ランサムウェア：必要な知識

あなたは忙しく疲れています。あなたはただ Pokémon Go で遊んだり、会社のイントラネットにアクセスしたりしたいだけです。理由はどうあれ、ソフトウェア アップデートで [後で通知（Remind me later）] をクリックしたときには必ず、デバイスがランサムウェアのリスクにさらされることになります。

ランサムウェアがシステムに侵入する方法は多数あり、これはその 1 つに過ぎません。敵がシステムを攻撃する際に使用する一般的な戦術として、マルバタイジングやフィッシング電子メールがあります。また、高度なサムドライブ スキームを使用することさえあります。ある一般的なシナリオについて詳しく見てみましょう。

[後で通知（Remind me later）] をクリック

完璧なソフトウェアは存在しません。開発者は定期的にプログラムのバグを見つけ、それを修正するためのパッチをリリースします。プラグインやアプリケーションの更新を怠ると、敵はそれらの既知の脆弱性を簡単に悪用できます。一般的なエクスプロイト キットで言えば、成功した試みの 80 % を Flash が占めます。Flash であれ、Silverlight であれ、Google Chrome であれ、定期的な更新とパッチの適用を怠らないでください。

感染

デバイスで、ランサムウェアがターゲット システムを掌握します。続いて、非対称キー交換を使用してファイルを暗号化します。基本的に、ランサムウェアはユーザの同意なしにユーザ データにスクランブルをかけることができます。そしてこれを解除するキーを持っているのはランサムウェアの開発者だけです。一部のランサムウェアはネットワーク経由でも広がります。セキュリティの専門家は、この自己増殖型ランサムウェアが今後さらに蔓延すると予測しています。

身代金要求メッセージの表示

感染が完了すると、データと引き換えに身代金をビットコインで支払うように要求するメッセージが画面に表示されます。身代金の一般的な金額は 200 ～ 10,000 ドルですが、これよりもはるかに大きな金額を支払った組織もあります。カリフォルニアのある病院は、データと引き換えに 17,000 ドル支払いました。この病院は、身代金を支払うまでの間、毎日 100,000 ドルの損失を被り、正常な運営ができませんでした。

セキュリティ専門家は身代金を支払わないように勧めています。一部のランサムウェアは、ファイルのロック解が不可能であるか、あるいはファイルを自動的に破壊します。Talos の脅威研究者によると、このような悪意のある「すべて破壊」型のランサムウェアは急速に広がっています。2016 年の中期セキュリティ レポートでは、脅威研究者はデータの整合性がランサムウェアにおける新たな懸念事項になっていると警告しています。攻撃者が暗号化したデータの整合性を保持するとは考えられず、医療記録やエンジニアリング設計などの改ざんによる潜在的影響は計り知れません。

さらに、身代金を支払うことで犯罪組織をサポートしています。攻撃者は、この方法から収益を上げることができる限り、より強力なランサムウェアを作成し続けます。

ランサムウェアを阻止する方法

ランサムウェアに備える最善の方法は、階層化セキュリティ アプローチを導入することです。

攻撃前

いくつかの簡単な方法で防御態勢を強化できます。最悪の事態が発生した場合にもビジネスを円滑に継続できるように、ディザスタ リカバリ パートナーをバックアップ プランとして使用することを積極的に検討する必要があります。ただし、よりシンプルな対策も実施できます。ファイルを定期的にバックアップして重要なデータを保護することです。広告ブロッカーをインストールし、更新を求められた際には必ず更新することです。

ただし、広告ブロッカーだけですべてのマルバタイジングを検出してブロックしたり、不正なリンクを特定したりすることはできません。Cisco® Umbrella を使用することを検討してください。わずかな時間でインストールできるこのソフトウェアは、悪意のあるサイトを検出し、ホスト レベルで要求をブロックします。

攻撃中

Umbrella があれば、ランサムウェア ファイルの大多数が DNS レイヤで阻止され、エンド ユーザのデバイスに到達することさえできません。防御に最大限の努力を払っているにもかかわらず、マルウェアから完全に保護する方法はありません。

ネットワーク内で起こっていることを把握し、攻撃が起こったときにそれを特定する必要があります。Cisco Stealthwatch™ 脅威検出は、ネットワーク トラフィックを監視してランサムウェアの感染などの異常事態の発生を検知し、システムが侵害されたというアラートを出します。

ランサムウェア：必要な知識

シスコには、ファイルの実行を未然に防ぐ強力なツールがあります。

- Umbrella は、ファイルの暗号化キー インフラストラクチャへの要求をブロックしてシステムを保護します。つまり、ランサムウェアは暗号化キー インフラストラクチャからの応答を受信できず、データの暗号化に必要な情報を取得できません。
- Umbrella が要求をブロックすると同時に、シスコの次世代ファイアウォールが接続をブロックします。これにより、保護がさらに強化されます。
- ファイルが DNS レイヤとファイアウォールの両方を通過した場合は、Advanced Malware Protection（AMP）for Endpoints がファイルの実行をブロックできます。これにより、さらに一歩進んだ保護が実現します。AMP は、システム全体におけるファイルアクティビティをすべて分析し、悪意のあるファイルをすべて検出して削除できるようにします。

攻撃後

すでにランサムウェアに侵害されている場合は、被害状況を詳しく調べ、被害の拡大を食い止める必要があります。AMP は、エンドポイントで既知のマルウェア ファイルが実行されるのを阻止し、そのファイルを削除できます。

Cisco TrustSec® テクノロジーの動的セグメンテーションを使用すると、ランサムウェアがネットワークのどの部分まで到達したかを特定し、マルウェアがそれ以上広がるのを食い止めることができます。これにより、ランサムウェアがネットワーク全体に拡散するのを阻止できます。

詳細を知りたくありませんか？ cisco.com/jp/go/ransomware をご確認ください。

C11-737870-00 12/16