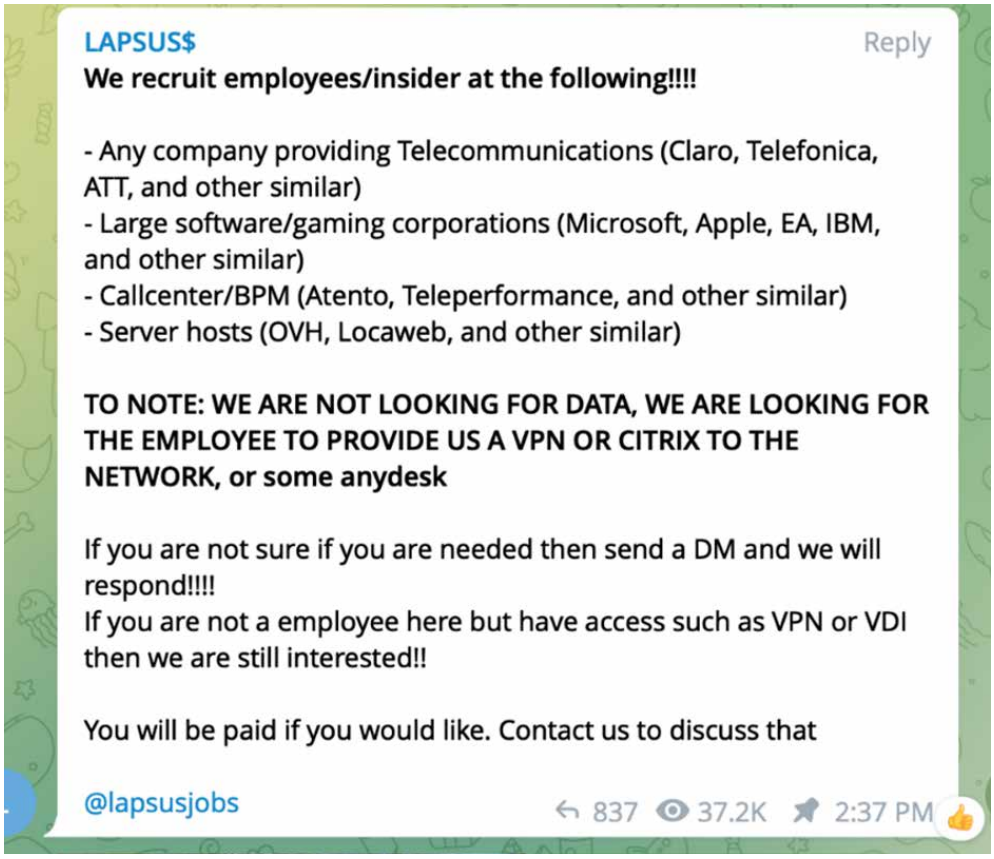


図 11：過去 1 年間の週ごとのランサムウェア件数

進化する脅威環境に対応するため、フォーティネットは、ランサムウェアやその他のマルウェアの ML ベースの分析やその他の検知戦術に継続的に投資しています。週ごとの平均デバイス数が 2020 年 7 月～ 2021 年 6 月に 10.7 倍増を記録した後に、高いレベルを保ちながら推移しているようです。これが「ニューノーマル」と言えるのかもしれません。

RaaS である REvil（別名 Sodinokibi）が法執行機関の国際的な連携により解体されるなどの大きな成果もありましたが、ランサムウェアは、あらゆる規模や業種の組織にとって大きな脅威であり続けています。REvil の解体は RaaS 市場に波紋を投げかけはしたものの、その穴を埋めるほど注目されたランサムウェア攻撃も発生しました。

Lapsus$ は 2021 年 12 月のブラジル保健省のコンピュータシステムへの侵入を皮切りに、LG、Microsoft、T-Mobile などの大企業を次々と攻撃しました。Microsoft によると、Lapsus$ はソーシャルエンジニアリングを使ってアカウントを乗っ取り、標的システムに侵入しました。Microsoft はさらに、Lapsus$ が標的となる企業の従業員からアカウントを買い取り、アクセス権を手に入れていた例も見つけました。



（出典：Microsoft：https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction）

しかしながら、Lapsus$ の背後にいるのが経験豊富な人物ではなく、自慢気に攻撃を宣伝することが多いことから、子供の集団だろうと囁かれていました。英国警察が 3 月 24 日に、Lapsus$ の関係者とみられる 16 ～ 21 歳の 7 人を逮捕しました。

2020 年から存在する RaaS 集団である Conti は、不正添付ファイルや不正リンクを付加してカスタマイズした E メールを使用したスピアフィッシング攻撃を実行し、被害者のネットワークに侵入しようとする、と CISA は警告しています。Conti の犯罪集団は、リモートの管理や監視のソフトウェアを悪用して検知を回避しようとすることでも知られています。2022 年 6 月に Conti は残っていた最後の 2 つの TOR サーバーを停止し、解散しましたが、小規模の派生した集団と同様に、今後も活動を継続することになるでしょう。

ランサムウェア、エクスプロイト、サプライチェーンへの攻撃は、その注目度や破壊的な活動により、今後も大きく報道されることになり、消滅することはないでしょう。

ワイパーの新しい亜種

ウクライナ戦争で、攻撃者が使用するディスクワイパー型マルウェアが大幅に増加しました。フォーティネットは 2022 年上半期に、ウクライナの政府、軍、民間企業に対するさまざまな標的型攻撃で使用された少なくとも 7 つの新しい主要ワイパー亜種を特定しました。この数が重要な意味を持つのは、攻撃者が Saudi Aramco とカタールの RasGas の数万台のコンピュータを停止させる目的で、Shamoon ワイパーを使用した 2012 年以降に検知されたワイパー亜種の合計数とほぼ同じであるからです。

必ずしもその帰属を断定できるわけではありませんが、セキュリティ研究者は、2022 年上半期にウクライナで発生したワイパー攻撃の多くの背後にロシアの軍事目標に同調する集団がいると考えているようです。その一例である CaddyWiper は、ウクライナの一部の組織が所有するシステムのドライブからデータやパーティション情報を消去する目的で使用された亜種です。それ以外にも、Microsoft によって 2022 年 1 月にウクライナ企業に対する攻撃で使用されていることが確認されたワイパーである WhisperGate、SentinelLabs によって同様の攻撃で使用されていることが確認された起動エラーを発生させるツールである HermeticWiper、ディスクドライブや接続ストレージのデータを上書きするマルウェアツールである IsaacWiper などがあります。フォーティネットはこれ以外にも、ウクライナの企業やインフラストラクチャを標的にする、WhisperKill、DoubleZero、AcidRain という 3 つのワイパーを 2022 年上半期に確認しています。

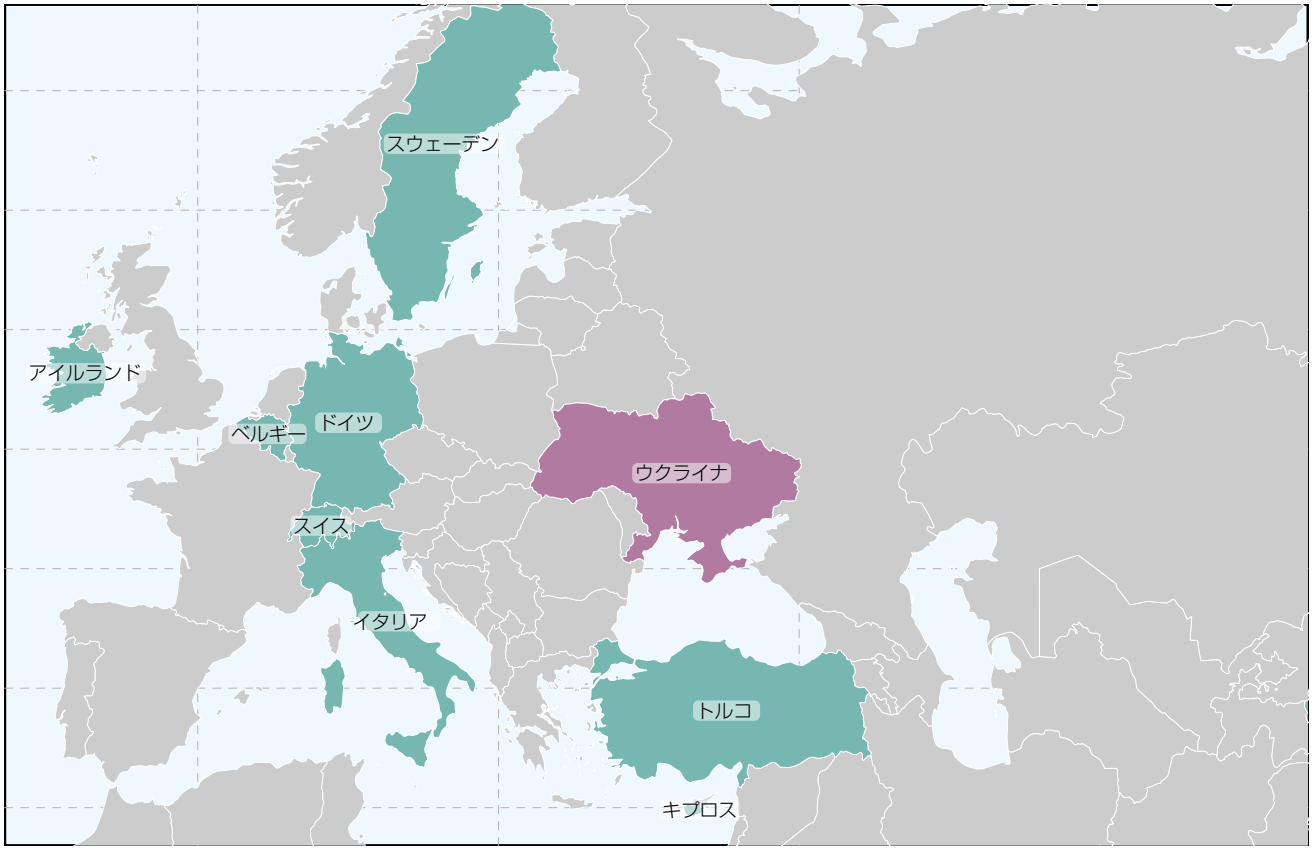


図 12：ロシアによるウクライナ侵攻に関連するワイパーが検知された国

これらの攻撃での驚きは、この地域での過去の紛争の時期と同じように、多くの攻撃が他の国にも拡大していることです。2022 年 2 月に紛争が始まって以来、ウクライナ国内を上回るマルウェアワイパーが国外で検知されています。これらのワイパーの活動は、今年の上半期にウクライナ以外の 24 ヵ国で検知されました。その一例である、ウクライナの衛星ブロードバンドサービスプロバイダーを標的にしたワイパーである AcidRain は、ドイツで約 6,000 基の風力タービンを停止させた攻撃にも使われました。このような攻撃が国境や IT と OT の境界を難なく飛び越えることがわかります。

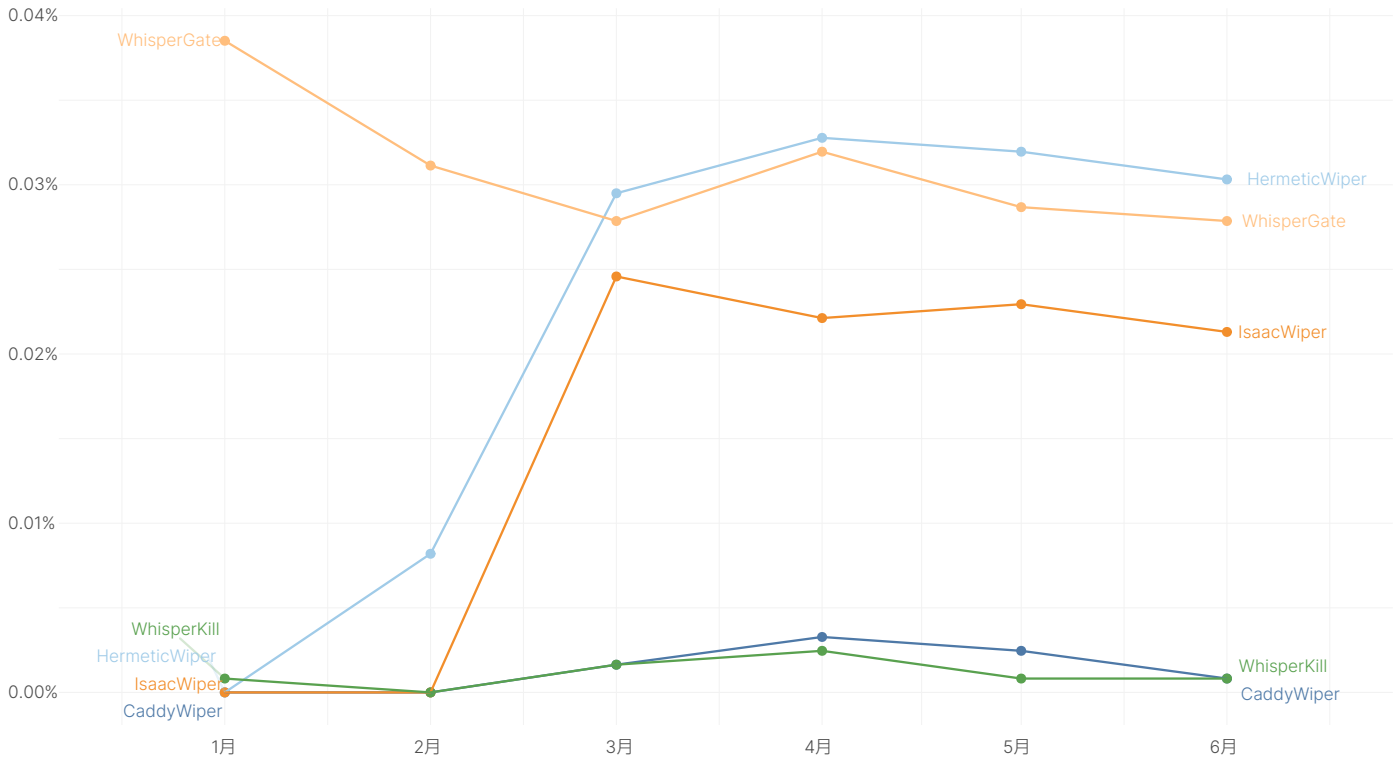


図 13：ロシアによるウクライナ侵攻に関連するワイパーの月別検知

このようなワイパー型マルウェアの急増は、企業のセキュリティチームの悩みの種になっています。現状では検知数は少ないものの、マルウェアの特性や犯罪者の手口を考えれば、ワイパー型マルウェアは特に危険であり、セキュリティチームは十分に警戒する必要があると言えるでしょう。フォーティネットによるワイパーマルウェアの分析で、金銭を得るための攻撃、妨害工作、証拠隠滅、サイバー戦争などのさまざまな目的でワイパー型マルウェアが使用されていることがわかりました。

米国の CISA（Cybersecurity and Infrastructure Security Agency）が 2 月に、ワイパーが日常業務の直接的な脅威になる可能性があると警告し、ウクライナでの攻撃が他の国の組織にも影響する恐れがあると指摘しました。CISA は、「組織は、ワイパー攻撃対策を強化し、自らの計画、準備、検知、レスポンスの能力を評価する必要がある」と警告しました。

ウクライナでの攻撃は、このマルウェアを広範な戦闘目標を達成する手段の 1 つとして使用し、重要なインフラストラクチャの能力やサービスを低下させ、混乱させることができることを示しています。しかしながら、このことだけが脅威ではありません。Shamoon は、ワイパーをサイバー妨害の武器として使用できることを示すものであり、2017 年の NotPetya や GermanWiper などの他の亜種は、攻撃者がワイパーを偽ランサムウェアとして使用して被害者から金銭を強奪できることを示しています。

まとめ

サイバー犯罪者がチャンスを見逃すことはありません。脆弱性、エクスプロイト、あるいは戦争のいずれであっても、常に誰かが誰かに損害を与え、利益を得ようとしています。増え続ける多様な脅威からの保護を可能にし、自信を持ってビジネスを遂行できるようにしていただくことを願っています。

フォーティネットは、あらゆるセキュリティアーキテクチャの異なるレイヤーのニーズに対応するテクノロジーや製品を常時追求し、開発しています。個人や組織が常に意識し、備えることで、刻々と変化するサイバー脅威環境に対応するためのいくつかの重要なヒントを以下に紹介します。

1. **評価、トレーニング、パッチの適用：**FortiRecon を利用することで、外部からの視点で攻撃対象領域を評価し、セキュリティ問題を特定して修復し、現在および差し迫った脅威についてのコンテキストが付加された実用的インテリジェンスを取得できます。NSE Institute のトレーニングは、サイバーセキュリティの基礎からフォーティネットのすべてのソリューションの専門知識まで、あらゆるニーズに対応します。このレポートで紹介した情報は、お客様の環境の保護に必要なパッチの優先度の判断に役立ちます。
2. **エンドポイントセキュリティ：**フォーティネットは、エンドポイントの保護に役立つ、脆弱性とパッチの適用からエクスプロイト対策までの広範なテクノロジーを提供しています。これらのテクノロジーが、ゼロデイ脆弱性に対する攻撃の検知と保護のニーズを解決します。
3. **データ、分析、レスポンスの一元化：**セキュリティはビッグデータの問題であり、最も高度な攻撃を検知する作業は干し草の山から針を見つけるようなものです。エンドポイント、クラウド、ネットワークからのデータの検知と相関付けが、これらの攻撃の阻止にあたって最も重要になります。
4. **ZTNA：**アプリケーションデバイスやネットワークへのアクセスを細かく制御することは、企業環境における侵害の範囲を限定する最も強力な手段の 1 つです。
5. **機械学習ベースのセキュリティテクノロジーの採用：**機械学習は、サイバーセキュリティを含むすべての分野のゲームチェンジャーです。フォーティネットは 7 年前から、応用可能と判断したすべての製品への機械学習と AI の実装を進めてきました。機械学習は、エンドポイント、クラウド、ネットワークベースのソリューションなどのフォーティネット製品に組み込まれています。このテクノロジーにより、フォーティネットが脅威の急速な変化を的確に捉え、お客様によるセキュリティインシデントのトリアージと優先度の判断が容易になります。

本レポートに含まれるデータと実用的インテリジェンスをセキュリティ計画と戦略の指針としてぜひご活用ください。次回のレポートで脅威環境についての最新の実用的インテリジェンスを再びお伝えすることを楽しみにしています。

参考文献

* 本文中のハイパーリンクは、本レポートの電子版（https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/ja_jp/TR-22H1.pdf）よりご参照ください。

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-22H1-202209-R1