Zscaler Workload Segmentation によるランサムウェアの防御

水平方向のアプリケーション通信を保護し、
脅威の水平移動を阻止

Harry Sverdlove
Zscaler、セキュアワークロード通信担当チーフテクノロジスト

コンテンツ

はじめに：米国の医療機関が（再び）標的にされている

2020年に世界は多くの危機に次々と直面し、サイバーセキュリティの世界もその例外ではありませんでした。CISA（Cybersecurity and Infrastructure Agency）、FBI（Federal Bureau of Investigation）、HHS（Health and Human Services：米国保健社会福祉省）は先日、公衆衛生業界に対するランサムウェア攻撃の脅威が増大しているという警告を発表しました。米国の複数の病院がすでに標的になりました。

そのような攻撃は今に始まったものではなく、2019年には、政府機関や医療機関に対する140件以上のランサムウェア攻撃が確認されています。過去10年間、ランサムウェア攻撃の増加に伴い、同時に高度化や効率化も進みました。

ランサムウェアは、重要なファイルやオペレーティングシステム全体をユーザの知らぬ間に暗号化し、被害者（または被害者の組織）が身代金（一般的には暗号通貨）を払って復号鍵を手に入れるまでシステムを使用できなくするという攻撃です。すなわち、ランサムウェアとは、サイバー犯罪組織が金銭を手に入れる目的で仕掛ける攻撃です。この攻撃が標的のインフラストラクチャを混乱させることのみを目的に仕掛けられることも稀にはありますが、一般的には、身代金という利益を得ることが攻撃の動機です。

ランサムウェアの動作

ランサムウェアが確実に目的を達成するには、ネットワークで可能な限り多くのシステムに影響を与える必要があります。たとえば、数千ものシステムで暗号化して無効化できたシステムがひとつしかないのであれば、被害者がそのシステムの電源を切って再構築するだけですむ可能性も高くなります。影響を受けたシステムやファイルが多いほど、被害者が身代金を支払う確率が高くなります。警察やサイバーセキュリティのエキスパートは、身代金の支払いに応じないように呼びかけていますが、実際には、ダウンタイムによって 1 日あたり数百万ドルを失い、手作業で復旧するまでに数週間から数か月もかかるケースもあることから、支払いに応じて早く問題を解決しようと考えるのは自然な流れと言えます。

この攻撃では、標的とされた組織に関連する個人にフィッシングメールが送信され、そのメールに、マルウェアの一部（添付ファイル）やマルウェアの最初のペイロードを提供する不正 Web サイトへのリンクが含まれています。最初のマルウェアは、TrickBot（およびそれに関連する BazarLoader/BazarbackDoor トロイの木馬）ファミリに属します。

TrickBot はその後、さまざまな Windows プロセスに巧妙に自らをインストールし、コマンド&コントロール（C&C）サーバへのバックドアを確立し、追加コンポーネントをダウンロードし、一般的なツールを使用してネットワークマップを作成し、最終的にはネットワーク全体に活動の場を広げ

ます。TrickBot には、SMB エクスプロイトまたは RDP（リモートデスクトッププロトコル）経由でドメインコントローラまでを掌握できるモジュールが含まれています。

TrickBot が拡散すると、感染したコンピュータが Ryuk（またはその後継の Conti）ランサムウェアをダウンロードして起動します。このランサムウェアは、ローカルと共有ネットワークのどちらのファイルも暗号化することができます。

ランサムウェアスクリプトはいずれの場合も、以下の手順を実行します。

1. ユーザを誘導し、不正ローダファイルをダウンロードして実行するように仕向ける（または、エクスプロイトを使い、ユーザに知られることなく同様の処理を実行する）
2. ローダファイルを使ってサーバ（またはその他の侵害されたシステム）にアクセスし、他のコンポーネントをダウンロードする
3. ネットワークを詳しく調べ、他のシステムやファイル共有を特定する
4. 可能な限り多くのシステム、特にドメインコントローラなどの重要なインフラストラクチャに拡散する
5. ファイルを暗号化して、システムを完全に無効にするか、特定のデータにアクセスできないようにする

細かい点が異なったり、難読化や破壊の手段が多岐に渡ることもありますが、攻撃の本質が変わることはありません。

ランサムウェアの防止

セキュリティ対策の推奨事項のほとんどに、この攻撃シーケンスで上記の手順 1 と 5 への対策が含まれています。手順 1 の対策として推奨されているのは、電子メールのフィルタリングとユーザ教育を活用し、ユーザが不審なダウンロードや Web リンクをクリックしないようにすることです。効果的な方法ではありますが、これだけでは明らかに不十分です。ランサムウェア攻撃の頻度が増加し続けるのを防ぐことはできません。攻撃者が高度化し、不正と正規のメールを区別するのがこれまで以上に困難になっています。さらには、ユーザを騙す方法は他にもあり、たとえば、ウォーターホールと呼ばれる、標的にするユーザがよくアクセスする Web サイトを侵害するなどの方法があります。

手順 5 の対策としては、堅牢なバックアップとリカバリの計画を策定し、セキュリティ侵害によって暗号化されてしまったシステムを簡単に初期化し、復元できるようにしておきます。これは、ディザスタリカバリの方法としても有効です。ただし、（a）ランサムウェアは高度化しており、バックアップコピーも標的にできるようになっていて、（b）1 つのシステムだけを復元しようとしたものの、ドメインコントローラだけではなく、組織全体の数百のシステムの復元が必要になったとしたら、どうでしょうか。それは、悪夢であるのみならず、数週間を要することもあり、一部のデータは復元できない場合もあります。

Zscaler Workload Segmentation は、主として手順 2～4 の対策として、不正ペイロードによる C&C サーバの接続を防止し、ネットワークを詳しく調べて他のシステムに拡散するのを防止することで、攻撃の影響を最小限にします。

この対策においては、水平方向のトラフィックへのゼロトラストのアプローチの採用が有効な手段となります。ゼロトラストとは、アプリケーション、ユーザ、デバイスなどの承認されたエンティティだけに他の承認されたエンティティとの通信が許可されることを意味します。その前提となるのが、ネットワークそのものとそのアドレス/ポート/プロトコルは本質的に安全ではないという考え方です。トラストは、通信の「方法」だけでなく、通信する「ユーザ」によって確立されます。

同じネットワーク内のシステムが相互に通信できる場合、ほとんどのネットワークに過度のトラストが付与されます。ほとんどの企業ネットワークで許可されている経路の少なくとも 87%は、使用されないか、不要な経路です。このように不要な部分まで許可してしまうのは、従来のファイアウォールでは、接続を使用するエンティティに基づいてトラフィックをきめ細かく制限できないためです。たとえば、Active Directory を使用し、ドメインコントローラとクライアントがポート 88 と 135 で通信する必要がある場合を考えてみましょう。従来のファイアウォールで最も有効なのは、ネットワークの IP アドレスとそれらのポートに基づいてトラフィックを制限する方法です。この方法では、不正コードもこれらのアドレスとポートを使用し、情報収集やエクスプロイトの目的でコントローラと通信することができます。

NGFW（次世代ファイアウォール）は、トラフィックをインスペクションして条件に適合しているかどうかを確認できますが、不正ソフトウェアであっても、NGFW が「正規」と判断する構文を使用すれば、簡単にバイパスできてしまいます。また、NGFW が不審であると特定するには、実際に接続が発生する必要があり、エクスプロイトによっては、接続が「不正」と特定される前に既に攻撃が進行している場合もあります。さらには、すべてのシステム間のすべての通過点に NGFW を導入するには非常に多くのコストが必要で、物理ネットワークまたは仮想クラウドのどちらの環境でも、大きなネットワークラグが発生します。

Zscaler Workload Segmentation（ZWS）は、マイクロセグメンテーションの異なるアプローチを採用し、通信するアプリケーションとサービスの真のアイデンティティに基づくネットワークセキュリティを提供します。非承認や不正であるソフトウェアが、従来のファイアウォールで許可されているのとまったく同じアドレス、ポート、プロトコルを使用したり、NGFW のパケットインスペクションで特定されるとまったく同じ構文を使用したりした場合でもあっても、通信がブロックされます。

アイデンティティベースのマイクロセグメンテーションをネットワークで使用するメリットは他にもたくさんあり、具体的には、導入が容易になる（インフラストラクチャの変更が不要）、ポリシーが少なくてなり、管理も容易になる（必要なポリシーが大幅に少なくなる）、ポリシーの自動スケーリングが可能になる（ポリシーがネットワークアドレスではなくアイデンティティベースになる）、ネ

ットワークの可視性が向上する（アドレスだけでなく、アプリケーションの通信方法も把握できる）といったメリットがあります。セキュリティに限定したメリットという点でも、ZWS のアイデンティベースセキュリティによって、不正ローダが追加コンポーネントをダウンロードしたり、システムにすでに存在する正規のソフトウェアを使用してネットワークの調査やカタログの作成を実行したり、RDP や PSEXEC などの手段を使用して他のシステムにまで拡散したりするのを簡単に防止できるようになります。

攻撃シーケンスを止めて攻撃を阻止する

フィッシング攻撃を防ぐためのユーザ教育やシステムが破壊された場合の復元を可能にするバックアップ戦略の策定は有効ではありますが、ランサムウェアの阻止にはそれだけでは不十分です。ランサムウェア攻撃の多くの段階で、不正ソフトウェアや侵害されたソフトウェアとの不正通信が発生します。従来のファイアウォールはその対策にはなりませんが、ZWS のアイデンティベースのセグメンテーションであれば、ランサムウェアが環境で処理を繰り返しながら拡散するのを防止する有効な手段となります。金銭を要求するランサムウェア攻撃の対策を今こそ始める時です。

注：ゼットスケーラーの脅威ライブラリとクラウドサンドボックスは、Ryuk と Conti のどちらも検知できます。技術的な詳細は、こちらでご確認ください。