SOPHOS

ランサムウェアからネットワークを保護するためのベストプラクティス

ランサムウェア攻撃やその他のネットワーク攻撃の保護を強化

ソフォス ホワイトペーパー 2024 年 10 月

最も重大なサイバー脅威は依然としてランサムウェア

ランサムウェアは、今も最も深刻なサイバー脅威の一つであり、壊滅的な被害をもたらすことも多くあります。「ランサムウェアの現状 2024 年版」で公開している調査結果では、回答者の 59% が、前年に自分の組織がランサムウェアの被害を受けたことを報告しています。これらのインシデントの 70% で、攻撃者は暗号化データに成功しています。

ここ数年で攻撃率が急増した背景には、RaaS (サービスとしてのランサムウェア) モデルが成功し続けており、スキルが低い攻撃者でもランサムウェア攻撃に参加しやすくなっていることがあると考えられます。

攻撃を受けた影響を修復するための平均費用は 273 万ドル (前年比で 50% 増加) に急増しており、34% の企業が復旧までに 1 か月以上を要していました。復旧までの期間が長くなっているのは、攻撃が複雑化しており、セキュリティチームへの負担が増大していることを示しています。実際、95% の回答者が重要なセキュリティ運用タスクの管理に苦労していると回答しています 1。

これらの傾向からも、強力なランサムウェア対策と復旧戦略を緊急に取り入れる必要があることは明らかです。高度なエンドポイント保護機能を導入し、ネットワークセキュリティスタックを最適化することは、ランサムウェアに対する最も効果的な防御策の一つとなります。このホワイトペーパーでは、ランサムウェア攻撃の仕組み、予防戦略、およびネットワークスタックを最適化してセキュリティを向上する方法について説明します。

1 中小企業におけるサイバーセキュリティスキル不足の解消 - ソフォス

ランサムウェア攻撃の仕組み

ランサムウェアの攻撃から身を守る方法を理解するためには、まず、その仕組みについて知る必要があります。典型的なランサムウェアの仕組みは以下のとおりです。

最近のランサムウェア攻撃者は、VPN や RDP (リモートデスクトッププロトコル) など、正規の IT ツールやユーザーが一般的に使用するツールを使用して攻撃の足掛かりを得るが多くあります。RDP は、2023 年にソフォスのインシデント対応チームが調査したサイバー攻撃の 90% 以上に関与しており、前年の 83% から増加しています。2

これらのツールは、権限を持つスタッフが業務の一環として使用しているため、最新のランサムウェア攻撃の初期検出が困難になっています。問題の根底にあるのは、これらのツールの使用において暗黙的な信頼がありすぎることです。VPN や RDP にアクセスできるユーザーは誰でも信頼できると思われていますが、この考え方は賢明ではないことが何度も証明されています。

ランサムウェアからネットワークを保護するためのベストプラクティス

ここまでは、ランサムウェア攻撃の仕組みとサイバー攻撃者の活動について簡単に見てきましたが、ここからはネットワークセキュリティの防御を強化する 3 つのベストプラクティスを紹介します。

1. 露出 (攻撃対象領域) を減らす

2. ネットワークに入り込むネットワークトラフィックを検査して危険性を取り除く

3. ネットワークに侵入した脅威を特定して阻止する。

2 ソフォス「アクティブアドバーサリーレポート」2024 年上半期版 - ソフォス

露出 (攻撃対象領域) を減らす

インターネットに接続しているネットワークインフラが攻撃者の標的となるのは避けられないことです。従って、最初のベストプラクティスは、このような露出をできるだけ少なくすることです。次の対策をお勧めします。

1. ネットワークインフラを統合する

多くの組織は、ファイアウォールを使用してネットワークを保護しています。また、VPN コンセントレータやネットワークゲートウェイ製品を追加している組織も多く存在します。このようなインフラをできるだけ減らすことが重要です。少なくともファイアウォールをリモートアクセスが統合されているファイアウォールにアップグレードし、現在使用している既存の VPN コンセントレータを置き換えます。理想的には、ZTNA (ゼロトラストネットワークアクセス) に切り替えます。ZTNA ついては、後ほど詳しく説明します。

2. パッチを適用し、ファームウェアを常に最新の状態にする

すべてのランサムウェア攻撃は望ましくない結果を引き起こしますが、パッチが適用されていない脆弱性の悪用に起因する攻撃は、特に深刻な損害をもたらすことをご存じでしょうか？この方法によって攻撃を受けた組織は、侵害された認証情報を起点とする攻撃を受けた組織と比較して、復旧のコストが 4 倍となり、復旧までの時間も長期化したことを報告しています。[3]

2024 年におけるランサムウェア攻撃の最大の根本原因は、パッチを適用していない脆弱性でした。[4] ファイアウォールやその他のインフラストラクチャのファームウェアを最新の状態に維持することは不可欠な対策です。ファームウェアのアップデートを定期的に (少なくとも毎月) チェックし、他の業務への影響があまりない時間に適用するようにスケジュールしてください。

3. ネットワークインフラがセキュリティを重視した設計になっていることを確認する

ファイアウォールなど、インターネットに公開されているネットワークインフラ製品が、セキュリティを重視した設計 (セキュリティ・バイ・デザイン) になっていることを確認します。攻撃の防止を重視した設計になっており、堅牢化されているファイアウォールを選んでください。以下のような機能を取り入れているファイアウォールを選んでください。

- **デフォルトでインターネットに接続しない：**ファイアウォールは、初期設定ではインターネットにアクセスしない状態になっており、公開する内容をきめ細かく管理できるアクセスコントロールが提供されている必要があります。
- **堅牢な設計：**ファイアウォールには、多要素認証 (MFA) や、公開するサービスやポータルのコンテナ化などのセキュリティメカニズムが組み込まれ、攻撃者による脆弱性への攻撃を抑止できなければなりません。
- **ホットフィックスの自動適用：**現在の脅威環境は急速に進化しており、ホットフィックスを自動的に適用する機能が非常に重要になっています。ファイアウォールは、新たな脅威に速やかに対応するために、大規模なファームウェアアップデートがリリースされるのを待つのではなく、セキュリティアップデートを速やかに受け取ることができなければなりません。
- **プロアクティブな監視：**導入済みの顧客全体にわたるベンダー側のモニタリングは、攻撃の特定と対応をより迅速に行うのに役立ちます。

4. インターネットに接続するサーバーやアプリケーションを極力減らす

リモートデスクトップツール (RDP や VNC) を使用している、あるいは、リモートから管理するためにインターネットから直接アクセスできるシステムがネットワークにある場合、そのようなアクセスを直ちに無効にしてください。前述したように、このようにインターネットに接続しているシステムは攻撃者がネットワークに侵入するために最も多く悪用している手段の一つです。ファイアウォールの NAT ルールを確認して、絶対に必要なシステムを除いてインターネットに接続しないことを確認してください。ZTNA を使用してサーバーと管理システムを保護し、攻撃者から見えないようにすると同時に、これらのシステムを利用しなければならないユーザーには安全なリモートアクセスを提供してください。

5. リモートアクセス VPN を ZTNA に置き換える

ZTNA (Zero Trust Network Access) は、リモートアクセス VPN に代わる最新のテクノロジーです。これにより、VPN が提供する暗黙の信頼と広範なアクセスを排除し、代わりにゼロトラストの原則 (何も信頼せず、すべてを検証する) を使用します。ZTNA は、リモートアクセス VPN と比較して、管理の簡素化、可視性の向上、およびセキュリティとユーザーエクスペリエンスの向上を実現します。

ZTNA は、脆弱な VPN クライアントを排除し、多要素認証 (MFA) とデバイスの状態を利用してアクセスを制御し、特定のネットワーク アプリケーションへのアクセスのみを提供して、ネットワークを効果的にマイクロセグメント化します。ZTNA を統合でき、単一のゲートウェイソリューションとなるファイアウォールを検討してください。単一のコンソールから管理でき、ZTNA とエンドポイント保護機能の両方をユーザーのデバイスで単一のエージェントで実行できるソリューションであれば理想的です。

6. 強力なパスワードと多要素認証 (MFA) を使用する

脆弱なパスワードが利用されていることと、多要素認証 (MFA) が導入されていないことは、依然として重要な問題であり、多くのサイバー攻撃が成功する原因になっています。外部に公開されていないシステムも含め、ネットワークのすべてのシステムで強力なパスワードを使用し、ブルートフォース攻撃を防ぐために MFA で保護されていることを確認してください。

3 パッチが適用されていない脆弱性：最も凶悪なランサムウェア攻撃ベクトル - ソフォス
4 ランサムウェアの現状 2024 年版 - ソフォス

ネットワークトラフィックを検査して危険性を取り除く

もう一つの一般的な攻撃手法は、インフラとやり取りされる通常の Web やメールトラフィックに悪意にあるコードを忍ばせてネットワークに侵入する方法です。Web やメールはすべてのビジネスにとって不可欠であり、これらのトラフィックを簡単にブロックすることはできません。しかし、これらのトラフィックを検査して危険性を取り除くことは可能です。ネットワークトラフィックを保護するために推奨されるベストプラクティスを以下に紹介します。

1. 暗号化されたトラフィックを検査する

90% 以上のネットワークトラフィックが暗号化されています。これは、プライバシーの観点では好ましいことですが、セキュリティを悪化させる側面もあります。一般的な脅威検出ツールは、暗号化されたトラフィックストリームの内部を見ることができないためです。攻撃者はこのセキュリティ上の盲点を悪用しています。多くのファイアウォールの処理能力では、暗号化されたトラフィックの 90% を解読して検査する負荷に耐えることができません。復号すべきトラフィックストリームと、信頼できるトラフィックストリームをインテリジェントに判断でき、多くのトラフィックが暗号化されている現在の環境のために特別に設計されたファイアウォールを選択してください。ファイアウォールは、ネットワーク全体のパフォーマンスを損なうことなく、トラフィックを効率的に復号および検査し、暗号化されたトラフィックに潜む脅威を特定できなければなりません。

2.IPS を活用する

ネットワークの多くのシステムにはパッチが適用されていない脆弱性が存在している場合があります。脆弱性が存在している可能性があるシステムには、Windows や Linux システム、カメラなどの IoT デバイス、産業用制御システム、または有線または無線のネットワークに接続するあらゆるデバイスなどが含まれます。すべてのファイアウォールには、脆弱性を悪用するネットワーク攻撃を検出するテクノロジーが含まれており、これは侵入防御システム (IPS) と呼ばれます。残念ながら、多くの組織は IPS を十分に使用していません。すべてのネットワークトラフィックフローに IPS を使用していることを確認してください。インターネットから受け取るトラフィックはもちろんですが、ネットワーク内のトラフィックにも IPS を使用して、すでにネットワークに侵入している可能性のある攻撃者を特定する必要があります。

3. ゼロデイ脅威への対策

多くの攻撃は、カスタマイズしたマルウェアをファイルに埋め込み、ユーザーが意図せずに Web からそのファイルをダウンロードするように仕向けています。これらの脅威は過去に検出・特定されていないことから、「ゼロデイ」と呼ばれています。従来型のアンチウイルススキャンではゼロデイの脅威を検出することはできません。新しい脅威を特定するには、何百万もの過去の検体によって訓練した AI や機械学習を取り入れた脅威スキャンが必要になります。ファイアウォールのインスペクション機能にゼロデイ脅威の分析が含まれていることを確認してください。この高負荷の処理をファイアウォールからオフロードでき、世界的に共有される脅威インテリジェンスを即座に活用できるように、クラウドでリアルタイムに分析を実行することができれば理想的です。

4. 強固なメールセキュリティ対策を実施し、フィッシングメールを見分ける方法をユーザーに教育する

正規のように見えるメールの悪意のあるリンクを、うっかりクリックしてしまった経験は誰にでもあるでしょう。サイバー犯罪者にとって、フィッシングは依然として常套手段となっていますが、この難題への効果的な対策やユーザーを教育する方法も存在します。

ユーザーの受信トレイから悪意のあるメールをプロアクティブにフィルタリングできるメールセキュリティソリューションを見つけてください。一部のフィッシングメールが受信トレイに到達した場合でも、配信済みのメールを削除し、URL を書き換えて Time-of-Click プロテクションを有効にできる機能が必要です。さらに、ユーザーがフィッシング攻撃を特定する能力をテストする機能や、注意すべきフィッシング攻撃についてトレーニングを実施する機能があるメールセキュリティ製品を探してください。

ネットワークに侵入した脅威を特定して阻止する

最善の防御を尽くしていても、攻撃者がネットワークに侵入してくることを想定しておくことが重要です。このときには、侵入した脅威を特定して対応するまでの時間が非常に重要になりますが、多くのネットワークセキュリティソリューションは求められるレベルのレスポンスを提供できません。以下のような機能を提供できるソリューションを検討してください。

1. ネットワークのセグメント分割

攻撃者は、何らかの方法でネットワークに侵入すると、ネットワーク内を必ず嗅ぎまわります。ネットワークをセグメントに細分化 (マイクロセグメンテーション) することで、攻撃者による移動を制限し、攻撃者を早期に発見できます。ネットワークが、いくつもの小さなゾーンや VLAN セグメントに細分化されており、マネージドスイッチやアクセスポイントを介して接続され、IPS がトラフィックフローを検査するファイアウォールに、これらのゾーンや VLAN が接続されていることを確認してください。また、リモートアクセスには ZTNA を使用してください。ZTNA によって効果的なアプリケーションのマイクロセグメンテーションが可能になります。

2. 複数の攻撃手法を即座に特定する

攻撃者がネットワークに侵入した場合、迅速な検出しなければなりません。ランサムウェア攻撃の 91% は通常の営業時間外に発生しており [5]、24 時間体制でサイバー攻撃者をリアルタイムに検出し、脅威インテリジェンスを即座に共有できるサイバーセキュリティソリューションが必要です。管理者に単に警告する機能だけではなく、すべてのセキュリティ製品間でシームレスな連携を可能にし、迅速かつ協調的に脅威に対応して封じ込めることができなければなりません。

ファイアウォール、エンドポイント、スイッチ、ワイヤレス、ZTNA、メールセキュリティなどの製品が完全に統合されているソリューションスイートを選択してください。これらのツールは、セキュリティチームおよびツール間で脅威インテリジェンスを共有でき、深夜であっても自動的に対応し、攻撃を無効化できる必要があります。

3. 進行中の脅威に合わせて自動的に防御を調整して対応する

脅威を検出したのがユーザー自身であれ、セキュリティアナリストであれ、エンドポイント、ファイアウォール、あるいはサイバーセキュリティシステムの他の機能であっても、脅威を封じ込め、無力化するためには、迅速な連携と対応が求められます。このような連携を可能にするために、以下のようなファイアウォール (および統合型のセキュリティソリューション) を選択してください。

- 手動で介入することなく、**進行中の脅威に合わせて自動的に対応**し、攻撃を特定した時点で迅速に脅威を封じ込める。
- 新しいファイアウォールルールや管理者による操作を必要とせずに、**脅威を動的にブロックする。**
- **エンドポイントや ZTNA のような他のセキュリティツール**とシームレスに連携し、ラテラルムーブメントを防止して脅威を隔離することができる連携型の防御を実現する。

5 通常の営業時間とは、月曜日から金曜日の午前 8 時から午後 6 時までを指します。最前線のサイバー防御からの教訓 – ソフォス

ランサムウェア攻撃を防ぐためにセキュリティテクノロジーを利用し多層防御を実現する

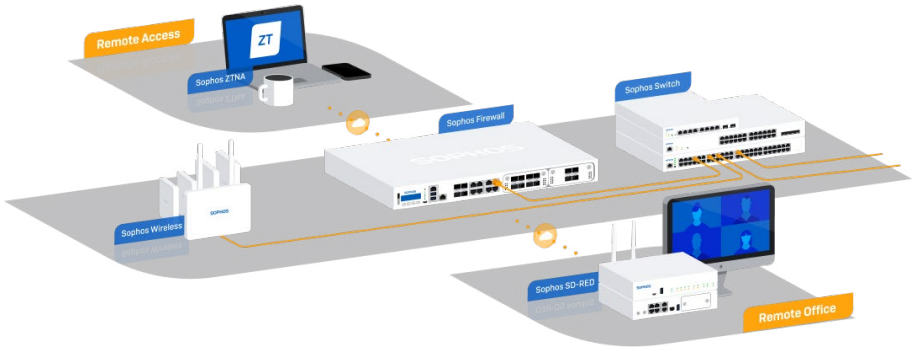
「*予防は治療に勝る*」という諺があります。できる限り早期に問題を食い止めることができれば、被害を軽減できます。ランサムウェアから組織を守るには、複数のテクノロジーを連携させて優れた防御と可視化を可能にする多層防御のアプローチが有効です。多層防御のアプローチでは、ファイアウォールとエンドポイント保護から始め、ニーズの変化に応じてレイヤーを追加し、保護と可視性を強化できます。

以下のコンポーネントを多層防御に追加できます。

- **NDR (Network Detection and Response)** 製品は、保護できないあるいはされていないデバイスを検出し、ネットワーク内でラテラルムーブメントを行っている攻撃者を検出できます。NDR は、ファイアウォールでは対応できない社内のネットワークトラフィックを可視化します。
- **XDR (Extended Detection and Response)** プラットフォームは、脅威ハンティング、調査、無力化のための機能を提供します。また、他の IT セキュリティソリューションと連携させることができ、共通のプラットフォームからすべてのセキュリティコントロールを可視化して管理できます。
- **MDR サービス** は、テクノロジーソリューションだけでは防ぐことができないサイバー攻撃の検出と対応を専門とする専門家が 24 時間年中無休体制で脅威ハンティングを提供するサービスです。MDR サービスを検討するときには、追加のコストをかけずに、攻撃を中断および封じ込め、完全に排除できるフルスケールのインシデント対応を提供していることを確認してください。MDR サービスは、環境全体を完全に可視化するために、既存のサイバーセキュリティツールと統合できる必要があります。MDR は、人間が主導する高度なランサムウェア攻撃に対しても、最高レベルの保護を提供します。
- **外部攻撃対象領域管理 (EASM) または脆弱性管理ソリューション**は、優先的に対応すべき脆弱性を特定するために使用できます。これにより、攻撃者に脆弱性が悪用される前に、適用されていないパッチを特定することが可能になります。

ソフォスは、ランサムウェアからネットワークを保護します。

ソフォスは、ランサムウェアやその他の攻撃からネットワークを保護するために必要なすべての機能を提供します。ソフォスは、ファイアウォール、ZTNA、スイッチ、ワイヤレス、リモートエッジデバイス、メッセージ保護、次世代エンドポイントプロテクションなどが含まれる統合されたサイバーセキュリティスタックをあらゆるデバイスとサーバーに提供しています。



最も優れている点は、これらのすべての製品を共通のクラウド管理プラットフォームである Sophos Central から管理できることです。これにより、ソフォスのソリューションと専門家による分析による脅威に関する知見を集約でき、脅威への自動的な対応が可能になります。

製品間をこのレベルで緊密に統合および同期しているのは、ソフォスだけであり、他社の追随を許していません。このような連携は、進行中の攻撃に対応するときに最も重要となります。

Synchronized Security の実行

侵害されたホストが検出されると、Sophos Firewall は直ちにそのホストを隔離し、ソフォスが管理しており、脅威の影響を受けていないエンドポイントは侵害されたデバイスからのトラフィックを自動的に無視します。さらに、スイッチやアクセスポイントも侵害されたホストからのパケットをドロップし、ZTNA によって侵害されたデバイスによるアプリケーションアクセスを防止できます。このように、脅威がネットワークに入り込んだ場合でも、自動的にネットワークで速やかに隔離され、脅威の進行を防ぐことができます。

ソフォスのネットワークセキュリティの概要

Sophos Firewall

Sophos Firewall および XGS シリーズアプライアンスは、導入してすぐにベストプラクティスを実装でき、ネットワークをランサムウェアから保護します。

- **セキュリティを重視した設計**：Sophos Firewall が市場で最も安全なファイアウォールとなるよう多大な投資を行っているだけでなく、プロアクティブな監視を通じてお客様のネットワークと組織を将来の攻撃から守りながら、Sophos Firewall が攻撃者にとって最も攻撃しにくいターゲットとなるよう継続的に取り組んでいます。
- **統合型の ZTNA**：Sophos Firewall には ZTNA ゲートウェイが組み込まれているため、製品を追加で導入することなく、旧来の VPN からゼロトラスト VPN に簡単に切り替えることができます。さらに、ZTNA はファイアウォールと同じクラウドコンソールから管理できるため、アプリケーションやリモートアクセスの保護とセグメンテーションを容易に行うことができます。
- **AI を活用したゼロデイ脅威への対策**：Sophos Firewall は、高度な AI テクノロジーを取り入れし、標的に合わせてカスタマイズされているランサムウェア攻撃も特定し、ネットワークに侵入する前に阻止します。ソフォスは、何百万もの検体によって訓練した高度な AI と機械学習を組み合わせ、リアルタイムサンドボックス機能を使用して、これまで検出されていない脅威も特定します。
- **アクティブな脅威対応**：Sophos Firewall は、さまざまな脅威インテリジェンスソースに基づいて、ネットワークに侵入したアクティブアドバーサリーを即座に特定し、さまざまな製品を連携・同期させて対応を調整することで、アクティブな脅威が実際に被害をもたらす前に自動的に隔離します。

Sophos ZTNA

Sophos ZTNA は、従来のリモートアクセス VPN よりも強力なセグメンテーション、セキュリティ、可視性を提供しながら、ユーザーが業務に必要なアプリケーションやシステムに安全に接続できるようにします。

- **アプリケーションのマイクロセグメント化と保護**：Sophos ZTNA は究極のマイクロセグメンテーションを提供し、アプリケーションがオンプレミス、データセンター、パブリッククラウドのいずれのインフラでホストされている場合でも、外部からアクセスを完全に見えないようにし、アプリケーションへの安全なアクセスを実現します。
- **ランサムウェアや脅威の阻止**：ZTNA を使用すれば、ランサムウェアやその他の脅威が、侵害されたユーザーデバイスからネットワーク全体に広がる恐れはなくなります。ユーザーとデバイスには、特定のアプリケーションに対する、明示的にポリシーで指定されたアクセス権のみが設定されます。これによって、VPN の重要な課題の 1 つであった、暗黙的な信頼と広範にわたるネットワークアクセス権は排除されます。
- **侵害されたデバイスからのアクセスのブロック**：Sophos ZTNA は、リモートの従業員が必要なアプリケーションやデータに安全かつシームレスにアクセスできるようにします。ユーザーのデバイスが侵害された場合、アプリケーションへのアクセスは自動的に遮断され、脅威がクリーンアップされるまでラテラルムーブメントを防止できます。

ソフォスのスイッチおよびアクセスポイント

ソフォスのスイッチとアクセスポイント は、Sophos Firewall やその他のソフォスのサイバーセキュリティプラットフォームと緊密に統合されており、共通のコンソールから管理でき、脅威への対応を自動化します。

- **アクティブな脅威対応**：ソフォスのスイッチとアクセスポイントは、アクティブな脅威にも対応でき、アクティブアドバーサリーによる攻撃の進行を防止します。侵害されたデバイスはスイッチやアクセスポイントで即座にブロックされ、同じ LAN セグメント内であってもラテラルムーブメントを防止できます。
- **単一コンソールでの管理**：ソフォスのスイッチとアクセスポイントはすべて、ファイアウォール、ZTNA、その他のソフォス製品と一緒に Sophos Central で管理されるため、優れた可視化と容易な管理を実現できます。

Sophos Email

Sophos Email は、高度なフィッシングおよびメッセージ対策を提供し、メールを介した脅威の侵入を阻止します。

- **フィッシング攻撃対策**：Sophos Email は、AI を活用した自然言語処理 (NLP) によって、フィッシングによってユーザーを騙すなりすましの手口を特定します。また、多層型のマルウェアや悪意のある URL の分析、URL の書き換え、クリックされた場合に追加のチェックを強制する Time-of-Click プロテクションも含まれています。また、Sophos Email は、不審な送信者を特定するための複数のテクノロジーを取り入れており、SPF、DKIM、DMARC、およびメールヘッダーの異常を分析する機能を活用しています。
- **Phish Threat による従業員のトレーニング**：Sophos Phish Threat は、攻撃をシミュレーションする機能とセキュリティ意識を向上するためのトレーニングを従業員に提供します。不審なメールやフィッシング攻撃を識別する方法を従業員にトレーニングし、テストを行って追加のトレーニングが必要なユーザーを特定するために非常に役立ちます。

結論

ランサムウェアは進化を続けており、標的組織に身代金の支払いを強制させる手段として依然として猛威を奮っています。攻撃者が組織に侵入するのを阻止し、万一侵入された場合は迅速に検出して排除しなければなりません。本書で説明したネットワークセキュリティのベストプラクティスを確実に取り入れ、エンドユーザーへの教育を継続し、自社環境における脅威や攻撃者に対する警戒を怠らないようにしてください。24 時間 365 日体制で検出および対応する多層防御のアプローチは、ランサムウェアや最新の脅威から組織を守る最善の方法です。

ソフォスがランサムウェア対策の最適化を支援する方法について、ソフォスのアドバイザーにご相談いただくか、www.sophos.com をご覧ください。

2024-10-14 (WP-PC)