サイバー AI による対応：2019 年世界脅威レポート

はじめに

デジタル時代のビジネスリーダー達は現在、自動化された高速なサイバー脅威という非常に緊迫したリスク要因に直面しています。脅威の高度化とデジタルビジネスの複雑性、多様性、規模の拡大により、これらのリスクはここ数年間で劇的に高まりました。

過去、脅威アクターのレベルが現在ほど高くなく、ネットワークもある程度の予測可能性があったときには、セキュリティに対する従来型のアプローチでも多くの場合、サイバー脅威を十分抑えることができました。セキュリティチームはルールやシグネチャの組み合わせを使ってセキュリティツールを構成し、「良性」または「悪性」をあらかじめ定義しておくことにより脅威を検知しようとしていました。攻撃をルールの形で表現したもの、あるいは実際に観測された攻撃を将来の検知に使えるようにリバースエンジニアリングしたものに頼っていたのです。

ところが、外部からの新種の攻撃や内部関係者からの脅威の頻度が高まり、また日常業務の複雑さと緻密さが増すにつれて、従来型のセキュリティコントロールに依存するチームの防御力は次第に失われていきました。従来型のサイバー防御は、ネットワークの雑音に紛れて大規模かつ複雑なインフラを数秒でスイープできるような洗練されたサイバー犯罪者の最新の戦術やテクニックを検知することができません。

最新の脅威が侵入してくることは避けられないというのが現実です。そこで業界の関心は、サイバーセキュリティ担当者がすでにビジネスの内部に入り込んだ脅威を検知し、それが危機に発展する前に対処できるようにするにはどうすれば良いかという問題に移りつつあります。ビジネスリーダーとセキュリティチームは脅威のペースに後れをとらないために、人工知能の採用に踏み切っています。

Darktrace 独自の AI のアプリケーションは、個々のビジネスの正常な「生活パターン」を学習し、脅威の可能性のあるわずかな逸脱を、既知か未知か、外部か内部か、目立たないものか動きの速いものかに関係なく見つけ出すことができます。「オンザジョブ」で学習し新しい証拠に照らして絶えず適応しつづける Darktrace の人工知能は、ルール、シグネチャ、事前の仮定に頼ることなく、これまで見逃されていたサイバー脅威の早期の兆候を特定します。

概要

本レポートでは Darktrace が遮断し無害化した内部関係者からの脅威、ランサムウェア、IoT 攻撃を含む 7 つのケーススタディを紹介します。

動きが高速なものから低速で目立たないものまで、脅威シナリオはそれぞれ異なりますが、すべてのケースにおいて疑わしい活動のかすかな兆候は、ビジネス環境において何が正常かを学習し攻撃に自動的に対処する Darktrace の AI を使うことによってのみ検知可能であったものです。

Darktrace Antigena による脅威の撃退

攻撃スキルと防御側のギャップが拡がり、攻撃の量と速度が高まる中で、AI は新しい脅威を検知するのに極めて重要であるだけでなく、組織の一次対応を強化するのにも使われています。その AI とはリアルタイムに脅威を撃退できる AI のことで、これによりセキュリティチームは対応のための時間を稼ぐことができます。

あらゆるユーザー、デバイス、およびビジネスにおいて関連するグループの通常の「生活パターン」に対する、詳細かつ変化する理解により、Darktrace の AI はサイバー脅威の早期の兆候に対して損害が発生する前に対応できるだけでなく、それを高度に的を絞った形で実行することができます。画一的な検疫を行うことでさらに大きな混乱を招くことなく、サイバー AI 対応ソリューション Darktrace Antigena は感染したデバイス、または不正を行う従業員に対して通常の「生活パターン」を外科的に強制することにより、数秒で脅威を無害化し、通常の業務を続けられるように設計されています。

高度なサイバー犯罪者との戦いにおいて、Darktrace のサイバー AI は防御する側に主導権を取り戻し、最も複雑かつ脆弱な組織を弾力性のある自己防御型のデジタルビジネスへと変容させるために活用されています。

内部関係者からの脅威

ネットワークをスキャンし脆弱性を探す従業員

悪意があり持続的

内部関係者からの脅威は悪意のあるなしに関わらず、組織において最も危険かつよくある攻撃ベクトルの 1 つです。悪意を持つ内部関係者はビジネスにとって特に大きな脅威となります。彼らの持つアクセス権限とネットワークの知識により、広範囲の攻撃ミッションを遂行し、疑いを招くことなく重要なデータを静かに漏えいさせ、または操作することが可能だからです。

Darktrace の AI はそのような悪意のある内部関係者による攻撃を、南アフリカ共和国の大手投資会社で検知し無害化しました。自己学習型 AI は偵察からスクリプトの記述、そしてスクリプトの実行に至るまで、アタックチェーンに沿って段階的に進行する持続的な脅威を封じ込めることに成功しました。「オンザジョブ」での学習により Antigena は脅威の進化に沿って適応し、各段階で効果的に封じ込めることができたのです。

疑わしい挙動

偵察行動は、1 台のラップトップが数百の内部 IP アドレスを、どれがアクティブか調べるために「プリント」することから始まりました。その後、このラップトップは応答したマシンの名前をネットワーク上で探し、通信に使えるオープンなチャネルがないかスキャンしたのです。Darktrace の AI はこの疑わしい動作を異常なネットワークスキャニング活動としてフラグし、Antigena は即座にアクションをとりました。脅威に対する動的な評価に基づき、Antigena はこのデバイスが属するグループの「生活パターン」を、1 時間にわたり強制的に維持することを決めました。これでこのラップトップは以前の動作またはグループ内のデバイスの動作から逸脱することができなくなりました。

ところが数時間後、脅威は戻ってきました。このラップトップは最初に特定した IP 範囲内にある数百台の社内のコンピュータでコマンドを実行し始めたのです。これには多目的スクリプトファイルの移動や、リモート管理ツールの使用も含まれていました。これらのプログラムは、機密性の情報や文書を探したり、外部の攻撃者が乗っ取りに使用するバックドアを開くために悪用できるものでした。

> Antigena はデバイスグループの「生活パターン」を 1 時間にわたり強制維持することを決めました

Antigena による介入

同じ時間帯に同様のファイル書き込みはネットワーク全体で他に見られなかったため、Darktrace の AI はこれを非常に稀な動作と見なしました。ネットワークおよび以前の自動対応のコンテキストに対応して変化する脅威の理解に基づき、Antigena は SMB ファイル転送チャネルを使ったすべての送信接続をブロックすることを決定し、ネットワーク内のあらゆる水平移動を即座に封じ込めました。

脅威が無害化されると、セキュリティチームによる調査が可能になり、このラップトップが IT チームのメンバーのものであることと、この人物が不正なスキャニングツールを使ってネットワーク内の弱点を探ろうとしていたことを確認しました。これは Darktrace の AI の持つ力と、Antigena がいかに攻撃チェーンのさまざまな段階で介入し持続的な攻撃を早い段階で無害化できるかということを歴然と示す例であると言えます。

ゼロデイのトロイの木馬

疑わしいダウンロードと接続

新種のマルウェア

従来のセキュリティツールでも大抵の場合、発見済みの既知の脅威を特定することは可能ですが、AI はこれまでに全く見たことがない、サイバー脅威の弱い、かすかな前兆をとらえるという特有の能力を持っています。この能力は近年高度なサイバー犯罪者が、過去の攻撃のシグネチャを使って事前定義したセキュリティコントロールを回避するために特に設計された新しい戦術やテクニック、手順などを次々と開発するなかで必要なものとなりました。

このような微細なインジケータに反応する Darktrace の能力は、ゼロデイのトロイの木馬攻撃を受けた米国のある IoT 制御機器メーカーにとって極めて重要なものとなりました。

木曜日の午後 1 時 30 分、Darktrace の AI はこの会社の IT マネージャーに対し、'OfficeActive.bin' という名前のファイルの疑わしいダウンロードがあったことを知らせました。このファイルはマイクロソフトの製品のように見えましたが、Darktrace はこのファイルがネットワークにとって 100% 未知のソースからダウンロードされていることを示していました。

> このファイルはマイクロソフトの製品のように見えましたが、Darktrace はこのファイルが未知のソースからダウンロードされていることを示していました

AI による対応への信頼醸成

Antigena はそのとき、「パッシブモード」に設定されていました。これは導入初期向けのモードで、AI が実際にアクションを取ることはせず、AI ならば脅威にどう対応するかを伝えるだけに制限することにより、セキュリティチームがシステムの意思決定に対する信頼を醸成できるようにするためのものです。IT チームは Antigena が攻撃を早い段階で止めることができたであろうということ、また新種の脅威の進行に Antigena がどう適応していったかを目の当たりにすることができました。

非常に稀な活動のパターンに対し、Antigena はまずこのデバイスが属するグループの「生活パターン」を 2 時間にわたって強制維持することを推奨しました。これにより通常の業務は継続したまま脅威の進行を止められたはずです。

さらに多くの疑わしいダウンロードが観測されると、Antigena は対応をエスカレートし、当該デバイス固有の「生活パターン」を 5 分間強制することを推奨しました。そしてこのデバイスが新たな外部接続を行おうとすると、Antigena は再度これに反応し、AI がこのデバイスからのすべての外部接続を 1 時間にわたって外科的にブロックすることを提案しました。

脅威への対策

警告を認識してから数分のうちに、IT マネージャーはエンドユーザーに連絡し、脅威対策のための緊急対応をこのマシンに対して実施しました。このすべてのプロセスは 20 分以内に完了しました。脅威が無害化された後、IT マネージャーはトロイの木馬の URL とファイル名を Virus Total に入力し、この脅威が他のところで観測され記録されていないか調べました。検索では何も見つからず、この脅威が事実としてゼロデイのトロイの木馬攻撃であり、Darktrace の AI の独自の能力により発見されたことが分かりました。

IoT ハッキング：CCTV

企業スパイ？

侵入を受けたセキュリティカメラ

日常的によく使われる機器がインターネット接続されるようになり、組織にさらなる脆弱性をもたらしています。IoT 機器には多くの場合、統合されていない基本的なセキュリティコントロールが使われており、脅威アクター達に絶えず標的とされ、ネットワークへの侵入経路に使われています。

ある日本の投資顧問会社において、Darktrace はインターネットに接続された CCTV システムが未知の攻撃者に侵入されていることを発見しました。犯人はそこを足掛かりにネットワークに侵入し、カメラのビデオ録画をすべて閲覧できる状態でした。CEO のオフィスから会議室まで、オフィス全体を監視するよう設置されたカメラそれ自体がセキュリティリスクとなってしまったのです。

> AI がマシンスピードで対応したことにより、深刻な漏えいを防ぐことができました

迅速な反応

Darktrace の AI は何かがおかしいことを素早く検知しました。大量のデータが暗号化されていない CCTV サーバーから送受信されていたからです。これは攻撃者が機密情報を盗み出す準備としてデータを収集していたものでした。

攻撃者がデータを取り出そうとした時点で、Antigena は迅速かつ正確な防御のための対応を取りました。システムはデバイスから外部サーバーへのデータ移動を外科的にブロックすることを決め、CCTV は引き続き本来意図された機能を果たすことができました。

AI がマシンスピードで対応したことにより、証券市場の機密情報の深刻な漏洩を防ぐことができました。脅威に見合ったアクションをとり、早い段階で攻撃を封じ込めることにより、Antigena はセキュリティチームに対し、調査を行い損害が発生する前に事態を是正する重要な時間を提供することができたのです。

IoT ハッキング：スマートロッカー

機密性が高い顧客データが標的に

IoT の脆弱性

北米の遊園地で、脅威アクターが脆弱な IoT 機器を介して機密性が高い顧客データを盗み出そうとしました。狙われた IoT 機器は来場者の持ち物を保管する「スマートロッカー」でした。

「スマートロッカー」はそのデフォルト設定の一部として、サプライヤーのサードパーティ製オンラインプラットフォームと定期的に通信していました。脅威アクターはこの自動化プロセスのソースを特定し、これを乗っ取ることでデバイスに侵入しました。

少しずつ時間をかけて行われる攻撃

Darktrace の AI は、このロッカーが普段よりも大量の暗号化されていないデータを未知の外部サイトに送信し始めるとすぐに攻撃を特定しました。これらの接続はデバイスのサプライヤーのプラットフォームとの定期的な通信のタイミングに合わせて行われており、これがルールベースのセキュリティ防御を回避するために特に設計された「ローアンドスロー」型攻撃であることを示唆していました。

このロッカーの以前の挙動および他の機器の動作と比較しながら通信を継続的に分析することにより、Darktrace の AI は AI によるサイバー対応が必要であると判断しました。 数秒のうちに、Darktrace Antigena はアクションを起こし侵入されたデバイスからのすべての送信接続をインテリジェントにブロックし、セキュリティチームが脅威を緩和することでさらなるデータ漏えいを防止するための時間を確保しました。

この遊園地やその他の企業において、Darktrace の AI は数えきれないほどの「ローアンドスロー」型攻撃を早い段階で無害化してきました。「オンザジョブ」での学習により、システムは他のツールでは見逃されてしまうかすかな脅威の兆候を特定します。そして、その理解を新しい証拠に照らして継続的に作り直し、脅威の展開に適応した自動的なアクションを生成します。

ランサムウェア

高速かつ致命的

自動化された恐喝

金曜日の夜7時5分、ある大手通信企業の従業員は会社用スマートフォンで私用メールにアクセスし、騙されて悪意のあるファイルをダウンロードさせられてしまいました。ランサムウェアが含まれていたのです。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を開始しました。

Darktrace の AI は瞬時に反応しました。SMB 暗号化活動が開始してからわずか 9 秒後、Darktrace はこの異常に対して詳細な調査が必要であることを知らせるアラートを生成しました。この動作がその後数秒間継続する間、Darktrace は判定を更新して Antigena を始動させました。

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、Darktrace Antigena は自動的に対応し、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阻止しました。これにより、脅威がこの通信企業の広大なインフラに拡散する前に即座に無害化することができ、セキュリティチームには対策を取るための時間ができました。

自動化されたタイプのランサムウェアが、ダークウェブ上そして世界中の企業ネットワーク内で次々と生まれており、このペースに後れをとらないためには AI による対処が必要とされています。ここでも、Darktrace の AI 対応は極めて重要な戦力となりました。高速な攻撃が重要なデータを暗号化し、ビジネスを停止に追い込む前に封じ込めることに成功したのです。

スピアフィッシング

標的型電子メール攻撃

電子メールによる攻撃

米国のある地方自治体が標的型の電子メールによる攻撃の被害者となりました。フィッシング攻撃の多くは手あたり次第の無差別型作戦ですが、この攻撃は計画的で洗練されたサイバー犯罪の特徴を示していました。それぞれのメールが意図した受信者に合わせて巧妙に作成されていたのです。脅威アクターは市のアドレス帳も所有しているようでした。攻撃メールは受信者に対して A から Z へとアルファベット順に届いていたからです。

それぞれのメールは受信者に合わせた害のない内容に見えましたが、それらすべてには悪意のあるペイロードが含まれ、それらは 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隠されていたのです。

> Antigena はアルファベットの ‘A’ の時点で攻撃を発見しましたが、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

隠されたリンク

Darktrace の AI はこれらの隠されたリンクを、ネットワーク内の受信者の通常の「生活パターン」との関連で分析しました。最初のメールを受信した時点で、すぐに Antigena はこの受信者もその所属するグループの他の人も、そして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認識しました。Antigena は即座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推奨しました。

興味深いことに、Antigena が「パッシブモード」で運用されていたことにより、他のツールでは見逃されてしまう巧妙な攻撃を阻止するこのシステムの能力についての明確かつ具体的な証拠が提示されました。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求めましたが、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 は攻撃を 1 人のユーザーにも到達させることなく無害化していたはずです。

サプライチェーン攻撃

信頼関係を悪用したなりすまし

乗っ取られた電子メールアカウント

今日の抜け目のないサイバー犯罪者の中には、企業に侵入する最も簡単な方法は、しばしば正面玄関からであるということを学んだ者もいます。ただし、それには正当なユーザーの信頼を得なければなりません。信頼のおける同僚、ビジネス上の関係者、サプライチェーン内のベンダーなどのアカウントを乗っ取ることにより、脅威アクターはメール受信者に悪意のあるリンクをクリックさせたり、会社から何百万ドルも送金させることができます。

Darktrace の AI はロサンゼルスにある映画製作スタジオを標的としたこのような攻撃の 1 つを発見しました。それは信頼のおけるサプライヤーの担当者のアカウント情報が盗まれた後でした。

アカウント情報はさまざまな方法で不正利用されますが、このケースでは、犯罪者たちはこの情報を使って映画製作スタジオの従業員とこの担当者との間の過去のやり取りを読んだのです。メールの過去スレッドを読み、この担当者とスタジオの従業員が普段どのようにやり取りしていたかを理解すると、攻撃者は従業員からの最新のメールにもっともらしく返信しました。

> **メールは説得力のあるものでした— 担当者の文体や雰囲気も真似ていたのです**

信じるかどうか

メールは説得力のあるものでした — 担当者の文体や雰囲気も真似ていたのです。そして二人の関係やこれまでのやりとりからしてもっともらしい内容でした。そしてこのメールには、悪意のあるリンクが含まれていましたが、これはよく知っている取引先の担当者からリンクを受け取った常識的な、従業員の誰から見ても害のないものに見えたはずです。この種の攻撃はますます増えており、検知が非常に難しいものです。

Darktrace のサイバー AI は、弱いインジケータを判別してこの「信頼できる連絡先」が攻撃者に乗っ取られたアカウントであることを明らかにしました。AI 対応は、このメールと内容が、送信者とされている人の「生活パターン」から逸脱しているという知識を基にネットワークを分析しました。この従業員には警告が送られ、悪意のあるペイロードは無害化されました。

重要な点は、Antigena の判断が、このリンクが送信者と受信者の両方にとって、彼らの過去の通信や従業員のネットワーク内での通常の「生活パターン」から見て不明であるという事実に基づいていることです。セキュリティチームは、Darktrace の AI がネットワーク内の受信者を単なる電子メールアドレスとして扱っているのではないということを知って、自社のセキュリティ体制に自信を深めることができました。Antigena は 1 人の従業員の「生活パターン」の範囲はネットワーク内のさまざまな場所に現れていることを認識しており、サイバー AI はこれらを相関づけて効果的に分析することができます。

ダークトレースについて

ダークトレースは、サイバーセキュリティ分野で世界をリードする AI 企業です。世界各国において数千社の顧客を擁する Enterprise Immune System は、クラウド、SaaS、企業ネットワーク、IoT、産業用システムで機能する自己学習型プラットフォームにより、内部脅威やランサムウェアなどあらゆる種類のサイバー脅威や脆弱性をリアルタイムに検知・遮断します。従業員数は 800 名を超え、本社は米国サンフランシスコと英国ケンブリッジにあり、東京オフィスを含めて世界に 40 の拠点を置いています。

お問い合わせ

日本: +81 (03) 5456 5537
シンガポール: +65 6804 5010
米国: +1 (415) 229 9100
ヨーロッパ: +44 (0) 1223 394 100
japan@darktrace.com | darktrace.jp
@darktracejp

Darktrace © Copyright 2019 Darktrace Limited. All rights reserved. Darktrace は Darktrace Limited の登録商標です。Enterprise Immune System と Threat Visualizer は Darktrace Limited の商標です。その他本書に含まれる商標は各所有者に帰属します。