「ランサムウェア」への備えはできていますか？ 本当に効果の出るセキュリティ施策の最新トレンド

ペネトレーションテストとEDRで見直すサイバー攻撃対策

サイバー攻撃の中でも依然として大きな被害をもたらしているのがランサムウェアです。その手口はますます悪質化すると同時に、いまや被害の対象は大企業にとどまらないため、あらゆる企業が脅威に備えなければならないと言えるでしょう。対策のアプローチはいくつかありますが、ここでは「攻撃側の視点」と「防御側の視点」の両軸から対策の方法を解説します。

ランサムウェアなどのサイバー攻撃は身近な脅威に

サイバー攻撃によって被害を受ける企業が後を絶ちません。たとえばある食品会社は2021年3月、ネットワーク機器の脆弱性が原因と推定される不正アクセスがあったことを公表しました。顧客、取引先担当者、派遣スタッフ、同社社員など累計約6万5,000件の個人情報が流出した可能性があるといい、同社商品を取り扱っている取引先も消費者に謝罪文を出す事態に発展しました。

さらに、ここ数年の傾向として、侵入後にデータを暗号化または窃取し、それらを人質として身代金を要求する「ランサムウェア」が大きな脅威となっています。2021年7月には大手の国内製粉会社が、データをバックアップも含めて暗号化されてしまい、財務・会計システムが使用できない状況に。その結果、四半期報告書の提出期限を延長する事態となりました。専門家の見立てでは、ランサムウェアによる被害ではないかと推測されています。

「ランサムウェアによる被害」は、IPA（独立行政法人情報処理推進機構）が公表する「情報セキュリティ 10大脅威」において、2021年版・2022年版と連続して「組織」向け脅威の1位に選ばれています。これは情報セキュリティ事故や攻撃の状況等をもとに専門家らが選出した結果であり、ランサムウェアの脅威が身近に迫っているものと理解できます。

ランサムウェアに感染してしまう原因は複数存在しますが、特に企業が注意しなければならないのがシステムの脆弱性です。実際に世の中で報道されているランサムウェアのうち、VPN装置やWindowsに潜む脆弱性をついて侵入したものも多く、逆に言えば脆弱性を対処していれば防ぐことができたであろう事故も多いということです。

IPAなどが運営する脆弱性対策情報ポータルサイト「JVN」に登録される脆弱性は、2021年の第1四半期だけで約1,700件もの数が報告されており、日々次々と報告がなされています。もちろん、すべての脆弱性にタイムリーに対応し続けることは困難ですが、対応せずに放置すれば、取引先や社会に影響を及ぼすこととなり、企業の存続を脅しかねません。脆弱性とどう向き合い、対応することが望ましいのでしょうか。

脆弱性対策は「攻め」「守り」両者の視点が重要

対応すべき脆弱性は膨大であると同時に、攻撃者が着目する脆弱性は企業のシステム環境によって異なります。そこで有効なのが、攻撃者視点に立ち、まず何が狙われる対象となるかを判断し、優先順位を付けて対応することです。攻撃者の視点を得るには、ホワイトハッカーが実際にシステムを攻撃することで対処すべき脆弱性を見つける「ペネトレーションテスト」が有効です。

もっとも、仮にすべての脆弱性に対応できたとしても万全とは言えません。脆弱性は常に増え続けており、それを狙う最新の攻撃手法に対して既存のファイアウォールやアンチウイルスでは侵入を防ぎきれないためです。そこで効果的な対策となるのが、感染してしまったことを前提にその後の被害拡大を抑えることができるEDR（Endpoint Detection & Response）の導入です。

攻撃側視点のペネトレーションテストと防御側視点のEDRの両輪でどのような対策を講じることができるのか、以降でその役割を見ていきましょう。

攻撃側視点の対策：ペネトレーションテスト

ペネトレーションテストとは、システムの脆弱性を検証するテスト手法の1つです。ホワイトハッカーの手で実際にシステムへの攻撃を試みることで、現在のセキュリティ状況を診断します。リアルな攻撃によってシステムの脆弱性を洗い出し、脆弱性が悪用されるとどのような結果が引き起こされるかを認識しておくことが重要です。

しかし、ペネトレーションテストは人の手で行うテストであるため、高い効果を期待できる一方、費用と時間を要します。また、攻撃手法や脆弱性は変化するため、定期的に実施し直すことが望ましいとされています。

そこで昨今では、自動でペネトレーションテストを実行できるツールの活用が始まっています。ツールを用いることで、コストを抑えつつ繰り返しテストを実施できるため、システムの変化や新たな脅威に対して迅速に対応できるようになります。

防御側視点の対策：EDR

昨今では、高度化するマルウェアの侵入を食い止められないケースが増加しているため、防御側は侵入されることを前提に、被害を広げない対策が重要視されています。

IPAが公表した「情報セキュリティ 10大脅威 2022」では、「組織」向け脅威のうち1位から4位までを、エンドポイントに関連もしくは発端とする脅威が占めています。また、「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」が初登場で7 位に入りました。「ゼロデイ攻撃の場合、修正プログラムが提供された時点ですでに攻撃が行われているため、脆弱性対策に加え、外部からの侵入を検知/防御する機器を導入するなどの備えが重要」だとしています。

脆弱性対策を行っていないシステムを公開していることは攻撃を受けるリスクにつながることは先述の通りですが、さらにIPAは「脆弱性情報の公開後に攻撃コードが流通し、攻撃が本格化するまでの時間が短くなっている」としています。こうした傾向からも、エンドポイントを守ることや侵入を前提に対策を講じることの重要性がわかるでしょう。

このようなニーズに対応し、エンドポイントの監視や保護を行う製品がEDRです。感染を早い段階で検知して手動または自動で対応を行い、情報漏えいなど最悪の事態を避けるために導入されます。具体的には、PC端末の一挙手一投足をモニタリングし、相関分析を行い不審な動きを検知します。また、ログを常時記録し、マルウェアに感染した前後の挙動を振り返ることもできます。

東京エレクトロンデバイスが推奨するソリューション

ここでは、上記に触れたペネトレーションテストおよびEDRソリューションに関して東京エレクトロンデバイスが推奨する2つのソリューションと、それらを導入することで得られる価値をご紹介します。

自動ペネトレーションテスト「PenTera」

イスラエルのPentera社が提供する「PenTera」は、ホワイトハッカーと同様の攻撃を自動で行うツールです。ホワイトハッカーが行うペネトレーションテストでは、コストや時間がかかるため、頻繁に実行できないという大きな欠点がありますが、それを短期間で繰り返し実行できるようにするのがPenTeraの最大のメリットです。発見した脆弱性に対して、対策を行い、再度テストするというサイクルを繰り返すことで、エンドポイントセキュリティを高めていくことが可能です。

Pentera社は「継続的なペネトレーションテストによるサイバーレジリエンスの構築」をミッションとして掲げ、これまで世界数十カ国の銀行、保険、官公庁などへの導入実績が豊富にあります。

PenTeraの大きな特徴は、「最新ハッキング技術」の迅速な反映です。Pentera社は、イスラエル国防軍のエリートサイバー部隊出身者による強力なリサーチチームを擁しており、最近では「Zerologon」と呼ばれるWindows Serverの管理者権限を奪われる可能性がある深刻な脆弱性について、話題になり始めてから2週間ほどでPenTeraに反映された実績があります。

また、PenTeraは使いやすさも優れています。テスト実施は難しくなく、いくつかの項目を指定して実行ボタンをクリックするだけで、すべて自動で攻撃が実行できます。実行後は、その結果を基に対応すべき脆弱性について、攻撃者の視点で優先順位付

けしたレポートが即時発行されます。

ランサムウェアの攻撃フローにも対応

オプション機能として、PenTeraにはランサムウェアによる実際の攻撃を想定したエミュレーション機能があります。侵入からデータ流出までエンドツーエンドの攻撃フローを実行し、どのようなふるまいが行われ、どの段階でブロックできたのかを明らかにするので、自社のセキュリティ対策製品がどれだけ機能しているのかを検査するのに効果的です。最近のランサムウェア攻撃ではデータ暗号化とデータ窃取を同時に試みる「二重脅迫型」が増加していますが、PenTeraでは、その両方をチェック可能です。

現時点では主要な攻撃者グループであるREvil、Conti、Mazeの3つにランサムウェアを再現するシナリオが用意されていますが、新たな脅威の状況に応じて追加されていく予定です。

EDR「SentinelOne」

SentinelOne社のEDRソリューション「SentinelOne Endpoint Protection Platform（以下、SentinelOne）」は、攻撃フローの可視化と脅威プロセスの強制停止による情報搾取の防止、OSの標準ツールを用いた攻撃の検知・防御が可能です。SentinelOneが持つ3つの特徴によって高い導入効果を得られます。

①100%の検知力

セキュリティ製品がマルウェアの検知を行う際、SentinelOneの場合は、ファイル構造を見るAIと怪しいファイルのふるまいを見るAIの2種のAI検知エンジンを利用することで、高い検知力を実現しています。

100%とする根拠は、米国の連邦政府が資金を提供する非営利組織MITRE社が2020年に実施したテストの評価結果です。実在するハッカー集団の攻撃手法をベースにしたシナリオについて、EDRベンダー 29社のソリューションでテストしたところ、SentinelOneは検知漏れゼロを記録しました。また、検知後の対応については、トップのスコアを獲得しています。

※SentinelOneはMITRE Engenuity ATT & CK評価で優れた効果を実証しました。
詳細はこちら https://jp.sentinelone.com/lp/mitre/ （SentinelOneサイト）

②AIによる自動対応

EDRではしばしばツール運用の難しさが指摘されますが、SentinelOneではそうした課題を解消する機能を備えています。例えば、マルウェアに感染してしまった端末を自動隔離して感染拡大を防ぐことができます。

③マルウェア感染からの回復

例えばWannaCryなどのランサムウェアによって機密ファイルを暗号化されてしまったときでも、ワンクリックで元通りにできます。

実際に行われる攻撃の手口とは

サイバー攻撃は、どのような手口で行われるのでしょうか。ここでは一例としてWindowsサーバーのログオンパスワードを搾取するケースを見てみましょう。

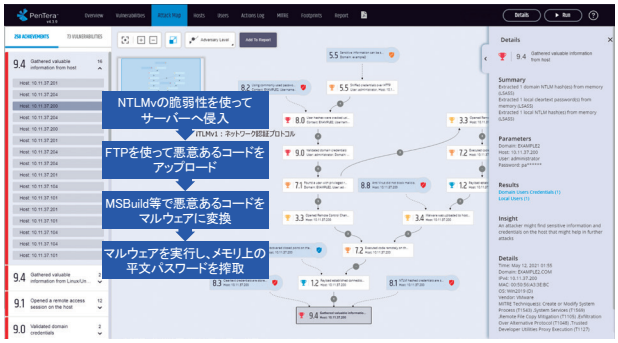
攻撃者は企業のネットワークに侵入するための足掛かりとして、エンドポイントへ侵入します。そして、攻撃者にとって使いやすい脆弱性がないかをスキャンします。例えば、共有フォルダへのログオンにNTLMv1を使用していることが判明すれば、次に目指すサーバーへの侵入が容易になります。

NTLMv1は、古いWindowsで標準的に用いられていた認証方式で、利用者アカウントを管理するドメインコントローラーや共有フォルダなどのログオンに使用されてきました。Windows 2000以降はKerberos認証が標準となり、NTLMv1についてはMicrosoftが使用を中止するように呼びかけてきましたが、現在でも広く使われていることが調査結果で判明しています。

NTLMv1の脆弱性を突いてサーバーへの侵入に成功すると、次に攻撃者はメモリ上に保持している平文パスワードの搾取を試みます。平文パスワードとは暗号化されていないパスワードのことです。

続いて、攻撃者はファイルの転送コマンドであるFTPを用いて、平文パスワードを搾取するマルウェアの元となるコードをサーバーに送り込みます。そして、そのコードをWindows標準ツールであるMSBuildを用いて実行形式（exeファイル）に変換し、マルウェアを作成。それを実行し、メモリ上の平文パスワードを搾取するのです。

最初から実行形式のマルウェアを送り込むと、アンチウイルスソフトウェアに検知されてしまう可能性が高いため、回避するためにこのような手法が使われています。FTPはユーザーが普段から使っているコマンドであり、MSBuildはWindowsの標準ツールです。つまり、ユーザーの自然な行動を装って、悪意のあるコードを送り込んでいるのです。



Pentera を用いた平文パスワード窃取のフロー

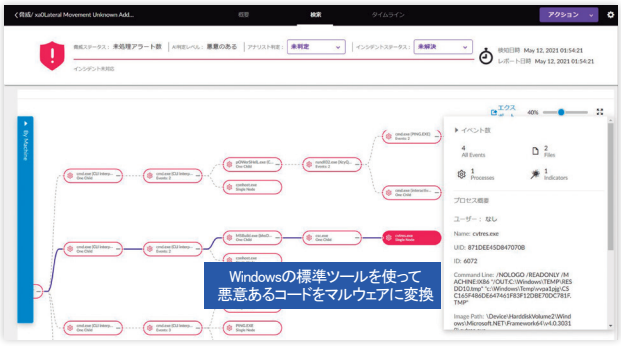
より攻撃の成功率を上げるために、アンチウイルスソフトウェアやEDRに検知されにくい、OSの標準機能だけを用いる手口もあります。コードの取り込みにFTPを使うのではなく、OS標準のPowerShellを使用してコードが書かれたライブラリ（DLLファイル）をアップロード。さらにOS標準のrundll32というコマンドを用いて、ライブラリ化されたマルウェアを実行するのです。

EDRによる防御の実例

先ほど例に挙げた平文パスワード搾取のケースについて、SentinelOneがどのように攻撃を検知し対応しているのかをご紹介します。

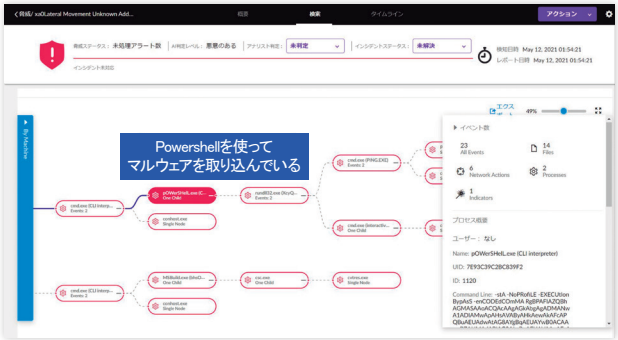
SentinelOneのインシデント画面にて、攻撃者の挙動を検知しているのが以下の図です。左図はFTPで悪意のあるコードが送り込まれたものを検知したもので、画面右側のポップアップ表示ではFTPを使用した際のコマンドラインも示されています。

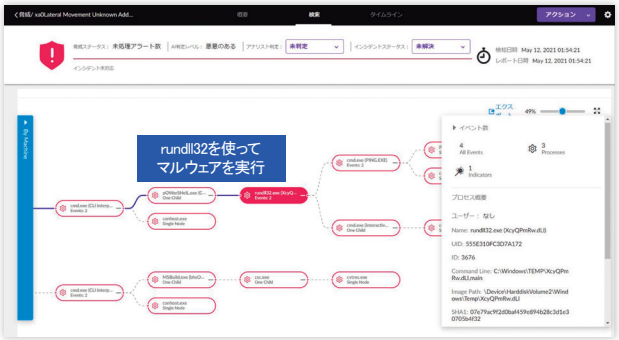
悪意のあるコードを実行形式のマルウェアに変換しているステップを検知したものが右図です。変換に使用するMSBuildはWindowsの標準ツールですが、SentinelOneではこちらも検知に成功しています。



FTP で悪意あるコードが送り込まれていること（左図）、コードがマルウェアに変換されたこと（右図）を SentinelOne で検知

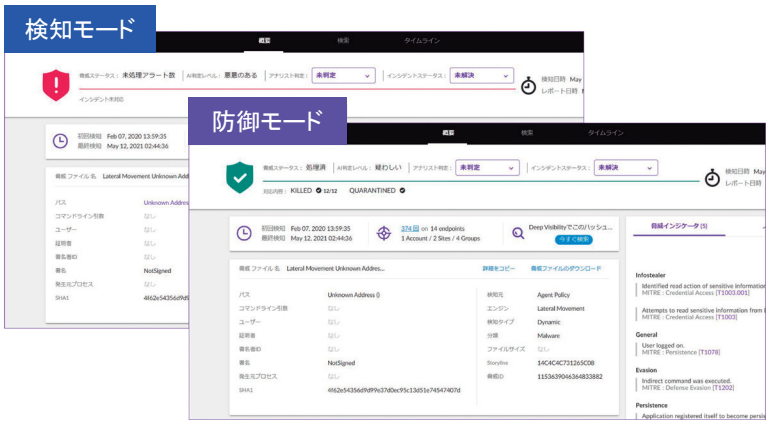
また、検知されるのを回避するために、OS標準のPowerShellとrundll32を用いたケースでも、その挙動が検知できています。





PowerShell でマルウェアを取り込んでいること（左図）、マルウェアが実行されている様子（右図）を SentinelOne で検知

SentinelOneはアラートを上げるだけで防御を行わない「検知モード」と攻撃プロセスを止める「防御モード」が用意されており、その画面が右のものです。盾のマークが赤い状態は攻撃プロセスが進行している状態を表し、緑の状態は攻撃プロセスが停止・隔離され安心できる状態を直感的にわかるように示しています。



検知モードと防御モードの画面の例

上記にて、PenTeraを用いた、シミュレーションではないリアルな攻撃のフローとSentinelOneによって脅威の可視化と対処ができる例を紹介しました。この例はランサムウェアではありませんが、システムに存在する脆弱性を探索し、それを突破口に攻撃を拡大する点では施すべき対策に大きな違いはありません。

感染前の防御や感染後の対処のためにEDRは有用ではありますが、もちろん完全な防御を保証するものでもありません。日々発見されるセキュリティの穴を防ぐために、攻撃者視点で優先度の高い脆弱性を発見できるPenTeraを組み合わせるなど、複数のアプローチからセキュリティ体制を強化する仕組みを検討してみるとよいでしょう。

東京エレクトロン デバイス株式会社
CN BU
https://cn.teldevice.co.jp

新宿：〒163-1034 東京都新宿区西新宿 3-7-1 新宿パークタワー S34 階
Tel.03-5908-1990 Fax.03-5908-1991

大阪：〒540-6033 大阪府大阪市中央区城見 1-2-27 クリスタルタワー 33 階
Tel.06-4792-1908 Fax.06-6945-8581

名古屋：〒451-0045 愛知県名古屋市西区名駅 2-27-8 名古屋プライムセントラルタワー 8 階
Tel.052-562-0826 Fax.052-561-5382

つくば：〒305-0033 茨城県つくば市東新井 15-4 関友つくばビル 7 階
Tel.029-848-6030 Fax.029-848-6035

お問い合わせは、Web サイトの下記フォームよりお願いします。
https://cn.teldevice.co.jp/product/pentera/form.html
https://cn.teldevice.co.jp/product/sentinelone/form.html