ランサムウェア

主要な利点

- 自己学習する Cyber AI がルールや脅威シグネチャに頼ることなくランサムウェアを無害化
- Enterprise Immune System は新種および高度に標的型のランサムウェアであっても特定
- Antigena は攻撃がどこで、いつ、どのように発生したかを問わずリアルタイムに自動対処
- Cyber AI Analyst はランサムウェアインシデントを自動的に調査し、迅速に緩和策を取るために必要な主要情報を収集

図 1: Cyber AI がランサムウェア攻撃を特定

ランサムウェアにより、昨年は 350 社だけでも合計 3 億 8100 万ドルの損害が発生しました。

出典: Hiscox, 2020

近年、ワークフォースの標準的なあり方と技術的イノベーションの急激な進化に伴って、ランサムウェア攻撃はますます洗練され、広範に発生しています。

ファイルレスのマルウェアやデータ抽出戦術を使った新種のランサムウェアが出現しており、便乗型の攻撃者は環境のあらゆる変化を利用してより効果的な攻撃を仕掛けようとしています。ルールやシグネチャを使用して既知のサイバー脅威のみを検知する従来のセキュリティツールは、そのようなシグネチャが存在しない、進化系のランサムウェアにはまったく通用しません。

セキュリティチームは従来型のコントロールだけではこれらの脅威に対抗できません。特に人員不足やオフィスに不在の時などはお手上げです。このような状況においては、ランサムウェアの被害が発生する前、出現と同時に阻止できるようなセキュリティテクノロジーが必要とされています。

Darktrace Cyber AI Platform: ランサムウェアの出現を自動的に特定・対処

Darktrace Cyber AI Platform は既知の脅威インテリジェンスやシグネチャに頼ることなく、最新のランサムウェアをリアルタイムに無害化する独自の能力を備えています。教師なし機械学習および深層学習テクニックを基盤とした Cyber AI は、組織内のあらゆるユーザーとテクノロジーの正常な「生活パターン」を学習し、脅威の発生を示す可能性のあるわずかな逸脱を認識することができます。

Enterprise Immune System はそれぞれのビジネスの「自己」についての進化する知識を使って、他のすべての防御戦略をすり抜けるこれまでに見たことのないランサムウェアも含めた、あらゆるサイバー脅威を明るみに出します。免疫システムアプローチの中でも重要な役割を果たす Cyber AI Analyst は、すべての脅威を自動的に調査するため、ユーザーは影響を受けたすべてのデバイスを簡単に確認し、ランサムウェアインシデントの全貌を関係者に連絡することができます。

深刻な攻撃のフラグが発生すると、自動対処テクノロジーである Darktrace Antigena が悪意あるアクティビティを数秒で封じ込め、攻撃を的を絞って無害化すると同時に、ビジネスに関連した通常の操作は続行させます。このテクノロジーは脅威の展開に応じてインテリジェントに適応し、24 時間週 7 日、セキュリティチームが多忙または不在の時にも、ワークフォース全体の保護を提供します。

ほんの数分で企業インフラを暗号化してしまうこともある、ランサムウェアの影響を最小化するには、マシンスピードのレジリエンスがきわめて重要です。Cyber AI Platform は、ビジネスのあらゆる場所からのパターンを相関づける独自の機能を有しており、E メールや SaaS プラットフォームからコーポレートネットワークまたは産業用システムまで、企業の多様なデジタルエコシステムのどこでランサムウェアに攻撃されても、統一された情報とコントロールを提供することができます。

Antigena Network:
攻撃をマシンスピードで無害化

ランサムウェアが出現したとき、脅威が高度に標的型である、またはまったく未知のものであっても、Antigena Network はマシンスピードかつ異常な通信にのみ的を絞って攻撃を中断できる唯一のソリューションです。Antigena Network はインテリジェントかつ適切なアクションを使って、接続の切断から特定のデバイスに対する正常な「生活パターン」の強制まで、自律的に対応します。セキュリティチームが手一杯である、またはオフィスに不在の時にも、Antigena Network は 24 時間週 7 日、ビジネス全体が常に守られているという安心を提供します。

Darktrace が開発した Antigena 自動対処テクノロジーは、Cyber AI の組織に対する変化する知識を使用して脅威にリアルタイムに適応し、その環境独自のコンテキストに基づいて最も適切なアクションを実行します。従来型のツールのような二項選択ブロック（例：当該デバイスを完全に検疫）を適用するのではなく、Antigena は異常な通信にのみ的を絞って攻撃を阻止し、他のあらゆる通常の業務の継続を可能にします。また、既存のセキュリティシステムとの統合によりセキュリティスタック全体を強化し、AI による考察とアクションを、ファイアウォール、SIEM、またはその他のツールにフィードすることができます。

Darktraceのトライアル利用中にRyukランサムウェアを遮断

Darktrace をトライアル利用中のある企業に Ryuk ランサムウェア攻撃が発生すると、Enterprise Immune System は即座にこれを検知し、また Antigena Network であればこれを完全に阻止できたことが明らかになりました。

最初に、Cyber AI はネットワーク上でこれまで見られたことのない、非常に稀な管理アクティビティを検知しました。このインシデントの後、この会社はトライアル期間中に Darktrace を適用していなかったネットワーク上のある部分に初期の侵害を発見しました。

その後、Cyber AI は悪名高い TrickBot バンキングトロイのダウンロードを検知し、それに続いて C&C トラフィックが観測されました。多数のデバイスが異常な動作を示しましたが、Cyber AI はその大元である 1 台のデバイスを特定しました。

Ryuk ランサムウェアが最後に展開されると、20 万以上のファイルがわずか 12 時間の間に暗号化されました。疑わしい SMB アクティビティが多数発生する「ノイズの多い」この期間中にも、Cyber AI はさらに明確に攻撃の範囲を指摘しました。

この会社のセキュリティチームは Darktrace が発したアラートに対し、暗号化が行われるまでにアクションを取ることができませんでしたが、このランサムウェア攻撃は Enterprise Immune System が侵害の最初の兆候を検知した直後に阻止できていたはずでした。

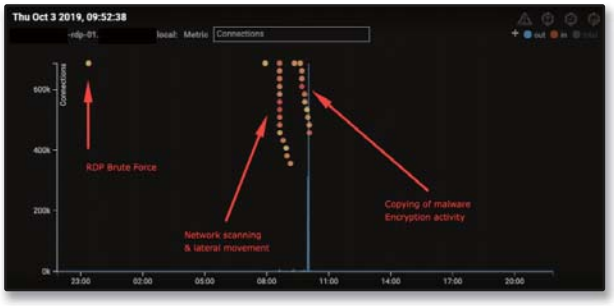

図 2: UI のグラフに表示されたランサムウェア攻撃の例：それぞれの点が Darktrace アラートを示しています。

数秒で自動対処

この会社が Antigena Network 自動対処テクノロジーを適用していれば、Darktrace のアラートに対する注意が欠如していたことも問題とはならなかったでしょう。実行形式のダウンロードから最初のファイルが暗号化されるまでに 4 時間が経過していましたが、Antigena であれば数秒で脅威を無害化していたはずです。このインシデントのいくつかのアラートに対して Antigena が取っていたであろうアクションには次が含まれます：

- **普段と異なる管理者 SMB セッション：**認証情報の不正使用によりサーバーにログインされた
  - **Antigenaアクション：**この単一の異常だけではアクションは実行されませんが、アラートのレベルが引き上げられます。
- **クライアント上の新しい管理者認証情報：**攻撃者が当該デバイス上で複数の新しい管理者認証情報を使用した
  - **Antigenaアクション：**これは高い信憑性で脅威を示す証拠となるため、Antigenaはこのデバイスの通常のログイン「生活パターン」を強制します。このデバイスに通常ログインするすべての管理者は継続してログインできますが、新しいログインは1時間ブロックされます。
- **ネットワークスキャン：**攻撃者がさらなる標的を探してネットワークをスキャンした
  - **Antigenaアクション：**このサーバーはネットワークをスキャンしたことはありませんでした。スキャンを行うのは管理者デバイスだけです。そのため、Antigenaはネットワークのスキャンを2時間に渡り停止します。
- **未知の外部ロケーションから実行形式ファイル：**さらに感染を進行させる後段のペイロードがダウンロードされた
  - **Antigenaアクション：**Antigenaは未知のロケーションからのダウンロードはブロックしますが、デバイスが通常のダウンロードを行うことは許可します。

Antigena Email:
ランサムウェアを発生源で阻止

多くのランサムウェアは E メールプラットフォームから侵入しています。このことは、従来型の E メールゲートウェイや、ルールやシグネチャに依存する従来の検知アプローチでは高度なランサムウェアを確実に捕捉するには不十分であることを証明しています。さらに、これらの従来型ソリューションはその範囲が限定されており、E メールのアクティビティと、デジタルインフラのさまざまな場所でのこれに関連した悪意あるアクティビティを結び付けることができません。

Cyber AI の力を利用した Antigena Email は、E メールアドレスの背後に存在するそれぞれの人間についての深い理解を構築します。このテクノロジーは今日の動的なワークフォースに適応することにより、ランサムウェア攻撃の兆候かもしれないわずかな挙動の変化を認識します。

そして、自律的かつ適切な対応により脅威をマシンスピードで阻止し、E メール全体の保留や、リンクに対するロック、あるいは添付ファイルを無害なファイルタイプに変更するなど、組織を露出から守ります。

万一ランサムウェアが受信箱を通過してネットワークに入った場合にも、Antigena Email は Enterprise Immune System との連携により攻撃の発生源を追跡し、水平方向の拡散を防止することができます。

ビジネスの他の部分でのアクティビティのパターンと E メール環境を相関づけることにより、Cyber AI は原因分析を行って元の E メールやインシデントに関係するかもしれないその他の E メールアクティビティを特定することができます。Antigena Email はその後、脅威と思われるその他の E メールを他の従業員の受信箱からも回収し、ランサムウェア攻撃の範囲を最小化します。

2021 年までに、11 秒に 1 回の割合でランサムウェア攻撃が発生するようになります。

出典: Cybersecurity Ventures

図 3: Antigena Email がランサムウェア攻撃に関連した一連の E メールを検知

市役所を狙った悪意あるリンクを無害化

米国のある有名な地方自治体が最近、おそらくランサムウェアを送り込もうとした、標的型の E メールによる攻撃の被害者となりました。Antigena Email は脅威が出現すると即座にこれを認識し、悪意あるペイロード、ランサムウェアその他がダウンロードされないように対応しました。

この脅威アクターは市役所のアドレス帳にアクセスできたものとみられ、それぞれが念入りに作成された E メールは受信者に合わせたもので、A から Z へとアルファベット順に送信されていました。メール自体は害のない内容に見えましたが、それらすべてには Netflix や Amazon など信頼されているサービスへのリンクに偽装されたボタンの背後に、悪意のあるペイロードが隠されていたのです。

Antigena Email はこれらの隠されたリンクを、受信者の通常の「生活パターン」との関連で分析しました。最初のメールが来た時点で、Antigena はこの受信者もその所属するグループの人や市の他のスタッフも、誰もこのドメインを以前に訪れたことがないということを即座に認識しました。

Antigena は直ちに確度の高い警告を発し、各リンクがネットワークに受信され次第自動的にロックすることを提案しました。

Antigena は「パッシブモード」で運用されていたため、マシンスピードで即座に脅威を阻止することはしませんでした。しかしこれにより Cyber AI と自動対処の有効性が明らかになりました。Antigena はアルファベットの 'A' の時点で攻撃を発見し無害化を指向しましたが、セキュリティチームが使用していた従来のツールが攻撃に気づいたのは 'R' に到達してからでした。

「アクティブモード」で運用されていたならば、Antigena は攻撃が 1 人目のユーザーに到達する前に無害化し、広範なランサムウェア攻撃の可能性から組織を保護していたでしょう。

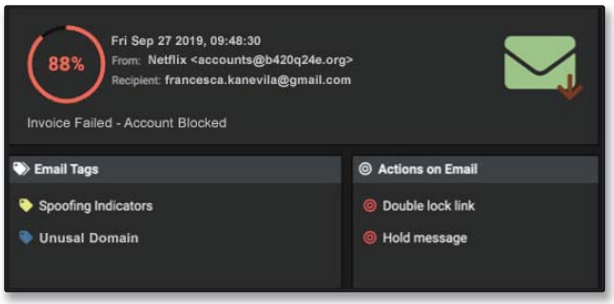

図 4: Antigena Email は各メールの異常性が高いと判定しました

ランサムウェアの発生源となった個人用 E メールアカウント

ある大手通信企業の E メール受信箱にランサムウェアが到着すると、Darktrace Cyber AI Platform は攻撃を検知し、1 つのファイルも暗号化させることなく自律的に攻撃を封じ込めました。

最初の侵害が発生したのは、1 人の従業員が会社用スマートフォンから個人用メールにアクセスし、騙されてランサムウェアが含まれる悪意のあるファイルをダウンロードさせられたときでした。数秒後には、彼の端末は Tor ネットワーク上の外部サーバーに接続し、SMB 暗号化アクティビティが開始されました。

9 秒以内に、Cyber AI はこの未知の動作に対して至急調査の必要性を知らせる優先アラートを発行しました。

この動作がその後数秒間継続する間、Cyber AI は判定を更新して自律的な対処を開始しました。

この時セキュリティチームは既に帰宅し週末の休みに入っていましたが、Antigena Network は単独で攻撃を阻止し、暗号化されたファイルをネットワーク共有に書き込もうとする試みをすべて遮断しました。

図 5: 類似の異常な SMB アクティビティについて報告する Cyber AI の UI 表示例

この会社が Antigena Email を導入していれば、ランサムウェアがダウンロードされることはおそらくなかったでしょう。絶対のツールというものはありません。しかし、もしランサムウェアが E メールを通じてネットワークに侵入してしまったとしても、Antigena Email はネットワーク内で検知された悪意あるアクティビティを、原因となった E メールに関連づけることができます。そして、他の同様に危険な E メールについても、ワークフォース全体から回収していたはずです。

組織の DNA に対する、深く、変化する理解によってのみ、Antigena Email および Darktrace Cyber AI Platform は、洗練されたランサムウェア攻撃に対してもこのようなリアルタイムの検知および対応を行うことができます。

Enterprise Immune System と Cyber AI Analyst: ランサムウェアインシデントの全貌を理解する

自己学習する Cyber AI により、Enterprise Immune System はランサムウェアの出現を示すアクティビティの微妙な変化を、既知の脅威インテリジェンスに頼ることなく検知することができます。お客様それぞれのインフラ全体の正常な「生活パターン」についての変化する理解により、Enterprise Immune System はごくわずかな逸脱についても特定し、セキュリティチームはマシンスピードの攻撃をその発生と同時に知ることができます。

免疫システムアプローチの重要な構成要素である Cyber AI Analyst は、検知されたあらゆる異常なイベントを自動的に調査します。ランサムウェア攻撃についても、影響を受けたあらゆるデバイスや感染源を特定し、対応を即座に開始するために必要なすべてのコンテキスト情報を提供します。

Cyber AI Analyst はトリアージまでの時間を 92% 短縮した実績があり、ランサムウェアの出現を、人間による検討が必要な重大な脅威として鋭く指摘します。AI により生成された「インシデントレポート」には、インタラクティブなタイムライン、攻撃についての簡潔な経過のまとめ、ならびに関連するデバイスやユーザーの動作についての詳細なデータが含まれます。

これらのレポートは脅威の展開に応じて自動的に更新され、セキュリティエキスパートが状況認識を得るため、また技術を専門としないステークホルダーに主要な情報を共有する上でもきわめて重要な役割を果たします。

Dharma攻撃を専門的に分析

標的型の Dharma ランサムウェア攻撃が英国のある企業に対して開始されたとき、Enterprise Immune System は脅威の検知に決定的な役割を果たし、また攻撃の発生を認識しレポートする Cyber AI Analyst の強力な能力が実証されました。

RDP サーバーが未知の IP アドレスから多数の接続を受け始めると、Cyber AI は瞬時にリスクを認識しました。後の調査により、この RDP の認証情報が攻撃前のどこかの時点で漏えいしていたらしいことがわかりました。

翌日、Cyber AI は脅威アクターが SMB バージョン 1 プロトコルを悪用していることを検知しました。その後、通常は行われない、未知のモロッコの IP に対する外部接続が行われ、IP に対する非常に特異なポートを使った SMB セッションが失敗している様子が観測されました。2 時間後、脅威アクターはより強力な C&C チャネルを確立し、インド、中国、イタリアにある未知の IP に接続を始めました。

さらに、Cyber AI は内部偵察活動を検知しました。これは受信 RDP 接続がネットワークスキャンを開始し、大量のデータがパナマの IP に転送され始めたときでした。

最後に、Dharma ペイロードが実行されました。暗号化アクティビティと並行して、ランサムウェアは内部偵察時に見られたのと同じ管理者認証情報を使って他のマシンへの感染を試みていました。暗号化が始まると、IT スタッフが RDP サーバーを停止させました。

セキュリティチームは当初、Darktrace の発したアラートに対するアクションをおろそかにしてしまいましたが、Cyber AI はこの高度な攻撃のすべてのステップを引き続き認識していたため、チームは有効な対応を取り、さらなる損害を防ぐことができました。

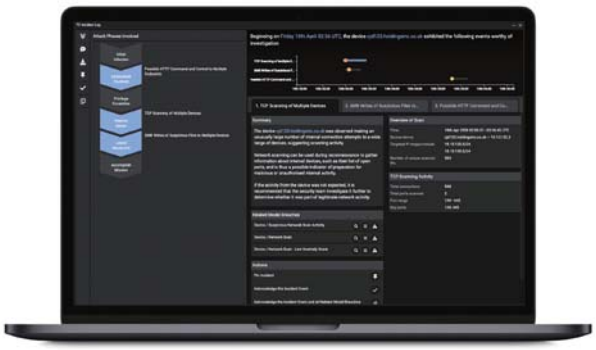

図 6: ランサムウェア攻撃について報告する Cyber AI Analyst の UI 表示例

Enterprise Immune System はこの攻撃のすべての段階を、この会社のコンテキストから見た異常な挙動に基づき、脅威シグネチャの一致に頼ることなく検知しました。

この攻撃のように、長期間に渡って実行され、悪意あるアクティビティの兆候がばらばらに発生するケースでは、脅威の性質と範囲を明確に提示する Cyber AI Analyst はきわめて重要になります。

Cyber AI Analyst のインシデントレポートから、セキュリティチームはランサムウェア攻撃についてのハイレベルな概要と、インシデントのあらゆる段階の詳細な情報のどちらも簡単に読み解くことができます。

The Industrial Immune System:
ランサムウェアから産業用システムを守る

ランサムウェアからの防御に関しては、Industrial Immune System が最新 OT 環境のセキュリティに対する最も強力なソリューションです。特に、ICS 特有の装置を標的とした最初のランサムウェアとして知られる EKANS ランサムウェアのような脅威が存在する状況では、OT 環境に適応し、ゼロデイ攻撃であってもこれらのシステムを保護することのできるセキュリティツールを活用することが死活的に重要です。

また、多くのランサムウェア攻撃は IT インフラの脆弱性を利用して産業用環境を狙います。間接的な侵害もさらなる脅威となります。OT システムが IT を狙った攻撃の巻き添えで被害を受ける可能性があるからです。重要インフラに起こり得る損害を考慮すれば、異質なインフラ全体に渡ってパターンを相関づけることができるセキュリティテクノロジーの必要性はますます切迫しています。

自己学習型 AI により、Industrial Immune System は新種のランサムウェアのような高度な脅威であっても明確に識別することができます。このテクノロジーは、古いタイプの PLC から分散型センサーや産業用 IoT にいたるまで、多種多様なテクノロジーおよび運用形態についての正常な「生活パターン」を学習することが可能です。

さらに、統一されたビューにより、Cyber AI は IT システム内の悪意あるアクティビティと OT システム内の挙動の間の関連性を理解することができ、これまでセキュリティサイロと呼ばれていた分断されたシステム間を移動する脅威を阻止する独自の能力を備えています。

石油製油所でランサムウェアを発見

ある石油元売会社において、Darktrace の Industrial Immune System はコーポレートネットワークに端を発したランサムウェア攻撃の阻止に重要な役割を果たしました。Cyber AI がランサムウェア感染の最初の兆候を特定したのは、ネットワーク上のデスクトップデバイスでした。

Cyber AI がランサムウェア感染の最初の兆候を特定したのは、ネットワーク上のデスクトップデバイスでした。脅迫状ファイルの書き込みに加え、このデバイスは内部プロキシサーバーを使って未知の外部サイトに対する一連の接続を行い、次いで悪意あるファイルと思われるものをダウンロードしていました。これはこの企業の自己についての詳細な知識に基づいて Darktrace が検知して相関づけた情報です。

このデバイスは続いて多数の SMD ディレクトリクエリを実行し始めました。これも Cyber AI がこのデバイスに対する理解に基づいて逸脱と認識したアクティビティです。

Industrial Immune System はこのアクティビティを特定してランサムウェアの可能性が高いと警告したため、この会社のセキュリティチームは感染が OT 環境に拡大する前に気づくことができました。

多様なインフラに渡ってパターンを結び付ける Cyber AI の能力により、このようなマシンスピードの攻撃から産業用制御システムを守ることができました。

図 7: Cyber AI によりランサムウェアに感染したデバイスが特定されたことを示す UI 例