SOPHOS

【決定版】ランサムウェアを阻止するためのファイアウォールとエンドポイントのベストプラクティス

ソフォス ホワイトペーパー 2020年 8月

目次

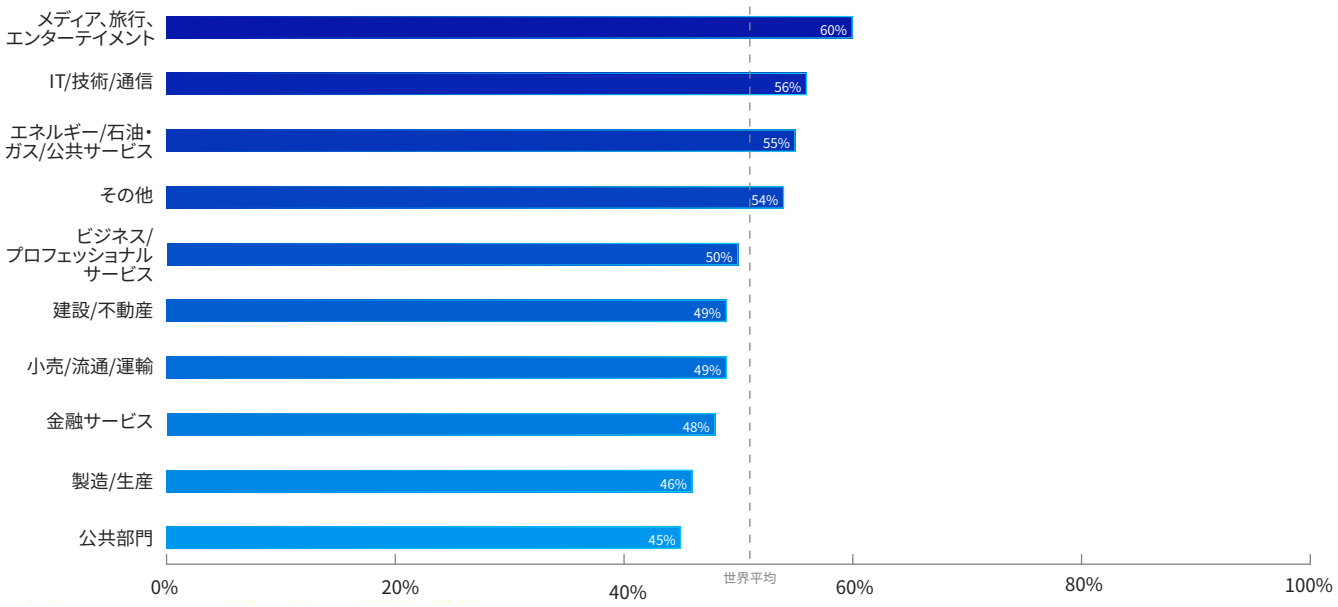
ランサムウェアを阻止するためのファイアウォールのベストプラクティス

ランサムウェアは組織を悩ませています。調査対象の 26カ国の参加企業の半数以上が、昨年ランサムウェアの被害にあったことを認めています* 。このような攻撃は、ますます複雑化するばかりで、より効果的にネットワークやシステムの脆弱性を悪用しているため、組織は多額の復旧費用を被っています。世界的な平均は、8,293万円 (761,106 米ドル) という莫大な金額です。

次世代型ファイアウォールはこうした攻撃の阻止に非常に効果的ですが、適切に機能するように設定・運用する必要があります。このホワイトペーパーでは、これらの攻撃の仕組みと阻止の方法、および最善の保護のためのファイアウォールとネットワークの設定のベストプラクティスについて説明します。

ハッカーの攻撃対象

ハッカーは、誰を攻撃の対象にしているのでしょうか？簡潔な答えは、「あらゆる組織」です。最近実施された調査では、回答者の 51% が昨年ランサムウェアに感染したと回答しており、組織の規模は重要な要因ではないと考えられます。47% の組織は従業員 1,000名未満で、53% の組織は 1,000名以上でした。被害を逃れた国、地域、業種はありませんでした。



「昨年、ランサムウェア攻撃を受けましたか？」回答者数：5,000名

「ランサムウェア攻撃」のニュースを検索すると、毎週、複数の新しい攻撃が発生していることがわかります。その影響は破壊的で、膨大な身代金の要求、長期間に渡るダウンタイムとビジネスの中断、評判の低下、データの損失などがあります。また、機密性の高い企業データが攻撃者によってオークションにかけられるというケースがますます増えています。

* ランサムウェアの現状 2020年版 - ソフォスが委託し、Vanson Bourne 社が実施した、26ヶ国 5,000人の IT 管理者を対象とした調査

ランサムウェア攻撃がネットワークに侵入する方法

2020年の傾向として、サーバーベースの攻撃が増えているということが挙げられます。これらは、高度に標的化された複雑な攻撃であり、展開するのに多くの労力が必要です。しかし、暗号化されるアセットの価値がより高いため、一般的にはるかに致命的な攻撃であり、数百万ドルの身代金の要求で組織は甚大な被害を受ける可能性があります。しかし、このような攻撃は、適切なセキュリティのベストプラクティスを施行することで防止することができます。

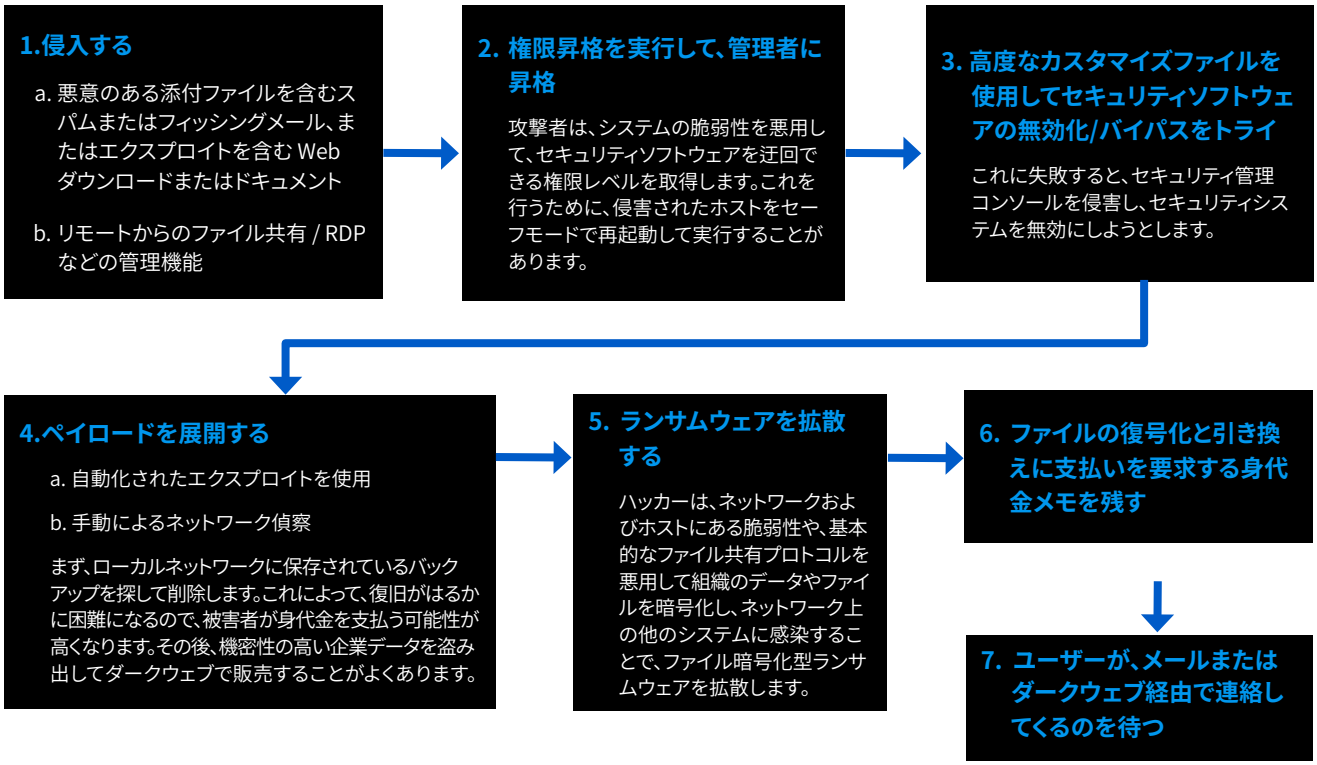
組織へのランサムウェアの侵入方法	% インシデント
悪意のあるリンクを含むファイルのダウンロード / メール経由	29%
サーバーへのリモート攻撃を経由	21%
悪意のある添付ファイルが添付されたメール経由	16%
間違ったパブリッククラウドのインスタンスの設定	9%
リモート デスクトップ プロトコル (RDP) を使用	9%
当社の組織と連携するサプライヤーを経由	9%
USB / リムーバブル メディア デバイスを使用	7%
その他	0%
不明	0%
合計	100%

ランサムウェア攻撃はどのようにして組織に侵入しましたか？昨年ランサムウェアの被害にあった組織の回答者への質問。回答者数：2,538名

ただし、上記の表にある調査の回答からわかるように、ランサムウェアの最大の侵入口は、スパムやフィッシング攻撃でユーザーがダウンロードした、またはユーザーに送信されたファイルです。セキュリティ対策をユーザーだけに委ねておくことはいけません。この種の攻撃に対しては、強力なファイアウォール機能を使用して組織を保護することを推奨します。

ランサムウェア攻撃の仕組み

典型的な標的型ランサムウェア攻撃の動作方法は次のとおりです。



RDP は「Remote Desktop Protocol」、それとも事実上「Ransomware Deployment Protocol」?

リモート デスクトップ プロトコル (RDP) や、Virtual Network Computing (VNC) などの他のデスクトップ共有ツールは、大半の OS にある、無害で非常に便利な機能で、リモートからユーザーがシステムにアクセス / 管理することを可能にします。残念ながら、適切な保護対策を適用していない場合、攻撃者が便利な侵入口として使用することが可能で、標的型ランサムウェアによって頻繁に悪用されています。

仮想プライベートネットワーク (VPN) の背後にある RDP や他の同様のリモート管理プロトコルに適切なセキュリティ対策を適用していない場合、または、最低でも、リモートツールを介して接続を許可する IP アドレスを制限していない場合、攻撃者に絶好の機会を与えることになります。攻撃者は、総当りのハッキングツールを使用することがよくあり、パスワードを破るまで、何十万種類のユーザー名とパスワードの組み合わせを試みます。

ランサムウェアから身を守る方法

ランサムウェアから組織を確実に保護するには、次の 3つの主要な対策を実行する必要があります。

1. IT セキュリティのアップグレード

ファイアウォールとエンドポイントセキュリティは、初期段階でネットワークへの攻撃を防ぐことができます。そして、攻撃が何らかの方法でネットワークに侵入した場合でも、他のシステムに拡散したり感染したりするのを防止できます。しかし、ファイアウォールとエンドポイントセキュリティソリューションのすべてがこれを効果的に実行できるわけではないので、それを実行可能な IT セキュリティシステムがあることを確認してください。

次の事柄を確認してください。

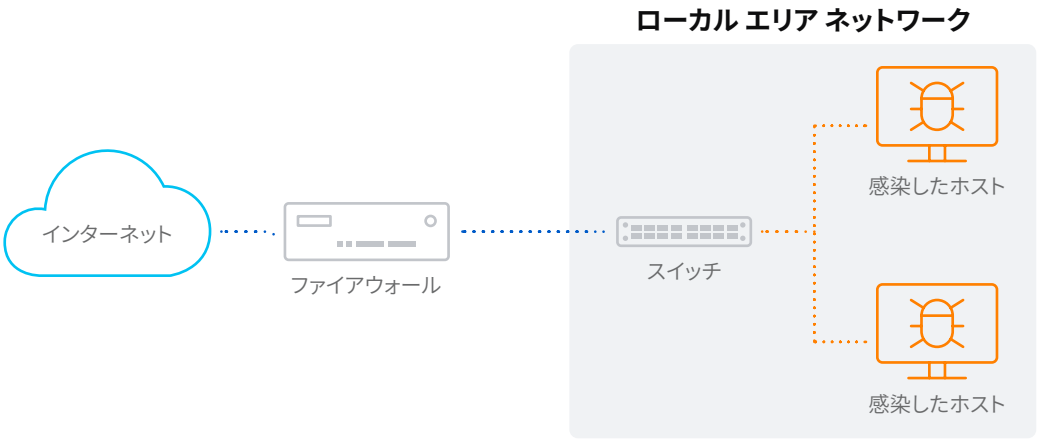
- ネットワークに入り込む前に、実行時のファイルの動作を分析する、手頃な価格のサンドボックス
- ファイアウォールを通過するファイルすべてにおいて、新しいゼロデイ亜種を検出する最新の機械学習テクノロジー
- ネットワークのエクスプロイトをブロックするための、ファイアウォールの IPS とシグネチャのライブ更新
- セキュリティを損なうことなく、ネットワークをリモートで管理する、無料で簡単に使えるリモートアクセス VPN
- ランサムウェア対策機能のあるエンドポイント保護

2. リモートアクセスおよび管理のロックダウン

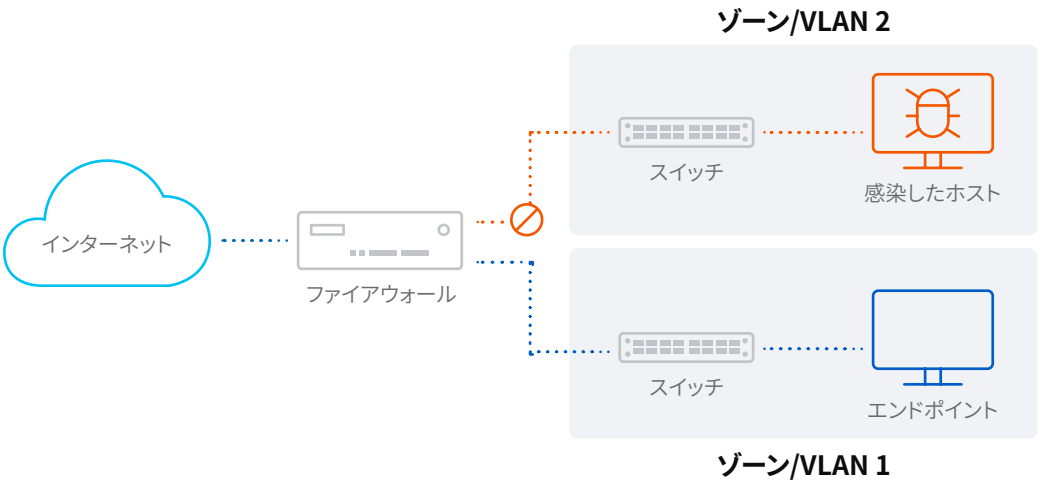
ネットワークでは、外部から接続可能な拠点はすべて、ランサムウェア攻撃によって悪用される可能性のある脆弱点です。組織の Remote Desktop Protocol アクセス、開放されているポート、および他の管理プロトコルをロックダウンすることは、標的型ランサムウェア攻撃から防御する最も効果的な対策の 1つです。これを実行するには多数の方法があります。よく使用される方法として、RDP へのアクセスを許可する条件として VPN への接続をすべてのユーザーに要求し、VPN アクセスを既存の IP アドレスのみに制限するなどがあります。また、サーバーに適切なセキュリティを提供する、頻繁に変更される複雑なパスワードを使用する、多要素認証を活用する、などもその例です。

3. ネットワークのセグメント分割

多くの組織は、すべてのエンドポイントを共通のスイッチに接続する、というフラットな構成のネットワークトポロジーで運用しています。このトポロジーの場合、ファイアウォールはスイッチを経由するトラフィックの可視化と制御を行えないため、ラテラルムーブメント (ローカルネットワーク内部での拡散・感染) を容易に発生させてしまう可能性があります。



ベストプラクティスは、ゾーンや VLAN を使用して LAN を小さなサブネットにセグメント分割することです。その上でこれらを共にファイアウォールに接続してセグメント間にマルウェア対策や IPS 保護を有効にすることです。これにより、脅威がネットワーク上で横断的に拡散しようとすることを効果的に特定しブロックできるようになります。



ゾーンまたは VLAN のいずれを使用するかは、お客様のネットワークのセグメント分割の方法や目的によって変わってきますが、どちらの場合でも、セグメント間のトラフィックの動きに適切なセキュリティと制御を適用できるオプションがあり、同じようなセキュリティ機能を提供しています。小さくセグメント分割を行う場合や、管理されていないスイッチを持つネットワークではゾーンを使用するのが適切です。VLAN は、多くの場合、内部ネットワークをセグメント分割する場合に適切な方法で、柔軟性とスケーラビリティが非常に高くなっています。しかし、管理型のレイヤー 3 スイッチの使用 (および設定) が必要になります。

ネットワークをセグメント分割することはベストプラクティスですが、どの分割方法が「ベスト」であるかは簡単には言えません。セグメント分割は、ユーザーの種類 (社員、契約社員、ゲスト)、部署 (営業、マーケティング、エンジニアリング)、サービス、デバイスやロールの種類 (VoIP、Wi-Fi、IoT、コンピュータ、サーバー)、またはネットワークアーキテクチャとして意味をなすような、これらのあらゆる組み合わせによって分けることができます。しかし、一般的には、ネットワークの信頼性が低く、脆弱な部分を、ネットワークの他の部分からセグメント分割することが望ましくなります。また、大規模なネットワークを小規模なセグメントに分割することが懸命です。これらはすべて脅威の侵入と他の部分への拡散リスクを減らすことを目的にしてします。

ファイアウォールおよびネットワーク設定に関するベストプラクティス

- **最適な保護機能が導入されていることを確認する**: IPS、TLS インスペクション、ゼロデイサンドボックス、機械学習によるランサムウェア対策などを含む、最新の高性能な次世代ファイアウォールを推奨します。
- **ファイアウォールを使用して、RDP およびその他のサービスをロックダウンする**: ファイアウォールで、VPN ユーザーのみにアクセスを制限したり、承認済み IP アドレスをホワイトリスト化したりします。
- **可能な限り攻撃経路を減らす**: すべてのポートフォワーディングのルールを徹底的に再確認し、不必要に開放されているポートを閉じます。開放されているすべてのポートは、ネットワークにおける開放された侵入路になる可能性があります。社外から社内ネットワークのリソースにアクセスする際は、ポートフォワーディングではなく、可能な限り VPN を使用します。
- **開いているポートのセキュリティを確保する**: トラフィックのルールに IPS による適切な保護対策を適用します。
- **TLS インスペクションを有効化する**: Web トラフィックで最新の TLS 1.3 標準に対応して、暗号化されたトラフィックフローを介して脅威がネットワークに侵入しないようにします。
- **ラテラルムーブメントのリスクを最小化する**: 隔離された小さなゾーンまたは VLAN に LAN をセグメント化し、それらをファイアウォールによって保護・結合することによって、ネットワーク内での感染の拡大を防止します。これらの LAN セグメントを通過するトラフィックのルールに適切な IPS ポリシーを適用して、LAN セグメント間でエクスプロイト、ワーム、ボットが拡散するのを防止します。
- **感染したシステムを自動的に隔離する**: 感染が発生した場合、IT セキュリティソリューションが感染したシステムを迅速に特定し、クリーンアップできるようになるまで自動的に隔離できることが重要です (Sophos Synchronized Security はこれを実行します)。
- **強力なパスワードおよび多要素認証を使用する**: 総当りのハッキングツールによってパスワードを破られないよう、リモート管理ツールおよびファイル共有ツールで、強力なパスワードを使用します。

ソフォスが提供する支援

ソフォスは、最新のランサムウェアから防御するための究極の IT セキュリティソリューションを提供しています。すべてのポイントで最高の保護を提供するだけでなく、ファイアウォールとエンドポイントの長年にわたる統合によるメリットも得られます。これにより、ネットワークのセキュリティ状態を可視化し、セキュリティインシデントに自動対応できるという点で大きなメリットが得られます。

受賞歴のあるソフォスの XG Firewall では、攻撃がネットワークに侵入することを防止することが最優先されます。万が一、ランサムウェアがネットワークに侵入した場合でも、二重にカバーされています。XG Firewall は、業界をリードするエンドポイント保護プラットフォームである Sophos Intercept X との統合により、ランサムウェアを即座に自動阻止します。ネットワークを自動操縦するようなもので、セキュリティチームの能力を増強します。

ソフォスでは、このテクノロジーを「Sophos Synchronized Security」と呼んでいます。Synchronized Security は、ソフォスのエンドポイント保護とネットワーク保護機能を、強力かつ緊密に統合された 1つのサイバーセキュリティシステムとして提供します。そして最大の強みは、Sophos Central クラウド管理コンソールから、他のソフォス製品すべてと共に、非常に簡単に管理できることです。

ランサムウェア対策に的を絞った、主な XG Firewall テクノロジーおよびソフォスのテクノロジー

- XG Firewall の Sandstorm サンドボックスと、ネットワークに入ってくるファイルの機械学習分析により、未知のランサムウェアの亜種、エクスプロイト、マルウェアが、スパム、フィッシング、Web ダウンロードを介して拡散しないようにします。
- XG Firewall の侵入防御システム (IPS) は、防御の脆弱性を見つけるために、ハッカーが利用している可能性のある最新のネットワークエクスプロイトや攻撃を検出します。
- XG Firewall の広範でシンプルな VPN オプションを使用すると、承認済みユーザーによるネットワークへのフルアクセスを提供しつつ、ネットワークにあるすべてのセキュリティホールを閉じ、脆弱な RDP 接続への依存を排除します。
- XG Firewall は、柔軟なポリシー制御を備えた高性能 Xstream TLS 1.3 インスペクションを提供します。プライバシー、保護、およびパフォーマンスの最適なバランスを確保し、暗号化されたトラフィックフロー経由で脅威がネットワークに侵入しないようにできます。
- Sophos Synchronized Security は、XG Firewall と Intercept X エンドポイント保護を統合し、最初の攻撃の兆候を検出して阻止し、通知することで、ランサムウェア攻撃に自動的に対応します。
- CryptoGuard を含む Sophos Intercept X エンドポイント保護は、進行中のランサムウェア攻撃を検出して停止し、自動的にロールバックすることができます。XG Firewall にはサンドボックス環境での CryptoGuard テクノロジーが組み込まれており、ランサムウェアがネットワークに到達する前に即座に検出できます。

結論

サイバー脅威が長年続いているにも関わらず、ランサムウェアは進化し続けています。ランサムウェアを完全に根絶することは決してできないかもしれませんが、このドキュメントで説明しているファイアウォールのベストプラクティスに従うことで、組織は、最新のランサムウェアおよびその他の悪意のある脅威から保護するチャンスを最大化させることができます。

まとめ:

- 最適な保護機能が導入されていることを確認する
- ファイアウォールを使用して、RDP およびその他のサービスをロックダウンする
- 可能な限り、攻撃の侵入口を減らす
- 適切な IPS 保護を適用して、開放されたポートを保護する
- ダウンロードと添付ファイルに対して、サンドボックスと機械学習分析を活用する
- LAN をセグメント分割して、ネットワーク内のラテラルムーブメンによるリスクを最小化する
- 感染したシステムを自動的に隔離する
- リモート管理ツールおよびファイル共有ツールで、強力なパスワードおよび多要素認証を使用する

ランサムウェアを阻止するためのエンドポイント保護のベストプラクティス

26か国、5,000人の IT 管理者を対象としたソフォスの調査では、回答者の 51% が過去1年間にランサムウェアに感染したことが分かりました。これらのインシデントの 73% で、攻撃者は暗号化データに成功しました。さらにこれらの攻撃の修復にかかる世界的な平均コストは、761,106 米ドルという莫大な金額でした。

ランサムウェア攻撃から防御する最も効果的な対策の 1 つは、適切に構成されたエンドポイント保護ソリューションを使用することです。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と阻止の方法、および最強の保護に向けたフエンドポイント保護の設定のベストプラクティスについて説明します。

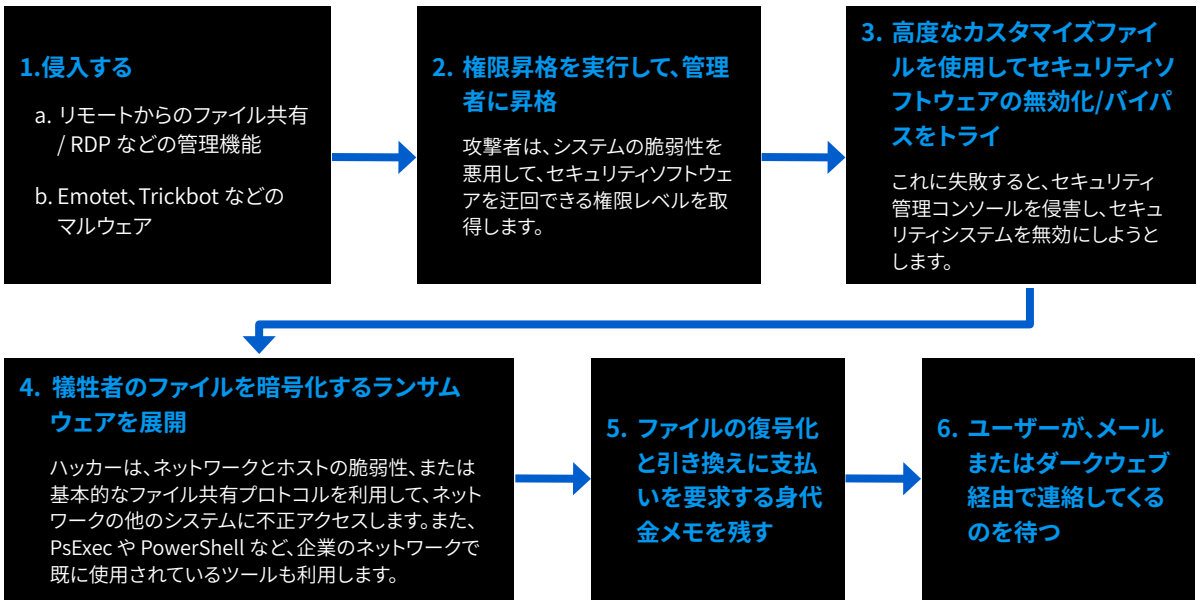
ランサムウェア攻撃の展開方法

近年では、ランサムウェア攻撃は、総当りの大規模な攻撃から、手動で実行される、検出 / ブロックがより困難な標的型 / 計画的な攻撃に移り変わりました。以下で、各種のランサムウェアの動作方法、および悪用される脆弱性を最小限に抑えるために組織ができることについて見てみましょう。

標的型ランサムウェア攻撃

標的型ランサムウェア攻撃は手動で行われます。通常、一度に 1 社の被害者に焦点を当て、大抵は非常に高額な身代金を要求します。攻撃者はネットワークにアクセスしてラテラルムーブメントを行い、プロセス内の価値が高いシステムを特定します。一度に多くのシステムに影響を与えようとするこれらの攻撃は、防衛側にとって最悪の時間帯である、夜間、週末、休日に開始されることがよくあります。また、特に効率的に働けるよう、攻撃者は複数の攻撃手法を活用して、レイヤー型の保護機能を回避します。

典型的な標的型ランサムウェア攻撃の動作方法は次のとおりです。



このような攻撃を受けたユーザーは、甚大な被害を受ける恐れがあります。ハッカーたちは、ますます大胆になっており、6 桁の支払いを要求こともよくあります。さらに、ソフォスの調査では、実際に身代金を支払うことで、攻撃に対応するコストが 2 倍になることが明らかになりました。これは、世界で平均 140 万ドルを超えるという致命的なビジネス上の損害をもたらしています。

Remote Desktop Protocol もしくは Ransomware Deployment Protocol ?

リモート デスクトップ プロトコル (RDP) や、Virtual Network Computing (VNC) などの他のデスクトップ共有ツールは、合理的かつ非常に便利な機能で、管理者がリモートからユーザーがシステムにアクセス / 管理することを可能にします。残念ながら、適切な保護対策を適用していない場合、攻撃者はこれらのツールを便利な侵入口として使用することが可能で、標的型ランサムウェアによって頻繁に悪用されています。

仮想プライベートネットワーク (VPN) の背後にある RDP や他の同様のリモート管理プロトコルに適切なセキュリティ対策を適用していない場合、または、最低でも、RDP を介して接続を許可する IP アドレスを制限していない場合、攻撃者に絶好の機会を与えることになります。攻撃者は、総当りのハッキングツールを使用することがよくあり、何十万種類のユーザー名とパスワードの組み合わせを試み、パスワードを破ることができたらネットワークに侵入します。

ランサムウェアからの保護を維持するための一般的なベストプラクティス

ランサムウェアを防ぐためには、最新のセキュリティ製品を導入するだけでは十分ではありません。セキュリティ製品をセットアップしたうえで、従業員に定期トレーニングを実施するなど、正しい情報セキュリティ対策を心がけることが必要不可欠です。以下の 10 つの対策を習慣化するようにしましょう。

1.パッチを即座かつ頻繁に適用する

マルウェアは、一般的なアプリケーションのセキュリティバグに依存することがよくあります。エンドポイント、サーバー、モバイルデバイス、およびアプリケーションにパッチを少しでも早く適用すれば、その分悪用されるホールも少なくなります。

2.バックアップは定期的に行い、最新のバックアップをオフラインとオフサイトに保管する

調査では、暗号化されたデータを使用している IT 管理者の 56% が、バックアップを使用してデータを復元できました。バックアップデータを暗号化し、オフラインおよびオフサイトに保管することで、クラウドバックアップやストレージデバイスが悪用される心配がなくなります。さらに、データの復旧に対応するディザスタリカバリを実行します。

3.ファイル拡張子を表示する

Windows のデフォルトの設定では、ファイルの拡張子は非表示になっており、ファイルのサムネイルで識別しなくてはなりません。拡張子を表示するようにすれば、普通は送られてくることのない JavaScript ファイルなどのファイルを簡単に見分けられるようになります。

4.JavaScript (.JS) ファイルはメモ帳で開く

JavaScript ファイルはメモ帳で開くようにすれば、悪質スクリプトの実行を防ぎながら、ファイルの内容をチェックすることができます。

5.メールを介して受信したドキュメントのマクロを有効にしない

Microsoft はセキュリティ対策の 1 つとして何年も前からマクロの自動実行をデフォルトで無効に設定しています。マクロを有効にするようにユーザーを誘導することで感染するマルウェアが多数存在しているので、有効化しないでください。

6.不審な添付ファイルには細心の注意を払う

サイバー犯罪者は、使い古されたジレンマを利用することがよくあります。つまり、正当であると確信するまでは文書を開くべきでないことは分かっていても、文書を開くまでは悪意があるかどうかを判断することはできません。疑わしい場合には、開かないようにしましょう。

7.管理者権限を管理

ローカル管理者権限とドメイン管理者権限を常に確認してください。誰に権限があるかを確認し、必要としないユーザーは削除します。管理者として必要以上に長くログインしたままにしないでください。管理者権限でログインしているときに、Web の閲覧、ドキュメントを開く、またその他の日常業務を実行することは避けるようにしましょう。

8.ビジネスアプリケーションの最新のセキュリティ機能を取り入れる

たとえば Office 2016 には、「インターネットから取得した Office ファイル内のマクロの実行をブロックする」というオプションが追加されています。これを使用すると、内部でのマクロ使用は禁止されずに、外部からの悪意のあるコンテンツを阻止することができます。

9.外部ネットワークアクセスを規制する

ポートを公開したままにしないでください。組織の RDP アクセスおよびその他のリモート管理プロトコルをロックダウンします。さらに、2 要素認証を使用して、リモートユーザが VPN に対して認証されるようにします。

10.強力なパスワードを使用

些細な事ように思えますが、実際はそうではありません。脆弱で予測可能なパスワードを使用すると、ハッカーは数秒でネットワーク全体にアクセスできます。少なくとも大文字と小文字を混ぜた 12 文字の長さで、句読点をランダムに使用した、個人を特定できないパスワードを作成することを推奨します。例: Ju5t.LiKETh1s!

エンドポイント保護ソリューションのベストプラクティス

次世代型ファイアウォールに加えて、ランサムウェア攻撃から保護する最も効果的な方法の 1 つは、エンドポイント保護ソリューションを利用することです。ただし、最適な保護を提供するには、正しく設定する必要があります。

エンドポイントデバイスをランサムウェアから保護するには、次のベストプラクティスに従ってください。

1.すべてのポリシーをオンにし、すべての機能が有効になっていることを確認する

当たり前のようですが、エンドポイントソリューションから最善の保護を得る確実な方法です。ポリシーは特定の脅威を阻止するように設定されており、ポリシーがすべてオンになっていることを定期的にチェックすることで、特に新種のランサムウェアからエンドポイントを確実に保護します。

さらに、ファイルレス攻撃の手法やランサムウェアの動作を検出する機能を有効にすることは、犯罪者がエンドポイントに侵入したり、有害なランサムウェアの亜種を展開するのを防ぐために重要です。また、攻撃が何らかの形で環境に侵入した場合に、簡単に修正することもできます。

2.定期的に除外機能を確認する

信頼できるディレクトリやファイルの種類がマルウェアにスキャンされないようにする除外機能は、保護ソリューションによってシステムの速度が低下している感じるユーザーの不満を軽減するために利用されることがあります。除外を使用して、誤検出のリスクを軽減することもできます。

時間が経つにつれて、除外されたディレクトリとファイルタイプのリストが増加し、ネットワーク全体でより多くの人々に影響を与える可能性があります。また、除外されたディレクトリになんとか侵入したマルウェア (おそらく、ユーザーが誤って移動した可能性のある) は、チェック対象から除外されているため、成功する可能性があります。

脅威保護設定内の除外リストを定期的に確認し、除外の数をできる限りゼロに近づけてください。

3.セキュリティコンソール内で多要素認証 (MFA) を有効にする

多要素認証 (MFA) は、最初の要素 (通常パスワード) の後に追加のセキュリティの追加レイヤーを提供します。アプリケーション全体で MFA を有効にすることは、一般的に適切な IT セキュリティのプラクティスであり、セキュリティコンソールにアクセスするすべてのユーザー対して MFA を有効にすることが重要です。

これにより、エンドポイント保護ソリューションへのアクセスが安全になり、設定を誤って変更したり意図的に変更したりすることがなくなり、エンドポイントデバイスが攻撃に対して脆弱なままになる可能性があります。MFA は RDP のセキュリティ保護でも重要です。

4.すべてのエンドポイントが保護され、最新の状態であることを確認する

デバイスが保護されているか、最新の状態になっているかを定期的に確認することは、最適な保護を確保する簡単な方法です。デバイスが正しく機能しないと、保護されず、ランサムウェア攻撃に対して脆弱になる可能性があります。エンドポイントセキュリティツールは、この使用状況データを提供することが多く、IT 予防策管理プログラムは潜在的な IT の問題を定期的にチェックするのにも役立ちます。

5.IT の予防策を維持

定期的な IT 予防策管理により、エンドポイントおよびエンドポイントにインストールされているソフトウェアが最大限の効率で実行できます。サイバーセキュリティのリスクを軽減するだけでなく、将来発生する可能性のあるインシデントを修正する際に時間を大幅に節約できます。

IT 予防策を維持するプログラムを実装することは、ランサムウェア攻撃やその他のサイバーセキュリティの脅威から保護するために特に重要です。たとえば、RDP が必要な場所でのみ実行されていることを確認し、設定の問題を定期的に確認し、デバイスのパフォーマンスを監視し、不要なプログラムを削除します。IT 予防策チェックでは、セキュリティソフトウェアを含むソフトウェアアプリケーションを更新する必要性が強調される場合があります。また、大切なデータを定期的にバックアップする確実な方法でもあります。

6.ネットワーク内でアクティブな攻撃者を追跡する

今日の脅威の状況では、悪意のある攻撃者はこれまで以上に高度な実行をしており、悪意のある手法を導入してランサムウェア攻撃の被害を与えています。組織は、高度な脅威やアクティブな攻撃者を特定できるように、詳細な質問を行えるツールが必要です。一旦見つけたら、組織はこのような脅威を阻止するために適切な行動を迅速に実行できるツールも必要になります。

EDR (Endpoint Detection and Response) などのエンドポイントソリューション内のテクノロジーはこの機能を提供するため、EDR 機能がある場合は必ず有効にして使用してください。

7.人間の介入でギャップを埋める – ランサムウェアは単なるエンドゲーム

ランサムウェアはハッカーにとって単なるエンドゲームです。ランサムウェアを展開するために、ハッカーはすでにネットワークに侵入しており、攻撃を実行するのに数か月かかることもありますが、知らないうちにデータを引き出している可能性があります。

こうした侵入を阻止するには、テクノロジーだけでは不十分なことがよくあります。現実世界の例では、防犯カメラを使用すると、窃盗犯がどのように敷地に侵入しているかを確認できますが、盗難を防止できるのはセキュリティガードが配置されている場合のみです。これと同じ理論をサイバーセキュリティにも当てはめることができます。このような侵入から真に保護する最善の方法は、レイヤードセキュリティ戦略の一環として人間の専門知識を追加することです。

ここでは、Managed Detection and Response (MDR) サービスが重要となります。社内の IT チームとセキュリティチームを外部の優秀な脅威ハンターチームやレスポンスの専門家チームと組み合わせることで、再発するインシデントの根本原因に対処するための実用的なアドバイスを提供できます。

Sophos Intercept X Advanced with EDR

Sophos Intercept X Advanced with EDR には、Ryuk、Sodinokibi、Maze、Ragnar Locker などのランサムウェア攻撃から組織を保護するために必要なすべての機能が含まれています。

Intercept X には、悪意のある暗号化プロセスを検出してシャットダウンするランサムウェア対策テクノロジーが搭載されています。ランサムウェアの侵入や導入を防ぐエクスプロイト対策テクノロジーをはじめ、ランサムウェアを実行前に検出・ブロックするディープラーニングや、ファイルが勝手に暗号化されるのを防ぎます。万一暗号化されてしまった場合「CryptoGuard」でファイルを安全な状態に戻すことができます。

さらに、Sophos EDR は、脅威ハンティングと IT 運用の予防策を組織全体で円滑に実行し続けるようにします。Sophos EDR は、高度な脅威、アクティブな攻撃者、潜在的な IT の脆弱性を特定する詳細な質問をする権限をチームに与え、適切な処置を講じて迅速にそれらを阻止します。これにより、ネットワークに潜んでいる攻撃者や、気づかれなかった可能性のあるランサムウェアの展開を待っている攻撃者を検出することができます。

Sophos MTR (Managed Threat Response)

Sophos MTR サービスは、レイヤードセキュリティ戦略に人間の専門知識を追加します。一流の脅威ハンターチームが、潜在的な脅威をお客様に代わってプロアクティブに探して検証します。承認されている場合は、脅威を阻止、封じ込め、無効化するための措置を講じ、再発するインシデントの根本原因を対処する実用的なアドバイスを提供します。

結論

サイバー脅威が長年続いているにも関わらず、ランサムウェアは進化し続けています。ランサムウェアを完全に駆除することは決して出来ないかもしれませんが、このドキュメントで説明しているエンドポイント保護のベストプラクティスに従うことで、組織は最新の脅威から保護された状態の維持を最大限に高めることができるでしょう。

まとめ:

1. すべてのポリシーをオンにし、すべての機能が有効になっていることを確認する
2. 定期的に除外機能を確認する
3. セキュリティコンソール内で MFA を有効にする
4. すべてのエンドポイントが保護され、最新の状態であることを確認する
5. IT の予防策を維持する
6. ネットワーク内でアクティブな攻撃者を追跡する
7. 人間の介入でギャップを埋める – ランサムウェアは単なるエンドゲームであることを留意する

Sophos Intercept X 無償評価 (30日間)
www.sophos.com/endpoint

Sophos MTR の詳細については、
www.sophos.com/MTR を参照

Sophos XG Firewall の無料トライアル:
www.sophos.com/xgfirewall

ソフォス株式会社営業部
Email: sales@sophos.co.jp

200702 WPEN (NP)

SOPHOS