VECTRA
SECURITY THAT THINKS

Eブック

ランサムウェアを阻止する：最前線情報

要約

「自社環境でランサムウェア攻撃が進行中」というのは嫌な事実です。しかし、その兆候を素早く特定できれば、ほぼ確実に攻撃を阻止できます。では、どうすべきでしょうか？まさにこれが今回のトピックです。本書では、当社と関係の深いお客様企業がVectraのSidekickチームとタッグを組んで初期段階のRansomOps（ランサムウェアオペレーション）攻撃に対応した際のプロセスを、実例を交えて解説します。ランサムウェアのデプロイを阻止することで、業務中断という惨事を回避できます。

本書では、攻撃者の活動や偵察行為（いわゆるRansomOps）を検知することがランサムウェアのデプロイ阻止の鍵となる理由を詳しく解説すると共に、今日の戦術的なランサムウェア攻撃を撃退するためにセキュリティ専門家が実施している様々な施策をご紹介します。また、Vectra® Sidekickサービスを活用して攻撃の進行をほぼリアルタイムで検知する方法（お客様の活用事例）や、すべての組織が知っておくべき主な課題、所見、推奨策もご紹介します。

確実に言えることは、ランサムウェア阻止の成否は「対応のスピードと迅速なアクション」にかかっています。早速取り入れて、ランサムウェアを阻止しましょう。

Vectra Sidekick MDRサービス

Vectra Sidekick MDR (Managed Detection and Response、管理型検知および対応) は、Vectra Detectが検知した悪意ある活動を当社の人員が常時監視して、先を見越した調査を実施する、24時間365日体制のサービスです。

SideKick MDRは、経験豊富なセキュリティアナリストを配置することで、VectraのAIを十分に活用して脅威を早期に検知し、侵害を阻止することを支援します。VectraプラットフォームとSideKick MDRを組み合わせることで、以下を実現します。

- Vectraの経験豊富なセキュリティアナリストが、お客様のセキュリティチームの追加戦力となって、巧妙なサイバー攻撃やランサムウェア攻撃の撃退を支援します。
- 攻撃、脅威、ランサムウェアの予兆検知に関するVectra Detectと当社アナリストのノウハウ、コンテキスト、可視性をもとに迅速な対応を行います。
- 24時間365日体制の先を見越した監視により、緊急出動や対応を要する「高優先度」の脅威やランサムウェアが検知された際に、ただちにお客様に通知します。
- 環境や事業目標、業界固有のリスクに合わせてVectra 製品の実装形態をカスタマイズできます。それには、コントロール設定のカスタマイズ、専門家による対策アドバイス、対象環境のトレンドや測定指標の提供、スピーディーな調査などを含みます。

「ランサムウェア＝ビジネス」と考えることが大前提

不快に思われるかもしれませんが、ランサムウェアの運営組織およびその傘下で活動するアフィリエイトは、ビジネスとしてランサムウェア攻撃を行っています。一般的な企業と同様に営利を目的とし、投資効果 (ROI) の意識も高く、「窃取可能なシステムやデータに最短でアクセスし、窃取した財産の返却と引き換えに高額な料金を所有者に請求すること」で収益を得ているのです。

本書で解説する調査結果の多くはこうした収益重視の考えによるものと言えるのですが、このように、セキュリティ戦略の根幹は攻撃者を駆り立てる動機を解明することです。攻撃の理由を理解し、侵害されると業務中断が生じかねない社内システムやデータを明確に特定できれば、攻撃しづらい環境づくりの土台が整ったと言えます。

ここからは、前述の特性に的を当てた机上演習の効果、および自社の現状を、レッドチーム演習で客観的に評価するための方法をご紹介します。

まずは基本から

最初に、ランサムウェアが決してアクセスできない環境を構築することが理想です。防御策だけで絶対安全とは言えないものの、ROI意識の高い攻撃者に対しては効果があります。実際に、認証管理（サイバー衛生）の徹底や適切なパッチ適用などの基本的な対策でリスクを劇的に減らせます。

攻撃者は、非武装地帯 (DMZ) に露出している脆弱性、パッチ未適用の脆弱性、多要素認証 (MFA) 適用外のアカウントなどの、手っ取り早い方法を使って初期アクセスを確立することが多いため、基本的な防御対策が役立ちます。つまり基本対策に隙があれば、時間のかかる高度な攻撃戦術を使わなくても簡単に侵入されてしまいます。

ランサムウェアが決してアクセスできない
環境を構築することが理想です。

幸い、自社のVPN、IDP、その他のエントリーポイントでMFAを有効化すれば攻撃者の活動を制限できます。あきらめて他の獲物を探そうとするかもしれません。パッチ管理も同様です。DMZ全体にパッチ適用を徹底することも、攻撃者を確実に撃退する方法です。今日見られる攻撃の多くは、セキュリティ防御の網をすり抜けるために高度な手法を使っていますが、それでも最初の段階から可能な限り攻撃しづらい状況を整えておくことはプラスになります。

昼夜を問わず即応できる態勢づくり

基本対策によって態勢が整備できても、リスクは排除できません。様々な理由がありますが、アカウント設定ミスやパッチ不備、ユーザーによる不審なリンクのクリック操作、または社内VPNで発覚した未解決のゼロデイ脆弱性などがたった一つでもあれば、資金源が豊富なランサムウェア・エコシステムの標的となり、突破されてしまう、というのが真の理由です。こうした被害は数多く報道されてきました。

さらに、いったん侵入したランサムウェア攻撃者の動きは「非常に速い」ということを覚悟してください。もちろん対応事案のなかには数日にわたって緩やかに進行する攻撃もありましたが、標的組織の業務終了時（夕方）に発生した攻撃が一晩で完了するというケースは珍しくありません。ROIの意識が高い攻撃者は、一刻たりとも無駄にしたくないはずです。攻撃者によっぽど自信があるのか、または計算によるものかはわかりませんが、検知の網を避けて潜伏活動をしている兆候はほとんど見られません。実際、ランサムウェア攻撃者の滞留時間（世界全域の中央値）はこの数年で大幅に減少しています。

幸い、攻撃者が短時間で活発に動くため、適切な検知テクノロジーがあればスピード勝負で攻撃を特定できます。当社の検知システムでも、初期アクセスから2分以内に緊急性の高いホストが確認された事例があります。ただし、攻撃はあっという間に進行するため、日頃から臨戦・即応態勢を整えておかなければ、ランサムウェアのデプロイ前に脅威を阻止することはできません。

残念ながら、業務時間内だけ即応態勢を整えれば良い、というわけではありません。初期段階の偵察行為とラテラルムーブメント（横方向の移動）は昼夜を問わず（おそらくランサムウェア攻撃者の都合に合わせて）発生しています。日中、夜間、週末、さらには祝日に発生することもあるでしょう。当社の調べでは、攻撃の仕上げ（情報の持ち出しとデータ暗号化）は、インシデント対応チームの態勢が最も手薄な真夜中、週末または祝日に遂行される可能性が高いです。

つまり実質上、24時間365日体制での監視が不可欠となります。

対応戦略を用意する

ランサムウェアの脅威対処への第一歩は、自社環境に潜んでいる攻撃者を検知することです。同様に、様々なシナリオを想定し、攻撃を阻止するために何ができるのか(どこまで思い切った対策に踏み切れるのか)を把握しておくことも重要です。当社が関与したある案件で、お客様組織のドメインコントローラに到達した攻撃者に管理者権限が奪取されるという事態が発生しました。担当のセキュリティチームは対策を練る時間を稼ぐために「社内システムをインターネットから完全に遮断する」ことを瞬時に決め、結果的にこの判断が奏功しました。

この組織はあと少しでランサムウェアの被害に遭うところでしたが、こうしたシナリオはそれほど珍しいものではありません。自社に置き換えて「同じ状況になったらどうするか?この程度の業務中断を許容できるか?接続が遮断されても遠隔拠点のセキュリティ担当者が適切に対応できるか?対応に必要な追加手段を購入しておくべきか?」などの点を、改めて検討してみると良いでしょう。

こういったことからわかるように、緊迫した状況では迅速かつ迷いのない行動こそが対応成功の鍵となります。対応戦略を充分理解し、日頃から対応訓練を実施しておくことが大きな成果につながります。

ランサムウェア阻止の鍵は、ランサムウェア探しにあらず

今日のランサムウェア攻撃(実際にはRansomOps)では、攻撃の最終段階にならないとランサムウェアのバイナリはデプロイされません。つまり、ランサムウェア自体が検知された時点で、すでに手遅れである可能性が高いのです。

ランサムウェア攻撃の進行を阻止するためには、デプロイ前の攻撃ステップを検知して対応しなければなりません。そうでなければ、攻撃者の全容またはその最終目的が見えない状態で対応を模索することになるでしょう。多くの場合、攻撃はあっという間に進行します。ツールやコマンド&コントロール (C2)インフラに何らかの予兆があれば、現状把握の判断材料として活用できます。

こうした状況での対応計画では、より一般的な侵入形態や攻撃の進行プロセスに目を配り、「ランサムウェアがデプロイする確率は高いが確実ではない」という前提で進めることが重要です。

アカウントおよび管理者ツールが鍵となる

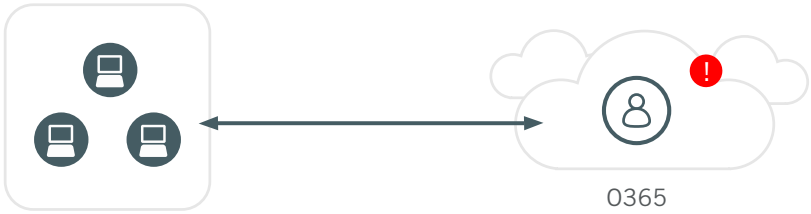
これまで、初期アクセスの確立、場合によってはラテラルムーブメントを目的とする悪意ある攻撃を目にしてきました。しかし、今日の一般的な攻撃と同様に、ランサムウェア攻撃者の主な狙いは認証情報(管理者およびサービスアカウント)です。ほぼすべてのランサムウェア運営組織のアフィリエイトが、こうした認証情報を管理者プロトコルと併用する攻撃戦術を好んで使います。

多くの攻撃と同様、攻撃者の意図はドメインコントローラのドメイン管理者権限を奪取して最終段階に進むことです。この優位な立場を利用すれば、最も価値のあるデータを簡単に窃取できます。また、GPOなどの管理ツールを使えばランサムウェアを驚くほどスピーディーにデプロイできます。

攻撃者は認証情報を狙うため、特権アカウントすべての使用状況を注意深く監視することがきわめて重要です。当社の実体験からもわかるように、「特権アカウントの使用状況」は、攻撃を検知するうえで大変貴重なシグナルとなります。

共通するテーマ

Vectraのお客様案件でよく見られる課題(ユーザー、プロセス、セキュリティの課題)を以下に取りまとめました。



初期アクセス:

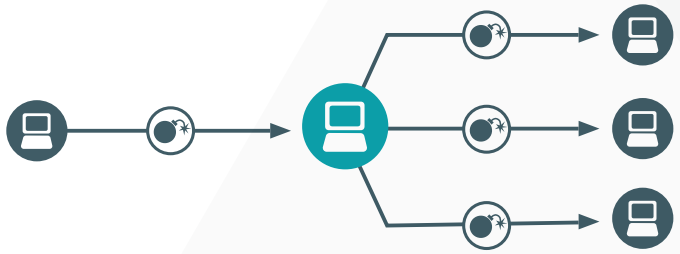
- インターネット接続する外部公開サービスやシステムが攻撃者によって執拗にスキャンされる。
- RDP、FTP、VPNの実行元サーバーが狙われやすい。サーバーを介して標的企業やクラウド環境への初期アクセスが確立される。
- MFAの不備も防御のギャップ(死角)として狙われやすい。
- 最初の侵入から数時間で攻撃が進行するケースもあるが、数日から数週間に及ぶこともある。セキュリティチームが早い段階で攻撃を検知して対応する時間的余裕はあるが、「24時間365日体制」での監視が必要。

C2:

- 現在主流の攻撃ツールはCobalt Strikeと見られる。
- 汎用リモートアクセスツール(認定ツール、非認定ツール)は、システムの乗っ取り手段としても使われている。当社が検知したある事象では、標的組織内のマシンを外部の第三者がコントロールする目的でCisco製ソフトウェアのAnyConnectが使用されていた。

偵察およびラテラルムーブメント:

- ほとんどのケースでは頻繁なスキャンに加えて、ネットワークマッピング、rDNSクエリー、ファイル共有の列挙なども行われる。(通常は、高速スキャンを手がかりに初期アクセスから数分以内に攻撃をあぶり出せる。)
- 認証情報を狙った偵察(保管場所をマッピングするためのLDAPクエリーやRPC要求など)なども常套手段として使われる。
- 初期段階でのラテラルムーブメントには汎用的なエクスプロイト手段などが用いられるが、後半段階になると認証情報や管理プロトコルが多用されている。



情報の持ち出し:

- 偵察で得た情報を分析するためのアップロード先は、Mega Upload (mega.com)やtemp.shをはじめとする無料のファイル共有サイトが多い。

推奨策

当社のチームは日々、Vectra製品(AIベースの脅威検知および対応ソリューション)から生成される重大なアラートに対応すべく、お客様のセキュリティチームと密に連携しています。開始時点では、脅威の種類がランサムウェアか否かは明らかではありません。アラートの重大度が高まるにつれ、攻撃の詳細やコンテキストがより明瞭に可視化され、攻撃の種類を判別できるようになります。ランサムウェア攻撃者の動きを封じ込め、確実に阻止するためのセキュリティツールや業務プラクティスは数多くありますが、その一部をご紹介します。

防御対策

- 対外的なセキュリティ態勢を定期的に見直し、優先度の高いパッチを実装しましょう。リモートアクセスインフラ、一般的に脆弱なサービス(RDPやFTPなど)などはこれまでの傾向から狙われやすいため、重点的に対策してください。
- アイデンティティプロバイダー (IDP) やリモートアクセスインフラにMFAが適用できる場合は、可能な限り有効化しましょう。
- 一般的に、予防的コントロール、ルール、ポリシーを厳格化すれば、たとえ侵入された場合でも攻撃者による権限昇格がしづらくなるため、対策を練るための時間を稼げます。
- 特権アカウントには細心の注意を払いましょう。運用面では手間がかかりますが、踏み台サーバーや特権アカウント管理システムを介した利用を増やせば増やすほど、権限昇格のパスを複雑化できます。

検知

- ランサムウェア攻撃者に侵入されたとしても、データが持ち出されたりランサムウェアがデプロイされる前に攻撃を阻止する時間はあります。
- 充分な予算を投じ、ネットワークやID管理インフラ、クラウド、エンドポイントにまたがる環境全体をカバーできる脅威検知・対応システムを導入して早期検知率を最大限高めましょう。

調査と修復対応

- ランサムウェア攻撃は昼夜を問わず、あっという間に進行します。社内体制を拡充する、または検知および対応のマネージド・サービス (MDR)、マネージド・セキュリティサービスプロバイダー (MSSP) のサービスを活用するなどの方法で、重大なアラートを24時間365日体制で確実に監視することがセキュリティ対策の鍵となります。
- ネットワークやエンドポイント、クラウドログの遠隔収集データを統合することで、脅威の調査および根本原因の確定に必要なコンテキストを最適化し、情報を補完・明瞭化できます。
- OSINTの手法を併用し、初期アクセス前にDMZ領域でのスキャン行為が増えていないか遡って検証すると、攻撃者のプロファイル分析や対応策の方向性決定に役立つ情報を得られる可能性があります。

お問い合わせ:info-japan@vectra.ai　vectra.ai/jp