Cisco Ransomware Defense：ランサムウェアを寄せ付けない

ランサムウェアがどれだけ侵入を試みたとしても、安全でいられるとしたらどうでしょうか。これを実現するセキュリティ製品とアーキテクチャを提供できるのはシスコだけです。

概要

ファイルと情報は組織にとって不可欠です。この情報を（そして組織の生産性を）完全かつ安全に保つことが何よりも重要です。

しかし、ランサムウェアは侵入してきます。ランサムウェアとは、個人または組織のコンピュータに保存されているドキュメント、写真、音楽などの情報をロックする、悪意のあるソフトウェア（マルウェア）です。これらのファイルは、ユーザがファイルのロックを解除して元に戻すための料金（身代金）を支払うまで解放されません。適切な防御がなければ、組織はランサムウェアによって大きな被害を被り、紙とペンでビジネスを行わなければいけなくなる可能性があります。

ランサムウェアは通常、エクスプロイト キット、マルバタイジング（マルウェアを配布可能な Web サイト上の感染広告）、フィッシング（信頼できる電子メールを装っている詐欺メール）、またはスパム キャンペーンを介して配布されます。実際の感染は、誰かがフィッシング電子メールのリンクや添付ファイルをクリックすると始まります。また、自動的にコンピュータに感染させる悪意のある広告を含むサイトにユーザがアクセスしたときにも感染が起こります。

Cisco® Ransomware Defense を導入しましょう。このソリューションは、DNS レイヤからエンドポイント、ネットワーク、電子メール、Web まで、階層型アプローチによってランサムウェア感染のリスクを軽減します。シスコは、究極の可視性とランサムウェアに対する究極の反応性を組み合わせたアーキテクチャ アプローチによって、統合的な防御を実現します。

メリット

- **ランサムウェアのリスクを軽減し**、ビジネスの運営に専念できます。
- 脅威が根付く前にブロックできるセキュリティにより、**即座に保護が実現します。**
- アーキテクチャ アプローチにより、DNS レイヤからネットワーク、エンドポイントまで**比類のない可視性と反応性が得られます。**
- 強力なネットワーク セグメント化により、**マルウェアが横展開するのを阻止できます。**
- ランサムウェアに関する **Talos の業界トップクラスの脅威研究**とインテリジェンスが提供されます。

急成長している強力な脅威

今年はランサムウェアの年です。ランサムウェアは収益性が非常に高いことが明らかになっています。ランサムウェアは瞬く間にこれまでで最も収益性の高いマルウェアの 1 つになりました。

FBI によると、その市場規模は年間 10 億ドルに近づいています。Cisco Talos の調査によると、単一のランサムウェア キャンペーンは年に最大 6,000 万ドルの収益を生み出すことができます。ランサムウェアは現在非常に注目されており、TV 番組で取り上げられたこともあります。

攻撃者には、ランサムウェアの革新を継続し、これまでよりもはるかに感染力の高いランサムウェアを作り出す資金と意欲があります。シスコでは、ランサムウェアは企業ネットワークの広い範囲をロックすることを目的に自己伝搬力を高めていくと予測しています。これにより、企業の IT 機能が打撃を受け、実質的に 1970 年代レベルの機能に戻されてしまう可能性があります。

現在のランサムウェアへの対応は、シングル ポイント製品を中心に展開される傾向があります。ランサムウェアが感染を広げるためにターゲットにするベクトルが多岐にわたることを考慮すると、アーキテクチャ重視のアプローチの実現に取り組む必要があります。

このソリューションの概要では、攻撃者が使用するさまざまなベクトルと手法について説明します。防御側で必要なのは、電子メールと Web の両方を保護すること、インターネット上の悪意のあるインフラストラクチャへのアクセスをブロックすること、ランサムウェア ファイルがエンドポイントに到達するのを阻止すること、使用される指揮統制コールバックをブロックすること、および感染が発生した場合にランサムウェアが水平方向に容易に移動できないようにすることです。

何を購入すべきか

Cisco Ransomware Defense は、ランサムウェアの問題に対応するために必要なシスコのセキュリティ アーキテクチャのすべての要素をまとめたものです。すべての要素を選択することも、差し迫ったセキュリティ ニーズを満たす要素のみを選択することもできます。

Ransomware Defense を構成するコンポーネントは次のとおりです。

- Cisco Umbrella：ネットワークから遠く離れた DNS レイヤで脅威をブロックします。
- Cisco Advanced Malware Protection（AMP）for Endpoints：悪意のあるランサムウェア ファイルがエンドポイントで実行されるのをブロックします。

- Cisco E メール セキュリティ：クラウドとオンプレミスの両方で、フィッシング メッセージとスパム メッセージがランサムウェアを配布するのを阻止します。
- Advanced Malware Protection：簡単なライセンスによって電子メール セキュリティ製品にすぐに追加でき、Cisco E メール セキュリティ ゲートウェイを通過する不明な添付ファイルの静的および動的な分析（サンドボクシング）を提供します。
- Cisco Firepower™ 次世代ファイアウォール（NGFW）：ネットワークを通過する指揮統制トラフィックと悪意のあるファイルをブロックします。
- シスコ ネットワークを介した Cisco ISE：ネットワークを動的にセグメント化し、ランサムウェアの横展開を防ぎます。

Ransomware Defense があれば、組織は自身のネットワークをエンフォーサとして使用して、マルウェアの拡散を封じ込めることができます。感染という最悪の事態が発生した場合でも、ランサムウェアはネットワーク上を容易には伝搬できません。

シスコ セキュリティ サービスは、感染後のインシデント対応において即座にトリアージを実施できます。また、AMP や NGFW などその他のソリューション製品の導入を合理化します。

主な機能

- ランサムウェアのネットワークへの侵入やラップトップへのダウンロードをブロックします。
- ネットワークへの侵入という最悪の事態が発生した場合には、ランサムウェアの封じ込めを行います。

セキュリティ サービスはランサムウェアとの戦いに役立つ

シスコ セキュリティ サービスのインシデント対応チームは、インシデント対応レディネス サービスとランサムウェア発生後のリアクティブなインシデント対応の両方を提供できます。

また、Cisco Security Integration Services は、ソリューションレベルのアーキテクチャの課題を解決します。さらに、AMP for Endpoints や Cisco Firepower NGFW などのソリューション テクノロジーの導入を合理化します。シスコのチームは、統合セキュリティ ソリューションの提供に関する深い専門知識があり、必要なセキュリティ テクノロジーをほとんど中断なしで迅速に導入できます。

さらに広く見れば、組織はランサムウェア感染の影響を抑制するために、適切なデータ バックアップ テクノロジーとポリシーを導入しておく必要があります。

「当社は、ランサムウェアの Web 攻撃ベクトルの大きなリスクを遮断し、インターネット接続のユーザ エクスペリエンスを大幅に向上させました」。

— Octapharma

Cisco Capital

目標の達成を支援するファイナンス

Cisco Capital® は、目的達成と競争力の維持に必要なテクノロジーの調達をサポートします。お客様の CapEx を削減し、成功を加速させ、投資金額と ROI を最適化します。Cisco Capital ファイナンス プログラムは、お客様がハードウェア、ソフトウェア、サービス、および補完的なサードパーティ製機器を柔軟に取得できるようにします。また、それらの購入を 1 つにまとめた計画的なお支払い方法をご用意しています。Cisco Capital は 100 ヵ国以上でサービスを利用できます。詳細はこちら。

シスコの優位性

ランサムウェアは、必要なあらゆる手段を使って組織に侵入しようとします。これには、フィッシング電子メール、感染した Web バナー、スパムなどが含まれます。そのため、多数のベクトルを保護する必要があります。ランサムウェアの問題に直面するなか、セキュリティ アーキテクチャの実現に取り組んでいるのはシスコだけです。ポイント製品だけでは不十分です。シスコのソリューションは、業界トップクラスの Talos Research Group の調査に基づいています。Talos Research Group は、ランサムウェアに関する広範な脅威調査を実施し、シスコの効果的な階層型保護の原動力となっています。シスコは、ランサムウェアをブロックするとともに、不幸にもランサムウェアが見落とされてネットワークに侵入した場合でも対処します。