Cisco Ransomware Defense：ランサムウェアを阻止

ランサムウェアがどれだけネットワークへの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。シスコがすべての攻撃ポイントで脅威情報を共有し、緊密に統合されたソリューションで問題を解決へと導きます。

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、組織のコンピュータに保存されているドキュメント、財務記録、顧客データ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、暗号化を解除するための身代金を支払わない限り元に戻りません。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。その後、パッチが適用されていない脆弱性をワームのように効率よくエクスプロイトすることにより、感染が組織の横方向に広がる可能性があります。

Cisco® Ransomware Defense は、エンドポイントからネットワーク、電子メール、Web まで、階層型のアーキテクチャ 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兼ね備えた、統合された防御を提供します。

利点

- **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。**
- DNS レイヤからネットワーク、エンドポイントに至るまでの**卓越した可視性と応答性が得られます。**
- 強力なネットワーク セグメンテーションにより、**マルウェアが横方向に広がるのを阻止できます。**
- すべての脅威ベクトルにわたる **Talos の脅威インテリジェンスにより、さらに多くの脅威を素早くブロックできます。**

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、ランサムウェアの市場規模は年間 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。

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。防御する側には、次のような対応が求められます。

- 電子メールと Web の両方を保護する。
- 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。
- あらゆる手段でエンドポイントにアクセスしようとするランサムウェア ファイルを阻止する。
- コマンドアンドコントロール コールバックが使用されるのをブロックする。
- 感染が発生した場合にランサムウェアが横方向に移動するのを阻止する。

購入するもの

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ネットワーク 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 :** 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 は、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。

Ransomware Defense があれば、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、感染した場合のトリアージを即座に実施できます。また導入を合理化し、ソリューションが環境内で最大限の効果を発揮する設定になるよう支援します。

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。
- すべての製品で脅威インテリジェンスを共有し、一元的かつ協調的な防御を実現します。

「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 社グローバル シニア ネットワーク エンジニア、Jason Hancock 氏

次のステップ

シスコのセールス担当者に Cisco Ransomware Defense の詳細を問い合わせることで、貴社の最も得意な分野に専念してください。シスコの Web ページ（https://www.cisco.com/jp/go/ransomware）をご覧ください。

ランサムウェアとの戦いを支援するセキュリティ サービス

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。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、AMP などの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。

Cisco Capital

Cisco Capital® ファイナンスは、目標を達成して競争力を維持するために必要なテクノロジーのご購入をお手伝いします。CapEx の削減をサポートし、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、支払に関しては予測可能な支払方法をご用意しています。Cisco Capital は 100 ヵ国以上で利用できます。Cisco Capital の詳細はこちらをご覧ください。

シスコのメリット

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、複数の製品や脅威ベクトルで可視性を実現して脅威インテリジェンスを共有することはできません。Cisco Ransomware Defense は、Web、電子メール、およびエンドポイント製品全体でランサムウェアの動作と詳細を共有する、業界トップレベルの Talos Research Group に支えられています。Talos の支援により、電子メールで検出された脅威が Web 接続からエンドポイントへと転送されないようにブロックできます（その逆方向も同様です）。この「一度検出した脅威をあらゆる場所でブロックする」機能が、検出までの時間を短縮して場所を問わずユーザを保護し、お客様の会社が将来大きく報道されることがないようにします。

C22-737492-02　10/17