WHITE PAPER

2023 年のサイバー脅威予測

FortiGuard Labs による年次予測

ネットワークとセキュリティの統合化戦略に伴い、それらの構成要素は複雑さを解消するため、少なくする方が好まれます（Less is More）。しかし、サイバー犯罪者の戦略は相変わらず多ければ多い方が良い（More is More）ようです。

サイバー環境で確認されている最も厄介なトレンドは、あらゆる種類の脅威がますます遍在化しているという状況であり、これは今後も続くと思われます。RaaS（Ransomware-as-a-Service：サービスとしてのランサムウェア）から、エッジデバイスや仮想都市などの従来とは異なる標的を狙う新たな攻撃に至るまで、ますます高度になるサイバー脅威の量と多様性に対し、セキュリティ部門は 2023 年以降も即座に対応できるように備える必要があります。

2022 年の予測を振り返って

昨年、我々は脅威情勢がどのように推移するかについて、攻撃者が攻撃前の活動により多くの労力を費やすようになる点、オペレーショナルテクノロジー（OT）に影響を与える攻撃が増加する点などをはじめ、多くの予測を立てました。ここでは、一部の予測について振り返り、2023 年に脅威がどのように進化していくのかを見ていきます。

持続的標的型攻撃の台頭

フォーティネットは、新たな脆弱性の増加や「左側」の活動（攻撃前の偵察や武器化）の増加によって、CaaS（Crime-as-a-service：サービスとしての犯罪）の成長がさらにエスカレートすると予測しました。また、2022 年上半期だけで、フォーティネットが特定した新しいランサムウェア亜種は、直前の 6 ヵ月間から 100% 近く増加しました。FortiGuard Labs チームが文書化した新しいランサムウェア亜種の数は、2021 年下半期には 5,400 件でしたが、2022 年上半期には 10,666 件に上りました。このように新しいランサムウェア亜種が爆発的に増加しているのは、主にダークウェブで RaaS の人気が高まっていることに起因していると思われます。一般の人々がストリーミングメディアやフードデリバリアプリを広く利用するようになったように、サイバー犯罪組織がサブスクリプションモデルのサービスを利用し、プラグアンドプレイのランサムウェアを購入して、手っ取り早く報酬を得るようになると予想されます。RaaS オペレーターは、被害者にさらなるプレッシャーを与えるため、身代金要求に応じなければ窃取したデータをダークウェブに流出させると脅すことがよくあります。

登場するランサムウェア亜種の急増は主に RaaS によるものですが、ランサムウェアの支払い額も増加しています。米国財務省の金融犯罪捜査網（FinCEN）は、ランサムウェア攻撃を受けた組織の支払い額が 2021 年上半期には約 6 億ドルに上ったことを報告しました。これは、1 年間の支払い額が過去 10 年分の合計額を上回る勢いで増加していることを示しています [1]。最近の調査によると、回答者の 72% は身代金に関するポリシーを策定済みであると回答し、そのうちの 49% は身代金支払いに即座に応じるという手順を定めています [2]。

2023 年以降、CaaS 市場が大幅に拡大し、新しいエクスプロイト、サービス、構造化されたプログラムが、サブスクリプションモデルにより攻撃者に提供されるようになると予測されます。

保護対策

CaaS の成長が攻撃数の増加に寄与していることは、すでに確認されています。組織にとっての問題は、もはや「侵害されるかどうか」ではなく、「いつ侵害されるか」です。EDR テクノロジー、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、NGFW といった標準的なセキュリティツールには、サイバー脅威の急増に対応できる拡張性が必要とされます。ダークウェブの活動を監視する新しい偵察ツールやサービス（漏洩し販売されている認証情報の特定など）は、組織が攻撃を未然に防ぐ上で不可欠です。データセンターから支社まで、組織が活動するあらゆる場所でこれらのテクノロジーを展開し、一元的に脅威を把握 / 共有 / 相関分析し、対応できる統合セキュリティプラットフォームを使用することが理想的です。最後に、安全なインフラストラクチャを整備し、キルチェーンの早い段階で攻撃者の活動を検知するためには、ハニーポットなどのディセプションテクノロジーを活用する必要があります。

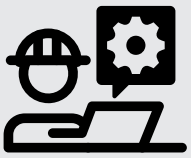
エッジに対する攻撃が主流に

OT システムのようなエッジデバイスや、衛星を介したインターネットネットワークは、以前は、狡猾な攻撃者にとっては非伝統的な（そして、あまり一般的でない）標的であると考えられていました。しかしこの 10 年間で、こういった標的に対するサイバー攻撃がより巧妙に、より大量に試みられるようになっています。IT と OT ネットワークのコンバージェンスがほぼ一般化していることから、攻撃者がホームネットワークやリモートワーカーのデバイスを経由して、容易に OT システムにアクセスできるようになりました。現在では、93% の組織が過去 12 ヵ月間に OT インフラストラクチャを標的とする侵入を経験し、83% が 4 件以上経験したことが、フォーティネットの「2022 年オペレーショナルテクノロジーとサイバーセキュリティに関する現状レポート」で示されています [3]。

フォーティネットは昨年、エッジ環境を標的として EAT（Edge Access Trojan：エッジにアクセスするトロイの木馬）を使用する攻撃が増加すると予測し、実際にそのような事例が確認されています。その一例として、2022 年 3 月に FortiGuard Labs が確認した「StartPage」は、ブラウザのホームページを変更して広告を表示する、誤解を招くアプリケーションや悪意のあるアプリケーションを宣伝する、ブラウザを悪用して脅威を引き起こすといった操作を実行する汎用のトロイの木馬です。そのために、OT デバイスへのマルウェア配布が世界的に増加しました。

フォーティネットはさらに、衛星を介したインターネットネットワークがサイバー犯罪者の新たな標的になると予測しました。このようなネットワークの大規模化と拡張に伴って、侵害の試行回数も増加しています。2022 年の初め、「AcidRain」という新種のワイパー型マルウェアを使ったハッカーが、ウクライナの衛星通信会社のインフラストラクチャを攻撃し、ヨーロッパ全域の衛星インターネット接続に影響を与えました。この攻撃の影響は、ドイツの 6,000 基近くの風力発電機にも及び、衛星接続の切断によってタービンが制御不能になりました。このような衛星ネットワークを標的とする攻撃は今後も続くと予想され、クルーズ船や貨物船、航空会社、石油 / ガス掘削の装置やパイプライン、遠隔の現場事務所など、低遅延の活動のために衛星接続を利用している組織が最大の標的になると考えられます。

エッジデバイスの悪用を企てるサイバー犯罪者の動機は単純です。OT システムや衛星ネットワークなどの標的は、攻撃者にとっては組織の環境への新たな侵入口となります。また、ネットワークエッジの増加は、環境寄生型脅威の潜伏場所が増えることを意味します。つまり攻撃者は、悪意のある操作を通常のネットワーク活動のように見せかけ、検知を回避できるようになります。



保護対策

OT システムやエッジシステムは、攻撃者にとって格好の標的となっており、この状況は今後も続きます。多くの場合、こういったシステムを標的とする専用ツールが攻撃に使用されますが、IT プラットフォームを標的とする侵害の試みによって、最終的に OT が被害を受けることもあります。このような攻撃は、OT プラットフォームの監視 / 制御に使用される IT システムにも影響を及ぼします。OT を確実に保護するには、IT も保護しなければなりません。IT / OT コンバージェンス戦略の一環として、最初からセキュリティに取り組む必要があるのです。

OT / IT 環境のセキュリティを確保するために、セキュリティリーダーが取るべき基本的な手順があります。ベストプラクティスとしては、ネットワークマッピングと接続の分析の実施、不審な活動の検知、ゼロトラストフレームワークの実装、適切なリモートアクセスツールの連携、強力なアイデンティティ / アクセス管理（IAM）戦略の実装が挙げられます。

猛威を振るうランサムウェアとワイパー

ランサムウェアは悪質化し続け、被害額も右肩上がりで増えています。フォーティネットが実施したグローバルランサムウェア調査では、67% の組織がランサムウェア攻撃を受けたと報告しています [4]。さらに悪いことに、半数近くは攻撃を 2 回以上経験し、3 回以上攻撃を受けた組織も 6 社に 1 社に上ります [5]。

2021 年には、攻撃者がランサムウェア攻撃にワイパー型マルウェアを追加して、攻撃を巧妙化させていることを示す兆候が現れ始めました。ワイパー型マルウェアは 10 年前に発見されたものですが、サイバー犯罪者は、身代金に応じない場合にデータを削除し、OT、製造装置、サーバーなどの重要システムの可用性を麻痺させるために利用しています。さまざまな攻撃手法と持続的標的型攻撃（APT）のコンバージェンスが進んでいることを踏まえ、フォーティネットは、ワイパー型マルウェアのような破壊的能力を持つランサムウェア攻撃が増加すると予想しました。

今年は、ロシアのウクライナ侵攻を契機として、主に重要インフラストラクチャを狙う攻撃者の間でディスクを消去するマルウェアの増加が顕著に見られました。FortiGuard Labs は、2022 年前半期だけで、少なくとも 7 つの主要な新しいワイパー亜種が、政府、軍、民間の組織に対するさまざまな攻撃に使用されたことを確認しました。これは、2012 年からの 10 年間に公に検知されたワイパー亜種の総数に迫る数であり、増加の勢いを示しています。さらに、こういったワイパーは 1 ヵ所にとどまらず、ウクライナの他に 24 ヵ国でも検知されました。

ワイパー型マルウェアのトレンドは、攻撃手法が破壊力を高め、高度化しているという不穏な進化を明らかにしています。ワイパー型マルウェアの急増は、武器化されたペイロードが特定の標的や地域に限定して使用されるのではなく、今後は他のサイバー犯罪のプレイブックとの組み合わせで使用される可能性が高いことを示唆しています。被害者に支払いを強要しようと目論む犯罪者にとって、ワイパー型マルウェアとランサムウェアを組み合わせることで新たな巧妙化が可能となります。

保護対策

ワイパー型マルウェアの影響を最小限に抑えるには、いくつかのベストプラクティスを実施すべきです。インラインサンドボックスの使用は、ランサムウェアやワイパー型マルウェアから保護する上で優れた出発点となります。これによって、無害なファイルのみがエンドポイントに配布されるようになります。また、バックアップを用意しておくことも重要な対策です。ただし、マルウェアは多くの場合、マシン上やネットワーク上でバックアップ（Windows シャドーコピーなど）を積極的に探して破壊しようとします。そのため、バックアップをオフサイト、オフラインで保管し、高度な攻撃にも耐えられるようにしなければなりません。また、ネットワークを適切にセグメント化することによって、攻撃が発生した場合でも、インシデントをネットワークの一部のみに封じ込めることが可能です。さらに、ディザスタリカバリやインシデントレスポンスの計画を策定します。データの損失を回避できるか、あるいはデータが完全に破壊されるかが、このような備えによって決定付けられることも少なくありません。

そして、いつもどおりシステムのパッチ適用を実行します。成功している攻撃の多くは、パッチを容易に利用できる脆弱性を標的としたものです。既知の脆弱性を狙った悪意ある攻撃に対しては、サイバーセキュリティ対策の確実な実践が計り知れない価値をもたらします。

人工知能の武器化

AI は、すでに防御に活用され、通常はボットネットによる攻撃の可能性を示す IoT（モノのインターネット）の異常な振る舞いを検知しています。フォーティネットが予測したように、サイバー犯罪者は、ネットワークの異常な活動を検知するアルゴリズムの妨害、人間の行動の模倣といった多くの悪意ある活動を支援するため、ますます AI を活用するようになっています。

このように攻撃者が AI を武器化する例として、ディープフェイクの開発が挙げられます。「ディープフェイク」という言葉は 5 年前に使われ始めましたが、この攻撃ベクトルをめぐって懸念が高まっています。ディープフェイクにはいくつかの作成方法があり、そのテクノロジーも急速に進歩しています。最も一般的なのは、画像の偽造にも使用可能なアルゴリズムによりパターン認識を自己学習する敵対的生成ネットワーク（GAN：Generative Adversarial Network）を使用する方法です。また、顔の置換やスワップのテクノロジーに用いられるエンコーダーと呼ばれる AI アルゴリズムを利用する方法もあります。デコーダーが顔の画像を検索して入れ替えることで、特定の人物の顔を別人の体に重ね合わせることが可能になります。

この 1 年で話題になった多くのディープフェイクは、NVIDIA が CG 映像を使い、CEO の Jensen Huang 氏が自宅のキッチンから記者会見をしているように見せたものなどであり、機密情報を盗み出そうとするサイバー犯罪者が作成したものではありません。しかし、ディープフェイクは、セキュリティチームとその組織が考慮しなければならない潜在的な脅威ベクトルであることは間違いありません。ハッカーがこうした手口を犯罪行為で利用しているいくつかの事例も、すでに確認されています。

保護対策

Web フィルタリング、アンチウイルスソフトウェア、EDR テクノロジーはすべて、AI の武器化から組織を保護する役割を果たしています。しかし、AI に関連する攻撃を阻止する上では、サイバーセキュリティに対する意識を向上する教育が非常に有効な防御方法となります。多くの組織は、基本的なセキュリティトレーニングプログラムを従業員に提供しています。しかし、AI を活用する脅威を識別するための新しい教育モジュールの追加も検討すべきです。例えば、不自然な目の動き、まばたきの少なさ、顔の向きの不一致など、ディープフェイク動画を見分けるヒントを提供するセッションなどがあります。

暗号ウォレット強盗の増加

銀行取引や電信送金は、かつてはサイバー犯罪者の格好の標的となっていました。しかし、取引の暗号化や多要素認証（MFA：Multi-Factor Authentication）の義務化など、銀行がセキュリティ対策を強化するのに伴って、こうした取引をハッカーがインターセプトすることが難しくなっています。その一方で、「沈む瀬あれば浮かぶ瀬あり」と言われるように、保存された暗号クレデンシャルを狙うマルウェアやデジタルウォレットを流出させるマルウェアが増加したのは、フォーティネットが予想したとおりです。デジタルウォレットは、安全性が十分に確保されない傾向があるため、ハッカーにとっては狙いやすい標的となっています。

2022 年に発生した NFT（非代替性トークン）の大規模なハッキングの例は、枚挙にいとまがありません。2 月には、OpenSea のユーザーがフィッシング攻撃を受け、170 万ドルの NFT が窃取されました。さらに数ヵ月後には、Premint のユーザーから 40 万ドルの NFT が窃取されました。人気ソーシャルプラットフォーム「Discord」で発生した複数の NFT ハッキングも注目を集めました。しかし、こうしたブロックチェーンの脆弱性の利用やさらなる悪用は、現時点ではまだ拡大していません。このような攻撃が増加すると、暗号通貨市場に対する懐疑的な見方がさらに助長される可能性があります。

保護対策

暗号ウォレットの保護対策は、ウォレットの所有者から始める必要があります。自己管理型ウォレットは、資産保有者が暗号通貨を完全に管理し、秘密鍵を制御できるため、望ましいと言えます。管理委託型ウォレットは、第三者が管理するウォレットであり、ユーザーが自分のウォレットを完全に制御できないため、リスクが高くなります。

2023 年に注目すべき新たな攻撃トレンド

今後もハッカーは、確実に成果を上げている攻撃手法に依存し、特に実行が容易で手っ取り早く報酬を得られる手口を活用し続けることは明らかです。しかし、FortiGuard Labs チームは、2023 年にいくつかの新しい攻撃トレンドが現れると予測しています。ここでは、今後 1 年間に注目すべきセキュリティ攻撃の動向を紹介します。

新たな CaaS の提供

サイバー犯罪者が RaaS で成功を収めていることから、ダークウェブを通じてサービスとして利用可能な攻撃ベクトルが増えていくと予測されます。ランサムウェアなどの MaaS（Malware-as-a-Service：サービスとしてのマルウェア）の販売に加えて、新しい犯罪ソリューションや攻撃で侵害された標的へのアクセス権の販売が増加することが予想されます。

攻撃者にとっては、CaaS（Crime-as-a-Service：サービスとしての犯罪）が魅力的なビジネスモデルとなる可能性があります。今後は、サブスクリプションで攻撃者に提供されるターンキーソリューションが増えると予想されます。この新しいモデルによって、サイバー犯罪者はスキルレベルに関係なく、あらかじめ独自の計画に時間やリソースをかけずに高度な攻撃を展開できるようになります。また、熟練したサイバー犯罪者にとっては、「サービスとしての」攻撃ポートフォリオを作成して販売することで、シンプルかつ迅速で、繰り返し利用できる報酬を得られるようになります。

その結果、2023 年以降には CaaS のポートフォリオが拡張されていくでしょう。また、攻撃者はディープフェイクなどの新たな攻撃ベクトルを活用し、これらの動画や音声記録、関連するアルゴリズムをより広く販売するようになると予想されます。攻撃の標的は、著名人や政府関係者にとどまらず、インフルエンサー、特にデジタルで大きな存在感を持つ人物にまで拡大していくと思われます。このように範囲を広げることで、サイバー犯罪者は、他者になりすまし、疑いを持たないファンを誘って、実際には存在しない商品を「購入」するといった行動を取らせる機会を増やしています。

ディープフェイクに加え、サービスとしての偵察（Reconnaissance-as-a-Service）が広く利用されるようになると予測されます。標的型の攻撃が増えるにつれて、攻撃者は攻撃前に特定の標的に関する情報を収集するために、ダークウェブ上で「探偵」を雇うようになります。私立探偵を雇って得られる洞察のように、サービスとしての偵察は、組織のセキュリティスキーマ、主要なセキュリティ担当者、使用サーバー数、既知の外部脆弱性、さらには漏洩し販売されている認証情報といった攻撃の青写真を提供します。これを役立てることで、サイバー犯罪者は標的を絞った効果的な攻撃を実行できます。

自動化がマネーロンダリングを促進

通常、リーダーやアフィリエイトプログラムは、犯罪組織の拡大のために「マネーミュール」を雇います。マネーミュールとは、自覚の有無を問わず犯罪組織のマネーロンダリングに利用される人々を指します。マネーミュールは一般的に広告を通じて募集され、別の国または金融機関に匿名で資金を移動するのに利用されます。一般的に、このような資金のシャッフルは、検知を回避するために匿名の電信送金サービスや暗号通貨取引所を通じて行われます。取引や金銭の物理的な移動のため、自覚のないミュールを使うことは、デジタルの痕跡を残すことを避けるのに役立ち、現在でも一般的です。マネーロンダリング防止法で義務付けられている警告を回避するため、多くの場合に資金が小口化され、複数のチャネルを介して送金されます。

従来、マネーミュール募集キャンペーンを仕掛けるのは時間のかかるプロセスです。サイバー犯罪のリーダーは大きな労力を費やし、偽組織の Web サイトを立ち上げて求人情報（売掛金管理業務など）を掲載することで、合法的なビジネスを装ってミュールを雇い入れ、法執行機関の監視を逃れようとします。今後、サイバー犯罪者は、採用の標的に機械学習（ML：Machine Learning）を利用することで、潜在的なミュールの特定に役立て、採用者を見つけるまでの時間を短縮しようとすると予想されます。

また、手作業によるミュール募集キャンペーンに代わって、暗号通貨取引所を何重にも経由して資金を移動させる自動サービスが利用されるようになるため、プロセスが高速化し、追跡がより困難になると予想されます。コインランドリーの機械にコインを入れるように、サイバー犯罪者は料金を支払うだけで自動化された攻撃を実行できるようになります。これによって、手作業で募集する必要性が減り、場合によってはプロセスから完全に削除されます。

サービスとしてのマネーロンダリング（Money Laundering-as-a-Service）の兆候は、明らかに現れています。これは、成長しているCaaS ポートフォリオの一部として、早期に含まれるようになる可能性があります。また、自動化への移行によってマネーロンダリングの追跡が困難になることから、この種のサイバー犯罪の被害を受けた組織や個人が、窃取された資金を取り戻す可能性は低くなります。

仮想都市に進出するサイバー犯罪

メタバースは、オンライン世界で新しい完全没入型のエクスペリエンスを生み出しています。拡張現実（AR）、仮想現実（VR）、複合現実（MR）のテクノロジーを駆使した、この新しいバージョンのインターネットには、一部の都市がいち早く参入しています。ドバイをはじめとするこれらの仮想都市は、現実のエクスペリエンスや場所を再現することを約束しています。個人は、アバターを作成し、仮想空間で仕事、遊び、買い物などの活動を行うことができます。小売業者は、こういった仮想世界向けにデジタル商品を開発し、販売しています。昨年末、ファッションブランドの Ralph Lauren は、オンラインゲームプラットフォーム「Roblox」で独占的にデジタルコレクションを投入しました。

このようなオンラインの新しい場所は、可能性を大きく広げる一方で、サイバー犯罪がかつてないほど増加する危険も生み出しています。個人のアバターは本質的に個人情報（PII）への入り口であり、攻撃者にとって格好の標的となります。個人は仮想都市でモノやサービスを購入できるため、デジタルウォレット、暗号通貨取引所、NFT、取引に使用される通貨は、攻撃者に新たな攻撃対象領域をさらに提供することになります。また、こうした仮想のモノや資産は窃取や転売が可能です。生体情報のハッキングが現実に起きる可能性もあります。AR や VR を駆使したコンポーネントが利用される仮想都市では、サイバー犯罪者が指紋マッピングや顔認識データ、網膜スキャンを窃取して悪用することが容易になります。

（攻撃の）長期戦に備える

サイバー犯罪者は、特定の新しいテクノロジーを活用して新たな侵害の機会を得ると予測されます。Web3 のような新しいテクノロジーや、これまで以上に猛威を振るっていると見られるテクノロジーについて、現在わかっていることを踏まえ、今後 1 年間にとどまらず、これからの数年間にわたって脅威がどのように変化していくかについて、いくつかの長期的な予測を立てることができます。

ワイパーによるリスクの高まり

10 年来の攻撃手法であるワイパー型マルウェアは、今年劇的な復活を遂げ、攻撃者は新たな亜種を導入しています。ワイパー型マルウェアの蔓延自体も警戒すべきですが、攻撃者は継続的に破壊力を最大化させようと、多様な脅威を組み合わせるようになると予想されます。例えば、コンピュータワームとワイパー型マルウェアは簡単に組み合わせることができ、これによってマルウェアの迅速な複製や広範な拡散が容易になります。脆弱性によっては、このような悪用によって短時間で大規模な破壊が起こる可能性があります。このため、早期に検知し、セキュリティチームが迅速に修復することが非常に重要となります。

今後、ワイパーと他の攻撃ベクトルの組み合わせは、セキュリティコミュニティが直面する新たな脅威の中でも著しく大きなものとなります。ワイパーは、サイバー空間を席巻し、官民を問わず世界中の IT ネットワークに影響を及ぼしかねません。コモディティ化しているワイパーは、飛躍的な勢いでネットワークに影響を与える潜在性があります。

開拓が進む Web3

Web3 は、デジタルエコノミーの分散管理を目指すブロックチェーンベースの新しいインターネットとして、急速に主流になりつつあり、Web3 ツールを試す企業も増え始めています。その理由は簡単に理解できます。Web3 は、多くの潜在的メリットを企業に提供します。例えば、開発チームがアプリケーションを展開する際に、そのプロセスをサポートするための新しいインフラストラクチャを維持管理する必要がありません。

しかし、他の新しいテクノロジーと同様、Web3 にもセキュリティ上のリスクがないわけではありません。Web3 で重要となるのは、ユーザーが自分自身のデータを制御できることです。しかし、過去のセキュリティインシデントからわかるとおり、往々にしてユーザーが最も弱いリンクとなります。また、ブロックチェーンの不可逆的な側面は、メリットと同時に課題ももたらします。例えば、現在の Web3 ウォレットは MFA を使用せずパスワードのみに依存するため、紛失すると回復が困難です。

Web3 が主流になる前に、ネットワークの状態維持を担うネットワークノードが不正行為や窃取されたデータに対処するための規制が導入されると予想されます。クレジットカードが不正に使用された場合と同じように、不正行為を追跡して封じ込めるためのプロトコルが必要です。

「Q デイ」への備え

量子コンピューティングは 40 年以上前に始まりましたが、近年はこのテクノロジーへの投資が官民ともに増えています。McKinsey and Company は、最近発表したレポートで、「量子コンピューティングは、従来の高性能コンピュータの範囲や速度では対応不可能な問題をビジネスが解決できることを約束するが、現在の初期段階ではユースケースの大部分が実験的で仮説的である [6]」と断言しています。量子コンピューティングは、これまで解読不可能だった暗号化アルゴリズムの解読などで、すでに画期的な成果をもたらしています。

現在は、すべての量子コンピューティング能力を広範に適用または利用できない可能性があります。しかし、一部の専門家は、Q-Day、つまり量子コンピューティングが現在の暗号化メカニズムを破壊するほど強力になる日が急速に近づいていると警告しています。また、セキュリティコミュニティは量子コンピュータに対抗できる新しい暗号化アルゴリズムを開発していますが、この取り組みはまだ道半ばです。

例えば、NIST は数ヵ月前に、複数年にわたって量子コンピュータに対抗できる新しい暗号化標準を設計するコンテストの勝者を発表しました。Supersingular Isogeny Key Encapsulation（SIKE）も、そのような耐量子暗号化アルゴリズムですが、シングルコアのコンピュータによるサイバー攻撃によって暗号が解読されました。その数ヵ月後、米国国家安全保障局（NSA）は、現在使われている暗号化アルゴリズムを置き換える暗号化アルゴリズム集として、商用国家安全保障アルゴリズム（CNSA 2.0）を発表しました。これらはすべて、解析を経て、量子コンピュータに対して安全であると判断されたものです。NSA は、これらのアルゴリズムを実装するためのガイダンスと推奨スケジュールを発表しましたが、これらの新しい暗号標準の実装率や成功率を理解するには時期尚早です。

量子コンピューティングは、いずれ暗号化アルゴリズムを解読する能力を獲得しますが、その段階を超えて強力化していくことは間違いありません。量子コンピューティングは処理能力の計り知れない向上をもたらすことから、サイバー犯罪でさらなる活動に利用されるようになると考えられます。例えば、量子コンピューティングを利用して AI を武器化し、それをアプリケーションのファジングに応用して、新たなゼロデイ脆弱性を探し出すような悪質な行為が考えられます。

進化する脅威環境に対する防御

攻撃者の手口は多様化していますが、サイバー犯罪のエコシステムに対抗するためのさまざまな取り組みが行われているという朗報もあります。米国司法省（DOJ）は今年、ランサムウェアオペレーター対策で大きな功績を上げました。1 月には、米国当局の要請により、悪名高いサイバーセキュリティ組織「REvil」のメンバー 14 人がロシア国内で逮捕されました。REvil は Kaseya の攻撃を実行した組織であり、ハッカーの 1 人はコロニアルパイプラインのインシデントにも関与していました。その 1 ヵ月後、仮想通貨取引所から窃取された 119,754 ビットコインの収益のマネーロンダリングで共謀し、2,000 件以上の不正取引を実行した容疑で、2 人がニューヨークで逮捕されました。法執行機関はこれまでに、このハッキングに関連して 36 億ドル以上の暗号通貨を押収しています。

複数の国やベンダーにまたがる連携は、サイバー犯罪組織の特定にも貢献しています。フォーティネットは、世界経済フォーラム（WEF）の Partnership Against Cybercrime（PAC）の設立メンバーとして、サイバー犯罪のエコシステムを解き明かして破壊することを目的とする「Cybercrime ATLAS」プロジェクトを推進しています。FortiGuard Labs は、Microsoft Active Protections Program（MAPP）、Forum of Incident Response and Security Teams（FIRST）、Cyber Threat Alliance（CTA）、INTERPOL Global Cybercrime Expert Group（GCEG）、Gateway Project、NATO Industry Cyber Partnership（NICP）、World Economic Forum の Centre for Cybersecurity、MITRE Engenuity の Center for Threat Informed Defense といった多くの組織とインテリジェンスを共有し、連携しています。

攻撃者や手口を追跡することで、攻撃への対処法を理解しやすくなります。また、暗号ウォレットや通貨の動きを含め、資金の流れを特定することも役立ちます。また、オペレーターだけに焦点を絞るのではなく、アフィリエイトに対する捜査も増えており、「オペレーター以外も訴追される可能性がある」というメッセージとなっています。

このような進展は期待できるものの、現実にはサイバー犯罪者を完全に排除できるわけではありません。しかし、現在確認されている脅威の多くは、攻撃者が長年利用してきた典型的な手口を進化させたものに過ぎません。ゼロデイ攻撃であっても、「ネットワークに侵入して機密情報を窃取する」というサイバー犯罪者の目的は変わりません。大量かつ迅速に実行される脅威への対処は、困難な戦いのように感じられるかもしれませんが、攻撃に使用される手口の大部分は目新しいものではないため、セキュリティチームが対策を取りやすいと言えます。

そこで、環境を守り、犯罪者の一歩先を行くための最善のアドバイスを以下にご紹介します。

サイバー攻撃のライフサイクルを理解する

組織を効果的に防御するためには、サイバー犯罪者、動機、手口、行動様式について理解を深める必要があります。ここで役に立つのが、企業ネットワークに対して APT が一般的に使用する TTP（戦術、手法、手順）を文書化している MITRE ATT&CK フレームワークです。ATT&CK は、セキュリティオペレーション、脅威インテリジェンス、セキュリティアーキテクチャをサポートするための複数の方法を提供します。

サイバーセキュリティメッシュプラットフォームを採用する

とりわけ、ネットワークが拡大し、犯罪者が新たな攻撃方法を編み出している中で、複雑さを軽減してセキュリティの効果を高めるには、統合され自動化された広範なサイバーセキュリティメッシュプラットフォームが不可欠です。従来のサイバーセキュリティの防御は、新たな課題に対応するために、その都度ソリューションを導入してきました。しかし、ポイントソリューションを集めただけでは、現在の状況で効果を上げることはできません。緊密な統合、自動化の促進、ネットワーク全体の脅威に対する高速かつ調整された効果的な保護と対応を実現する上では、単一のサイバーセキュリティプラットフォームへの統合とコンバージェンスが極めて重要となります。迅速で連携した対応を可能にするため、セキュリティソリューションを AI で強化し、攻撃パターンを検知してリアルタイムに脅威を阻止できるようにする必要があります。攻撃の増加に対応できる拡張性も、ソリューションに求められます。理想的には、組織は以下のソリューションを導入すべきです。

- 偵察段階で攻撃に対抗するためのデジタルリスク保護サービス（DRPS）とディセプションテクノロジー
- Web、DNS、C2 の保護
- AI 検知シグネチャを含むアンチマルウェアツール
- 高度侵入防止システム（IPS）による検知
- EDR（Endpoint Detection and Response：エンドポイントの脅威検知とレスポンス ）
- MITRE ATT&CK マッピングによる AI 搭載インラインサンドボックステクノロジー

ソリューションは、理想としては、データセンター、キャンパス、ブランチ、マルチクラウド、ホームオフィス、エンドポイントなど、分散したネットワーク全体で一貫して展開すべきです。

ネットワークセグメンテーションとマイクロセグメンテーションを実装する

ネットワークセグメンテーションは、企業に多くの利益をもたらします。セグメンテーションは、ネットワーク上での攻撃の拡散や保護されていないデバイスへの侵入を防止して、セキュリティを向上させます。攻撃を受けた場合も、マルウェアが他の企業システムに拡散しないように確保できます。

マイクロセグメンテーションは、セキュリティアーキテクトが環境をさらに細分化し、同じブロードキャストドメイン内のすべての資産を水平方向に可視化するネットワークセキュリティ手法です。ネットワーク環境を明確なセキュリティセグメントに論理的に分割して、ワークロードごとのレベルまでの粒度が達成されます。マイクロセグメンテーションによって、個々のワークロードにポリシーが適用されるため、攻撃に対する耐性が向上します。また、侵害が発生した場合でも、侵害したアプリケーションの間でハッカーが移動する能力を制限できます。

FortiGuard Labs について

FortiGuard Labs は、グローバルな脅威インテリジェンスを提供するフォーティネットのリサーチ部門です。悪意のある活動や高度なサイバー攻撃からお客様を保護するために設計された業界最高の脅威インテリジェンスを提供することをミッションとしています。世界各地の専用の脅威リサーチラボに従事する、業界で最も知識の豊富な脅威ハンター、リサーチャー、アナリスト、エンジニア、データサイエンティストで構成されています。FortiGuard Labs は、何百万ものネットワークセンサーと何百ものインテリジェンス共有パートナーを使用して、世界中の攻撃対象領域を継続的に監視しています。FortiGuard Labs は、人工知能（AI）やその他の革新的な技術を使用してこの情報を分析 / 処理し、そのデータから新たな脅威を探し出しています。これらの取り組みがタイムリーで実用的な脅威インテリジェンスとなり、フォーティネットのセキュリティ製品の更新、お客様が直面する脅威と攻撃者の理解を深めるための積極的な脅威リサーチや、セキュリティ対策を強化するための専門的なコンサルティングサービスを提供しています。詳細は、フォーティネットの Web サイト、ブログ、FortiGuard Labs の脅威インテリジェンスページをご覧ください。

[1]「Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021」、U.S. Treasury Financial Crimes Enforcement Network、2021 年 10 月 15 日（英語）：https://www.fincen.gov/news/news-releases/ransomware-trends-bank-secrecy-act-data-between-january-2021-and-june-2021

[2]「フォーティネットの調査で多くの組織のランサムウェア対策の不備を確認」、フォーティネット、2021 年 9 月 29 日：https://www.fortinet.com/jp/blog/business-and-technology/new-fortinet-ransomware-survey-shows-many-organizations-unprepared

[3]「2022 年オペレーショナルテクノロジーとサイバーセキュリティに関する現状レポート」、フォーティネット、2022 年 6 月 21 日：https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ja_jp/report-2022-ot-cybersecurity.pdf

[4]「フォーティネットの調査で多くの組織のランサムウェア対策の不備を確認」、フォーティネット、2021 年 9 月 29 日：https://www.fortinet.com/jp/blog/business-and-technology/new-fortinet-ransomware-survey-shows-many-organizations-unprepared

[5] 同上

[6]「Quantum Computing: An Emerging Ecosystem and Industry Use Cases」、McKinsey and Company、2021 年 12 月（英語）：https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20computing%20use%20cases%20are%20getting%20real%20what%20you%20need%20to%20know/quantum-computing-an-emerging-ecosystem.pdf

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-2023.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

WP-Cyber-Threat-Predictions-for-2023-202302-R1