COHESITY

ホワイトペーパー

ランサムウェア レジリエンスの構築に向けたロードマップ

目次

サイバーレジリエンスとデータレジリエンスの比較

大半の企業には、事業継続と災害復旧 (BC/DR) という形でデータレジリエンス戦略がありますが、**データ**レジリエンスのために設計されたテクノロジーとプロセスが、ランサムウェア時代における真の**サイバー**レジリエンスに繋がるとは限りません。

サイバーレジリエントな企業になるには、コミュニケーション、コラボレーション、セキュリティツール、認証システム、バックアッププラットフォーム、そして以下を行うその他多数のシステムが必要です:

- 攻撃の発生経緯に関する調査
- 影響を受けたデータ主体、規制当局、法執行機関とのコミュニケーション
- 脅威再発リスクの軽減
- 本番環境への復旧

ワイパー攻撃とも呼ばれる破壊的なサイバー攻撃は、従来の「検知、対応、復旧」の流れを繰り返し行う形に変化させています。そのため、調査作業を開始する前に、まず対応や通信機能を復旧しなければなりません。このような場合、インシデント対応者がフォレンジックを行う際の信頼できる情報源として機能する、バックアップと復旧プラットフォームが重要な役割を果たします。

企業がサイバーレジリエンスを実現し、最新のサイバー攻撃に対抗するには、成功の基盤となる次の2つの領域を考慮する必要があります:

1. 復旧能力を敵の手の届かない範囲に配置すること
2. 対応計画に、本番システムだけでなく、インシデントに効果的かつ効率的に対応するために必要な、セキュリティ、認証、通信プラットフォームにも対応した迅速な復旧を含めること

ランサムウェアやワイパー攻撃が持つ復旧と対応を繰り返す性質に対抗するには、こうした攻撃の影響を最小限に抑えるべく、セキュリティチームとIT運用チームが緊密に連携する必要があります。

サイバーレジリエンスプログラムの構築

洪水、火災、自然災害といった従来のBC/DRシナリオでは、事象の根本原因を迅速に特定することができます。ランサムウェア攻撃の場合、攻撃者は、被害者にとっての唯一の選択肢が身代金の支払いになるよう、復旧の阻止に向けて積極的に行動します。

このような攻撃者は標的の防御に絶えず適応します。従って、攻撃の性質を明確にし、適切な復旧プロセスを理解するためには、標準化された調査と対応プログラムが不可欠です。また、この調査により、攻撃が成功した原因となった脆弱性を明らかにし、将来のインシデントを防ぐために防御を強化することもできます。これは、ほぼ瞬時に対応できることもある従来の災害とは対照的です。

サイバー攻撃に対するレジリエンスを確保し、あるいはそこから生き延びるためには、単にテクノロジーを使うという計画だけでは不十分です。ITチームとセキュリティチームは、攻撃者とその攻撃の種類を理解する必要があります。このようなインテリジェンスを活用することで標的を絞った防御策を策定できるようになり、攻撃の阻止や早期検知の可能性が高まります。MITRE ATT&CKなどのフレームワークを利用すれば、組織は脅威を定量化し、標準化された方法で是正措置を共有することができます。

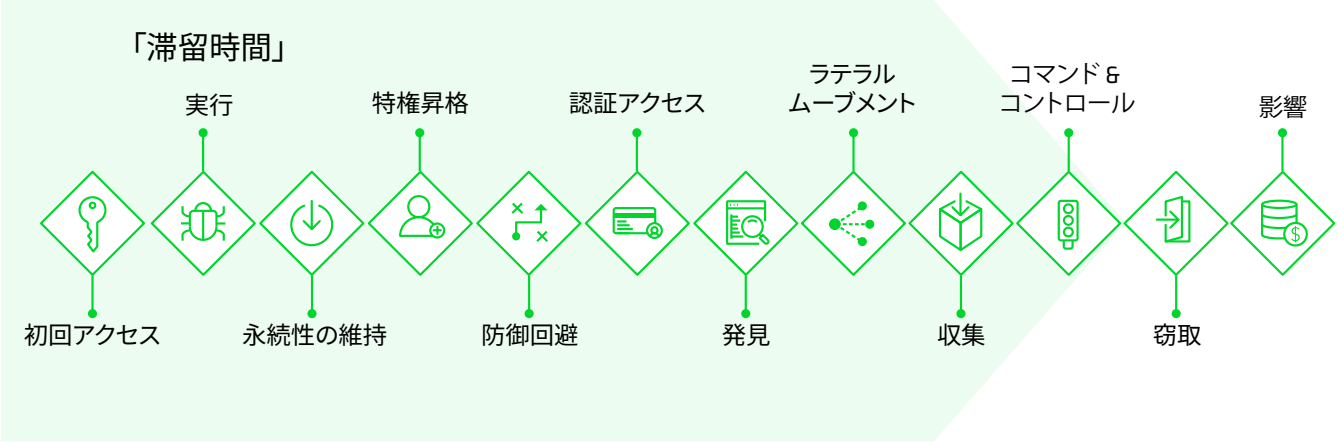
例えば以下の図は、ランサムウェアを起動させる前に、攻撃者が環境内に潜んでどのような行動を取る可能性があるかを示しています。場合によっては、ランサムウェアのペイロードを成功させるために必要な行動であることもあれば、攻撃者がネットワーク内に持続的に留まり、将来の攻撃を仕掛ける行動であることもあります。「滞留時間」は、数日から数か月に及ぶ場合があります。攻撃者が環境内でどのように活動しているかを把握することで、セキュリティチームは攻撃の兆候を積極的に探すことができます。

> 滞留時間とは、悪意ある攻撃者が、攻撃が検知されるまでに侵害されたシステムにアクセスできる時間の長さを指します。滞留時間が長くなるほど、攻撃者が損害を与えたり機密情報を盗んだりする可能性が高まります。

図中の各アクションを攻撃の段階として考えてください。12段階のうち10段階がペイロードの起動前に実行されているという事実は、驚くべきことかもしれません。ランサムウェア攻撃では、暗号化やデータ窃取が始まる前にシステムが完全に侵害されます。ネットワーク内にこのような足がかりを得た攻撃者は、復旧作業を妨害し、身代金を複数回要求するための新たな攻撃を仕掛けることが可能です。これは「二重恐喝/二重脅迫型」ランサムウェアと呼ばれ、攻撃者にとって安定した収益源を確保する方法として急速に広まっています。

被害者にとっては、1回の攻撃だけでも商品やサービスの提供が妨げられる可能性があり、壊滅的な被害を受けることがあります。しかし、複数の攻撃を受けると、次のような二次的損失の可能性がさらに高まります:

- 評判の低下
- データ主体やパートナーからの訴訟
- データ主体の情報を適切に保護しなかったことに対する規制上の罰金



さらに厄介なのは、攻撃者がネットワーク内に留まる時間が長くなればなるほど、攻撃の痕跡がバックアップに保存される可能性が高まることです。これらの痕跡が特定や除去されることなく復旧した場合、再び攻撃が始まる可能性があります。このようなシナリオは、ランサムウェア攻撃から復旧した組織が、クリーンなデータの復旧を確実に行わない場合によく発生します。

組織はデジタルフォレンジックとインシデント対応 (DFIR) のプロセスに従い、セキュリティオペレーションセンター内でクリーンなデータを確実に復旧する必要があります。これまで、DFIRでは以下のことを行ってきました:

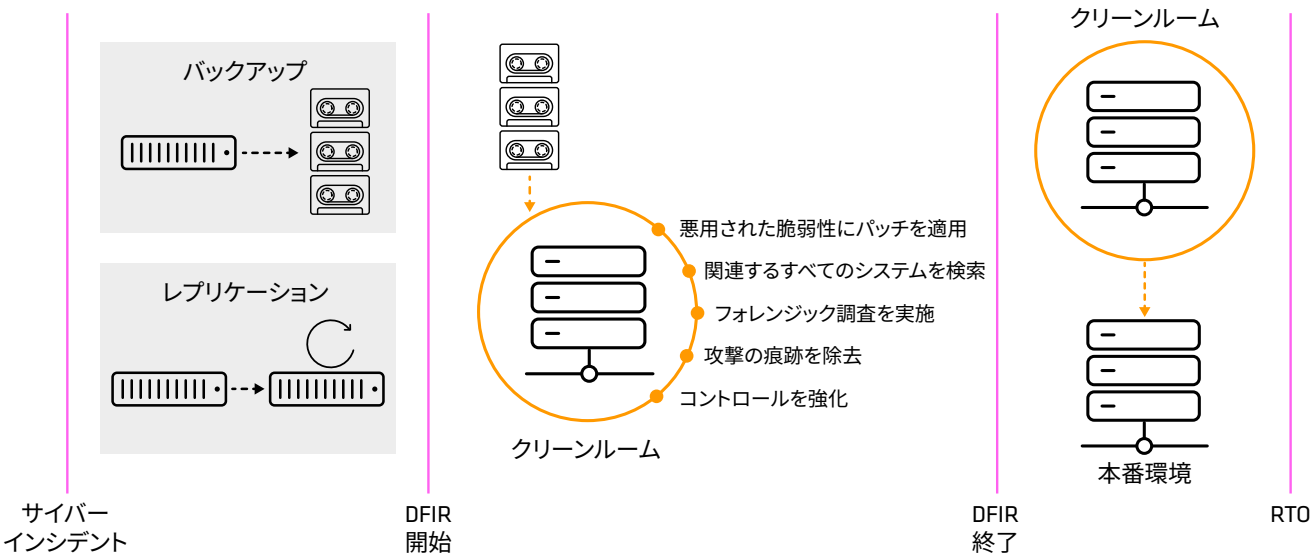
- 侵害されたホストのフォレンジックイメージ取得
- インシデントのタイムライン特定のための調査プロセスとツールの適用
- 攻撃で使用されたバイナリアーティファクトの検索と分析
- 権限昇格や永続化に使用された手法の解明
- インシデント範囲の拡大に関わる他の侵害システムの追跡
- プラットフォームを本番環境に戻す前の修復対象となる脆弱性のスキャン
- 予防や検知制御で攻撃を阻止または検知できなかった理由の究明

通常、これらの作業は、隔離された復旧環境 (IRE) または「クリーンルーム」環境で行われます。

もちろん、既に消去または暗号化されたシステムに対してフォレンジックイメージを取得しても有意義な証拠は得られないため、インシデント対応者はバックアップリポジトリを使って調査を始めます。バックアップデータを使用すると、時間の経過に伴う変化を確認し、攻撃のライフサイクルを追跡することができます。

Cohesityは、DFIRプロセスを開始するためのイミュータブルでフォレンジックに適したプラットフォームを提供しています。調査担当者は、APIを介して迅速にインスタンス化やオーケストレーションが可能な過去のファイルシステムのスナップショットにアクセスできます。そのため、影響を受けたシステムの背景情報だけでなく、インシデント発生中全体のファイルシステムに関するインサイトも得られます。これは、アナリストにタイムトラベルの超能力を与えるようなものです。アナリストは、永続性を維持するための構成ファイルの変更、正規のバイナリやライブラリの悪意あるコピーでの上書き、その他攻撃に用いられる悪意ある痕跡など、敵の手口を特定するためにファイルシステムを時系列で比較することができます。

RTO (目標復旧時間) は、想定外のシステム中断発生後に、ネットワークやアプリケーションをリストアし、データへのアクセスを回復するまでに許容される最大の時間のことです。



DFIRプロセスにバックアップインフラストラクチャを含めると、データを本番環境に戻す前に調査を完了することができます。ここでの課題は、組織が設定したRTO (目標復旧時間) の達成を妨げる可能性があるということです。結局のところ、ほとんどのRTOはサイバー攻撃時に必要な調査を考慮して設定されていません。

バックアップを活用してクリーンルーム環境を構築すると、全体のダウンタイムが短縮し、リストアされたデータがクリーンであることが保証されるため、再感染時に同じプロセスを繰り返す必要がなくなります。これにより、組織はRTOを達成し、長引くダウンタイムを回避できるようになります。

サイバーレジリエンスの計画から実行まで

万全の準備

全関係者を含む部門横断型のランサムウェアレジリエンスチームを発足します。

ランサムウェアのインシデントは、他のサイバー攻撃とは異なります。組織全体や、顧客への製品やサービスの提供能力に影響を及ぼすのです。対応と復旧にかかる一秒一秒が重大な損失となります。スタッフはコミュニケーションが取れず、業務も遂行できなくなります。報道機関はこぞってインシデントを報じ、顧客は不満を募らせます。組織全員が、サイバー攻撃時の自身の役割について確実に理解していることが重要です。

これには、以下に関する決定が含まれます:

- メールなどの主要な手段が使えない場合の連絡方法
- 各機能や対応の各段階における責任者
- チームメンバーが不在の場合に従うべきプロセスと、代理連絡先

対応や復旧に直接関わらない従業員も、自分に何が期待されているのかを把握しておく必要があります。これはなぜでしょうか? 信頼できる情報がない場合、噂や推測によって対応が妨げられ、復旧が遅れる可能性があるためです。

全関係者を交えた現実的なランサムウェアの机上演習を実施します。

組織を団結させる有効な手段のひとつは、組織の状況に即した現実的なランサムウェアの机上演習を実施することです。実際のランサムウェア攻撃で直面しうる脅威や対応上の課題について、インサイトが得られます。

ランサムウェアのリスク計算におけるあらゆる影響を考慮します。以下のような影響が挙げられます:

- 一次的な影響:
  - 組織が製品やサービスを提供できない
- 二次的な影響:
  - 専門サービスの利用料やランサムウェア攻撃者への支払いを含む、調査とインシデント対応にかかる運用コスト
  - 組織の評判の低下
  - ランサムウェアインシデントに関連する規制上の罰金や、制裁対象団体への支払い
  - 知的資本の損失
  - データ侵害に関するパートナーや顧客からの訴訟

企業のリスク管理にランサムウェアのリスクを統合します。

当たり前のことのように思えますが、多くの企業はランサムウェアの影響を重大な運用リスクとはみなしていません。ランサムウェアのリスクを組織の企業リスク管理に確実に統合することで、適切なレベルのガバナンスを確立し、サイバーセキュリティポリシーの十分な裏付けを得るとともに、適切なリスク管理を維持することができます。

組織全体のランサムウェアポリシーを策定します。以下を行う必要があります:

- **インシデントをランサムウェア攻撃と宣言するための明確な基準を設定します。**ランサムウェアに対する対応と復旧のワークフローは、従来のマルウェアやデータ流出に対する対応のワークフローとは異なります。SOCアナリ

ストがインシデントを宣言できる基準を確立し、適切な調査、封じ込め、根絶措置を取れるようにする必要があります。この基準が明確でなければ、SOCが対応の許可を求めている間に、ランサムウェア攻撃が組織内に拡大してしまう恐れがあります。

- **サイバーバックアップ戦略を定義します。**サイバーレジリエンスのシナリオにおけるバックアップ戦略は、従来の災害復旧や事業継続に関するデータレジリエンス戦略とは異なることがあります。これは、対応と復旧能力の構造や成熟度によって左右されるためです。
  - バックアップデータのみを使用する場合: インシデント調査に必要なサーバーを起動し、ベアメタルからインフラを再構築してからデータを復旧します。このポリシーでは、復旧に用いるゴールデンマスターイメージを維持する方法を確立する必要があり、その中には脆弱性や構成ミスのスキャンも含まれます。
  - バックアップインフラストラクチャを使用する場合: インフラストラクチャ全体を復旧した後、インシデント対応に従って各要素を異なる時点にリストアし、環境をクリーンアップします。
- **運用レジリエンスのカテゴリーを定義します。**既に確立されたデータレジリエンスのビジネスインパクト分析に基づいてカテゴリーを設定し、クリーンルーム内で対応ツールを利用できる能力や、サイバーレジリエンスのバックアップ戦略を含めます。
  - **インシデントにおける対応や復旧に必要な、通信やセキュリティインフラを復旧させる能力も含めます。**これには、以下を考慮します:
    - 物理的なアクセス制御
    - DNS
    - 音声通信
    - 電子メール
    - 対応の調整に使用されるコラボレーションプラットフォーム
    - ケース管理
    - フォレンジックやインシデント対応ツール
    - 脆弱性スキャンや管理
    - ID/アクセス管理
- **身代金の支払いを検討する条件を定義します。**
  - 身代金を支払うための資金をどのように確保するか?
  - 保険に身代金の支払いが含まれているか?
  - 保険会社は、特定の勢力に属するランサムウェア攻撃者を戦闘員として扱うのか?
  - 保険会社は、制裁対象団体への支払いを補償しているか?
  - ランサムウェア攻撃者に対する組織の交渉手法は?
  - 評判、規制、刑事罰面での影響とは? (支払い先が制裁対象の場合など)
  - 身代金の支払いに使用する暗号通貨の入手方法は? (本人確認の所要時間も考慮)
- **ランサムウェアポリシーが定期的に更新されるよう保証します。**これにより、ランサムウェア攻撃の変化し続ける性質を反映できるようになります。

先手を打つ対策

- **ランサムウェア攻撃者とそのツール、技術、手順 (TTP) を理解します。**
  - ランサムウェアの組織、キャンペーン、手法に関する、政府、商用、オープンソースのインテリジェンスを収集します。
  - 自社の業界または地域で活動しているランサムウェア攻撃者やワイパー攻撃の実行者に関するインテリジェンスの収集と分析を優先します。
  - 攻撃者が用いる手法をMITRE ATT&CKフレームワークにマッピングします。
  - ランサムウェア集団が使う最新の手口を取り入れた、定期的なフィッシングテストを計画します。

- ランサムウェア攻撃者に悪用された脆弱性が、脆弱性管理プログラムで優先的にパッチ適用されるよう設定します。
- ランサムウェア攻撃者が、サードパーティやマネージドサービスプロバイダーとの関係性を悪用し、自社と類似した組織を標的とする手口を理解します。これをサードパーティのリスク評価とコントロールで考慮します。

- **連絡先情報を文書化して保管します。**対応チームのすべてのメンバーと代替メンバー、主要な担当者、重要な関係者を含め、ランサムウェアインシデントの影響を受けない領域外のコミュニケーションチャネルでやり取りをするのが理想です。
- **報告用チャネルを作成します。**ランサムウェアインシデントを報告するため、顧客、同業組織、サプライチェーンパートナーなどのサードパーティを含めます。
- **社内ユーザーがランサムウェアに類する挙動を報告するための専用チャネルを作成します。**以下の内容を取得します:
  - 報告者の氏名と役職
  - 発生日時
  - 気付いたこと
  - ランサムウェアだと思った理由
  - 発見時の行動
  - 物理的な発見場所と接続していたネットワーク
  - 使用していたアカウント
  - 使用していたシステム (オペレーティングシステム、ホスト名、IPアドレス)
  - ログインしていたアカウント
  - 連絡を取った相手とその内容
  - 業務上、通常アクセスする情報
- **組織に関わるランサムウェアやワイパーのインシデントを、法執行機関やサイバーセキュリティ機関に報告するための報告チャネルを作成します。**
- **サイバー危機対応チームを編成します。**これには以下のメンバーが含まれます:
  - 事業部門のリーダー
  - IT部門 (復旧と脆弱性管理を含む)
  - OT部門 (関連する場合)
  - セキュリティオペレーション (インシデント対応マネージャー、デジタルフォレンジックに加え、存在する場合はマルウェアリバースエンジニアリング、ハントチーム、脅威インテリジェンスを含む)
  - 法務
  - 広報
  - 人事
- **必要に応じて、インシデント対応組織のサービスを利用します。**
  - インシデント対応組織と契約するための事前承認を得ます。
  - インシデント対応を保険会社に依頼する場合、保険会社は実際のランサムウェアインシデントの対応だけでなく、保険契約時に提出した管理体制の遵守証明に関する違反の証拠を調査する可能性があることに注意が必要です。
- **ホールディングステートメントや情報漏洩発表に関するテンプレートを作成します。**ステートメントの大部分を作成しておくことで、後で詳細を加える場合でも、迅速に対応しやすくなったり憶測を防いだりすることができます。
  - メディア対応とインシデント対応に関する説明の両方のトレーニングを受けた、組織のスポークスパーソンとその補佐役を任命します。
  - ブリーフィングやメディアインタビュー用のコミュニケーションチャネル (インシデントの影響を受けないチャネル) を用意します。
- **法執行機関や国のコンピューター緊急対応チーム (CERT) との関係を事前に構築しておきます。**
- **法執行機関との契約について、法律顧問によるレビューを受けます。**
- **提案された対応計画や声明、民事責任、規制責任、刑事責任の可能性について、法務顧問に確認してもらいます。**

攻撃対象領域の縮小

- **ランサムウェア集団に悪用されやすい脆弱性のあるシステムに対して、優先的にパッチを適用します。**重要資産の脆弱性を特定し、パッチを適用します。
- **システムを強化します。**脅威インテリジェンスを通じて特定された、ランサムウェア集団が攻撃に利用する重要なシステムと攻撃ベクトルを優先的に対応します。機器のポートとプロトコルを正しく設定し、業務目的で使用されていないものは無効にします。ランサムウェア攻撃者は「環境寄生型 (Living off the Land、LotL)」攻撃で正規のツールを悪用するため、これらのツールへのアクセスを制限することで攻撃の可能性を低減できます。
- **リモートデスクトッププロトコルやその他のリモートデスクトップサービスの使用に関するベストプラクティスに従います。**リモートアクセスサービスは、ランサムウェア攻撃者による初期の主な侵入経路です。特定の試行回数を超えた場合のアカウントロック、多要素認証、すべてのリモートデスクトップに対するログイン試行の記録を実施します。リモートデスクトップサービスの利用に、正当な業務上の理由があることを確認します。リモートデスクトップサービスの不正使用がないか、ネットワークを監査します。
- **ファイル共有プロトコルを無効にするかブロックします。**これには、SMB (Server Message Block) プロトコルのアウトバウンド通信や、古いバージョンのファイル共有プロトコルの削除または無効化が含まれます。脅威者は、組織全体にマルウェアを拡散するためにファイル共有プロトコルを使用します。
- **全システムの資格情報とアクセス権限が最小権限の原則に基づいて管理され、特権アカウントの数が制限されていることを確認します。**
- **特権アカウントが日常業務に使用されるのを防ぎます。**
- **ネットワークのセグメンテーションを実施します。**ネットワークのセグメンテーションは、ランサムウェアの拡散を抑え、ラテラルムーブメントを検知できる可能性を高めるための、最も有効な方法のひとつです。
- **ベースライン構成と変更管理を適用します。**ベースライン構成と変更履歴情報を活用すると、調査中にバックアップイメージを既知の正常なイメージと比較することができます。
- **組織内のセキュリティが不十分なデータリポジトリを特定します。**Cohesity DataHawkのデータ分類では、バックアップ全体をスキャンし、本番システムに影響を与えることなく機密データを特定します。機密データの所在を包括的に把握することで、組織はそのリスクを評価することができます。

バックアップの保護

- **バックアップシステムが十分にエアギャップされていることを確認します。**これにより、攻撃者による削除や破損を防ぐことができます。Cohesity FortKnoxは、仮想エアギャップを介してCohesityが管理するクラウド保管庫にデータのイミュータブルコピーを配置することで、サイバーレジリエンスを強化します。
- **バックアップシステムでは、攻撃者による破損や削除を防ぐイミュータブルなデータストアを使用するようにします。**例えば、Cohesity Data Cloudは、上位特権者でもバックアップを削除できないようにするデータロック機能を備えた、イミュータブルなストレージプラットフォーム上に構築されています。
- **バックアップ管理者アカウントで多要素認証を使用します。**主要なID/アクセス管理サーバーがランサムウェアの影響を受けた場合に備え、複数の対策を導入します。Cohesityは、SSOとTOTPの両方の多要素アプローチをサポートしています。
- **ロールベースのアクセス制御 (RBAC) を使用して、最小権限を割り当てます。**バックアップシステムのユーザーには、各役割に関連するタスクの実行に必要な最小限の権限のみを割り当てる必要があります。Cohesityには、最小権限をサポートするきめ細かい単位のRBACがあります。
- **バックアップシステムに職務分離を導入し、侵害された管理者アカウントによる悪意のある変更を防止します。**Cohesityのクォーラム機能では、バックアップと復旧に関するタスクに対して複数の認可レイヤーを定義することができます。
- **3-2-1バックアップ戦略を採用します。**データのコピーを3つ保持し、2種類のメディアに保存して、少なくとも1つのコピーをオフサイトに保管します。
- **バックアップを定期的にテストします。**バックアップのテストは定期的に実施し、自動化する必要があります。必要に応じて是正措置が取れるように、テスト結果を報告します。Cohesity DataProtectは自動テストをサポートしています。

- **重要システムのバックアップについて、完了/失敗/テスト済みを示す指標を収集し、報告します。**
- **拡張に備えてバックアップインフラストラクチャに十分な容量を確保します。**
- **バックアップシステムが、ランサムウェアインシデントの対応に必要なサイバーセキュリティ機能に対応できることを確認します。**インシデント発生時に被害を受けたシステムが暗号化されている場合、セキュリティチームはフォレンジックイメージを取得できません。そのため、インシデントの調査を行うには、バックアップシステムを利用する必要があります。Cohesityは、データ分類、脅威インテリジェンスフィード、脅威ハンティングなどの対応機能を、データ管理プラットフォーム自体に組み込んでいます。また、データセキュリティアライアンスを通じて、Splunk、Cisco、Palo Alto、Tenable、Qualys、Crowdstrike、ServiceNowなどの主要セキュリティベンダーと事前に統合されたソリューションも提供しています。
- **インシデント後の再構築を加速するため、重要システムのゴールデンマスターを作成して保管します。**クリーンルーム内のシステムを再構築できるよう、迅速に展開可能な、事前に構成されたオペレーティングシステムや関連するアプリケーションソフトウェアを含むイメージテンプレートを保管します。

ランサムウェアに対する保護の強化

- **ランサムウェア集団が用いるATT&CKの手法に対する、既存の予防・検知制御の適用範囲におけるギャップを特定します。**継続的にこれを実行することで、攻撃者が行動に適応させる中でも、予防や検知の効果を最大化することができます。
  - 予防、検知、対応の各段階で使用できる一般的な侵害指標 (IoC) には、以下のものがあります:
    - 異常なファイルトランザクション (暗号化と削除の量の逸脱)
    - サービスやアプリケーションの不審な起動タイミング
    - 不明または想定外のサービスやアプリケーションの存在
    - 不正なリモートアクセスやVPNソフトウェアの存在
    - システムパフォーマンスの低下 (CPUやRAMの使用率増加)
    - ホストのセキュリティ計測パフォーマンスの低下や無効化
    - セキュリティエージェントの無効化
    - 不明または想定外のドメイン名やIPアドレスによる接続
    - プロトコルの不一致
    - 既知の不正なファイルハッシュ
    - 構成ファイルへの不審な変更
    - インバウンドやアウトバウンドにおける異常な通信、送信元、送信先
    - メモリダンプ内の不審なプロセスやテキスト
    - ログオンユーザー内の不審なアカウント (過去と現在)
    - 不審なネットワーク共有やマウントされたネットワーク共有
    - 不審なユーザーアカウント
    - 不審なインストール済み証明書
    - ARPやDNSキャッシュ内の不審なエントリ
    - システム、ログファイル、NTPサーバーの日付や時刻の異常
    - DHCPログの不審なエントリやリース
    - 異常なユーザーエージェント文字列
    - 非標準のアプリケーションビーコンや更新
    - フルパケットキャプチャ内のバイナリ
- **予防と検知の内容をテストします。**ランサムウェアのIoCに対して作成されたルールをテストします。
- **ランサムウェアやワイパー攻撃に関連する、ファイルの暗号化や削除といったエンドポイントのファイルシステムの異常を検知できるようにします。**Cohesityは、機械学習を使用してこれらのパターンを特定します。
- **既知の悪意ある指標を含むメールをブロックするよう、メールゲートウェイフィルターを導入します。**

- **ランサムウェア関連のコンテンツを含むと特定されたメールをユーザーのメールボックスから削除する仕組みを実装します。**
- **DMARC (Domain-based Message Authentication Reporting and Conformance) のポリシーと検証を実装します。**有効なドメインからのなりすましメールや改ざんメールを受信する可能性が低くなります。
- **特定のビジネス要件がない限り、メールで送信されたMicrosoft Officeファイルのマクロを無効にします。**
- **承認されたソフトウェアのみが実行されるよう、重要資産のホワイトリスト機能を備えたアプリケーションを使用します。**Windowsプラットフォームでは、Microsoftのソフトウェア制限ポリシーやAppLockerを使用します。すべてのアプリケーションを個別にリスト化しようとするのではなく、ディレクトリ単位の許可リストを使用します。多数のランサムウェア攻撃ベクトルの実行を制限するデフォルト設定ではアプリケーションの実行場所をPROGRAMFILES、PROGRAMFILES (X86)、SYSTEM32に限定しています。ただし、これによって「環境寄生型」の攻撃を防ぐことはできません。特定のアプリケーションに対する例外が認められていない限り、それ以外のすべての実行場所を禁止します。
- **サプライチェーンのリスク管理やサイバーハイジーンの実践状況、サードパーティパートナー、マネージドサービスプロバイダー (MSP) について理解します。**多くのランサムウェア攻撃は第三者を通じて実行されます。
  - サイバーリスクの管理と制御における自社とパートナーの役割を理解します。役割と責任範囲が明確に定義・評価され、契約内容に是正措置のための仕組みが盛り込まれていることを確認します。
- **可能な限り多くのサービス、特にリモートアクセスや特権アカウントに対して多要素認証を採用します。**
- **事業部門やITリソースのカテゴリー、運用技術 (OT) 環境を分離するため、論理的または物理的なネットワークセグメンテーションを実施します。**これにより、攻撃を受けた際のランサムウェアの拡散が抑えられます。
- **PowerShellが「環境寄生型」攻撃に利用される機会を減らします。**
  - 状況に応じてPowerShellの使用を特定のユーザーに制限する
  - PowerShellをバージョン5.0以降に更新し、それ以前のPowerShellをすべてアンインストールする
  - モジュール、スクリプトブロック、トランスクリプションログが有効になっていることを確認する
  - PowerShellが有効になっているシステムでは、PowerShellのWindowsイベントログとPowerShellの運用ログの保持期間が180日以上であることを確認する
- **過去のネットワークトラフィックを分析し、東西 (East-West) や南北 (North-South) の異常なトラフィックパターンを検出します。**ネットワークトラフィックのメタデータ (NetFlow/sFlow) を使用するか、可能であればフルパケットキャプチャやネットワーク侵入検知/防止システムを使用します。
- **ドメインコントローラーのセキュリティを確保します。**
  - **ドメインコントローラーに、データ管理とセキュリティエージェント以外のソフトウェアがインストールされていないことを確認します。**ドメインコントローラーへのアクセスは、管理者グループに制限します。このグループに属するユーザーは、日常業務では別の制限付きアカウントを使用する必要があります。
  - **インターネットへのアクセスを防止するよう、ドメインコントローラーにホストファイアウォールを設定します。**
  - **ネットワーク上で送信されるのがNTLM v2応答のみになるよう、Kerberos認証を有効にし、可能であればNTLM監査も有効化します。**
  - **LSA (Local Security Authentication) による保護が有効になった場合に影響を受けるアプリケーションを把握するため、LSASS.EXEの監査を行います。**これによりコードインジェクションによる資格情報の取得を防ぎ、影響が許容できる場合はこれらの保護を有効にすることができます。
  - **ホストとドメインコントローラー間でSMB署名が必須となるようにします。**これにより、対象ネットワークでのリプレイ攻撃を防ぐことができます。

ランサムウェアに対する検知の強化

- **侵害を検出するため、履歴データを活用して積極的にハンティングを実施します。**予防ルールや検知ルールが設定されていない、ランサムウェア集団に関する新たな脅威インテリジェンスやIoCを活用します。Cohesityには、ランサムウェア集団が用いる110,000件以上のIoCを提供する統合型の脅威インテリジェンスフィードがあり、バックアップ内にそれらが存在するかどうかをハンティングする機能があります。稼働中のシステムではなくバックアップに対して受動的にハンティングを行うため、攻撃者はこの活動を検知できません。そのため、攻撃者がエンドポイントソリューションに対して用いる防御回避手法の影響を受けません。さらに、バックアップの保持期間はセキュリティソリューションよりも長い傾向があるため、長期にわたって検知することができます。
- **CPUやディスク使用率の異常な変動を検知する仕組みを導入します。**こうしたメトリクスは一般的にIT運用プラットフォームで収集されますが、検知強化のために追加のシグナルとしてセキュリティチームにも連携されることがあります。
- **異常なネットワークプロトコルを特定します。**これには、ランサムウェア集団が使用することで知られるI2PやTORが含まれます。
- **ランサムウェアやワイパーのコマンド & コントロールで使用される既知のポートや送信先を用いて、ネットワーク接続を特定します。**

インシデントへの対応

- **影響を受けた資産に関連する類似のアラートを特定し、グループ化します。**
- **以下を含む、インシデントの初期損失予測 (影響範囲) を作成します:**
  - 暗号化または消去されたエンドポイントの推定数
  - 暗号化または消去されたシステムの影響を受けるビジネスバリューチェーン
  - 影響を受けたデータの規制上の義務 (記録数やデータの種類)
  - 流出の疑いがある証拠

> Cohesityは、影響を受けたシステムのバックアップを自動的に検索し、ランサムウェアインシデントによる潜在的な規制上の影響を特定します。バックアップされているシステムは、インシデントの発生前でも対応中でも、オンデマンドで分類することができます。

- **データ窃取に使用されたステージング環境を特定します。**ネットワーク上のシステムで、予想外にデータ量が大幅に増加したシステムや、そのホスト上に通常存在しない種類のデータがあるシステムを特定します。Cohesityは、影響を受けたシステムのバックアップを自動的に検索し、ランサムウェアインシデントによる潜在的な規制上の影響を特定します。
- **有線と無線ネットワークの両方から感染しているホストを隔離します。**
- **ランサムウェアの亜種が既知で自己拡散する場合は、既知の通信経路や感染経路 (ホストやネットワークファイアウォール、メールゲートウェイ、ネットワークアクセス制御) をブロックします。**
- **クリーンルームを有効にします。**セキュリティツール、コミュニケーション、コラボレーション、アクセス制御システムに影響が出ている場合は、既知の正常なインスタンスを迅速に起動し、対応活動を開始できるようにします。
- **影響を受けたシステムの最終バックアップをクリーンルーム環境にリストアします。**これは、調査を開始するためのフォレンジックイメージとして機能します。別の時点でのシステムの状態は、過去の傾向を把握し、時間経過に伴うファイルシステムの変化を特定するのに役立ちます。
- **クリーンルーム内のシステムに、信頼できる検知/応答/フォレンジックツールを再展開します。**攻撃者は、検知を回避できるよう、エンドポイントツールを標的にします。これにより、エンドポイントツールが正しく機能しているかどうかに確信が持てなくなります。エンドポイントツールを再インストールすることで、正常に機能し、ツールの報告内容が正しいことに自信を持つことができます。

- **ランサムウェアの亜種が不明な場合は、以下の方法で判別します:**
  - 身代金要求メッセージを収集する (暗号化後に自動的に表示されるグラフィカルなポップアップ、テキストやHTMLファイル、連絡先メールアドレスを含む感染システムの壁紙画像、身代金要求を含む音声ファイル)
  - ランサムウェアの集団や亜種を特定するために身代金要求メッセージを分析する (ランサムウェア名、使用言語、構文、構造、表現、アートワーク、連絡先メールアドレス、ユーザー名、身代金の支払い方法 (暗号通貨の種類やギフトカードなど)、暗号通貨の場合は支払先アドレス、サポート用チャットアドレスやサポート用URL)
  - 暗号化されたファイルやその他の生成された痕跡を分析する (暗号化ファイルのリネーム規則や拡張子、対象ファイルの種類、対象ファイルの場所、ファイル所有者や影響を受けたファイルのグループ、ファイルの作成日時や変更日時の大規模な変更といったファイルのメタデータに対する変更、エントロピーやバイトプロットの可視化、暗号化ファイルに使用されたアイコン、ファイル属性、暗号化ファイルや鍵情報の一覧を含むファイル、その他データファイル)
  - 必要に応じて感染経路をより詳細に調査する
  - 既知の亜種ではない場合、リバースエンジニアリングを実施するために、インスタンス化されたファイルシステムから不審なバイナリを抽出する
  - 収集した痕跡を確認し、以下のようなサイトと照合してランサムウェアの集団や亜種を特定する:
    - Ransomware Census (https://goo.gl/b9R8DE)
    - CryptoSheriff (https://www.nomoreransom.org/crypto-sheriff.php)
    - ID Ransomware
- **永続性の証拠を探します。**Cohesityが取得した過去のスナップショットをインスタンス化することで、アナリストはファイルシステムを確認し、永続性の証拠を探すことができます。これには以下が含まれます:
  - 「外部から」の永続化メカニズム: 不正アカウントを使った外部システムへの認証済みアクセス、境界システムへのバックドア設置、境界システムの脆弱性の悪用など
  - 「内部から」の永続化メカニズム: 内部システムへのマルウェアの埋め込みや環境寄生型のさまざまな変更 (Cobalt Strikeなどの商用ペネトレーションテスト用フレームワークの展開、PsTools (特にPsExecによるリモートインストールとマルウェアの制御、情報収集) の使用、PowerShellスクリプトの利用など)
- **不審なプロセスやテキストの痕跡を検出するため、メモリ内容のイメージを取得します。**
- **変更されたレジストリキーを特定します。**
- **最近作成された圧縮ファイルを特定します。**
- **スケジュールされたプロセスやジョブを調べます。**
- **稼働中や実行中のネットワークサービスを、運用すべきものと照らし合わせて監査します。**
- **ステージングやデータ窃取の証拠を発見した場合は、データ損失対策のプレイブックを実行します。**Cohesity DataHawkは攻撃を受けた際にこれらのシステムにどのデータが存在したのかを特定できるため、インシデント対応者はコンプライアンス上の義務を特定し、データ主体や規制機関に通知することができます。
- **攻撃で悪用されたシステムの脆弱性を特定します。**Cohesity CyberScanでは、インシデント対応者が攻撃のポイント付近のスナップショットに対してTenable社の脆弱性スキャナー「Nessus」を実行することができます。これにより、システムを稼働状態に戻す前に適用すべきパッチ一覧を作成し、最後に予定されていた脆弱性スキャン以降に攻撃者が悪用した可能性のある脆弱性を特定することができます。

- **無許可の資産上の知的財産、財務情報、個人を特定できる情報をスキャンし、ステージングに使用された資産を特定します。**Cohesity DataHawkのデータ分類を使用すれば、ステージング環境で機密データを特定することができます。
- **インスタンス化された過去のファイルシステムから不審なバイナリを抽出します。**これらを分析したりリバースエンジニアリングしたり、VirusTotalのようなサービスにアップロードしたりします。過去のファイルシステムのインスタンス化は、ServiceNow Security Incident Response、Splunk Phantom、Palo Alto XSOARなどのSOAR (Security Orchestration, Automation, and Response) ツールを使い、Cohesityでオーケストレーションすることができます。
- **インスタンス化されたファイルシステムから不審なバイナリを抽出し、マルウェア分析サンドボックスで実行解析します。**
- **組織内の同様のシステムに感染がないかを確認します。**同様のユーザーやグループを持つホストを調査します。システムが暗号化されていない場合は、潜在的な影響を特定するため、これらのホストのインスタンスを感染したシステムと比較します。Cohesityには、組織のバックアップインフラストラクチャに対して迅速にクエリを行うことができる、インデックス作成機能と検索機能があります。
- **ローカルアカウント、ID/アクセス管理ツール、ディレクトリサービスで、新規アカウント、あるいは権限やアクセス権の変更を確認します。**
- **ランサムウェアのコマンドアンドコントロールに接続しようとしている他のシステムを特定します。**
- **ペイシェントゼロ (最初の感染者)、初期感染経路、感染している各エンドポイントを特定するため、MITRE ATT&CKを活用して調査を継続します。**
- **回避された予防・検知コントロールと、その回避に使用された手法を特定します。**これらを緩和計画に追加して、本番環境に復旧する前にコントロールを強化します。

コミュニケーション

- **報道機関に連絡します。**有害な憶測を防ぐため、報道機関に最新情報を提供します。
- **影響を受けたデータ主体に連絡します。**いかなる連絡も、規制上や法律上の義務を遵守していることを確認します。
- **内部関係者に連絡します。**内部のスタッフに対し、現在の状況と彼らに期待することを随時伝え続けます。特に、報道機関はLinkedInなどのプラットフォームを利用して従業員を特定し、直接連絡を取ることがあるため注意が必要です。
- **報告に関する規制上の遵守義務を果たすため、規制当局に連絡します。**
- **保険会社に通知します。**
- **法執行機関や、国や業界のCERTに通知します。**

インシデントからの復旧

最善のシナリオは、インスタントマスリストア (IMR) などのツールを使用し、感染を発見・除去し、システムを本番環境にリストアすることです。実際には、リストアされたシステムとベアメタルから再構築されたシステムの組み合わせることもあります。ベアメタルリストアを実行するには、最新のテスト済みパッチが適用され、安全に管理されている重要システムの「ゴールドイメージ」にアクセスできる必要があります。これらのテンプレートを展開すれば、復旧不能なシステムを迅速に再構築することができます。また、Cohesity Data Cloudにあるツールを使用してセキュリティを確保できるため、サイバー攻撃中に破損することはありません。その後、ベースのオペレーティングシステムやアプリケーションに加え、他のバックアップからの関連データをリストアすることができます。これによりRTOが最適化されると同時に、フォレンジック調査のために影響を受けたシステムの履歴バックアップも作成されます。

データとアプリケーションの復旧と並行して、インシデントを文書化し、再発防止策を講じる必要があります。

組織は、以下を行う必要があります:

- 初期の感染経路、悪用された脆弱性、永続化メカニズムの知識を活用し、将来の攻撃から守るための復旧計画を更新して、各要素が安全かつ安定した状態に回復できるようにする
- 残りのシステムをクリーンルームに配置し、上記の手順を繰り返してIoCを隔離する
- 検出した脆弱性にパッチを適用する
- 影響を受けたすべてのシステムとアカウントに対してパスワードリセットを発行する
- 隔離した受信箱から、悪用された痕跡を含む過去のメールを削除する
- 以前感染したシステムの集中監視を強化する

キーポイントと今後の対応の整理

ランサムウェア攻撃を受けた後、教訓を得るために以下の質問を行います:

- どのような製品とサービスが影響を受けたか?
- ビジネスにどのような影響があったか?
- どの関係者が影響を受けたか?
- 関与した脅威者は誰か?
- 対応過程で何が問題だったのか?
- 対応過程で何が正しかったのか?
- いつ攻撃を検知したのか?
  - 最初の感染から検知までの遅れは?
  - なぜもっと早く検知されなかったのか?
  - 検知や防止に失敗したコントロールはどれか?
- 回避されたコントロールとその方法は?
- 将来のインシデントを防ぐために、業務のどの部分を見直す必要があるか?
- 今後どうすれば避けられるか?
- 求められるRTOやRPO内で本番環境に復旧できたか?

新たに発見したIoCを認定パートナーとベンダーに共有します。

- ドキュメントとプレイブックを更新します。
- 最終的なインシデント報告と得られた教訓を、関係者と規制当局に伝えます。

Cohesityについて

Cohesity はAIを活用したデータセキュリティのリーダーです。Fortune 100のうち85社以上、Global 500の約70%を含む13,600社を超えるお客様が、膨大なデータに対して生成AI (Gen AI) によるインサイトを提供しながら、Cohesityを利用してレジリエンスを強化しています。Cohesityは、Veritasのエンタープライズ向けデータ保護事業との統合により誕生し、オンプレミス、クラウド、エッジ環境におけるデータのセキュリティと保護を実現するソリューションを提供しています。NVIDIA、IBM、HPE、Cisco、AWS、Google Cloudなどの支援を受け、Cohesityはカリフォルニア州サンタクララに本社を置き、世界各地にオフィスを展開しています。詳しくは、Cohesityの**LinkedIn**、**X (旧Twitter)** 、**Facebook**をご覧ください。

Cohesity.comの詳細はこちら

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000048-002 JP 4-2025