SOPHOS

リモートランサムウェア

悪意のあるリモート暗号化は、人間によるランサムウェア攻撃の約 60% で使用されている一般的なランサムウェアの手法です[1]。ほとんどの主要なエンドポイントセキュリティソリューションは、このアプローチに苦戦しており、Sophos Endpoint を使用していない場合は、危険にさらされる可能性が高くなります。このガイドでは、リモートランサムウェアのリスクと、それを阻止するソフォスの業界トップクラスのランサムウェア対策について説明します。

リモートランサムウェアとは？

リモートランサムウェアは、悪意のあるリモート暗号化とも呼ばれており、侵害されたエンドポイントを使用して、同じネットワーク上の他のデバイスにあるデータを暗号化します。

人間主導の攻撃では、攻撃者は通常、暗号化したいマシンにランサムウェアを直接展開しようとします。最初の試みが (たとえば、ターゲットデバイスのセキュリティ技術などによって) ブロックされた場合でも、諦めることはめったになく、その代わりに別のアプローチに切り替えて何度も試みることを選択します。

攻撃者が一旦デバイスの侵害に成功すると、組織のドメインアーキテクチャを活用して、管理されたドメインに参加しているマシン上のデータを暗号化することができます。悪意のあるすべてのアクティビティ (イングレス、ペイロードの実行、暗号化) は、すでに侵害されたマシン上で発生するため、最新のセキュリティスタックはバイパスされます。唯一のセキュリティ侵害の痕跡は、他のマシンとの間でドキュメントを送受信することです。

リモート暗号化の侵害の 80% は、ネットワーク上[2]の管理対象外のデバイスから発生していますが、攻撃者がデバイスに侵入するのを阻止するための防御策を欠いている、保護されたマシンから開始される場合もあります。

リモートランサムウェアが蔓延している理由とは？

このアプローチの普及を促進するようになった主な要因は、そのスケーラビリティ性です。管理されていない、または保護されていない単一のエンドポイントは、他のすべてのデバイスが次世代エンドポイント セキュリティ ソリューションを実行する場合でも、組織全体にわたって悪意のあるリモート暗号化にさらされる可能性があります。

さらに悪いことに、攻撃者はこれらの攻撃に対するランサムウェアの亜種の選択に制限がありません。Akira、BitPaymer、BlackCat、BlackMatter、Conti、Crytox、DarkSide、Dharma、LockBit、MedusaLocker、Phobos、Royal、Ryuk、WannaCry など、さまざまな有名なランサムウェアファミリーが悪意のあるリモート暗号化をサポートしています。

リモートランサムウェアが蔓延しているもう 1つの大きな理由は、ほとんどのエンドポイントセキュリティ製品は、保護されたエンドポイントで悪意のあるランサムウェアファイルやプロセスを検出することに重点を置いているため、このシナリオでは効果がないということです。ただし、リモート暗号化攻撃では、侵害されたマシン上でプロセスが実行されるため、エンドポイント保護は悪意のあるアクティビティを認識できなくなります。

これに対し、Sophos Endpoint は、業界をリードする CryptoGuard 保護機能により、悪意のあるリモート暗号化に対する堅牢な保護機能が備わっています。

Sophos CryptoGuard：業界をリードするユニバーサルなランサムウェア対策

Sophos Endpoint には、すべての Sophos Endpoint サブスクリプションに含まれる独自のランサムウェア対策テクノロジーである CryptoGuard など、ランサムウェアから組織を保護する複数の保護レイヤーが含まれています。

悪意のあるファイルやプロセスのみを探す他社のエンドポイント セキュリティ ソリューションとは異なり、CryptoGuardは、プロセスが実行されている場所に関係なく、データファイルを分析して悪意のある暗号化の兆候がないか調べます。このアプローチにより、悪意のあるリモート暗号化を含むあらゆる形態のランサムウェアを阻止するのに非常に効果的です。悪意のある暗号化が検出されると、CryptoGuard は自動的にアクティビティをブロックし、ファイルを暗号化されていない状態にロールバックします。

CryptoGuard は、ファイルの読み取りと書き込み時にすべてのドキュメントの内容を積極的に調査し、数学的分析を使用して暗号化されているかどうかを判断します。この普遍的なアプローチは業界でも類を見ないものであり、Sophos Endpoint は、リモート攻撃やこれまでに見たことのないランサムウェアの亜種など、他のソリューションでは見逃すランサムウェア攻撃を阻止できます。

CryptoGuard は、Sophos Endpoint の独自の機能の 1つで、すべての Sophos Intercept X Advanced、Sophos XDR、Sophos MDR サブスクリプションに含まれています。さらに、この機能はデフォルトで自動的に有効になっているため、組織はローカルとリモートの両方のランサムウェア攻撃から完全な保護をすぐに得られます。微調整や設定は必要ありません。

- **ファイルの内容を分析して悪意のある暗号化を検出**

  悪意のあるコードの検出に重点を置いたマルウェア対策の観点からランサムウェアを探す他社のソリューションとは異なり、CryptoGuard は、数学的アルゴリズムを使用してコンテンツを分析することにより、ファイルの大量かつ高速な暗号化を探します。

- **ローカルとリモートの両方のランサムウェア攻撃をブロック**

  CryptoGuard はファイルの内容に焦点を当てているため、悪意のあるプロセスが被害者のデバイスで実行されていない場合でも、ランサムウェアの暗号化の試みが検出できます。

- **悪意のある暗号化を自動的にロールバック**

  CryptoGuard は、変更されたファイルの一時的なバックアップを作成し、大量の暗号化を検出すると、変更を自動的にロールバックします。ソフォスは、攻撃者が回避することで知られている Windows ボリューム シャドウ コピーを使用する他社のソリューションとは異なり、独自のアプローチを使用しています。リカバリ可能なファイルのサイズと種類に制限がないため、ビジネスの生産性への影響が最小限に抑えられます。

- **リモートデバイスを自動的にブロック**

  リモートランサムウェア攻撃では、CryptoGuard が、被害者のマシン上のファイルを暗号化しようとするリモートデバイスの IP アドレスを自動的にブロックします。

- **マスター ブート レコード (MBR) の保護**

  CryptoGuard は、マスター ブート レコードを暗号化して起動を妨げるランサムウェアや、ハードディスクを消去する攻撃からデバイスを保護します。

保護されていないデバイスの検出

保護されていないエンドポイントが 1つあると、組織はリモート暗号化攻撃に対して脆弱になる可能性があります。Sophos Endpoint を導入することで、悪意のある暗号化に対する堅牢なユニバーサルランサムウェア保護が提供されますが、そもそもネットワーク上に保護されていないデバイスがあるかどうかを特定するにはどうすればよいでしょうか？

そこで役立つのが、Sophos Network Detection and Response (NDR) です。Sophos NDR は、ネットワークトラフィックの不審なフローがないか監視し、その際に保護されていないデバイスと環境内の不正なアセットを特定します。

リモートランサムウェア攻撃に対する強力な保護を実現するには、環境内のすべてのマシンに Sophos Endpoint をインストールし、Sophos NDR を導入してネットワーク上の保護されていないデバイスを検出します。

リモートランサムウェアに対する保護を今すぐ強化

悪意のあるリモート暗号化は、ほとんどの主要なエンドポイント セキュリティ ソリューションが阻止するのに苦労している一般的なランサムウェア手法です。Sophos Endpoint を使用していない場合は、危険にさらされる可能性が高くなります。

Sophos Endpoint の詳細と、リモートランサムウェアを含む今日の高度な攻撃に対する組織の防御を強化する方法については、ソフォスのアドバイザーまたはソフォスのパートナーにお問い合わせください。また、30日間の無償評価版で、ご自身の環境で試用することもできます。

1 Microsoft デジタル防衛レポート。https://www.microsoft.com/ja-jp/security/security-insider/microsoft-digital-defense-report-2023

2 Burt, T. (2023年 10月 5日)。Espionage fuels global cyberattacks.Microsoft. https://blogs.microsoft.com/on-the-issues/2023/10/05/microsoft-digital-defense-report-2023-global-cyberattacks/

ソフォスは、業界をリードするサイバーセキュリティソリューションをあらゆる規模の企業に提供し、マルウェア、ランサムウェア、フィッシングなどの高度な脅威をリアルタイムで保護します。実績のある次世代機能により、AI と機械学習を駆使した製品でビジネスデータを効率的に保護できます。

2023-12-06 (WP-DD)