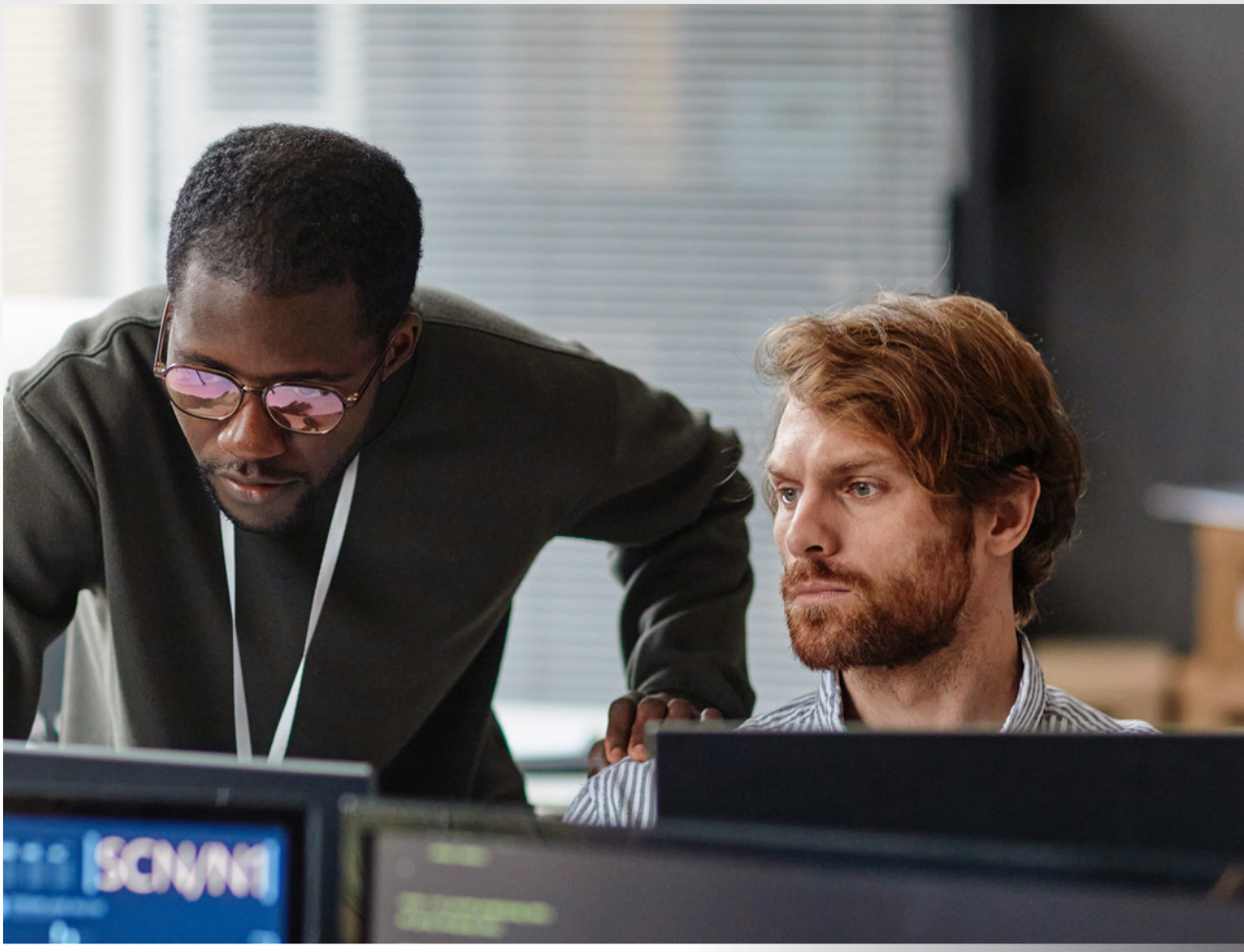
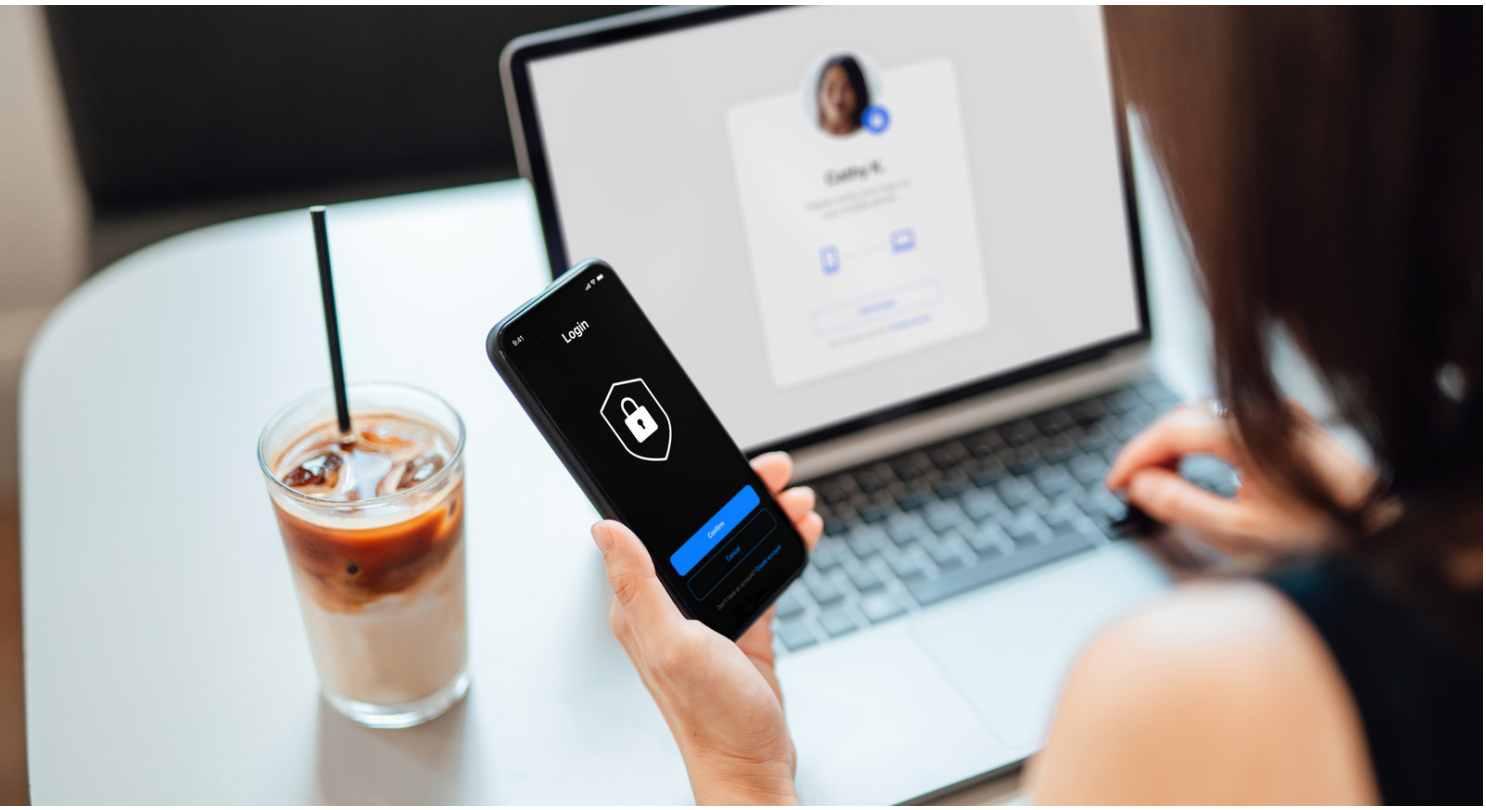


ランサムウェアが再び急増する中、企業に求められるのは、スマートな保護、そして迅速なリカバリを実現する 新たな戦略

Les experts suggèrent de plus en plus de s’intéresser plutôt à réduire les dommages qu’à assurer une détection à toute épreuve.



ランサムウェアの再来

ランサムウェア攻撃が2021年末に比べて大幅に減少した2022年は、企業も個人もようやく一息つけるようになったところでした。ところが、残念ながらその状況は一変しました。ランサムウェア攻撃件数は再び増加しており、事実、2023年第2四半期には前年比72%増と、過去最高を記録しています。[1]

「今年はランサムウェアが急増しており、2024年まで増え続けると予想しています」と、Zerto（HPEの子会社）シニアテクノロジーエバンジェリストのChris Rogersは話します。

急増の原因の多くは、人工知能の発達によるものと言えるでしょう。不正確な文法や崩れた画像を満載した、明らかなフィッシングメッセージの時代は終わりを告げました。AIによる今日のフィッシング攻撃は、はるかに洗練されており、着実に「本物」へと近づいています。

「AIを利用して大まかなメールを生成するだけでも、文法やスペルの間違いがなく、適切なブランディングが施された、最も洗練されたメールになる可能性があります」と、Rogersは言います。「評判の高い企業から送られたものと遜色ないメールになってしまうことでしょう」。すべてのメールはそれぞれの受信者に合わせた内容になり、見破るのがさらに難しくなります。

Rogersは、AIが新種の攻撃にも拍車をかけていると付け加えています。その攻撃とは肉声のディープフェイクです。たとえば、上司があなたに電話をかけてきて、「会社の銀行口座からお金を引き出してほしい」、あるいは「ホリデーボーナスとして従業員に配るギフトカードを100枚購入するように」と、指示されたとします。ところが、その声はただのコンピューターシミュレーションによるものであり、上司が参加していたYouTube™の公開ウェビナーを元に話し方のパターンを正確に模倣したものだったのです。

これを怖がるのは当然だとRogersは述べており、さらにここ数か月で顧客、パートナー、見込み顧客の態度に顕著な
変化が見られるようになったと付け加えています。「ほとんどの人は、攻撃を受けていないか、被った攻撃が思ったほどひどくないと考えていたと述べています」と、Rogersは言います。つまり、多くの人は、早い段階でガードを緩めてしまった 可能性があるということです。

「人々は、自分がサイバーセキュリティ対策を十分に講じていると考えていますが、大半の企業は攻撃を受け続けることに なり、また、あるポイントで攻撃がついに成功してしまうという統計データの裏付けがあります」

ここからわかることは明白です。セキュリティの備えは今でも大切なのです。

[1] 『Q2 Ransomware Report: Global Attacks At All-Time High』、Corvus、2023年7月31日

セキュリティ防御の最新化に関する新たな助言

今後ランサムウェアやその他の攻撃が勢いを増すことを考慮した場合、どうすれば身を守る準備を整えられるでしょうか。

Rogersは、過去数年で得られたアドバイスに従うことが最良であり、それに加えて、企業は攻撃を検出する能力について現実的な考えを持つ必要があると言います。「ランサムウェアは今まで以上に検出しにくくなっています」と、彼は述べています。「そして滞留時間も短縮する傾向にあります」

滞留時間とは、攻撃が検出されるかペイロードがアクティブ化されて被害者に損害を与えるまでの攻撃者の潜伏期間
です。Cyberintの報告によれば、2022年に世界中で発生したランサムウェアの滞留時間の中央値は9日間でした[2]が、2023年上半期は5日間と短くなっています。つまり、攻撃を受けた側が被害を受ける前に自分たちのネットワーク上でマルウェアを検出できる時間が短くなっています。「検出にかけられる時間が短いほど、攻撃を検出するチャンスが少なくなるということです」と、Rogersは言います。

組織は攻撃を検出するために、今後も必然的にサードパーティ製のツールに頼り続けることになりますが、この戦略は、まったく新しいエクスプロイトを利用したゼロデイスタイルの攻撃に より、最終的には機能しなくなるとRogersは説明しています。「ほとんどの企業は、ユーザーからアクセス不能になったファイルが大量にあると電話で報告を受けるまで、何が起こったのか分からない状況に陥ります」と、彼は述べています。

現在では、さまざまなセキュリティツールがAIを活用して攻撃の検出を支援していますが、万能薬と言うには程遠い状態です。「悪意のあるリンクをクリックしようとした際に、それを止めてくれるAI製品はまだ存在していないと思います」と、Rogersは言います。「そして、AIの使用について言えば、サイバーセキュリティ製品は攻撃者のペースに追いついていないと思います」。というのも、攻撃者は攻撃に失敗しても何のペナルティも受けず、その場はただ目的を達成できないだけで、あとで再び試せるからです。AIベースのサイバーセキュリティツールは完璧な性能に近づけていく必要があるが、この生まれて間もないテクノロジーでそれが実現されるのはまだ先のことだと、Rogersは言います。

Zertoでは現在、データをリアルタイムでスキャンし、ストレージデバイスに書き込まれる時にその安全なコピーを作成することで、セキュリティに対してより基本的なアプローチを採用しています。「私たちはリアルタイムに約5秒遅れで追随しています」と、Rogersは言います。「そのため、環境内で何か問題が発生しても、すぐにフラグを立ててセキュリティチームに伝達できます」。 このアプローチは、攻撃が拡がる範囲を制限でき、攻撃が他のシステムに広がる前に、アナリストが攻撃の発生場所を特定するのに役立ちます。

これまで以上に緻密なバックアップを

検出するとは準備するということです。そして準備するとは、これまで以上に、スマートなアプローチでバックアップを実行することを意味します。テープドライブをサーバールームの隅に置いて、徹夜で構成作業をしてバックアップを実行する時代はもう遠い過去になりました。また、長年信頼されてきた3-2-1ルール（3つのデータコピーを作成し、そのうち2つを異なる媒体に保管し、1つを別の場所に保管する）さえ、もはや十分とは言えません。

「攻撃者が侵入するには、パッチが1つ欠けていれば十分です」と、HPEセキュリティストラテジストのPaul Lloydは言います。「守る側は毎回正しく対応しないといけません。一方で攻撃側に必要なのは一度の好機だけです。これは、この業界にいるとうんざりするほど耳にする話ですが、否定しようのない事実なのです」

最新のバックアップガイダンスでは、企業はより積極的なアプローチである3-2-1-1-0バックアップルーチンに従うべきであると提案しています。ここでは、3-2-1と同じルールが引き続き 適用されますが、追加された「1」 はプライマリネットワークから物理的に切断されたエアギャップのバックアップを指し、このバックアップを取ることでプライマリネットワークから伝播する 可能性のあるランサムウェアの攻撃に対して耐性が得られます。

エアギャップを設けることは、今日ではきわめて重要です。「自宅からバックアップを取得できるというのは、ハッカーも同じことができることを意味します」と、Lloydは語っています。また、新たに追加された「0」は、バックアップが高い信頼性をもち、正確で完璧であり、またリカバリテスト中にエラーが無いことを確認することの大切さを強調しています。

「犯罪者は侵入してお金を奪うと、次のターゲットに移動しようとします」と、Lloydは述べています。サイバーセキュリティ会社のMandiant社によると、脆弱性が新しく発見されてから悪用されるまでの平均時間は、2018年と2019年は63日間でしたが、2020年と2021年初めには44日間まで短縮しました[3]。2022年には、この平均時間は32日間まで短くなっています。

Lloydは次のように続けます。「攻撃者のスピードが加速していますが、企業ではパッチのインストール作業が遅れており、攻撃に対してますます脆弱になっています。基礎の部分が脆弱になり続けていますが、これは何十年も前から続いている悪しき 習慣です。つまり一部のケースでは、攻撃が成功する範囲を 限定することがおそらく最良の対策になるでしょう」

2 『Ransomware Trends Q3 2023 Report』、Cyberint、2023年10月11日

リカバリの迅速化と精度向上への注力

幸い、攻撃後のリカバリについての見通しは以前よりも明るくなっています。「私たちは、1度の攻撃から数分以内にリカバリできるレベルにまで達しており、データ損失はわずか1秒分 です」と、Rogersは語っています。

重要なのは、データを迅速にリカバリすることではなく、データをクリーンにリカバリすることです。すでに感染しているバックアップを復元すると、問題がさらに悪化するだけなので、いつ攻撃が始まったのかを把握することが大切です。

クリーンルームとデータボルトの実装がこの取り組みの鍵です。こうした環境は、かつては大手金融企業やヘルスケア企業 など、十分な資金を用意できる企業のみが利用できましたが、コストが下がり、使いやすさが向上するにつれて、一般企業も利用可能になりつつあります。

クリーンルームは本番環境ネットワークから切り離されたインフラストラクチャ領域であり、データボルトはデータを不変 形式で保存するアーキテクチャーです。この2つを組み合わせることで、他の環境から機能的に分離されたネットワークが 実現し、攻撃者による侵入は事実上不可能になります。 検証済みのバックアップのみがクリーンルームのデータボルトに 保存されれば、ユーザーは、この環境からリストアされた ファイルは感染しておらず、安全だという確信をはるかに得やすくなります。

効果的なバックアップ検証には、リカバリプロセス中にデータをレビューして、データが暗号化されていないこと、または マルウェア製品に侵害されていないことを確認することが含まれます。また、データとアプリケーションを個別にリストアし、即座に確認して承認することも含まれます。このプロセス中に何か問題を発見した場合は、リストアを一時停止し、代わりにデータまたはアプリケーションの古いコピーを取得できます。Zertoのような最新セキュリティプラットフォームは、こうした作業をすべて前世代のリカバリツールよりもはるかに高速に実行 でき、ほとんどの環境を数週間ではなく数時間でバックアップして実行できます。

今日では、こうしたバックアップ/リカバリアーキテクチャーがほぼ必須となっています。「進んでこの2つの領域に投資しなければ、組織をリスクにさらすことになるでしょう」と、Rogersは話します。

最新のセキュリティ環境の複雑さにたじろぐことはありません。Rogersは次のように述べています。「必要な専門家を探しま しょう。そして貴社環境の管理を支援できるセキュリティサービスプロバイダーと連携しましょう」

3 『Analysis of Time-to-Exploit Trends: 2021-2022』、Mandiant、2023年9月28日

Visit HPE.com

詳細はこちら

HPE.com/data

今すぐチャット

a50010074JPN, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com