ホワイトペーパー

Akamai の各種エンタープライズセキュリティ製品でランサムウェアのキルチェーンを断ち切る

目次

はじめに

Akamai のエンタープライズ・セキュリティ・ソリューションを活用してキルチェーンの各段階でランサムウェアを阻止する

マルウェアの一種であるランサムウェアは、現在、組織が直面している最大のセキュリティ脅威の 1 つです。ランサムウェアは、デバイス上の重要なファイルを暗号化し、それらを使用不能にします。ランサムウェアのオペレーターは、それらのファイルを元のデータに復元できる復号鍵やソフトウェアと引き換えに金銭を要求します。ここ数年で、ランサムウェアの犯罪集団は手口を変化させてきました。被害者のデータを盗み出し、データの公開やダーク Web での販売を新たな脅しの道具として使い始めています。

この種の攻撃を防御するためには、ランサムウェア集団が目的達成のためにどんな手段を使用するのか、十分に理解することが重要です。そのために、ぜひこのホワイトペーパーをお役立てください。

ランサムウェアのキルチェーンとは

ランサムウェア攻撃は複雑であり、システムへの侵入は始まりにすぎません。攻撃者は最大限の損害を与えるために、暗号化を開始する前に悪性のペイロードをネットワーク全体に拡散させなければなりません。1 台のコンピューターを暗号化しただけでは、金銭を要求する脅しの道具として不十分だからです。ランサムウェア攻撃を成功させるためには、ネットワークアセットの発見、横方向の移動など、さまざまな手順を実行する必要があります。このような手順は一般的にランサムウェアのキルチェーンと呼ばれています。

このキルチェーンの各段階に、検知と緩和のチャンスがたくさんあります。Akamai の各種のエンタープライズセキュリティ製品で、あらかじめネットワークの備えを固めておけば、アタックサーフェスを縮小し、攻撃に気づく前に、ランサムウェアによって生じる可能性のある被害を緩和し、封じ込めることができます。このホワイトペーパーでは、Akamai Guardicore Segmentation、Enterprise Application Access、Secure Internet Access を使用して、キルチェーンのさまざまな段階でランサムウェアのアクティビティを検知しブロックする方法について、詳しく説明します。

最初のアクセス
攻撃の第 1 フェーズです。攻撃者は外側から内部ネットワークに侵入します

発見
これにより、攻撃者はネットワーク内部の重要なアセットを特定します

ラテラルムーブメント
このフェーズでは、攻撃者はネットワーク全体に拡散し、さらに多くのアセットを侵害します

コマンド & コントロール
さまざまな方法で攻撃者はネットワークへの通信チャンネルを維持し、侵害したアセットに情報やコマンドを送信します

データ窃取
攻撃者は、盗まれた機微な情報をひそかに持ち出します。

最初のアクセス

組織内にはインターネットを使用するインターフェースが数多く存在します。攻撃者はこのようなインターフェースを悪用してネットワークへのアクセス権を取得しようとします。Akamai を利用すれば、これらのインターフェースをシームレスに保護して、攻撃者をネットワークから閉め出すことができます。

インターネットに面したサーバーの保護

Secure Internet Access のペイロード分析機能を使用して、インターネットに面したサーバーを保護し、悪用されないようにします

Kaspersky によると、攻撃者が最初のアクセスを成功させるために使用する最も一般的な手口は、インターネットに面したアプリケーションの悪用です。特に多いのは、パッチが適用されていないシステムのワンデイ脆弱性が悪用されるケースです。また、Log4Shell（CVE-2021-44228）や ProxyLogon（CVE-2021-26855）などの脆弱性も、いまだにネットワークへの侵入やランサムウェアの導入を目的として悪用されています。

Enterprise Threat Protector は、設定により、インターネットに面したサーバーへの着信 Web トラフィックをすべて監視して分析できます。さらに、悪性のアクティビティや異常なアクティビティが特定された場合は、それらをブロックできます。

フィッシング URL のブロック

Enterprise Threat Protector の URL 検査機能を使用し、フィッシングの試みを検知してブロックします

フィッシングはネットワークへの侵入方法として頻繁に使用されています。多くの場合、攻撃者は、認証情報を盗むように設計された悪性の添付ファイルや偽りのログインページへのリンクをメールに入れて送信します。エンドポイントに Enterprise Threat Protector クライアントがあれば、ユーザーがクリックする各 URL をリアルタイムでスキャンできるので、悪性のリンクや異常なリンクの特定とブロックが可能となります。

VPN アタックサーフェスの縮小

Enterprise Application Access を使用して、アプリケーション単位での安全な VPN アクセスを可能にし、外部からのアタックサーフェスを縮小します

テレワークが増え、職場環境のハイブリッド化が進むに伴い、ユーザーが VPN を使用して会社のネットワークにログインするケースもますます一般的になりつつあります。攻撃者の方も適応し、内部ネットワークへのアクセス権を取得するために、このような環境を悪用し始めています。よく見られるのは、従業員のパーソナルコンピューターを攻撃して、その従業員の VPN 認証情報を侵害し、その情報を使用して内部ネットワークにアクセスする手口です。また、脆弱なサーバーを狙って認証情報を漏えいさせる攻撃者もいます。2022 年 11 月には、Fortinet VPN サーバーの脆弱性を悪用して最初のアクセスに成功し、ネットワーク全体にランサムウェアを拡散するという攻撃が発生しました。

Enterprise Application Access を使用すれば、アプリケーション単位でロールベースのアクセスを許可できるので、このようなリスクを大幅に軽減できます。重要なのは、従来の VPN のようにネットワーク全体へのフルアクセス権をユーザーに付与するのではなく、特定のアプリケーションへの限定的なアクセスのみを許可することです。こうすることで、たとえ攻撃者がユーザーの認証情報を侵害し、多要素認証（MFA）による保護を回避したとしても、ネットワーク全体にアクセスすることはできません。攻撃者のアクセス対象を一部のアプリケーションセットのみに限定できます。

コマンド & コントロール

コマンド & コントロール（C2）サーバーのブロック

Akamai Secure Internet Access を使用して、既知のマルウェアのコマンド & コントロールサーバーをブロックします

一般的なマルウェア、特にランサムウェアは、コマンドの送信や、感染させたアセットからの情報取得のために、外部 C2 サーバーとの通信を必要とします。Akamai の広範な通信データを分析することで、ランサムウェアとマルウェアの C2 ドメインを監視し、新しい攻撃キャンペーンやそれらの変化を追跡できます。Enterprise Threat Protector クライアントは DNS 通信全体のリアルタイム監視を可能にし、悪性ドメインとの通信をブロックできます。これにより、マルウェアは正常に稼働せず、目的を達成できなくなります。

発見

攻撃者は、いったんネットワークに侵入すると、横方向への移動を開始する前にまず、ネットワーク構造を理解するためにさらにアセットを特定しようとします。多くの場合、この間に内部通信が発生しますが、Akamai Guardicore Segmentation を使用すると、これを検知できます。

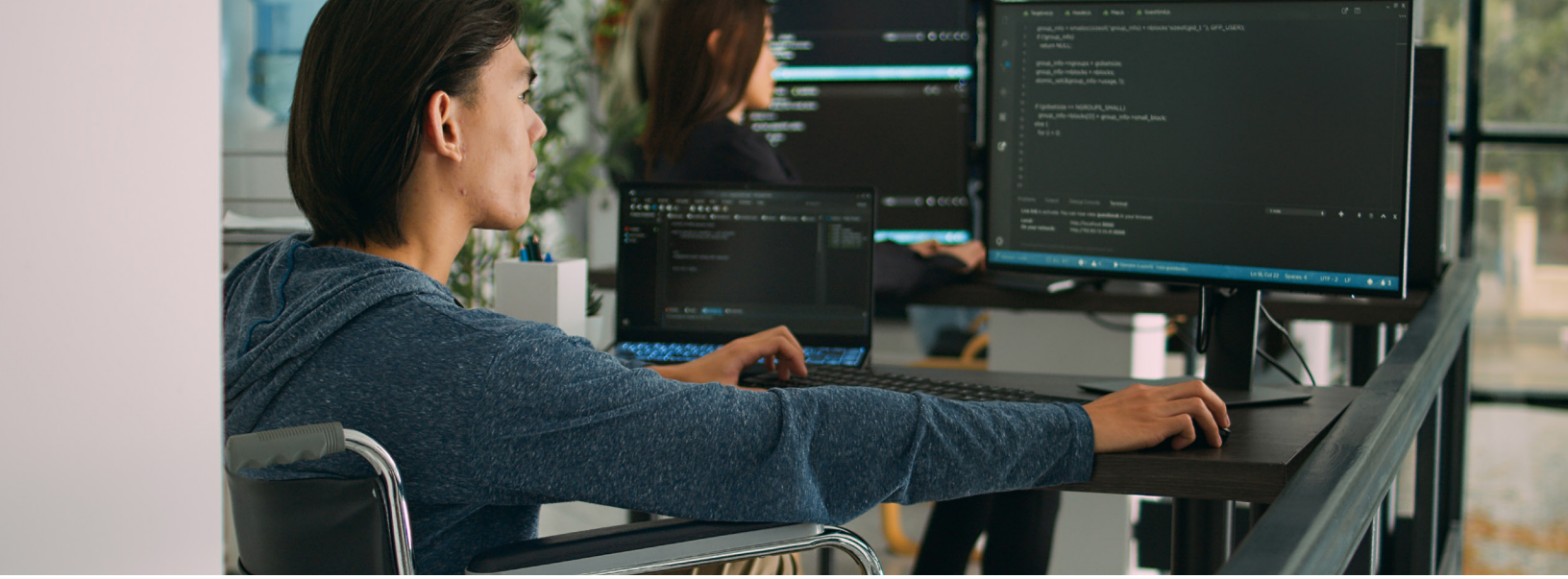
ネットワークスキャンの特定

> Akamai Guardicore Segmentation の検知機能を使用して、疑わしいネットワークスキャンを特定します

ポートスキャンによるネットワークサービスの特定は、攻撃者がネットワークを発見するために使用する一般的な手法の 1 つです。ランサムウェア集団の多くがオープンソースのネットワークスキャナーを使用しているようです。最近の LockBit 3.0 ランサムウェアに関する CISA Advisory では、ランサムウェア集団はポートスキャンに「SoftPerfect Network Scanner」を使用していると示唆されています。また、Nokoyawa ランサムウェア集団は機微な情報にアクセスするために、SQL サーバーのネットワークをスキャンしていることが観察されています。

Akamai Guardicore Segmentation は、お客様のネットワーク内のすべての通信を監視し、組み込まれている検知機能によってこうしたスキャンを特定し、アラートを送信します。これにより、拡散が始まる前にマルウェアのアクティビティを阻止できます。

図 1：Akamai Guardicore Segmentation でのネットワークスキャンインシデント



発見を阻止する手法

Akamai Guardicore Segmentation を使用して発見の試みを特定します

攻撃者は、ネットワークに侵入した時点ですでにそのネットワークの構造やさまざまなアセットについて知っているわけではありません。そのため、暗闇のなかを手探りで進む道を見つけようとします。Akamai Guardicore Segmentation のディセプションサービスを使用すれば、攻撃者をハニーポットサーバーにおびき寄せ、その活動を監視できます。そして異常が検知された場合はアラートが送信されます。

たとえば、攻撃者がネットワークに侵入し、総当たり攻撃で Linux サーバーの SSH 認証情報を取得しようとしたとします。Akamai Guardicore Segmentation はこの異常を特定し、動的に生成されたハニーポットに攻撃者を誘導します。ハニーポットでは攻撃者のアクションがすべてログに記録され、アラートが生成されます。

以下はこのようなアラートの一例です。

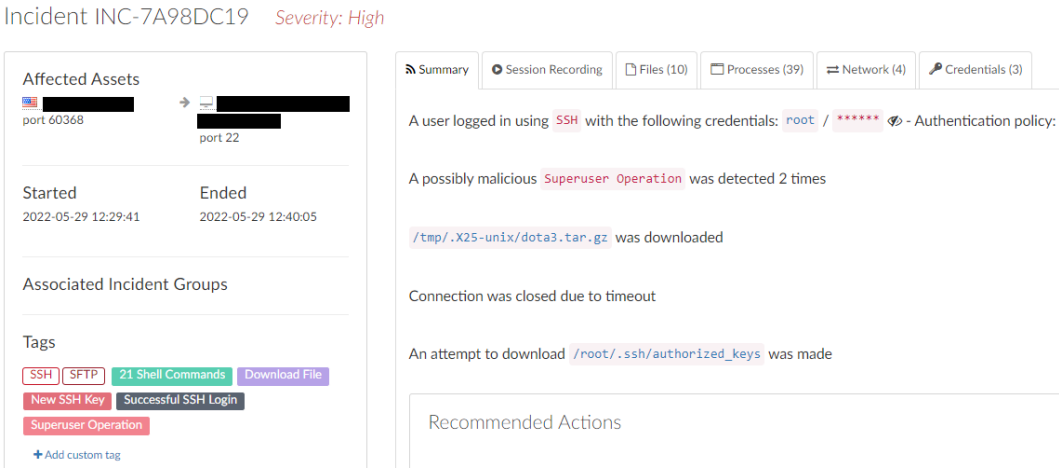


図 2 : Akamai Guardicore Segmentation でのディセプションインシデント

ラテラルムーブメント

ネットワークへのアクセス権を取得して、そのネットワークのトポロジーを詳しく知った攻撃者は、その知識を利用して横方向に移動しようとします。最近のランサムウェア集団は、ネットワークに侵入してから横方向に移動することで、できる限り多くのアセットを侵害し、それらすべてを暗号化します。Akamai のエンタープライズセキュリティ製品は、このような横方向の移動（ラテラルムーブメント）の可能性を制限し、侵入範囲を最小限に抑えます。

疑わしいホストインジケーターの特定

> Akamai Guardicore Segmentation の Insight モジュールを使用し、さまざまな方法で、疑わしいホストインジケーターを特定します

攻撃者は PowerShell ツールを使用して多様な目的を達成します。ラテラルムーブメントもそのような目的の 1 つです。PowerShell ドロッパーは非常に一般的なツールであり、多くの攻撃者が感染アセットで実行する最初のコードピースとしてこのドロッパーを使用しています。最近発生した Quantum ランサムウェアの感染はまさにこのような手口であったことが明らかとなっています。それは、Windows Management Instrumentation（WMI）を使用する PowerShell コードを実行する手法です。

Akamai Guardicore Segmentation の Insight モジュールを使用すれば、定期的にクエリーを実行して、すべてのアセットの PowerShell イベントログをスキャンし、悪性のインジケーターが見つかったアセットをラベル付けして隔離できます。

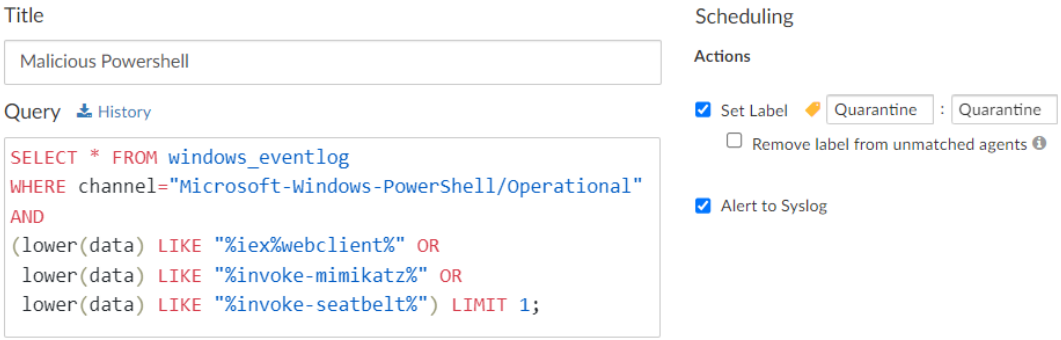


図 3：悪性の PowerShell を検知する定期的な Insight クエリーの作成

しかし、PowerShell は 1 つの例にすぎません。Insight では、たとえば、既存の osquery テーブルを使用してラテラルムーブメントのさまざまなインジケーターをスキャンすることもできます。

- File テーブルを使用すると、名前またはハッシュに基づいてマルウェアファイルを検知できます。
- Startup Items テーブルを使用すると、アセットでの疑わしい自動実行エントリを検知できます。
- Yara テーブルを使用すると、yara ルールを使用してアセットのファイルをスキャンし、マルウェアの痕跡を検知できます。

LAN 攻撃の阻止

Akamai Guardicore Segmentation を使用して、ローカル・ネットワーク・プロトコルに対する攻撃のブロックと検知を行います。

ネットワーク内の最初の感染後、攻撃者は ARP などの LAN プロトコルの脆弱性を悪用し、他のアセットに感染を拡げます。従来型のファイアウォールを使用すると、このような攻撃はレイヤー 2 で実行されるため、レーダーを容易にかいくぐることができ、このタイプの通信はファイアウォールに到達しません。

Akamai Guardicore Segmentation は、ソフトウェアベースのアプローチなので、アセットに出入りするすべてのトラフィックを監視してブロックできます。通常、ファイアウォールには到達しないようなローカルトラフィックでさえも対象となります。

管理ポートの制限

Akamai Guardicore Segmentation を使用して、プロセスレベルのポリシーを作成し、機微なポートのアタックサーフェスを縮小します

ネットワーク内に入った攻撃者は、通常、認証情報を盗むために、感染アセットに対する権限のエスカレーションを実行します。そして認証情報を取得すると、たいていは RDP、RPC、SMB、WinRM などの管理プロトコルを使用して、ネットワーク内のすべてのアセットに対してランサムウェアペイロードを実行します。しかし、多くの場合、これらのポートを完全にブロックすることは現実的な選択肢ではありません。管理者はこれらのポートを日常業務に必要としているからです。

Akamai Guardicore Segmentation では、プロセスレベルでポリシーを適用できるので、機微な管理ポートで通信すべきプロセスを区別できます。WinRM の例を見てみましょう。これは、Ansible など多くの管理プログラムで使用されていますが、悪用も多く、攻撃者はラテラルムーブメントを実行するために Evil-WinRM のようなツールを使用しています。Akamai Guardicore Segmentation を使用して、WinRM の着信接続を Ansible プロセスからの場合のみ許可するようなポリシーを作成すれば、同じポートを使用する他のプロセスをブロックできます。

Section	Source	Destination	Ports/Protocols	Action
Allow	ansible-operator	Windows Any	5985 TCP | UDP	Allow
Block	Any	Windows Any	5985 TCP | UDP	Block

図 4：WinRM 通信を制限する Akamai Guardicore Segmentation ポリシーの例

データ窃取

ここ数年、攻撃者は脅迫の手口を変化させ、被害者の機微なファイルの漏えいも脅迫の道具として使うようになりました。攻撃者はネットワークノイズに紛れて組織のデータを盗み出そうとしますが、この段階でもまだ、検知しブロックすることが可能です。

窃取ドメインのブロック

Akamai Guardicore Segmentation を使用して、データ窃取に悪用される可能性のあるサービスへのアクセスを制限します

攻撃者はたいていパブリックツールを使用してネットワークからデータを漏えいさせます。特によく使用されているのは、MEGA、Dropbox、Google Drive などのパブリック・ホスティング・サービスです。こうしたドメインの監視を難しくしているのは、これらの多くがネットワーク内で正当な目的に使用されているという事実です。たとえば、ブラウザーを通じて MEGA ドメインにアクセスすることは、正当な行為と考えられます。しかし、同じ行為に rclone ユーティリティが使用された場合は悪性とみなすことができます。このユーティリティは一部の攻撃集団がデータ窃取を目的として活発に使用しています。

Akamai Guardicore Segmentation を使用し、すべてのエンドポイントについて、そのドメインへの不要なアクセスをブロックし、ブラウザーなどの承認済みのアプリケーションによるアクセスのみを許可すれば、これらのツールによるリスクを最小限に抑えることができます。

多層防御

攻撃者が最終的な目的を達するためには、数種類の攻撃フェーズが必要とされます。それらの各段階に、悪性のアクティビティをブロックし、検知する、チャンスがあります。各種の Akamai セキュリティ製品を活用すれば、ランサムウェアキルチェーンの各段階で緩和策を実行し、攻撃者の動きを止めて、異常なふるまいを検知することができます。

Akamai Guardicore Segmentation の詳細、または個別対応の製品デモのご依頼については、akamai.com/guardicore をご覧ください。

Akamai は、お客様が生み出すものすべてにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、従業員、システム、データを守ります。グローバルな脅威に対する可視性を備えた Akamai のプラットフォームは、セキュリティ体制の適応と進化を後押しして、ゼロトラストの実現、ランサムウェアの阻止、アプリケーションと API のセキュリティの確保、DDoS 攻撃の撃退を支援します。これにより、お客様は自信を持って、継続して、イノベーションを起こし、可能性を広げ、新たな可能性を生み出すことができます。Akamai のセキュリティ、コンピューティング、デリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。公開日:2023 年 9 月。