プルーフポイントのランサムウェア対策

組織への侵入と拡散の阻止

製品

- Proofpoint Advanced Threat Protection
- Proofpoint Cloud Security

主なメリット

- 初期感染を阻止
- 探索、ラテラルムーブメント、潜伏を阻止
- データの持ち出しを阻止

ランサムウェアは、今日のサイバー攻撃の中で最も破壊的な脅威の一つです。攻撃を受けてしまった企業は業務の中断を強いられ、病院では患者の治療を継続できなくなり、政府機関は機能停止状態にならざるを得ません。ランサムウェアは、現在最も危険なサイバー脅威の一つとなりました。昨年だけでも、米国では65,000件を超えるランサムウェア攻撃が発生しています。この脅威はCISOにとって最大の懸念事項であり、国家の安全保障に関わる問題にもなっています。しかし、驚くべきことですが、多くの組織がランサムウェア攻撃への備えをまだ行っていません。Ponemon Instituteの調査によると、自分の組織はランサムウェアを阻止できると答えたIT専門家はわずか13%に過ぎません。一方で、自分の組織が「脆弱」または「非常に脆弱」と答えたIT専門家は68%を超えています[1]。

主なランサムウェアの侵入口はメールとWebですが、大半のランサムウェアは段階的に攻撃を展開してきます。これらの攻撃では、メールまたは侵害されたWebサイトが攻撃チェーンの初期段階で重要な役割を果たしています。多くの場合、最初の攻撃でマルウェアのダウンローダーを配信します。これら配信されたもの(ペイロード)は、ユーザーのシステムに侵入することを目的としています。また、認証情報の窃盗やネットワーク接続のためにも使用されます。ランサムウェアの攻撃者は、盗み出した認証情報を使用して、インターネット上に公開されているサービスにアクセスし、認証情報を求めるフィッシングメールの送信、総当たり攻撃によるパスワードの取得、ドライブバイダウンロード攻撃などを行います。

最初の侵入に成功すると、攻撃者は潜伏を開始し、偵察活動と横展開を試みます。攻撃者は、重要なファイルを単に暗号化するだけでなく、重要な情報を盗み出そうとします。

これまでランサムウェアに対してはバックアップとリカバリが効果的な対策でしたが、攻撃者はこの対策を上回る「二重脅迫」という戦術に切り替えています。この手法では、まず重要なデータを盗み出した後にファイルを暗号化します。暗号化したデータの身代金を要求し、被害者が支払いを拒むと、さらに次の脅迫を行います。

1 Ponemon Institute.「The Rise of Ransomware」(ランサムウェアの台頭)2017年1月

- データをネット上にばらまくと脅す
- データをオークションにかけて最も高い入札者に送信する
- 被害者の顧客やパートナーに直接メールを送信し、情報をリークすると脅す

ランサムウェア攻撃の大半はメールが侵入口となっています。多くのランサムウェアは、フィッシングメールによって直接的または間接的に攻撃を開始します。フィッシングメールはユーザーを騙して、悪意のある添付ファイルを開かせたり、危険なURLをクリックさせたりします。このような脅威を検出して認証情報の流出を防ぐには、高度なソリューションが必要です。クラウド上に多くのデータを保存している組織では、パスワードファイルや機密データもクラウド上に保存している可能性があります。攻撃者にわたる情報を最小限にするには、クラウドの外部にデータを流出させないことが重要になります。

最近の傾向を見ると、攻撃対象が絞り込まれ、より壊滅的な被害をもたらすものが増えています。このような脅威を阻止するには、Proofpoint Advanced Threat ProtectionとProofpoint Cloud Securityが役立ちます。この包括的な統合プラットフォームを使用すると、次のような多層的な対策を行い、ランサムウェア攻撃のリスクを減らすことができます。

- 最初の感染を阻止
- 最初の感染を検出して、探索、ラテラルムーブメント、潜伏を阻止
- データの持ち出しを阻止

最初の感染を阻止

Proofpoint Advanced Threat ProtectionとProofpoint Cloud Securityは、次の機能によって最初の感染を未然に防ぎます。

- ランサムウェアとそのダウンローダーを検知して、ブロックする
- 認証情報の侵害を防ぐ
- ランサムウェアのリスクを可視化する
- リスクに基づいてURLのクリックを隔離する
- 不正なメッセージを識別して報告できるように、ユーザーを教育する
- メールの脅威から自動的に修復する

ランサムウェアとそのダウンローダーを検知しブロックする

Proofpoint Advanced Threat Protectionプラットフォームは、最初のペイロードでランサムウェアを検知し、ブロックします。また、ランサムウェアを取得するマルウェアもブロックします。プルーフポイントでは、複数の機械学習を基にしたエンジンにより、マルウェア、不正なコード、検知回避の技術を検出します。これにより、不正なWebサイトやランサムウェアに感染したファイルからユーザーを保護します。

このプラットフォームでは、レピュテーションとコンテンツの分析を行います。また、サンドボックス内でURLまたは添付ファイルに潜む脅威を詳しく分析します。予測分析により、攻撃者の戦術変更に合わせて不審なURLを特定して、サンドボックス内に隔離します。たとえば、多くの攻撃者は正規のファイル共有サイトにマルウェアを潜伏させています。このプラットフォームでは、すべてのファイル共有URLをサンドボックスに隔離します。レピュテーション分析のみに依存するソリューションでは、このような攻撃を見逃してしまいます。

認証情報の侵害を防ぐ

攻撃者は、様々な手口を駆使してユーザーの認証情報を盗み出そうとします。たとえば、フィッシング、総当たり攻撃、ダークウェブ、ユーザーのクラウドストレージに保存されている公開情報などを手に入れようとします。認証情報が使用できるようになれば、マルウェアのダウンローダーを散布する必要はありません。盗み出した認証情報を使用して、VPNやインターネットに接続しているサービスに簡単にログインし、機密データを盗み出したり、ファイルを暗号化したりできます。利用しているクラウドサービスが多い組織では、セキュリティ意識の低いユーザーがパスワードファイルや機密データをクラウドにアップロードしている可能性があります。

Proofpoint Advanced Threat Protectionは、複数の検出エンジンを使用してフィッシング メッセージを検出して阻止します（たとえば、機械学習を使用した分類ツールでURLの調査を行います）。Proofpoint Cloud Securityでは、攻撃者から狙われる可能性のあるクラウドアカウントに機密情報が保存されていないかどうか確認できます。

図1：3層のセキュリティ対策

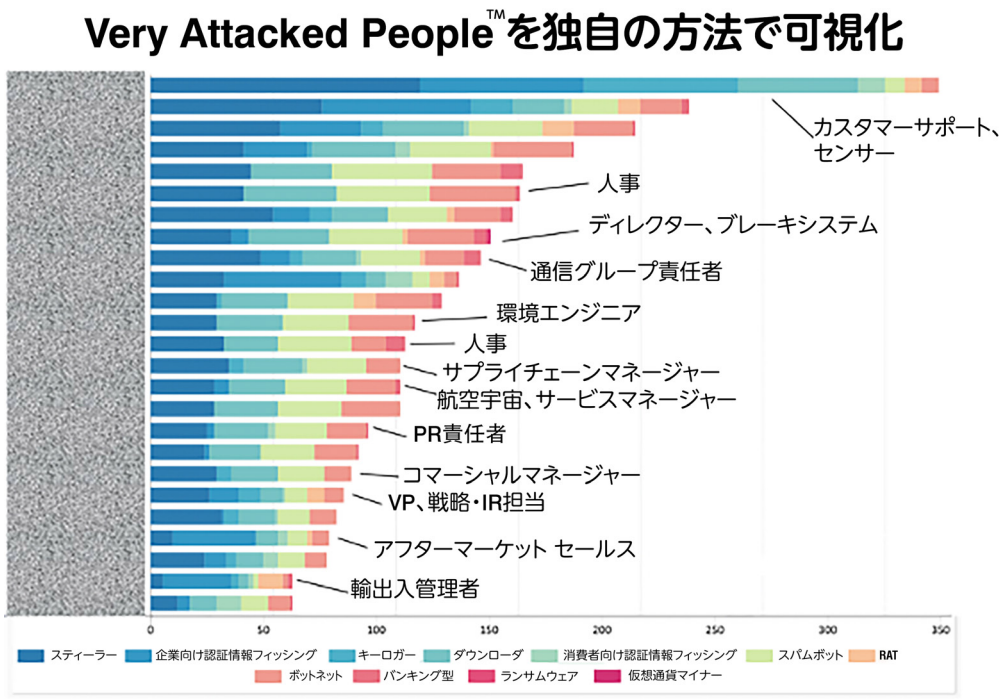

図2: プルーフポイントのソリューションを利用すると、Very Attacked People™（VAP）を可視化できる

ランサムウェアのリスクを可視化

プルーフポイントのソリューションを利用すると、Very Attacked People™（VAP）を可視化できます。VAPは、会社の中で最も攻撃を受けやすい人物です。この可視化機能により、最も狙われている人物と、その人物にどのような脅威が存在するのかを視覚的に確認できます。これにより、VAP™が直面している脅威に合わせて防御戦術を調整できます。

また、プルーフポイントは脅威とキャンペーンについて詳しい情報を提供します。Threat Insight ダッシュボードには詳細なフォレンジック情報が表示されます。たとえば、攻撃者、拡散範囲、メッセージのサンプル、標的とされる受信者、攻撃の進行状況などの情報が提供されます。

Email Isolationとの連携で影響を最小化

メールの受信後にURLが武器化される場合があります。攻撃者は、この戦略を使用して最初の侵入の検出を回避しようとします。Proofpoint Browser Isolationを使用すると、ユーザーが不正なURLをクリックしたときの影響を最小限に抑えることができます。会社のメールに含まれるURLがクリックされるとすぐに保護機能が作動します。閲覧アクティビティは安全なコンテナに隔離され、安全に生成されたページだけがユーザーに表示されます。また、最初の段階でダウンローダーの起動と認証情報の窃盗を防ぎます。これにより、攻撃の連鎖が途切れます。

ポリシーとVAP™の分析情報に基づいて、リスクベースに基づいてアイソレーションを実装し、最も警戒すべきユーザーがアクセスするURLをアイソレーション ブラウジング セッションに送信することもできます。また、すべてのユーザーのクリック動作を分離環境で実行し、標的となった人物により厳格なポリシーを設定することも可能です。狙われているユーザーによっては、ユーザーの危険度とそのユーザーがURLをクリックした際のリスクを考慮して、分離ポリシーを設定することもできます。

ユーザーのセキュリティ意識を高める

ランサムウェアを阻止するには、ユーザーの教育が欠かせません。組織を守る最後の砦になるのはユーザーです。ランサムウェア攻撃に成功するには、ユーザーがリンクをクリックするか、添付ファイルをダウンロードしなければなりません。最新のVerizon DBIRレポート（2021年版）によると、昨年発生した侵害の85%は人に起因するものでした[2]。

Threat Protection プラットフォームでは、セキュリティ意識向上のトレーニングを受講できます。このトレーニングにより、ランサムウェアについて理解し、不審なメッセージをクリックしないようにユーザーを教育することができます。最も狙われている人物や、現実の脅威と実際に直面しているユーザーに別のトレーニングを割り当てることもできます。エンドユーザーのトレーニングをさらに強化するために、膨大なコンテンツライブラリからコンテンツを選択し、従業員へのお知らせやセキュリティアラートで通知できます。また、プルーフポイントが分析した数十億のメッセージの実例に基づくテンプレートを使用して、攻撃シミュレーションを実行できます。このプラットフォームでは、[PhishAlarm]ボタンとEメール警告タグを使用して、不審なメールを簡単に報告できます。

2 Verizon.「DBIR: Data Breach Incident Report」(DBIR: データ漏洩/侵害調査報告書)2021年

ユーザーアカウントの認証情報は組織に侵入するための鍵になります。ランサムウェアの攻撃者は、1組のユーザー名とパスワードを入手できれば、組織の内外で簡単に攻撃を開始できます。

不正メッセージの自動修復

セキュリティスタッフの人員不足は常態化しています。また、大量に発生したアラートを迅速にトリアージし、調査しなければなりません。Threat Protection プラットフォームでは、mSOAR（メールに特化したセキュリティオーケストレーション、自動化、対応）を利用できます。これにより、ユーザーから報告された不正なメールや不要なメールを自動的に調査し、修復することができます。

これらのメッセージは、複数の脅威インテリジェンスとレピュテーション システムによって自動的に分析されます。不正なメッセージであることが判明すると、このメッセージとそれに関連するメッセージがすべて自動的に隔離されます。アラートごとに調査を行ったり、不正なメッセージを手動で修復する必要はありません。セキュリティチームの負担を軽減し、作業を効率的に進めることができます。ユーザーには、不正なメッセージであることが分かるようにカスタマイズされたメールが送信されるので、継続的な行動改善に役立ちます。

Threat Protection プラットフォームは、配信後もメッセージの分析を行います。配信後に不正なものが見つかった場合、ユーザーの受信ボックスから自動的に削除します。他のユーザーに転送されたり、配布リスト経由で送信されたメッセージも削除されます。

最初の感染を検出し、ネットワーク内のラテラルムーブメントと潜伏を阻止

Proofpoint Cloud Securityは、次の方法でランサムウェアの脅威を検出します。

- 侵害されたクラウドアカウントをモニタリングして検出する
- クラウドアカウントへの不正なファイルのアップロードをモニタリングする
- Proofpoint Web Security によりコマンド アンド コントロールから保護する

クラウドアカウントの乗っ取りを検出する

ユーザーアカウントの認証情報は組織に侵入するための鍵になります。ランサムウェアの攻撃者は、1 組のユーザー名とパスワードを入手できれば、組織の内外で簡単に攻撃を開始できます（特に、Microsoft 365やGoogle Workplaceなどのクラウドアプリの場合）。Proofpoint Cloud SecurityのCASBは、適応型のアクセス制御をリアルタイムで提供します。これは、リスク、コンテキスト、役割ベースで行われます。この機能は、危険な場所や既知の攻撃者からクラウドアプリへのアクセスを自動的にブロックします。また、コンテキストデータを使用して、ユーザーの身元を確認し、危険なアクセスを阻止します。コンテキストデータには、ユーザーの位置情報、デバイス、ネットワーク、ログイン時間などが含まれます。多要素認証の適用、管理対象外デバイスからのアクセス制限などのアクセス制御ポリシーを定義することで、ランサムウェアの攻撃を阻止できます。

不正アクセスされたアカウントの悪用、ネットワーク内のラテラルムーブメントやデータに対するリスクを視覚的に確認できます。また、不審なログインが不正なメールを送信したアカウントに関連するものかどうか確認できます。メールの転送と委任のルールを設定したり、OAuthトークンを使用することで、攻撃者が長時間潜伏するマルウェアのインストールを試みたかどうか確認できます。また、不審なファイル アクティビティが発生しているかどうかも確認できます。

クラウドアプリからのランサムウェアの拡散を阻止

ランサムウェアは、感染したファイルの共有や自動同期を介して拡散する可能性があります。これにより、組織、パートナー、顧客に重大な影響を及ぼす可能性があります。Proofpoint Cloud Securityは、クラウドファイル共有を常にモニタリングし、不審なファイルが見つかると警告します。サンドボックスに自動的に隔離してクラウドアプリのファイルを分析し、回避策を実行することで、クラウドに不正なファイルを封じ込めることができます。

Proofpoint Web Securityでコマンド アンド コントロールから保護

デバイスが侵害されると、そのデバイスから攻撃者のサーバーに信号が送信されます。信号を受信すると、攻撃者は次の指令を送信します。デバイスを乗っ取ることで、ランサムウェアの散布やデータの送出など、様々な操作が可能になります。

Proofpoint Cloud SecurityのWeb SecurityとBrowser Isolationは、侵害されたサイトとの接続をブロックします。これにより、ランサムウェアの攻撃者がデバイスを制御できなくなるため、被害の拡大を防ぐことができます。このインテリジェンスではProofpoint Nexus Threat Graphが使用されています。これは、世界中の複数の脅威ベクトルにまたがる何兆ものリアルタイムデータポイントを組み合わせた脅威インテリジェンス、高度なAIと機械学習、そして今日の最大のサイバー脅威の一歩先を行くグローバルリサーチチームにより実現されています。

データの持ち出しを阻止

Proofpoint Advanced Threat ProtectionとProofpoint Cloud Securityは、次の機能によってデータの持ち出しを防ぎます。

- データ持ち出しの兆候を早期に発見する
- 未承認のデータ移動を検出し、阻止する

Proofpoint Cloud SecurityのWeb SecurityとBrowser Isolationは、情報漏えい対策（DLP）をリアルタイムで実行可能なリスク認識型のデータセキュリティを提供します。Browser IsolationとWeb Securityを連携させることで、データをきめ細かく制御できます。たとえば、読み取り専用アクセス権を使用して、クラウドアプリとWebへのアクセスを許可またはブロックできます。Browser Isolationは、ブラウザー セッションをセキュアなコンテナに分離し、アプリやデータに対するユーザーのアクセスを保護します。

また、Proofpoint CASBを使用すると、不審なファイルのアクティビティをすぐに確認することができます。このようなアクティビティは不審なログインに関連しています。インシデント対応の担当者は、攻撃者が開始したファイル アクティビティとユーザーが開始したファイル アクティビティをすばやく分離し、よりタイムリーな対応が可能になります。

クラウドアプリの機密データを保護するだけでなく、機密情報のコマンド アンド コントロールへの送出、管理対象外デバイス（攻撃者のデバイス）へのダウンロード、メールによる送信も防ぐことができます。

詳細

詳細は**proofpoint.com/jp**でご確認ください。