REPORT

2023 年ランサムウェア グローバル調査レポート

概要

フォーティネットは先日、世界中のあらゆる規模 / 業種の組織の 569 人のサイバーセキュリティリーダーおよび意思決定者を対象に、ランサムウェアついての認識、ランサムウェアの自らの組織に対する影響、潜在的な攻撃を減災するための戦略についての調査を実施しました。今年の調査では、80% 以上の回答者がランサムウェアの脅威を「とても大きな」または「極めて大きな」懸念事項であると回答しましたが、調査対象組織のほぼ同数（78%）が、侵害を阻止するための備えを「かなり準備している」または「最大限準備している」と考えていることもわかりました。こうした懸念や備えにもかかわらず、調査対象組織の半数がランサムウェアの被害を受けています。

78% の組織が攻撃を減災するための自らの備えを「かなり準備している」または「最大限準備している」と回答したにもかかわらず、50% の組織が過去 1 年間にランサムウェアの被害を受けたことがわかりました。

ランサムウェアインシデントを経験した組織の 72% が数時間以内（多くは数分以内）にインシデントを検知したにもかかわらず、71% が要求された身代金の少なくとも一部を支払ったと回答しています。また、ほぼすべての回答者がサイバー保険に加入していましたが、被害額の全額の補償もデータの復元も保証されるわけではありません。事実、ランサムウェアの被害を受けた組織でインシデントの後にすべてのデータを復元できた組織は 35% に過ぎません。

しかしながら、すべてが悲観的な結果だったわけではありません。経済の不透明さにもかかわらず、調査対象のほぼすべてのリーダー（91%）が、翌年のセキュリティ予算を増額して、潜在的なランサムウェア攻撃からネットワークの保護を強化するテクノロジーやサービスに投資する予定であると回答しました。全体として、セキュリティリーダーは、脅威の迅速な検知を可能にする、AI（人工知能）や ML（機械学習）を活用した高度なテクノロジーの実装を最優先事項として挙げ、次いで、一元監視による迅速なレスポンスという回答が続きました。具体的には、セキュリティリーダーが投資を予定している分野や製品として多く回答したのは、IoT セキュリティと NGFW（次世代ファイアウォール）で、EDR（エンドポイントの脅威検知とレスポンス）と SEG（セキュアメールゲートウェイ）ソリューションの実装を計画している、という回答が最も増加しました。ランサムウェア攻撃における侵入で使用された方法として回答者が挙げた 1 位がフィッシングメールであったことから、これは有効な計画であると言えるでしょう。当然ながら、ランサムウェアが最終的に標的にするのはエンドポイントです。

多くのセキュリティリーダーがプロジェクトごとに最適な個別の製品を購入することで最強のサイバーセキュリティ態勢が実現すると従来から考えてきましたが、今年の調査データで、ポイント製品のアプローチを採用していると回答した組織がランサムウェアの被害者になる可能性が最も高いことがわかりました。しかしながら、テクノロジーはソリューションの一部にすぎず、今回の調査で、ランサムウェアの防止の最重要課題として回答が多かったのは、人とプロセスに関するものでした。

ランサムウェアの急増と攻撃者の手法の高度化に伴い、あらゆる形態と規模の組織が標的になるため、セキュリティリーダーには、テクノロジー、人、プロセスに正しく投資することで、将来のランサムウェアインシデントを防止することが求められています。

ランサムウェアの高度化であらゆる組織が標的になる

ランサムウェアは数十年前から存在しますが、この世界的な脅威は今なおピーク時のレベルを維持しています。また、ランサムウェアは常に進化しており、組織への被害は世界中で増大するばかりです。FortiGuard Labs のインシデントレスポンス（IR）チームは、2022 年に発生したインシデントの中で、金銭目的のサイバー犯罪が最も多く（74%）、その内 82% のケースではランサムウェアまたは不正スクリプトが送り込まれたことを確認しました [1]。

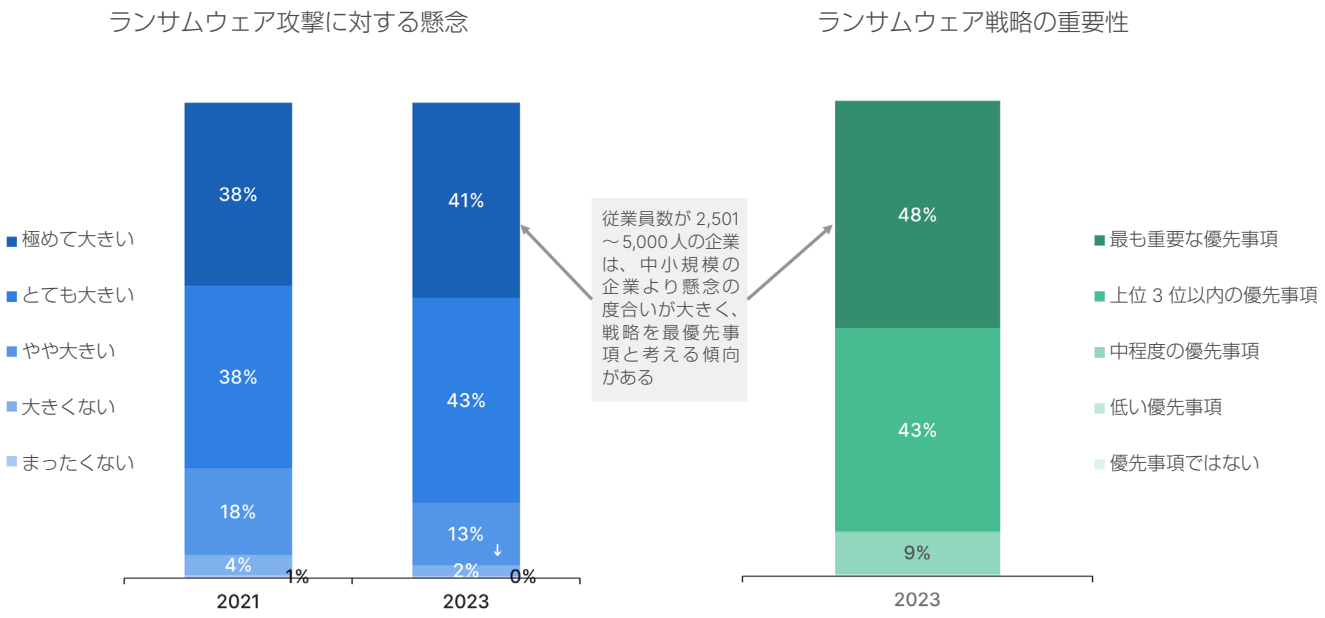
2021 年にランサムウェアの件数が爆発的に増加しましたが、2022 年にはその増加率は低下しました。しかし、その件数は依然として急速に増加しています。例えば、FortiGuard Labs は 2022 年上半期に、前半期の 2 倍となる 10,666 の新しい亜種を確認しました [2]。おそらくはこれは、RaaS（Ransomware-as-a-Service：サービスとしてのランサムウェア）の成熟に伴い、サイバー犯罪者がこれまで以上に高度で攻撃的な新しい亜種の展開に成功したためでしょう。また、高額の身代金を得られる可能が高い組織を標的にするようにもなっています。RaaS の初期の成功は、数で勝負する、すなわち、アフィリエイトを増やしてネットワークへの侵入や攻撃の機会を増やすというものでしたが、RaaS の運営者は、攻撃への参加者を選別するようになっています。

このように、ランサムウェア攻撃を体系的に実行することで大きな成功を収めるようになっています。具体的には、偵察に時間をかけて有利な標的を特定するようになっており、数千万ドルの身代金を要求する場合も多くなっています。さらには、全体の傾向として、これらの集団が標的に要求する身代金は、組織の規模や業種に見合うものになってきています。多くのサイバー犯罪組織は、被害者が支払いに応じる可能性を高くするために、被害組織の規模に応じて要求金額を決めています。

RaaS が CaaS（Crime-as-a-Service：サービスとしての犯罪）拡大の重要な要素であることを考えると、このようにランサムウェア攻撃の成熟度が向上するのは予想されることです。しかしながら、RaaS の運営者がさらに積極的な作戦に転じてワイパーを使用するなどの破壊的な要素を攻撃に取り入れるようになっているため、あらゆる形や規模の組織が、潜在的な侵害を減災する適切なセキュリティ戦略を導入する必要があります。

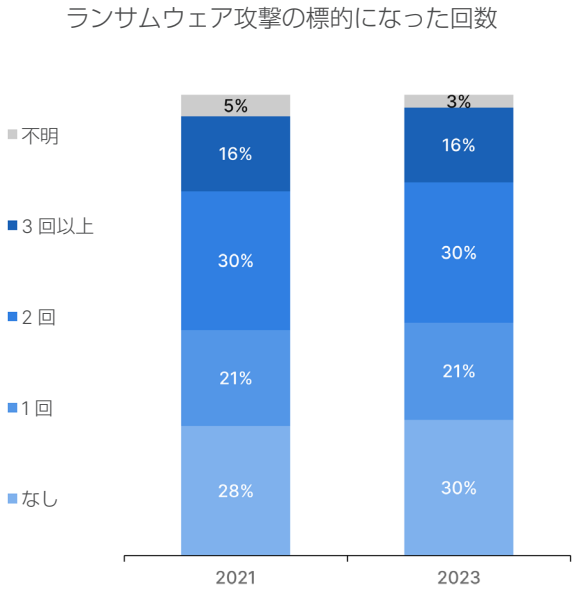
あらゆる場所に現れ、高いコストを強いるランサムウェア攻撃

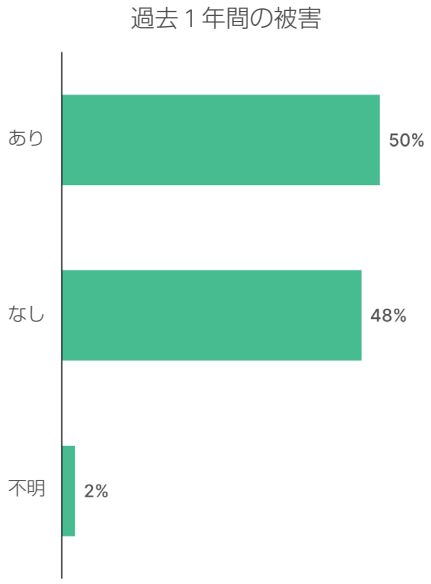
ランサムウェアの戦術の進化と高度化を考えれば、今年の調査にご協力いただいた組織の 84% が、ランサムウェアが「とても大きな」あるいは「極めて大きな」懸念事項であると回答し、2021 年の調査の 76% からさらに増えたことに驚きはありません。しかしながら、大きな懸念事項であるにもかかわらず、78% が、ランサムウェア攻撃の防止または減災の備えを「かなり準備している」または「最大限準備している」と考えていることもわかりました（前回の調査での 63% から大幅に増加）。事実、調査対象者の 90% 以上が、ランサムウェア戦略の実装は自らのチームの最優先事項あるいは上位 3 位以内の優先事項であると回答しました。また、88% がサイバー攻撃対策戦略の一部としてサイバー保険に加入していることもわかりました。



現実として、回答者の組織の備えとランサムウェアインシデントを阻止する能力に大きな隔たりが今もあることが明らかになりました。今年の調査対象企業の半数が過去 1 年間にランサムウェア攻撃の被害を受け、46% がランサムウェアに 2 回以上攻撃されたことがわかりました。

2022 年にランサムウェア攻撃の被害を受けた調査対象組織に対する攻撃方法で今回も最多だったのが、不正 E メールで個人やグループを標的にするフィッシング（56%）で、脆弱なネットワークサービス経由のアクセス（54%）、リモートデスクトッププロトコルのエクスプロイト（51%）がそれぞれ、2 位と 3 位に入りました。回答者の 50% 以上が複数の方法を回答したことから、ランサムウェアの攻撃者が同じ攻撃や後続の攻撃の一部として複数の侵入方法を試行するようになっているようです。





ランサムウェア攻撃を受けた調査対象企業の多くは、身代金を要求された場合の支払いに関する規定を設けています。注目すべきは、大半（72%）が数時間、場合によっては数分以内にインシデントを検知したにもかかわらず、70% 以上が、攻撃者が要求した身代金の少なくとも一部を支払ったと回答したことであり、これは、身代金の支払いに応じることは問題を助長するだけでなく、データを回復できる保証はないとする FBI の指導に反するものです [3]。

興味深いことに、特定の業種の組織が身代金を支払う可能性が他の業種より高いことがわかりました。例えば、製造業は他の業種よりも要求された身代金を支払った場合が多く、要求金額も一般的に高額で、事実、製造業での侵害の 25% で 100 万ドル以上の身代金が要求されました。ダウンタイムのコストが非常に大きいことを考えると、この業種で支払いに応じる可能性が高くなるのも納得できることであり、標的である企業に支払い能力があることを知っているからこそ、攻撃者は多額の身代金を要求するのです。

しかしながら、身代金を支払うことも、サイバー保険で損失を補償されると期待することも、攻撃を減災する有効な戦略ではありません。事実、回答者の 65% が、攻撃後にすべてのデータを復旧できなかったと回答しました。さらには、サイバー保険に加入している組織の半数近く（41%）が期待したほどの補償金を受け取ることができず、保険会社の免責条項によって補償金がまったく支払われなかったという回答もありました。

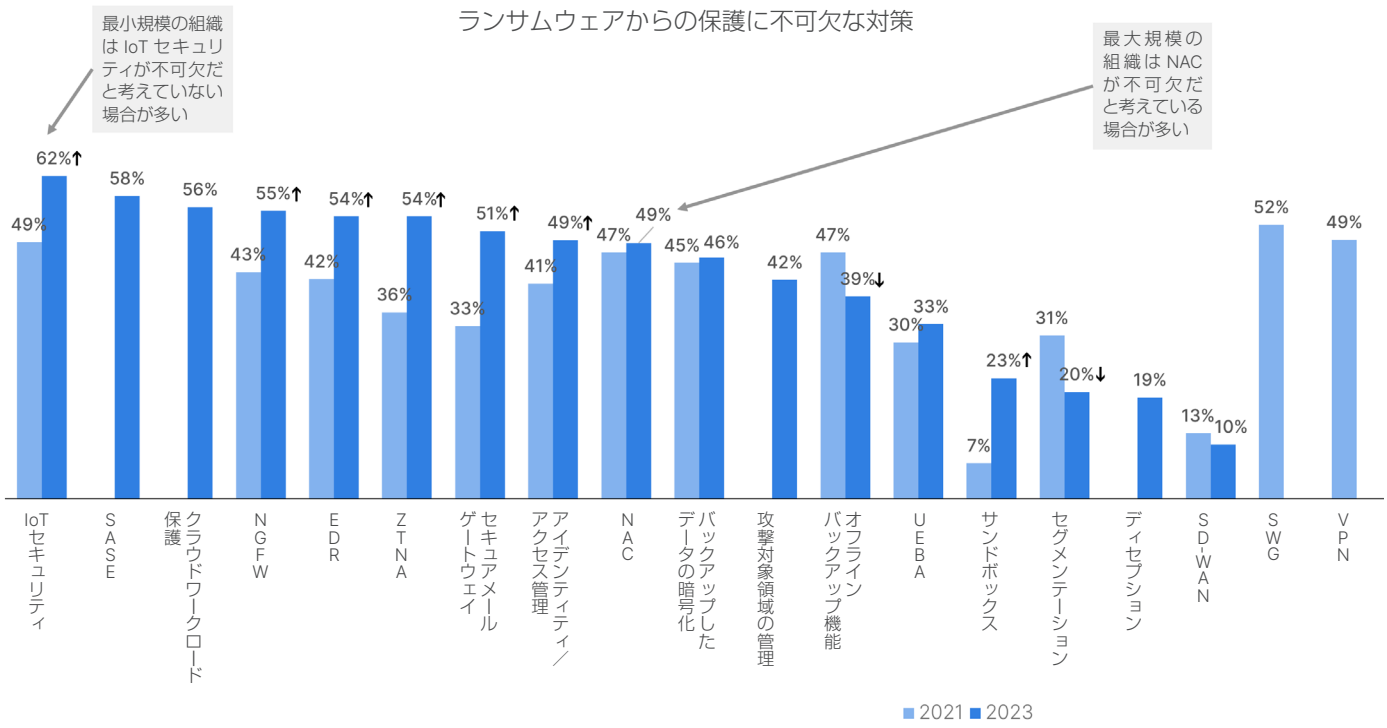
組織は積極的にランサムウェア対策に取り組んでいるが、多くの企業は必要不可欠な保護に優先して取り組んでいない

今回の調査で 2 回連続、脅威環境が高度化し、制御できなくなっていることが、攻撃の防止における課題として最多の回答になりました。しかしながら、これに次ぐ、「ランサムウェア攻撃に対するネットワークの適切な保護が明確でない」、「サイバーセキュリティに対するエンドユーザーの意識が欠如している」、「指揮系統が明確でない」、「従業員がソーシャルエンジニアリングに騙されないようにするのが困難である」という 4 つの課題はいずれも人とプロセスに関連するものであり、ランサムウェア攻撃への備えについての捉え方と矛盾するようです。その一方で、明るい材料として、2021 年に上位だった懸念事項、例えば、「増加するリモートワークの保護が複雑である」という回答は、今年の調査では上位に入りませんでした。

一般的な経済状況にもかかわらず、91% の組織が、来年のセキュリティ予算の増額を見込んでおり、その多く（42%）が 10% 以上の増額を予想していることから、ランサムウェアの課題を解決するための投資が可能であることも、明るい材料と言えるでしょう。また、自らの組織を保護するため、セキュリティチームは、サイバーセキュリティテクノロジーの追加に投資し、攻撃を法執行機関攻撃に報告する頻度を増やし、必要に応じてサイバー保険を利用していると回答しています。

ランサムウェアの減災についての回答で、目立った投資はありませんでした。その代わり、ランサムウェア攻撃からの保護には、さまざまなソリューションが必要であるという回答が挙がりました。調査対象者の半数以上が、IoT セキュリティ、SASE、クラウドワークロード保護、NGFW、EDR、ゼロトラストネットワークアクセス（ZTNA）、SEG を、自らの戦略に不可欠なセキュリティテクノロジーとして回答しました。2021 年の調査と比べると、ZTNA と SEG の両方を不可欠なツールとして挙げた回答者が 20% 近く増加しました。このような意識の変化が朗報と言えるのは、フィッシングが今なお組織のネットワークにアクセスする最も一般的な攻撃ベクトルであり、きめ細かいコントロールを導入してアプリケーションとデータの利用を管理することが重要なベストプラクティスであるためです。

ただし、企業がこれらの広範なセキュリティテクノロジーを採用するのは素晴らしいことです。しかし一方では、興味深いことに、サンドボックス、ネットワークセグメンテーション、データのオフサイトへの保存などの、ランサムウェアからの防御に不可欠なこれ以外の保護に対する認識は十分ではないようです。



「重視していること」だけでなく、「今後の投資予定」についても質問しました。ランサムウェアから保護する新しいツールを評価する場合、自社における現在のセキュリティ態勢を理解してギャップを特定することが、追加投資の前の重要な第一歩になります。MITRE ATT&CK フレームワークなどのツールを使用して、現在の防御を攻撃チェーンにマッピングすることで、これが可能になります。このようなアプローチは、ランサムウェアに対する最も効果的な防御策を講じたかどうかの確認や、どのような潜在的なセキュリティギャップを解消する必要があるかを理解するのに役立ちます。

回答者が計画しているとして挙げた上位 3 位までの投資は、IoT セキュリティ（57%）、NGFW（53%）、EDR（51%）でした。フォーティネットの前回の調査結果で最も意外だったのは、2021 年の侵入方法の首位が E メールフィッシングだったにもかかわらず、その防御を強化する計画があると回答した組織がわずか 3 分の 1 だったことです。E メールフィッシングが侵入方法の首位になったのは 2022 年が 2 度目でしたが、組織がこの分野に計画通りに投資しているとすれば（2021 年の 31% から 2022 年には 47% に増加）、減少に向かうことを期待できそうです。

集約と統合の必要性

企業がテクノロジーに投資してランサムウェア対策を講じているのは良い傾向です。しかし現実として、すでにツールの数が過剰である状況でさらにツールを追加するだけでは、多くの場合に攻撃されるリスクの軽減に十分ではありません。セキュリティプラットフォームとポイント製品の両方を使用しているという回答が 45% と増加しましたが、36% は引き続き最良とされるポイント製品のみを購入していることがわかりました。結果として、多くのセキュリティチームが、時間をかけて個別の製品を導入した後に管理にも多くの時間を費やし、いくつものテクノロジーを効果的に連携させて運用しようと苦労することになります。また、このような手動プロセスでは、セキュリティチームによる適切なデータの収集やランサムウェアインシデントへの迅速なレスポンスの能力が阻害されてしまう可能性があります。

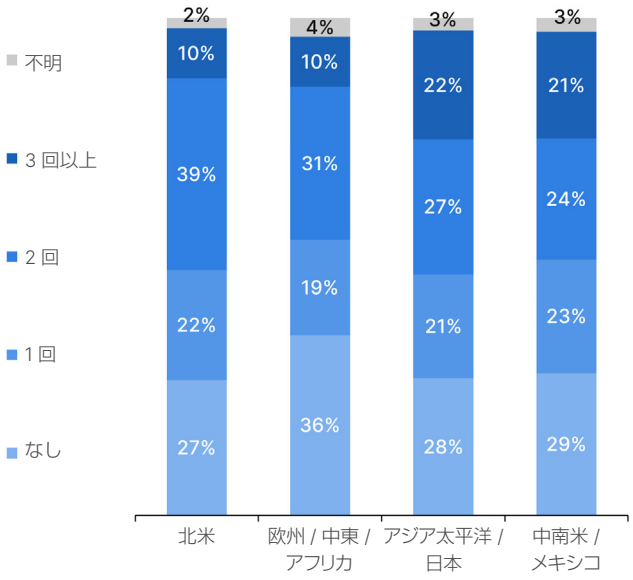
興味深いことに、最良とされる製品を使用するアプローチを採用していると回答した組織がランサムウェア攻撃の被害を受けた確率が高く（67%）、少数のプラットフォームに統合してポイント製品を補完することでベンダーのオーバーヘッドを減らした組織で被害が少なかった（37%）ことがわかりました。ポイント製品の数を減らして少数の戦略的プラットフォームを活用する組織が増えていることがわかります。今回の調査結果は、ほぼすべての回答者（99%）が統合ソリューションやプラットフォームがランサムウェア攻撃の防止に不可欠であると考えていることを裏付けるものでした。さらには、テクノロジーだけでなく、これらのプラットフォームを最大限に活用するための人やプロセスも重要です。

国や地域別に見る、ランサムウェア攻撃に対する認識と備え

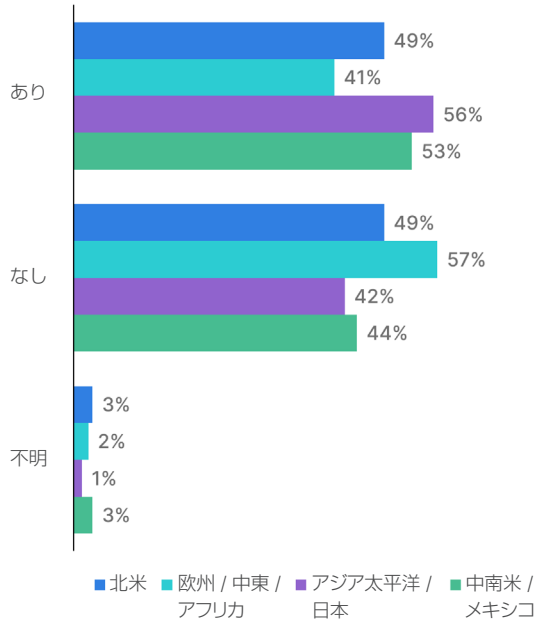
ランサムウェアに対する組織の認識、懸念、備え、最重要課題の度合いについては地域差が少なく、世界中のほぼすべての回答者が、ランサムウェア戦略の策定が最重要優先事項であるか、最重要事項の 1 つであると回答しました。同様に、いずれの地域でも早期の検知とレスポンスのツールを多くの組織が導入し、ほとんどが最良とされる製品を購入し、ほぼすべてがサイバー保険に加入していることがわかりました。

しかしながら、過去 1 年間にランサムウェア攻撃を受けた企業の割合は地域によって大きく異なり、アジア太平洋 / 日本（APJ）が最多（56%）で、欧州 / 中東 / アフリカ（EMEA）が最少（41%）でした。

ランサムウェア攻撃の標的になった回数



過去 1 年間の被害



件数だけでなく、攻撃を検知する速さや、要求された身代金を支払うべきだと組織が感じるかどうかなどといった、攻撃への対応にも地域差があります。例えば、中南米 / メキシコ（LATAM）は他の地域より攻撃を検知するのが早く、ソーシャルエンジニアリングに騙されることが少ない傾向がありました。セキュリティツールの実装については、北米（NA）と EMEA の回答者の方が APJ や LATAM の回答者より ZTNA への投資を計画していることがわかりました。身代金の要求額については、EMEA の要求額が他の地域より低く、約半数の回答者が要求された身代金の支払いに応じなかったことがわかりました。APJ の組織で、身代金の要求額が高く、44% が要求された全額を支払ったと回答しました。

今後の計画：セキュリティ戦略の強化

最後に、ランサムウェア対策としてこれから投資を計画しているセキュリティテクノロジーの分野を回答者に質問しました。注目すべきは、回答者の 50% が 1 位に挙げた領域で、AI や ML を活用する高度テクノロジーの採用が優先事項の 3 位までに入ったことです。セキュリティリーダーはさらに、セキュリティ情報 / イベント管理（SIEM）やセキュリティオーケストレーション / 自動化 / レスポンス（SOAR）など一元監視ツールを優先的に利用することで、迅速な検知とレスポンスを可能にしようとしています。回答者はさらに、新しいテクノロジーの評価で「非常に重要」とする属性として、実用的な脅威インテリジェンスを活用するソリューション（50%）、AI ドリブンの振る舞い検知が可能なソリューション（48%）、連携を前提に設計されているソリューション（45%）を挙げました。

最良とされるポイント製品を使用するアプローチをセキュリティに採用していると回答した組織はランサムウェアの被害に受けた確率が最も高く（67%）、テクノロジーを統合したプラットフォーム ドリブンのアプローチを採用している組織で侵害された確率が最も低く（37%）なりました。

たとえ経験豊富なセキュリティ専門家がいる組織であっても、成熟度の高いサイバー犯罪エコシステムを自力で阻止するためには対策を追加する必要があると組織が認識していることは、良い傾向と言えるでしょう。ランサムウェアの試行を阻止するには、攻撃のサイバーキルチェーンの早い段階で検知を可能にするテクノロジーを導入することが重要です。

しかしながら、セキュリティテクノロジーに関して言えば、必ずしも数の多さが強さを意味するわけではないことを認識する必要があります。多くのチームがあまりに多くの時間を費やして多種多様なポイント製品をチューニングし、結合させており、結果として、企業の保護を担うアナリストが不要な負担を強いられることがあります。セキュリティメッシュアーキテクチャのアプローチを追求し、フォーティネット セキュリティ ファブリックなどの連携を前提に設計されているセキュリティテクノロジーのコラボレーション型エコシステムを活用することで、セキュリティチームは、複雑さを緩和し、検知を強化し、セキュリティオペレーションセンター（SOC）の専門家の負担を軽減することができます。MDR（Managed Detection and Response）や SOC-as-a-service（SOCaaS）などのサービスを採用することで、実装した高度テクノロジーをセキュリティチームが最大限に活用できるようになります。

テクノロジーの調達だけでなく、人の備えや効果的なプロセスの作成も重要です。これらの作業を社内で実行することもできますが、ギャップ分析、机上演習、プレイブックや IR 計画の作成などにインシデント準備態勢 / レスポンスサービスを利用することで、新規の計画の策定、既存の計画のテスト、強化すべき領域の特定が容易になります。

組織の保護の最終責任はセキュリティリーダーやアナリストが負うことになりますが、攻撃者の侵入の防止については全従業員が重要な役割を果たします。企業の従業員は多くの場合に攻撃の防止にあたっての最初の防衛線であるため、継続的なサイバーセキュリティ意識向上の教育とトレーニングのプログラムは、リスク管理戦略の重要な要素になっています。

ランサムウェアの勢いがすぐに減速することはありませんが、組織のデータやネットワークの保護を強化するためにセキュリティリーダーができることはいくつもあります。必要なのは、それらの対策がランサムウェア攻撃のリスクや戦略と合致するものであることです。統合プラットフォームのアプローチを企業の保護に採用すること、AI ドリブンのツールと自動化を導入すること、計画とプロセスを（繰り返し）テストすること、外部から攻撃可能な脆弱性の有無をプロアクティブに監視すること、サイバー攻撃の可能性を判断する方法を幅広い従業員に教育することはいずれも、将来のランサムウェア攻撃の被害者になる可能性を少なくするために不可欠な、今すぐ実行すべき取り組みです。

[1]「FortiGuard Labs Reports Destructive Wiper Malware Increases Over 50%（FortiGuard Labs、ワイパー型マルウェアが 50% 以上増加したと報告）」、フォーティネット、2023 年 2 月 22 日（英語）：
https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent

[2]「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」、フォーティネット、2022 年 8 月 17 日：
https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/ja_jp/TR-22H1.pdf

[3]「How We Can Help You: Common Scams and Crimes」、FBI.gov（英語）：
https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware

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