WHITE PAPER

2022 年のサイバー脅威予測

FortiGuard Labs による年次予測

2022 年のサイバー脅威予測

サイバー犯罪は、過去 1 年でかつてないほど増加しました。FortiGuard Labs の調査（フォーティネットグローバル脅威レポート 2021 年上半期版）で、2020 年 7 月～ 2021 年 6 月の 1 年間でランサムウェアが 11 倍近く増加したことがわかりました。しかしながら、今後の課題は攻撃件数の増加だけにとどまりません。SolarWinds に対するサプライチェーン攻撃、コロニアルパイプラインや JBS Meats の大混乱などの注目度の高い組織を標的にする攻撃が増加しており、IT とは無関係の何千もの組織や何百万人もの人が影響を受けています。

新たな攻撃対象領域

ほとんどの攻撃に既知の脆弱性が悪用されますが、サイバー犯罪者は、新たな脆弱性を標的にする攻撃も加速させています。例えば、昨年 1 月に中国が支援する組織である Hafnium が、Microsoft Exchange Server の 7 つの新しい脆弱性を標的にする活動を、パッチ公開の 2 ヵ月以上前に開始しました。これらの脆弱性のうちの 3 つは Microsoft が以前指摘していたものですが、4 つは未知のゼロデイ脆弱性でした。Hafnium の大部分が自動化された攻撃は、パッチが適用されていない Exchange Server を標的にし、特別に細工された Web シェルでマルウェアを遠隔操作してデータを盗み、重要システムに不正アクセスしました。世界中の数万の組織が影響を受け、米国を拠点にする法律事務所、防衛関連企業、感染病の研究機関、非政府組織（NGO）なども攻撃されました。

2022 年には、Hafnium 以外の組織も新たな脆弱性を探そうと躍起になるでしょう。昨年の大々的に報道された攻撃を受けて、多くの企業が基本的なサイバーセキュリティ対策にようやく取り組むようになりましたが、サイバー犯罪者の多くが悪用する 1 ～ 3 年前の CVE（Common Vulnerabilities and Exposures）の修正が進む中で、2022 年には CVE の報告数が飛躍的に増加（おそらく初めて 2 万件を突破）し、攻撃者は対策が不十分な組織を標的にこれらの新しい脆弱性やゼロデイ脆弱性を悪用するようになるでしょう。

解決策と対策：

ゼロデイ攻撃がローカルで実行された場合、ネットワークを保護する高度な XDR（Extended Detection and Response：拡張検出および応答）やエンドポイントを保護する EDR（Endpoint Detection and Response：エンドポイント検出と応答）などのテクノロジーを使用することで、攻撃を検知し、C2 サーバーとやり取りして不正ペイロードをダウンロードするなどのマルウェアの重要な機能をブロックできます。サンドボックステクノロジーは、スタンドアロンソリューションあるいは仮想ファイアウォールの一部として、次世代ファイアウォール（NGFW）、セキュアメールゲートウェイ、クラウドベースのセキュリティソリューションなどのネットワークに統合するべき、必須のツールです。

もう 1 つの効果的な戦略は、攻撃パターンや手法を認識するように設計された自動化や分析のツールを導入することで、これには、振る舞い分析やディセプションネットワークの戦略、ハニーポットと組み合わせたソリューションなどがあります。今日のゼロデイ脅威でスピードと複雑さが加速する現状を考えれば、脅威を検知して中断させるように設計されたツールに、異常な振る舞いを発見するように訓練された高度な人工知能（AI）システムを追加し、ログファイルや IOC（Indicators of Compromise：侵害指標）を振り分けて相関付け、複雑で多面的な攻撃の検知を可能にする必要があるでしょう。

コンバージェンス：高度な持続型サイバー犯罪

サイバー犯罪は多くの場合、攻撃キルチェーンの「左側」と「右側」の攻撃に分かれます。右に該当するのは、システムを破壊したり、データを盗んだり、ネットワークを人質にしたりするマルウェアを構築して起動するといった、ほとんどのサイバー犯罪者が古くから手掛けてきた攻撃です。左側に該当するのは、初期アクセスの獲得、偵察の実行、脆弱性の武器化などです。APT（持続的標的型攻撃）が左側に該当するのは、攻撃に先立って脆弱なネットワークを特定して不正アクセスし、長期にわたって検知を逃れるなどなどの活動を実行するためです。APT には通常、国家が支援する脅威アクターなどのリソースが豊富な組織が関与しています。

サイバー犯罪の件数が増加し、より多くの犯罪者が利益を求めて競争するようになると、サイバー犯罪者の「左手」への投資が増加することが予想されます。国家が出資する APT 集団などによるこのような活動では、偵察やゼロデイの機能の発見に多くの時間と労力が投入されるため、今後の CVE の増加に拍車がかかることになるでしょう。

発見される脆弱性が増えるだけでなく、その脆弱性を悪用する攻撃が他の攻撃者にも簡単に利用され、他の攻撃キットに組み込まれるようになるでしょう。新たな脆弱性が増加すれば、当然ながら、MaaS（Malware-as-a-Service：サービスとしてのマルウェア）も増加するはずです。そのため、サイバー犯罪者がより多くのゼロデイ脆弱性を発見して武器化するようになるだけでなく、多数の脅威アクターが手を組んで同時に攻撃を開始するという要素が加わることで、それらのエクスプロイトが開始される件数が指数関数的に増加することが予想されます。

解決策と対策：

これらのサービスは、脆弱性のエクスプロイトを増幅させる大きな要因となります。企業は、高度なテクノロジーで武装した新しいサイバー犯罪者の増加で攻撃の可能性も規模も拡大することを認識する必要があります。標準ツールに拡張性を追加して、潜在的な攻撃件数の増加に対応できるようにし、AI も活用して強化し、攻撃パターンを検知してリアルタイムで脅威を阻止できるようにする必要があります。さらには、EDR、MITRE ATT&CK マッピングを活用するサンドボックスソリューション、AI 検知シグネチャを使用するアンチマルウェアエンジン、高度侵入防止システム（IPS）による検知、および NGFW などを重要なツールとして導入します。理想的な方法としては、統合セキュリティプラットフォームを使用して、これらのツールを一貫性ある方法で分散ネットワーク（データセンター、キャンパス、支社、マルチクラウド、ホームオフィス、エンドポイント）に展開し、統一されたソリューションとして脅威の特定、共有、相関付け、レスポンスを可能にします。

エクスプロイトの新たな分野

古くから攻撃されることが多い分野が今後も攻撃の標的になるでしょう。Windows 11 が公開されましたが、この OS にも脅威アクターに悪用される新たな脆弱性が存在するはずです。それだけではありません。来年は、新たな分野にもエクスプロイトが拡大することになるでしょう。

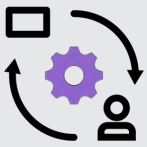
- **標的になることが少なかったシステム：**Linux は、ほとんどのネットワークの多くのバックエンドシステムで動作していますが、最近までハッカーにほとんど無視されていました。Vermilion Strike は、不正ツールとして有名な Cobalt Strike の重要な機能である Beacon の不正目的での実装です。Cobalt Strike は、レッドチーム（および脅威アクター）がネットワーク侵害のリスクの実証に使用する「脅威エミュレーション」ソフトウェアプログラムであり、Beacon は、Windows 環境に不正ペイロードを送り込んでコマンド & コントロール（C2）接続を確立します。Vermilion Strike は、Linux 環境ではまったく検知されずに動作するため、リモートアクセス機能を使って Linux システムを標的にします。
- **Linux のボットネット：**デバイスを武器化したり、パフォーマンスを低下させたりする、Linux プラットフォームを標的にする新しいボットネットマルウェアが作成されています。このようなボットネットマルウェアの存在により、脅威対象領域がネットワークのエッジにまで拡大し、エッジで防御しなければならない脅威が増加します。従来はサイバー犯罪者が見落としていたエッジデバイス（エッジコンピュートデバイスやサーバーなど）を標的にするこの種の活動がさらに増えることが予想されます。
- **Windows の新しい不正 Linux バイナリ：**Windows 10、Windows 11、Windows Server 2019 で Linux バイナリ実行ファイルをネイティブ実行するための互換性レイヤーである Microsoft の Windows Subsystem for Linux（WSL）を標的にする新たな不正バイナリが検知されました。この領域では 2021 年にすでにいくつかの動きが確認されており、ローダーとして機能する不正テストファイルが検知され、その多くに不正ペイロードが含まれていました。Microsoft が WSL 2 の Windows 11 への統合を推進することで、Linux が Windows デバイスを標的とする新たな攻撃ベクトルとなる可能性があるため、2022 年にはこの動きが加速することになるでしょう。
- **オペレーショナルテクノロジー（OT）ネットワークやこれまで標的になっていなかったその他のシステム：**今後は、オペレーショナルテクノロジー（OT）システムなどの従来とは異なる標的への攻撃が増加することが予想されます。米国のサイバーセキュリティ・インフラセキュリティ庁（CISA）は最近のレポートで、重要インフラストラクチャを標的にするランサムウェア攻撃が増加しており、「オペレーショナルテクノロジー（OT）の資産や制御システムに対するランサムウェアの脅威の増加が証明された」と報告しています。アメリカ国家安全保障局（NSA）の同様のサイバーセキュリティ勧告も、「OT コンポーネントの IT（情報テクノロジー）への接続が進むと、

IT エクスプロイトが OT に対する破壊行為で重要な役割を果たすようになる」と指摘しています。NSA は防衛ネットワークの所有者に対し、自らの OT の詳細リスク分析を実施するよう助言しています。OT システムへの攻撃は、かつてはこの分野を専門にする脅威アクターが独占していましたが、ダークウェブで購入できる多くの攻撃キットにこのシステムを攻撃する機能が含まれるようになったことで、多くの攻撃者が参入するようになりました。

- **量子の標的：**量子コンピュータの武器化、特に量子暗号化が始まることになるでしょう。すべての新しいテクノロジーに共通することですが、バグや脆弱性、抜け道を探す研究者は多くいるものです。このテクノロジーは、今はまだ大企業や大学、政府で主に使用されていますが、もちろん、犯罪者が悪用できないわけではありません。多くの国が他国や関心のある産業から大量のデータをすでに収集していて、その多くは暗号化されています。量子システムを活用してデータを保護している従来の暗号がまもなく解読されて、重要な情報が明らかになり、その情報が将来のさらなる攻撃に使用されることになるでしょう。
- **機械学習（ML）の標的：**機械学習ベースのシステム、特にインターネットに公開された外部システムの改ざんあるいは回避しようとする初の試行が確認されることになるでしょう。犯罪者は、いずれネットワークエッジに置かれた、インターネット接続された ML 学習ノードを標的にするようになります。ML を活用した攻撃の例として、セキュリティシステムを密かに訓練して、特定のタイプの攻撃が無視されるようにする方法が考えられます。この脅威カテゴリが非常に深刻であることから、MITRE は、ML システムに対する攻撃の特定と分類に役立つ、ATLAS（Adversarial Threat Landscape for Artificial-Intelligence Systems）と呼ばれる新しい脅威マトリックスを発表しました。
- **CaaS（Crime-as-a-Service：サービスとしての犯罪）の増加：**RaaS（Ransomware-as-a-Service：サービスとしてのランサムウェア）は、開発者やアフィリエイトに数十億ドルの収益をもたらしています。このビジネスモデルを活用する新しいサービスは、攻撃で侵害された組織へのアクセス権の販売、身代金の要求や交渉の支援、暗号通貨を含む資金のロンダリングなどのランサムウェアのサービスも提供しています。このモデルが他でも採用されるようになり、CaaS ポートフォリオにフィッシングやボットネット / SMS の aaS（as-a-Service）が追加されるようになるでしょう。

特に破壊力のあるランサムウェアによるこの種のクライムウェアが今後も拡大することが予想されます。サイバー犯罪者は、開発したマルウェアをオンラインで、特に aaS（as-a-Service）で再販すれば大金を稼げることを知りました。しかしながら、犯罪組織は、類似するツールを提供する他の組織と直接競合するよりも、これまでは標的にしてこなかった Linux や OT などを追加してポートフォリオを拡大し、従来は標的にならなかった、多くの場合にセキュリティが脆弱なシステムを標的にするサービスを提供するようになるでしょう。このようなシステムを入手すれば多額の身代金を手に入れることができますが、OT や重要インフラストラクチャを標的にすると、個人の命や安全を脅かすなどの悲惨な結果を招く恐れもあります。また、ネットワークの相互接続が進むことで、事実上あらゆるアクセスポイントを悪用して IT ネットワークに侵入できるようになるため、これらが新たな攻撃の入り口になることも予測されます。

解決策と対策：



拡大する攻撃対象領域の問題を解決するには、完全なセキュリティメッシュアーキテクチャを開発して展開することで、すべての攻撃対象領域を可視化する必要があります。エンドポイントエージェント、EDR ソリューション、ネットワークベースの IPS やアンチマルウェア、ファイアウォール、ハニーポット、サンドボックスなどのソリューションの連携により、このような攻撃に対する内部と外部の障壁を構築できます。ゼロトラスト戦略は、IT / OT が直接統合されていない分野などのネットワークの新たな領域を標的にする脅威にも非常に有効で、AI によるデバイススキャンが加わることで、さらなるメリットが生まれます。

犯罪組織同士の争い

興味深いことに、サイバー犯罪の急速な増加に伴い、犯罪組織が互いの領域を侵害するようになっているようです。犯罪集団がサイバー犯罪のパイを奪い合う「縄張り争い」がすでに始まっています。今に始まったことではありませんが、現在のトレンドから判断すると、このような活動は増加する可能性が高く、最終目標は競合相手の活動の妨害です。

脅威アクターの TTP（戦術、手法、手順）は、従来はフォレンジック分析で解明されてきましたが、この夏、Conti ランサムウェアグループに不満を抱く「ペンテスター」が、Conti がアフィリエイト向けに作成したプレイブック、攻撃のハウツー文書、参照ファイルなどの内部ファイルを流出させました。今後もこのようなプレイブックやソースコードの流出が増加することが予想されます。

他のサイバー犯罪者のサーバーやリソースの乗っ取りが一般化しており、自らのボットネット C2 システムにデジタル証明書を追加する犯罪組織も出始めています。さらには、インフラストラクチャの乗っ取りを防止するために、多要素認証（MFA）などの認証を義務付ける組織も増えています。後述するように、デジタルウォレットを標的にする活動が活発化し、今は現実化していないとしても、他の犯罪集団の暗号ウォレットを乗っ取ろうとするようにもなるでしょう。

解決策と対策：

サイバー犯罪者同士の争いが増えても、企業や公的機関への直接的な影響はないかもしれませんが、流出した脅威プレイブックを、攻撃の特定や防御を可能にするツールに組み込むことができるでしょう。同時に、犯罪者の振る舞いや攻撃のフィンガープリントに基づいてプレイブックを作成するレッドチームの取り組みも進んでおり、SOAR（Security Orchestration, Automation and Response：セキュリティオーケストレーション、自動化、レスポンス）などの高度なツールへのこれらのプレイブックの取り込みや自動化が可能になり、NOC（ネットワークオペレーションセンター）や SOC（セキュリティオペレーションセンター）の環境に統合できるようになることが期待されます。

エッジに対する環境寄生型攻撃

ネットワークエッジは拡大の一途をたどっており、昨年はパンデミックの影響でクラウドの導入や WFA（work from anywhere：場所に縛られない働き方）が大幅に増加しました。IoT（モノのインターネット）やエンドポイントデバイスの増加、さらには、リアルタイムの処理能力を必要とする新しいアプリケーションの登場により、新しいエッジも開発されています。5G と AI を搭載する高性能のエッジデバイスは、ビデオの処理や分析、車の自動運転、製造フロアの自動化などのリアルタイムアプリケーションの作成を可能にします。このような環境でのデータの収集と処理は、クラウドやデータセンターとの間を行き来することなく、エッジのローカルで進行するため、厳しいレスポンスタイムが求められる場合も迅速な意思決定が可能になります。

去年、エッジ環境を標的にする脅威アクターによる EAT（Edge Access Trojans：エッジにアクセスするトロイの木馬）の開発を予測しましたが、このアプローチには、サイバー犯罪者にとっていくつかのメリットがあります。第 1 に、時間的な制約が大きいネットワークのエッジでデータを収集し、場合によっては重要な判断を混乱させることもできます。一刻を争うプロセスの中断には、多くの場合に重要インフラストラクチャなどの安全に関わる要素が関係するため、ランサムウェア攻撃に対する緊急度がまったく新しいレベルに引き上げられます。EAT がデータの破壊に悪用され、結果として、エッジデバイスが収集したデータに依存する下流システムに重大な影響が及ぶ可能性があります。このような形でエッジを足掛かりにして、企業ネットワークに侵入されてしまう恐れもあります。

エッジベースの新たな課題も生まれています。「環境寄生型」攻撃では、感染した環境の既存のツールセットや機能をマルウェアが利用するため、攻撃やデータ流出が通常のシステム活動のように見えて、見逃されてしまうことがあります。最近の Hafnium による Microsoft Exchange に対する攻撃では、この方法でドメインコントローラに寄生し、常駐化しました。環境寄生型攻撃が効果的なのは、正規のツールを利用して不正活動が実行されるからです。

この 2 つの概念（EAT と環境寄生型）が、2022 年のいずれかの段階で統合されることが予想されます。エッジデバイスがより強力になり、より多くのネイティブ機能を備え、当然ながらより多くの特権を持つようになると、エッジデバイスの新たな環境寄生型攻撃が設計されるようになるでしょう。エッジマルウェアは、検知を逃れつつ、エッジでの活動やデータを監視し、重要なシステム、アプリケーション、情報を盗み、乗っ取り、さらには身代金も要求するようになるでしょう。

解決策と対策：

エッジベースのこれらの新たな脅威を防御するには、高度な EDR テクノロジーとゼロトラストネットワークアクセス（ZTNA）などのアクセス制御でエンドユーザーデバイスをアップグレードし、強化する必要があります。ネットワークの末端までの保護におけるセキュア Web ゲートウェイの重要性がさらに高くなるでしょう。

デジタルウォレット強盗

金融取引や電信送金を標的にするトロイの木馬は、ここ数年で着実に減少しました。金融機関はマルウェアや詐欺の検知と防止を強化し、資金移動に関する保護や法規制の整備も進んでいます。さらには、このような攻撃は追跡が容易であるため、すぐに法執行機関の捜査対象になります。しかしながらこれは、サイバー犯罪者が他人の金銭の詐取に興味がないという意味ではありません。

FortiGuard Labs が最近紹介した新しいフィッシング脅威では、偽の Amazon ギフトカードジェネレータで暗号通貨が不正取得されました。このマルウェアは、被害者のクリップボードを監視してウォレットのアドレスを攻撃者のウォレットに置き換えます（文字通り乗っ取りであり、デジタル強盗です）。偽文書で被害者を誘導し、オンラインショッピングサイトのクレデンシャル、クレジットカード番号、自宅の住所などの機密情報を取得する場合もあります。FortiGuard Labs がこの夏に検知した新しいフィッシング攻撃では、被害者の感染デバイスから暗号ウォレットの情報やクレデンシャルを窃取するマルウェアが使用されていました。ElectroRAT は、デジタルウォレットを標的にするもう 1 つの新しいツールで、ソーシャルエンジニアリングに、Windows、Linux、macOS などの複数の OS を標的にするカスタム暗号通貨アプリケーションと新しい RAT（リモートアクセスのトロイの木馬）を組み合わせて使用されます。

今後は、保存されている暗号クレデンシャルを標的にしたり、デジタルウォレットを流出させたりするマルウェアが増加することになるでしょう。このような変化の理由の 1 つとして、犯罪者が抵抗されにくい方法を選択するようになっている点が挙げられます。組織が取引を暗号化し、多要素認証を必須にするようになったため、電信送金の捕捉がますます困難になっています。これに対し、デジタルウォレットはセキュリティが緩い傾向にあるため、犯罪者にとってより大きな市場です。両者には、デジタルの銀行強盗とひったくりほどの相違があります。個人のウォレットから多額の金銭を手に入れるのは困難かもしれませんが、企業がオンライン取引でデジタルウォレットや通貨を使用する機会が増えれば、この状況も変わるはずです。

解決策と対策：

デジタルウォレットを保護する最良の戦略は、EDR テクノロジーの活用です。エンドポイントはほとんどの組織の主な脆弱性ポイントであり続けていますが、多くの組織は、その保護をアンチウイルスや既製のエンドポイントセキュリティソリューションだけに頼っています。EDR ソリューションに AI を活用した振る舞い異常検知や強化されたカーネル保護を組み合わせることで、C2 サーバーへの接触やマルウェアペイロードのトリガーなどの不正行動をブロックし、目的を達成する前に攻撃を実質的に中断させる必要があります。

ワイパー型ランサムウェア

ランサムウェアの目的は、データを暗号化したり、破壊したり、流出させたりすることで、企業に金銭を要求することです。初期の兆候として、ワイパー型マルウェアを追加することでデータを削除し、身代金要求に応じなければ、OT や製造に使用する機器やサーバーなどの重要システムを停止させることで脅迫のレベルを上げようとする攻撃が確認されています。ワイパー型マルウェアは 10 年近く前から存在します。例えば、DarkSeoul と Shamoon は、2012 年に確認されたワイパー亜種ですが、今日、さらに高度な脅威の一部として復活を遂げました。

サイバー犯罪者はすでにランサムウェア活動に恐喝を追加しており、重要なデータを盗み、公共のサーバーにそれを公開すると脅迫します。被害者の顧客に接触して支払いを迫るようにもなっています。SnapMC のように、暗号化の要素を完全に回避して脅迫を成功させる犯罪者も現れました。単純にデータを盗んで企業に支払いを要求し、要求に応じなければ内部データを公開すると脅迫します。

ランサムウェアの攻撃者はさらに、ランサムウェアともう 1 つの古い攻撃である DDoS（分散型サービス拒否）を組み合わせることで IT チームに圧力をかけて撹乱し、最初の攻撃の被害を減災するための最終判断を妨害します。データの破壊だけでなく、システムやハードウェアを破壊するワイパー型マルウェアという時限爆弾が加わることで、迅速に支払いに応じる必要を迫られることになり、支払いを先延ばしにして法執行機関に攻撃者を発見するための時間的猶予を与えることができなくなります。

ワイパー型マルウェアは今年の夏に、東京オリンピックを標的にする攻撃やイランでの列車運行の妨害という目に見える形で復活しました。攻撃方法と APT のコンバージェンスの現在のレベルを考慮すると、ワイパー型マルウェアのような破壊的な機能がほとんどのランサムウェアに追加されるのは時間の問題でしょう。

解決策と対策：

効果と破壊力を増す今日のランサムウェア攻撃をブロックして阻止する正しいツールを選択し、導入する必要があります。ここで紹介した予測の多くの対策は、EDR と高度なアンチウイルスを含む堅牢なエンドポイントセキュリティ戦略から始まります。ゼロトラスト制御は、特に動的ネットワークセグメンテーションやマイクロセグメンテーションと組み合わせることで、これらの攻撃の影響を抑える役割を果たします。さらには、組織としての復旧戦略を策定し、古くからあるオフネットワークのバックアップやデバイス、レッドチーム / ブルーチームの活動、さらには、シミュレーション方式の復旧訓練によるプロセス、指揮命令系統、ビジネス継続性戦略のチェックを盛り込む必要があります。

サイバー犯罪ゲーム

e スポーツとは、複数のプレイヤーがチームを編成して参加するビデオゲーム競技のことで、多くの場合、その参加者はプロの選手やチームです。今年の売上高が 10 億ドルを突破すると予測されている活気ある市場であり、Newzoo は 2022 年には市場規模が 18 億ドルに達すると予測しています。多くの大手カジノも低迷するゲーム収入を取り戻す手段として e スポーツに注目しており、ゲームフロアに大がかりな e スポーツ競技場や e スポーツ賭博を設置しています。あるレポートによると、2021 年上半期の e スポーツ賭博の売上は、38.6% 増の 5,840 万ドルを記録しました。

e スポーツは、特にランサムウェア、金融取引の窃盗、ソーシャルエンジニアリング攻撃などの魅力的な標的であるらしく、その成長率と関心の高さから、2022 年には e スポーツとオンラインゲームが攻撃の大きな標的になる可能性があります。

解決策と対策：

サービスプロバイダーや e スポーツのプロバイダーは、安全なゲーム環境を提供することで、DDoS などの攻撃を防止する必要があります。また、AI ベースのハンティングツールを導入して、ゲーム環境に潜む脅威を検知する必要もあります。さらには、ゲームコンソールの接続には暗号化された接続を利用し、EDR などのエンドポイント保護を採用する必要があります。

上空からのサイバー犯罪

衛星ネットワークを標的にする新しい POC（概念実証）エクスプロイトが来年のいずれかの時期に登場することが予想されます。衛星を利用したインターネットアクセスが増加し続けています。新しい低軌道（LEO：Low Earth Orbit）衛星システムは、高速化と低価格化が進んでいることで、リモートユーザーだけでなく、一般ビジネスユーザーにとっても現実的な選択肢となっています。Viasat、HughesNet、Starlink（ベータ版）がすでにサービスの提供を開始しており、OneWeb や（Amazon の）Project Kuiper なども間もなくサービスの提供を開始する予定です。Starlink は 560Mbps 以上のダウンロード速度がすでに報告されており、ギガビット速度も視野に入っています。

そのような中で、新たな攻撃がすでに確認されています。ICARUS は、世界中のどこからでも衛星に直接アクセスできることを悪用し、多数の場所から攻撃を仕掛ける POC DDoS 攻撃です。すべての衛星とそれを支える基地局がネットワークへの侵入口になる可能性があります。Starlink だけで 4,000 以上の衛星が運用されており、最終的には 30,000 以上の衛星が相互接続される見込みです。そして、攻撃を仕掛けることができる端末も数百万台にまで増加することになることから、LEO 衛星ネットワークにも、環境寄生型の戦術が間もなく拡大することになるはずです。

最大の標的となるのは、オンラインゲーム、あるいは、リモートへの重要なサービスの提供、リモートフィールドオフィス、パイプライン、さらには、移動中のクルーズ船や貨物船などの船舶や航空機での低遅延の活動のサポートに衛星ベースの接続を利用している組織です。ランサムウェアなどの他の攻撃も間違いなく追従するはずです。企業が衛星ネットワークを利用して、リモートの OT デバイスやシステムなど、従来はオフグリッドだったシステムを相互接続された環境のポートフォリオに加えるようになれば、潜在的な攻撃対象領域がさらに拡大します。

解決策と対策：

ゲートウェイファイアウォール、内部セグメンテーションファイアウォール、IPS はいずれも、拡大する攻撃対象領域や新たな攻撃ベクトルの保護で重要な役割を果たします。さらには、サンドボックスや振る舞い分析ツールなどの高度な脅威検知ソリューションも導入して、新たな環境を標的にするゼロデイ攻撃の検知とレスポンスを可能にする必要があります。

AI の武器化

サイバー犯罪者がいずれは AI を活用し、不正活動を強化するようになるのは、以前より予想されてきたことです。防御側はすでに AI を活用し、通常はボットネットによる攻撃である可能性を示す IoT の異常な振る舞いを検知していますが、サイバー攻撃者も AI を活用し、その異常な活動を検知する複雑なアルゴリズムを妨害するようになっています。

ディープフェイクが大きな脅威として注目されているのは、AI を活用して人間の行動を模倣し、ソーシャルエンジニアリング攻撃の強化にも利用できるためです。GPT-3（Generative Pre-trained Transformer）は、深層言語学習を活用して、より本物らしい E メールを生成する AI ベースのシステムです。攻撃者はこれを利用して、メールサーバーを侵害したり、中間者攻撃を実行したりすることで、管理職などの文体、言葉の選択、口調を模倣するメールや返信を生成し、場合によっては過去のやり取りを参照することもできます。

そして、文字の E メールだけではありません。人間の声をコピーするオンラインのソフトウェアツールがすでに存在し、開発中のツールもたくさんあります。数秒の音声を利用して音声フィンガープリントを作成し、任意の言葉をリアルタイムで生成することができます。8 月に公開された概念実証のディープフェイク動画では、俳優が NVIDIA の CEO を演じていました。初期段階ではあるものの、このような AI を活用したディープフェイクは、CPU（中央演算処理装置）や GPU（グラフィック処理装置）の性能が高く（安価に）なるほど、さらに深刻な問題になるでしょう。高度なアプリケーションの実用化で、このようなディープフェイクを簡単に作成できるようになり、最終的には、音声や動画のアプリケーションをリアルタイムで騙して生体認証分析を突破するようになる可能もなります。声を認証に利用できなくなるなどといった、数え切れないほど多くの影響が考えられます。

オープンソースの Counterfit と呼ばれるツールが公開されており、顔認証、画像認証、不正検知などの AI システムの侵入テストを実行して、使用しているアルゴリズムが信頼できるものかどうかを確認できます。このツールをレッド / ブルーウォーゲームにも利用できますが、攻撃者もこのツールを悪用して AI システムの脆弱性を特定するようになることが予想されます。

解決策と対策：

これらの POC テクノロジーが主流になれば、音声や映像のわずかな異常を AI で検知するといった、攻撃の検知と減災の方法の変更を迫られることになるでしょう。現在の最良の防御は、セグメンテーション、ユーザーやデバイスを定義済みの資産だけに制限するゼロトラストアクセス、さらには、攻撃を捕捉してその影響を限定するように設計された統合型セキュリティ ファブリックの採用です。エンドユーザーのトレーニングを強化し、E メールだけでなく、音声や動画で到着する不審あるいは予期しない要求を検知できるようにする必要もあるでしょう。マルウェアが埋め込まれた偽装通信の対策にあたっては、トラフィックを監視してペイロードを検知する必要があり、これは、ユーザーエクスペリエンスに影響することなくストリーミングビデオをインスペクションする十分な速度のデバイスが必要です。

モグラたたきゲーム

サイバーセキュリティプロフェッショナルの多くが現在のサイバー犯罪対策を「モグラたたきゲーム」と揶揄しますが、これは、ある場所で阻止した犯罪活動が別の場所で通常は同じ脅威アクターによって再発する傾向があるからです。そのような活動の一部は自動化されていて、例えば、ある C2 サーバーをシャットダウンしても、犯罪活動はほとんど中断することなく、別の場所に新しいサーバーが自動生成されます。結果として攻撃者が自動化を武器にすることで、攻撃サイクルが短くなっています。

防御側にとっての大きな課題の 1 つは、いかに攻撃を遅らせることができるかということであり、攻撃を中断させることが、特に有効な戦術となります。攻撃側の鎧を「打ち砕く」こと、すなわち、協調型の反撃の戦術で攻撃側のダウンタイムを長くすることで、組織の再編成を余儀なくさせて、弱体化させることができます。戦略的連携や官民の協力で犯罪組織の攻撃能力を長期にわたって奪うという目に見える成果がすでに上がっています。世界経済フォーラム（WEF）の Partnership Against Cybercrime（サイバー犯罪対策パートナーシップ）などの新しいツールや継続的に改訂されるサイバー脅威プレイブックを活用することで、サイバー犯罪者を容易に特定してその活動を妨害し、戦術の全容を明らかにすることができます。来年は、特に法執行機関と民間企業との協力がさらに拡大し、国や地域の間にも新たな協力関係が生まれることで、解体されたサイバー組織が復活するまでの時間が長くなることが期待されます。

解決策と対策：

攻撃対象領域のさまざまな要素を標的にする攻撃を防御するには、一貫性ある保護と通信を分散ネットワークに提供するセキュリティ ファブリックを完全統合し、エンドユーザーの教育と意識向上に取り組む必要があります。

未知の脅威に対する予測的防御

明日の脅威の多くは、現在の脅威の延長線上にあるものですが、脅威は常に高速化したり、検知が困難になったり、悪質化したりし、既存の脅威を新たに組み合わせたものになったりします。ただし、新しいゼロデイ脅威であっても、ファイルの変更、追加、あるいは削除、機能の追加や削除、通常のプロセスへのインジェクション、何かの取得やドロップといった、ネットワークやデバイスに対するユーザーが望まない行為をするという点は共通しています。このことを理解すれば、通常の運用を基準にして予期しない事態の発生を検知し、対策を講じるよう設計されたセキュリティ戦略を実装することができます。

もちろんこれは簡単なことではなく、単独で動作するのではなく、連携して機能するソリューションが必要です。リアルタイムの脅威インテリジェンスを取得して脅威のパターンやフィンガープリントを検知し、大量のデータを相関付けて異常を検知し、連携型のレスポンスを自動的に開始する方法を理解する、高度なソリューションでなければなりません。さらには、ストリーミングビデオのインスペクションや、電子取引立会場、ゲーム環境、あるいはビッグデータなどの大規模環境を保護するには、既存のツールでは提供できないスピードと容量を処理できるセキュリティソリューションである必要があります。しかしながら、そのようなツールはすでに存在しており、今日の拡大するデジタル経済で成功する唯一の方法は、高速かつ適応型で自動化され、完全統合されたセキュリティ戦略を見つけて導入することです。

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/white-papers/ja_jp/WP-Cyber-Threat-Predictions-for-2022.pdf）よりご参照ください。

FORTINET

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

WP-Cyber-Threat-Predictions-for-2022-202201-R1