REPORT

2024 年のサイバー脅威予測

FortiGuard Labs による年次予測

FORTINET

目次

はじめに

攻撃者は常にネットワークを侵害する新しい方法を見つけ出してきますが、常に攻撃を簡単に成功させてきたわけではありません。しかしながら、CaaS（Cybercrime-as-a-Service）市場の成長や生成 AI の普及により、サイバー犯罪者は、かつてないほど簡単に攻撃を始められるボタンを手に入れました。結果として、攻撃者は、自らのツールボックスに入れた新しい機能を積極的に活用し、サイバー犯罪の「時間をかけずに賢く働く」アプローチを拡大することになるでしょう。

今年の脅威予測レポートでは、APT（持続的標的型攻撃）の新時代を検証し、AI がサイバー攻撃のゲームをどのように変えるかを解説し、2024 年の注目すべき新たなトレンドなどを紹介します。脅威環境の今後の変化を予測し、それらの脅威から組織を保護する最善のヒントを提示します。

古くからある戦術の進化

2023 年脅威予測レポートなどで、数多くの攻撃トレンドを何年も前から紹介し、このような多くの攻撃者に支持されてきた戦術がさらに進化を遂げると予測してきました。例えば、持続的標的型のサイバー犯罪が高度化して標的型になり、サイバー犯罪グループ同士の「縄張り争い」が激化し、攻撃における AI の利用方法が変化していていることが確認されています。以下に、2023 年のいくつかの重要な予測を振り返り、脅威環境におけるこれらの長期のトレンドが 2024 年以降にどのように変化するかを予測します。

APT（持続的標的型攻撃）の新時代

数年前から、新たな脆弱性の増加とサイバー犯罪者の攻撃前の活動の活発化というトレンドが重なることで、CaaS 市場が拡大すると予測してきましたが、サイバー犯罪者と APT（持続的標的型攻撃）グループの協力関係が継続している今、ダークウェブにこれまで以上に多くの脅威が存在することは、その予測が的中したことを示しています。

セキュリティ担当者にとって残念なことに、これは氷山の一角に過ぎず、APT 攻撃は増加の一途をたどっています。2023 年上半期に、いくつもの APT グループが活発に活動し、MITRE が追跡している 138 のうちの 41 のグループ（約 30%）の活動がこの期間に確認されました。その中でも最も活動が活発だったのは、FortiGuard Labs によるマルウェア検知数によると、Turla、StrongPity、Winnti、OceanLotus、WildNeutron でした。

今後は、MITRE が特定した 138 のグループや CISA が活動サイクルを紹介しているグループだけでなく、さらに多くの APT グループが「覚醒」して活動し、サイバー犯罪とサイバースパイの二重の活動を開始することになるでしょう。また、もう 1 つのトレンドとして、ステルス性の高い革新的な手法に移行して攻撃を開始する APT グループが増えることが予想されます。HTML スマグリングなどの手法が人気を集めつつありますが、来年はさらに新しい手法が登場することになるでしょう。TTP（戦術、手法、手順）が進化し続け、古い分析方法を採用しているセキュリティ製品を回避するようになっています。新たな CVE（Common Vulnerabilities and Exposures）の当たり年になるのは確実ですが、それと同時に TTP が増加し、結果として MITRE ATT&CK フレームワークも増加することになるでしょう。

APT の進化に加え、サイバー犯罪グループは、攻撃の標的をさらに多様化し、すでに侵害された多くの組織に埋もれている（大きな利益を生む）宝石を探し続けるはずです。例えば、オペレーショナルテクノロジー（OT）分野においては、製造業がサイバー犯罪者の最大の標的になってきましたが、今後は、製造業にとどまらず、医療、公益事業、金融、石油 / ガス、運輸などの業界を標的にする OT 攻撃が増加するでしょう。そして、これらの攻撃は、データの暗号化にとどまらず、標的の恐喝に重点を置くようになるでしょう。攻撃者はさらに、サプライチェーン攻撃を今後も継続し、重要なサービスや組織を混乱させようとするはずです。

2023 年の脅威予測レポートでも、エッジ攻撃が主流になると予測しましたが、この活動が今後はさらに増加することが予想されます。そして、攻撃が増加しただけでなく、攻撃者が標的をさらに多様化し、一般的にエッジデバイスとされているもの以外の標的も攻撃するようになるでしょう。Flipper Zero やそれに類似するツールがあれば、RFID カードやホテルのキーカードを複製し、電話やノート PC などのデバイスで任意コマンドを実行することで、IoT デバイスをハッキングし、金銭を手に入れることができます。最近の例を挙げると、Flipper Zero を使用すれば、USB デバイスを差し込むことなく BadUSB 攻撃を開始できます。不正コマンドの実行にあたって必要なのは、1 人の従業員が Bluetooth で接続することだけであり、ゼロデイを悪用できれば、ユーザーによる操作を必要としない場合もあります。

潜在的な標的が広範囲で、攻撃チェーンの左側の活動が多いため、サイバー犯罪者は、被害者を次々と見つけて利益を得ることができるということです。

サイバー犯罪の縄張り争いの激化

数年前に、複数のサイバー犯罪者が同じ標的に狙いを定め、サイバー犯罪グループ同士が縄張り争いをするようになると予測したことがあります。

今日、複数のサイバー犯罪グループが短期間、時には 24 時間以内に同じ標的に侵入して、AvosLocker、Diamond、Hive、Karakurt、LockBit、Quantum、Royal などのランサムウェア亜種をさまざまな組み合わせで展開しようとしたことは、この予測が現実化した例と言えます。このような攻撃を経験した多くの組織で、数日以内に同様の攻撃が発生しましたが、いずれも異なる攻撃者によるものでした。このことから、他のサイバー犯罪者がダークウェブでのやり取りを注意深く監視して、同じ攻撃を実行したり、ライバルである犯罪者が最初に実行した攻撃に便乗したりしているという仮説を立てることができます。この新たなトレンドが拡大していることから、FBI は今年 2023 年 9 月に発表した警告でセキュリティリーダーに対し、ランサムウェアインシデントに対する組織の防御を見直し、強化するように呼びかけました。

今年の上半期に、MITRE の ATT&CK に分類された手法の 3 分の 2 近くが実際の攻撃で多く使われていることが確認され、防御の回避が戦術として最多であることがわかりました。また、侵害されたシステムでの回避の戦術としてプロセスインジェクションが数多く使われていることがわかりました。窃取された認証情報は攻撃者にとっては、ネットワークに侵入してランサムウェアやその他の攻撃を仕掛けることを可能にするフリーパスのようなものです。犯罪者にとっての窃取された認証情報の重要性を考えれば、認証情報や初期アクセスの仲介サービスという新たなトレンドが将来的に拡大し、攻撃の成功に必要な（場合によっては、同じ標的に対する）認証情報をサイバー犯罪者が手に入れやすくなることが予想されます。このようなサービスが、RaaS（Ransomware-as-a-Service）が市場のギャップを解消する目的で開発されたのと同様に成熟して進化し、ダークウェブで取引されるだけでなく、「商品」として販売されるようになるでしょう。

マネーロンダリングサービスの衰退

サイバー犯罪者が LaaS（Laundering-as-a-Service）を利用して、不正に得た金銭を「洗浄」するようになると予測したことがありますが、その予測通り、多くの犯罪者がこのサービスを利用して、違法な金銭の出所を難読化するようになりました。そのようなロンダリングサービスの 1 つである ChipMixer は、多くの犯罪者に利用されていましたが、2023 年 3 月に当局によって解体されました。その後も、暗号通貨の「ミキサー」や「タンブラー」がいくつも登場しました。親ロシアのハクティビスト活動で知られる脅威グループの Killnet も暗号資産取引所を開設し、ミキサーサービスを提供しています。

しかしながら、ビットコインの多くのミキサーを解体しようとする動きも活発化しているらしく、その人気も連動して低下しているようです。結果として、ハッカーのテレグラムグループのほとんどは、タンブラーの代わりに古くからあるマネーロンダリングのスキームの使用を奨励しています。

攻撃チェーンのあらゆる段階での AI の活用

AI の兵器化が、すでに猛威を振るっている脅威の現状に拍車をかけており、攻撃者は、攻撃のあらゆる段階を強化して、以前より優れた方法で、より速く、攻撃を実行できるようになっています。予想通り、サイバー犯罪者が、ソーシャルエンジニアリングを検知するアルゴリズムの妨害から、AI による音声合成やその他のディープフェイクの作成といった活動を通じて人間の行動を模倣することまで、多くの不正活動を助ける目的で AI を利用するようになっています。

しかしながら、攻撃者の悪知恵がこれで終わるわけではありません。サイバー犯罪者が AI をこれまでとはまったく違う方法で利用するようになることが予想されます。

- 攻撃者は AI を利用して、「生成プロファイリング」、すなわち、ソーシャルプロファイルやその他の公開されている Web サイトから PII（個人情報）を抽出するようになり、それらの情報をサービスとして提供するようになるでしょう。これも、サイバー犯罪者が攻撃を実行するために実施する調査の 1 つの方法です。
- サイバー犯罪者が実用的なモデルを使用して攻撃チェーンのモジュール化を進め、AI を活用した連携型攻撃がこれまで以上にたくさん確認されることになるでしょう。例えば、攻撃者は偵察活動の段階で ML を使用し、それを AI ドリブンの兵器化したペイロードに連携し、さらにそれを兵器化したペイロードの展開に連携する可能性があります。この連携型 AI のアプローチであれば、侵害までの時間を短縮することができます。
- サイバー犯罪者が AI を活用して、パスワードスプレー攻撃を「パワーアップ」するようになるでしょう。パスワードのブルートフォース、スタッフィング、スプレーは、攻撃者が認証情報の識別、窃取、販売の一般的な攻撃方法です。AI を利用してパスワードのパターンやテーマを特定すれば、この可能性が高くなり、攻撃者が短時間で攻撃を成功させることができます。
- サイバー犯罪者が AI モデルの学習データやシステムそのものを意図的に改ざんする AI ポイズニング攻撃が一般的になり、攻撃者は、自動化されたツールキットを使用してこれらのハッキングを実行するようになるでしょう。セキュリティチームは、これらの攻撃からの保護を開始し、侵入防御サービスやアプリケーション制御を活用して自らの AI 資産を保護する必要があります。

2024 年以降の新たな攻撃トレンド

サイバー犯罪者は今後も、目的の達成に繰り返し利用してきた、多くの犯罪者に支持されてきた戦術を使い続けるでしょう。しかしながら、現代の攻撃者は、かつてないほど多くの CaaS や AI ドリブンのテクノロジーなどのツールを自由に利用し、攻撃のあらゆる段階でスマートかつ迅速に攻撃を進められるようになっています。

サイバー犯罪業界の進化に伴い、2024 年以降には、新しい顕著な攻撃トレンドを目にすることになるでしょう。そこで、世界中のセキュリティチームに対する警戒を怠るべきではないという戒めとなる、いくつかの予測を紹介します。

攻撃の破壊力や規模の拡大

サイバー攻撃のタイプに人気投票があるとしたら、ランサムウェアは間違いなく首位に君臨するはずです。数年前から、ランサムウェア攻撃の件数が世界中で急増し、あらゆる規模、あらゆる業種のあらゆる組織が標的になっています。2023 年上半期の FortiGuard Labs グローバル脅威レポートによると、2023 年上半期の終了時に、年初の 13 倍のランサムウェア活動を記録しました。ビジネスリーダーの 78% がランサムウェア対策をしていると回答したにもかかわらず、半数がランサムウェアの被害に遭っています。

攻撃者は、2023 年のサイバー脅威予測レポートで紹介した、破壊力の大きいディスクワイピングマルウェアなどの高度で複雑なネットワーク侵入手法を採用することで、その手口をさらに進化させていますが、これには、RaaS の急速な拡大が大きく貢献しています。しかしながら、高額の報酬を期待してランサムウェア攻撃を仕掛けるサイバー犯罪者の増加に伴い、サイバー犯罪グループは、小規模で簡単にハッキングできる標的から急速に撤退し、方向転換しています。

結果として、サイバー犯罪者がこれまで以上に攻撃的になり、標的の候補とプレイブックの両方を拡大することが予想されます。大きな報酬を得ようとするサイバー犯罪者は、医療、公共事業、製造、金融などの重要産業を重点的に攻撃し、混乱させることができれば社会に多大な負の影響をもたらすことになる標的を追い求めるようになるでしょう。価値の高い標的に狙いを定めることに加え、攻撃者はすでに確立した手法以外も駆使して攻撃するようになるでしょう。手口がさらに攻撃的で破壊的になり、暗号化の代わりにサービス拒否や恐喝に重点を置くようになるでしょう。

価値の高い標的を狙うとはいえ、いずれはこの標的のリストが枯渇します。そこで、サイバー犯罪者が誰を（あるいはどの業界を）標的にするかという疑問が生じます。戦略の調整を迫られた攻撃者が、サイバー保険加入組織を魅力的な標的と考えるようになる可能性もあります。数年前からのトレンドとして、戦略の足りない部分を補う目的でサイバー保険に加入する組織が増えていますが、ランサムウェアの激化に伴い、サイバー保険会社は、保険金支払いの可否や金額を厳しく審査するようになっています。サイバー保険会社の審査がさらに厳しくなって、身代金が支払われる頻度が低くなれば、いずれはその金額が減額されることになるでしょう。サイバー保険会社が攻撃の直接の標的になった例は今のところ確認されていませんが、特に保険会社によって加入組織への支払いが制限されるようになれば、将来的にサイバー保険業界が価値の高い標的とみなされるようになる可能性はあるでしょう。

ゼロデイと攻撃者に多くの利益をもたらす N デイ

組織が日常業務のサポートに利用するプラットフォーム、アプリケーション、テクノロジーの数が増加し続けていることから、サイバー犯罪者には、ソフトウェアの脆弱性を発見して悪用する新たな機会がたくさんあります。これを裏付けるように、ゼロデイと新たな CVE（共通脆弱性識別子）が 2023 年に過去最多を記録し、その数は今も増加し続けています。数ある CVE の 1 つである MOVEit Transfer ハッキングは、少なくとも 6,000 万人に影響し、「現段階で今年最大のハッキング」とされています。新たに発見されるゼロデイは多くの利益をもたらしますが、その価値の高さから、その多くは恐らく報告されません。報告されないゼロデイは攻撃者にとって間違いなく価値が高いです。なぜなら、多くの人々がまだ気がついていないゼロデイを悪用することで、犯罪者はより多くの利益を上げられるからです。セキュリティチームは、これまで以上の警戒が必要です。そして、忘れてはならないのが、有効期間が延びたゼロデイと言うべき N デイの急増です。このような脆弱性は、長期間、場合によっては数年にわたってリスクをもたらす可能性があります。N デイは既知の脆弱性ではありますが、パッチが適用されていなかったり、適用できるパッチがなかったりすれば、組織にとってのリスクであることに変わりありません。

ゼロデイ攻撃がすぐに減速することはなく、ダークウェブで複数の買い手にゼロデイを販売するサイバー犯罪グループであるゼロデイブローカーが CaaS コミュニティに登場することになるでしょう。そして、そのようなゼロデイブローカーの登場によって、サイバー犯罪者が活動を拡大し、協調型の大規模攻撃で広範囲の攻撃対象領域を標的にするようになるでしょう。このような攻撃への移行が予想されるのは、保護が不十分な製品によって攻撃対象領域が拡大し、何万もの CVE を攻撃者が発見して悪用する機会があるためです。

次世代ファイアウォールの使用、脆弱性スキャンの実施、スマートパッチ管理戦略の実装などの、ゼロデイ脆弱性から保護するために組織が今すぐ実行できる対策はたくさんありますが、これらのツールや活動はいずれも、発見された脆弱性からの保護を前提にしています。エンジニアリングチームは、SDL（ソフトウェア開発ライフサイクル）手法を強化することで、ゼロデイエクスプロイトの増加を減速させることができます。サイバー犯罪者は、ソフトウェアのバグを発見するための自動ソフトウェアテスト手法であるファジングを使用して、悪用できる新しい脆弱性を探しますが、開発チームもファジングを使用することで攻撃者に対抗できます。開発者は、SDL プロセスにファジングを組み込むことを検討する必要があり、そうすることで、製品やセキュリティの強化に役立ち、潜在的なバグを攻撃者に先行して発見し、修正することができます。

内部関係者のリクルーティング

脅威環境の進化に伴い、多くの企業が、セキュリティを強化し、新しいテクノロジーやプロセスを採用して、自らの防御を強固なものにしようとしています。このような取り組みによって、攻撃者が外部からネットワークに侵入するのが困難になれば、サイバー犯罪者は、標的に到達する新たな方法を見つける必要があります。

このような変化を考えれば、攻撃者が戦術、偵察、武器化のプロセスをシフトレフトさせて、初期アクセスを手に入れるために標的である組織の内部の誰かをリクルーティングしようとするグループが現れることが予想されます。例えば、サイバー犯罪者は生成 AI を利用して、企業の重役や信頼できる個人の声を簡単に生成し、それを録音して、疑うことを知らない標的にコマンドを実行させたり、パスワードやデータを開示させたり、金銭を要求したりすることができます。このトレンドの次の段階として、Recruitment-as-a-Service が進化し、攻撃者が標的のプロファイリングに利用する多くの情報にアクセスできるようになることは、想像に難くありません。

知らぬ間にサイバー犯罪の被害者になってしまう標的もいますが、サイバー犯罪者と一度だけ協力して手っ取り早く小遣い稼ぎをしようと考える従業員がいないとも限りません。

大規模イベントに便乗する攻撃

2024 年には、多くの攻撃者が、米国大統領選やパリで開催される夏季オリンピックなどの大規模イベントに乗じた攻撃を仕掛けることが予想されます。攻撃者はこれまでも、大規模イベントを妨害したり、地域紛争に乗じて攻撃を開始したりしてきましたが、サイバー犯罪者たちは今や、自由に攻撃に利用できる新しいツール、中でも生成 AI という強力なツールを手に入れました。関係者はすでに、次の選挙における AI の脅威について警告しており、このテクノロジーがオンラインでの偽情報の拡散を加速させる可能性が高いと述べています。パリで開催される夏季オリンピック大会の観客や視聴者は、ファン心理につけ込んだ詐欺の被害者になる恐れがあります。また、競技の計測、管理、放送にテクノロジーが多用されるようになっていることから、それらのシステムが標的になる可能性も高くなっています。

しかしながら、大混乱を発生させる機会は、このような大規模イベントだけではありません。リソースが少ない地方自治体がかなり前からサイバー攻撃の標的になっていますが、攻撃者は、これらの組織にも侵入する新たな方法を探すようになるでしょう。例えば、ML と AI を活用すれば、サイバー犯罪者が地域に合わせて簡単に攻撃をカスタマイズし、大規模な言語モデルを使用してコミュニケーションをその地域の言語に翻訳できます。

TTP の活動の場を限定する

攻撃者が標的を侵害する目的で使用する戦術、技術、手順（TTP）が増え続けるのは、恐らく避けられないことです。しかしながら、活動の場を限定し、活動を妨害する方法を見つけることで、防御側が優位に立つことができます。

サイバーセキュリティの防御側の日常的な作業のほとんどは、侵害指標のブロックに関連するものですが、攻撃者が自らのプレイブックを強化する目的で使用することの多い TTP に注目し、攻撃モデルを分断できる箇所を見つけることには、大きな価値があります。攻撃者には、ランサムウェアやフィッシング攻撃を実行するさまざまなツールキットがあるかもしれませんが、その手法は多くの場合に似たものです。防御側は、攻撃者の行動をマッピングし、そのインテリジェンスをセキュリティコミュニティで共有し、特定の手法を軽減することができます。

MITRE Engenuity の Center for Threat-Informed Defense が主導し、フォーティネットなどの複数のパートナーが参加する Attack Flow プロジェクトは、攻撃者の TTP の活動の場を限定するのに役立つ情報をセキュリティ担当者に提供しています。プロジェクトの参加者は、犯罪者が攻撃の一部として実行するステップを文書化することで、セキュリティコミュニティが戦いの場で攻撃者を追い詰める機会を見つけるのに役立つデータモデルを作成しています。サイバー犯罪者の活動が高度化し、従来の検知手段を巧みに回避するようになっているため、その活動を妨害できる可能性のある場所の特定がこれまで以上に重要になりました。

攻撃手法の長期的な変化

かつては、OT システムなどのエッジデバイスがサイバー犯罪者に攻撃されることはそれほどありませんでしたが、この 10 年間で、これらを標的にする攻撃が高度化し、その数も増加しました。数年前に、エッジ環境を標的にするエッジアクセスのトロイの木馬が増加すると予測したことがありますが、それが現実化した例がいくつか確認されています。

Lynk Global によって、5G によるデバイスのダイレクト接続が現実のものになりました。さらには、低軌道衛星空間が混み合ってきていることは、以前はオンラインではなかったデバイスへの接続が増えていることを意味します。当然ながら、接続デバイスが増えれば、攻撃対象領域が拡大し、侵害の無限の機会を攻撃者が手にすることになります。5G インフラストラクチャに対する攻撃が成功すれば、石油 / ガス、運輸、公共安全、医療などの重要産業が簡単に混乱に陥る恐れがあります。

集団的レジリエンスを強化して、進化し続ける脅威から保護する

サイバー犯罪者は、組織をハッキングする、より高度で新しい方法を次々と見つけるはずですが、それでも、サイバー犯罪者の次の動きを予測し、その活動を妨害するために、セキュリティコミュニティでできることはたくさんあります。官民協力の強化からインシデント報告標準の厳格化までの、サイバー犯罪に集団で対抗するいくつかの方法を以下に紹介します。

パートナーシップはサイバー犯罪との戦いに不可欠である

サイバー犯罪はすべての人に影響し、侵害の影響は多くの場合に広範囲に及びます。業界としてできる最も有効な活動の 1 つが、情報共有を容易にするためのパートナーシップの構築です。

官民どちらにおいても、知識とベストプラクティスを共有することで攻撃者を混乱させる多くの取り組みが進行中です。しかしながら、やるべきことはまだまだ残されており、誰にも果たすべき役割があります。フォーティネットは、さまざまなグローバルパートナーシップに重要なリソースを投資しており、世界経済フォーラム（WEF）の Partnership Against Cybercrime（サイバー犯罪に対抗するパートナーシップ）にも積極的に参加しています。さらには、フォーティネットは WEF と協力して、Cybercrime Atlas を 2023 年初めに立ち上げましたが、これは、サイバー犯罪のグローバルなエコシステムやインフラストラクチャに新たなレベルの可視性を提供することで、攻撃者を分断しようとする業界、法執行機関、政府機関を支援するプロジェクトです。

政策改定に関する予定 / 予測

強力なパートナーシップは、サイバー犯罪と優位に戦うためのパズルの 1 ピースにすぎません。2024 年以降に、特定の業種におけるサイバー防御の強化の義務化から、インシデント報告に関するより強固な標準の実装までの、いくつかの政策改定案が提出されることが予想されます。

各国政府が重要インフラの脆弱性や相互接続性を正しく理解するようになってきているため、「重要」に分類されるシステムが増えることになるでしょう。ほとんどの重要インフラが民営であることから、これまでより厳しい要件が新たに導入され、重要インフラを運用する組織は、より強固なサイバー防御の維持を強いられることになるでしょう。

また、政府機関が標準化されたインシデント報告の必要性を認識し、報告の要件を統一する取り組みを進めているのも、心強いことです。米国の CISA（Cybersecurity and Infrastructure Security Agency）は来年前半に、Cyber Incident Reporting for Critical Infrastructure Act of 2022（重要インフラのサイバーインシデント報告法）に基づき、インシデント報告を義務化する予定です。米国の DHS（国土安全保障省）が最近発表したレポートには、政府機関が共通の用語を使って共通のレポートプラットフォームを構築し、最終的により良い情報共有を可能にするための作業テンプレートが紹介されています。インシデント報告に関する法規制やテンプレートがどのように進化し、DHS のこのレポートが CISA の最終要件でどのような役割を果たすのかに注目することにしましょう。

サイバーセキュリティの側面に重点を置いた、報告や責任ある情報開示などの法規制の導入は、サイバー犯罪者の活動の阻止に不可欠です。法規制がないために、企業が悪意の目的に使用できるツールやサービスの販売を許してしまっている例がいくつもあります。例えば、NSO Group とライバル企業の QuaDream はどちらもハイエンドの監視ソフトウェアを世界中の顧客に販売する企業ですが、悪意の目的でこれらの企業の監視ソフトウェアを利用する顧客もいるでしょう。

組織はサイバー犯罪エコシステムの解体で大きな役割を果たす

グローバルなサイバー犯罪への対抗にコラボレーション型のパートナーシップと強力な法規制が不可欠であるのと同時に、エコシステムの解体においてはすべての組織が極めて重要な役割を果たします。これは、全社的なサイバーセキュリティ教育プログラムやエグゼクティブ向けの机上演習のような対象者を限定した活動などの継続的な取り組みを実施することで、サイバーセキュリティという仕事に全員が参加する、サイバーレジリエンスの文化の創造から始まります。新たな人材プールの活用などのサイバーセキュリティのスキルギャップを解消する方法を見つけることで、企業は、IT やセキュリティの担当者の長時間勤務や脅威の増大という問題を解決することができます。脅威の共有は、保護の迅速な準備に役立つことから、その重要性は将来的にさらに大きくなるでしょう。

エコシステムとしての集団的な脅威に対するレスポンスには、サイバー犯罪や攻撃の阻止でより大きな効果があり、組織は、この分断で重要な役割を果たすことを理解する必要があります。

FortiGuard Labs について

FortiGuard Labs は、2002 年に設立されたサイバーセキュリティの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。この分野のパイオニアで、セキュリティ業界のイノベーターでもある FortiGuard Labs は、機械学習と AI の最先端のテクノロジーの開発と活用により、タイムリーかつ一貫した方法でトップクラスの保護と実用的な脅威インテリジェンスをお客様に提供しています。FortiGuard Labs は、フォーティネットの膨大な数のセンサー（世界中に 600 万以上のデバイスを配備）から収集されるテレメトリーに基づくデータを活用して、今日の組織が直面している実際の脅威を可視化しています。

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/white-papers/ja_jp/wp-cyber-threat-predictions-for-2024.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-2024-202312-R1