deep instinct
BEFORE YOU KNOW IT

net one Partners
ネットワンパートナーズ株式会社

ディープラーニングを使用したマルウェアの分類

2020 年 1 月

エグゼクティブサマリー

サイバーセキュリティ被害の増加とスタッフの専門知識の欠如から、自社のセキュリティの状態について懸念している組織が増え続けています。この結果、多くの組織がサードパーティ製の脅威情報ソリューションを採用していますが、その大半はリアルタイムで実行されず、人の関与と追加の費用を必要とします。

さらに、どの脅威が危険なのかを完全に理解するには、SOC (セキュリティオペレーションセンター) および IR (インシデントレスポンス) チームが脅威の深刻度を評価する必要がありますが、これには、時間、リソース、および費用がかかります。

つまり、人の介入を最小限に抑えながら、人工知能、より具体的に言うのであれば、ディープラーニングを利用して、リアルタイムでこのようなサイバー攻撃に対処する必要性が増え続けているのです。

このホワイトペーパーの内容:

- ディープラーニングがサイバーセキュリティにどのように実装されているか
- ゼロデイマルウェアをリアルタイムで分類することが重要な理由
- ディープラーニングを使用してマルウェアのタイプを分類する方法
- マルウェア分類の結果

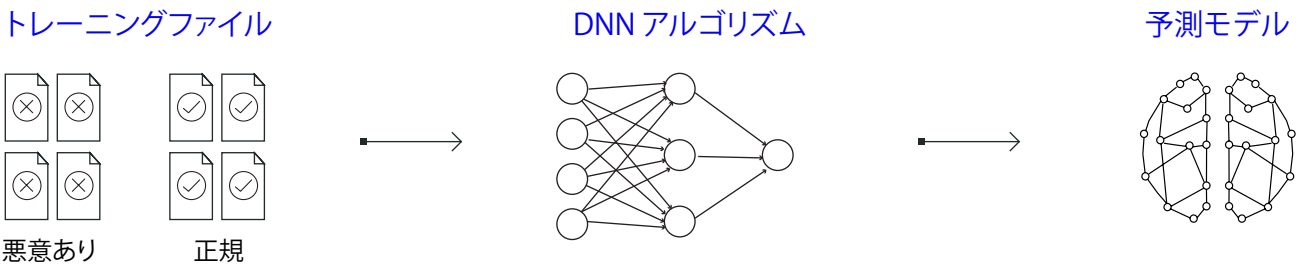
背景

人工知能の一形態であるディープラーニングは、脳の学習能力から発想を得ています。人間の脳はある物体を識別することを学習すると、それを元に予測ができるようになります。 現在、複雑なニューラルネットワークから構成されるディープラーニングの人工頭脳は、大量のデータを処理することにより、解析対象のデータについての深く、きわめて正確な特徴を捉えることができます。 このことから、 音声と画像の認識や自律走行車、 そして健康診断についても、 ディープラーニングが推奨されます。

同様に、ディープラーニングはサイバーセキュリティにもまったく新しいアプローチをもたらします。サイバーインテリジェンスの人工頭脳は、あらゆるタイプのサイバー脅威を識別することを学習し、ゼロデイ攻撃と APT 攻撃を比類のない精度で、 ゼロタイムで検知し、 予防することができます。

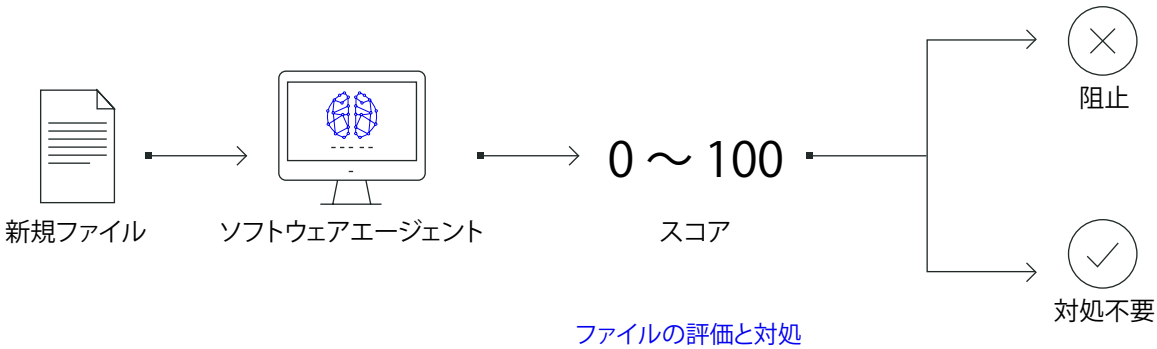
しくみ

人工頭脳は、ディープラーニングとも呼ばれる、ディープニューラルネットワーク (DNN) アルゴリズムを使用して、数億個の悪性ファイルおよび良性ファイルでトレーニングされます。このトレーニングの成果である予測モデルが、各エンドポイント、サーバー、およびモバイルデバイス上のソフトウェアエージェントに配布されます。このモジュールは、 サードパーティ向けの OEM エンジンとしても提供可能です。



ディープラーニングトレーニング

モジュールの配布後、デバイスへのアクセスを試みるすべての新規ファイルはモデルによりスキャンされ、スコアが付けられます。これはすべて数ミリ秒内で実行されます。スコアは悪性ファイルへの合致レベルを表します。その後、事前に定義されているポリシーのしきい値に基づいて、ソフトウェアエージェントによりファイルをブロックして阻止すべきか、 実行を許可すべきかが判断されます。



ファイルの評価と対処

ディープラーニングは、悪意のあるファイルの実行を予防するために使用できるだけでなく、どのタイプのマルウェアが組織を標的としているかをリアルタイムで分類することにより、 脅威情報も提供できます。

課題

ゼロデイマルウェアファイルをリアルタイムで分類することが重要な理由

1 知識と洞察

現在、多数の組織では、スタッフのリソースと専門知識が限られているために、一般的にリアルタイムでは実行されない脅威情報サービスを使用しています。このようなサービスは、特定のマルウェアについての詳細な情報を取得するために、サードパーティのインテリジェンス企業によって提供されています。また、これらのサービスでは、場合によっては人の介入や、別のエンティティにファイルをアップロードして追加の解析やその他の評価を行う必要がありますが、これには数日かかることもあります。しかし、その間、攻撃は組織のデバイスやネットワーク上ですでに実行されているかもしれません。マルウェアのタイプを知ることで、攻撃についての洞察をすばやく得ることができます。これは、ランサムウェアなどの金銭目的の攻撃や、バックドアやスパイウェアなどのデータ窃盗の場合には不可欠です。さらに、他の情報との相関により、組織全体に与える可能性のある影響について、より理解することができます。

2 迅速な対応

SOC および IR チームができるだけ早く適切な対策を取るためには、今何に取り組んでいるのかを理解する必要があります。その対策により、環境のセキュリティを担保できなければなりません。同時に、ユーザーの生産性にも影響を与える可能性があるため、脅威の深刻度に基づいた評価も必要です。脅威の深刻度をすばやく把握する能力がない組織は、たとえば悪意のあるファイルをアンインストールすることによりリモートから脅威を修正するだけで十分な場合でも、対象のデバイスの物理的調査を (そしてこれらのすべてのデバイスでのイメージの再適用までも) 行う羽目になる可能性があります。

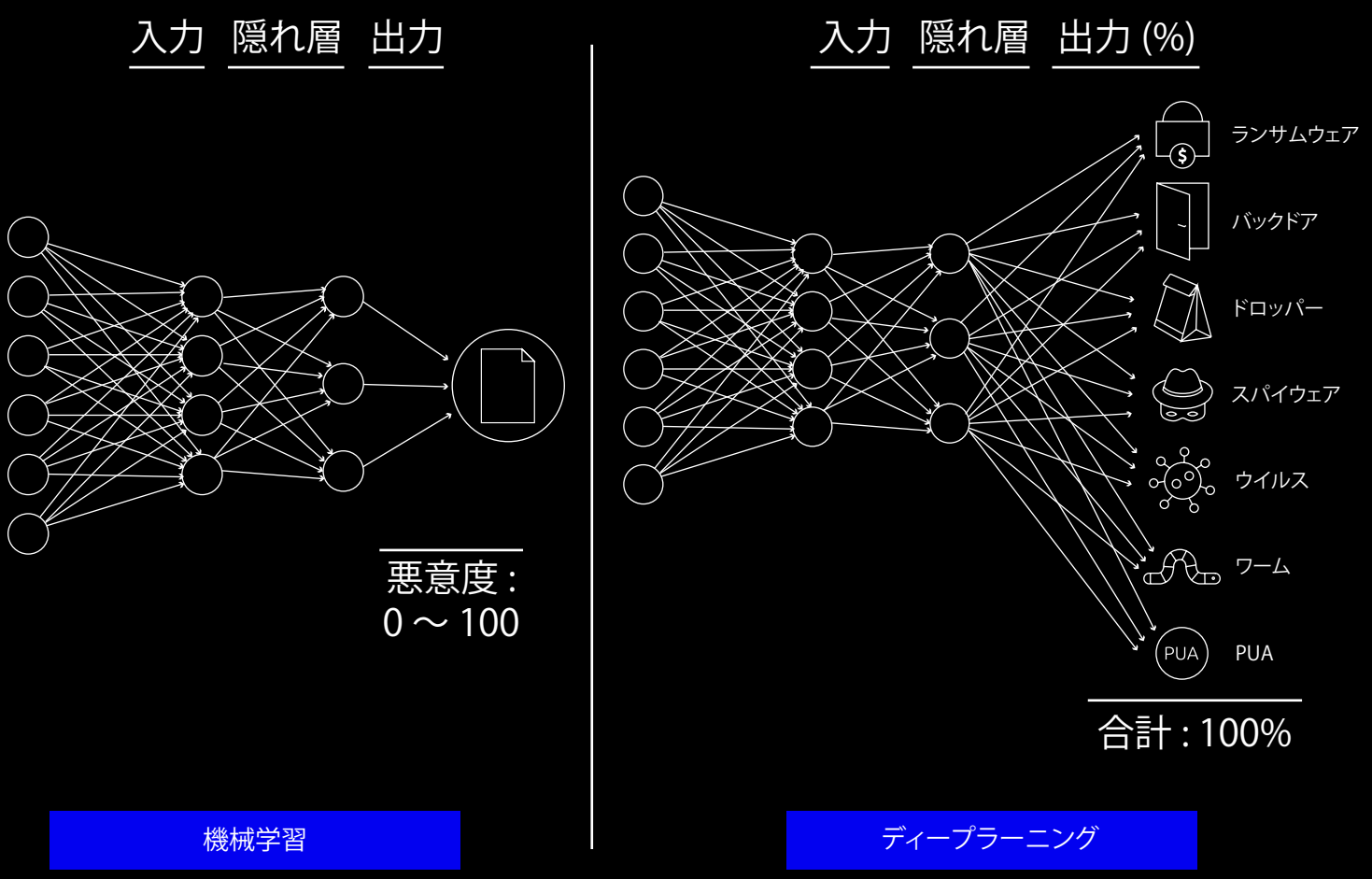
3 自動化された運用が可能

マルウェアタイプを分類できる能力があれば、セキュリティ管理者は、ファイルの悪意度とマルウェアタイプの両方に基づいて対策を講じることによって、より細かいポリシールールを設定することができます。2 番目の理由でも述べたように、セキュリティの実施とユーザーの生産性は相反します。セキュリティポリシーの制限が厳しいほどユーザーの生産性が影響を受ける可能性が高くなり、その逆もまた同様です。したがって、マルウェアタイプをリアルタイムで分類することにより、組織は悪意があると判定されたすべてのファイルをただちにブロックするのか、または実際に侵略的なマルウェアファミリーのみをブロックし、その他のファイルの実行は許可して、後で SOC と IR チームに対処してもらうのかを選択することが可能になります。たとえば、悪意があると判定されたファイルについては、セキュリティ管理者はブロックするようにポリシーを設定しながら、PUA については許可をしたり、また検知したファイルに対してもランサムウェアやスパイウェアとして分類されたファイルだけはブロックしたままにするなどのルールを適用できます。

解決策

ディープラーニングを使用したマルウェアの分類により即時に脅威情報を取得

一般的な標準のネットワークでは 1 つの出力しか得られないのに対し、ディープニューラルネットワーク (DNN) の出力層では複数の出力が得られます。したがって、各出力が 1 つのマルウェアファミリータイプを表すような、マルウェアタイプの分類にも使用することができます。各出力は、ファミリー特性を表すパーセンテージとともに表示され、すべての出力の合計が重み 100 になります。



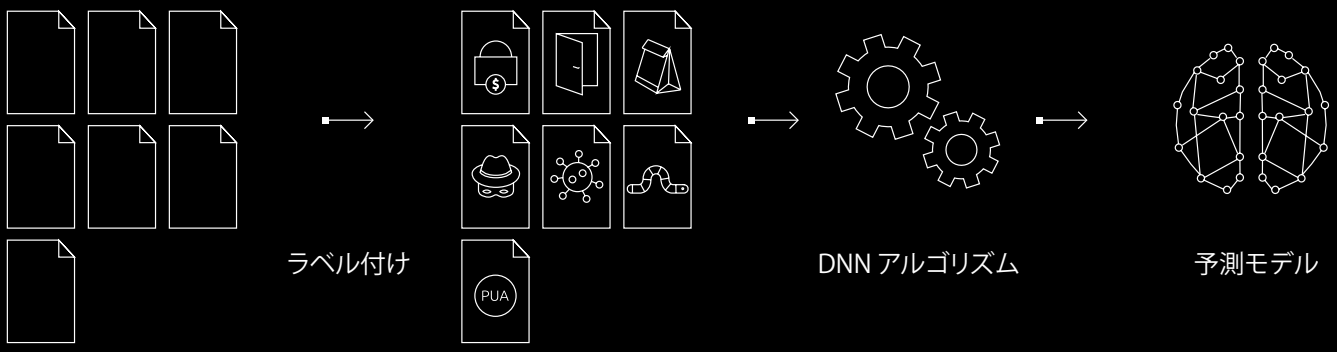
機械学習

ディープラーニング

複数の出力を持つ DNN のトレーニング方法

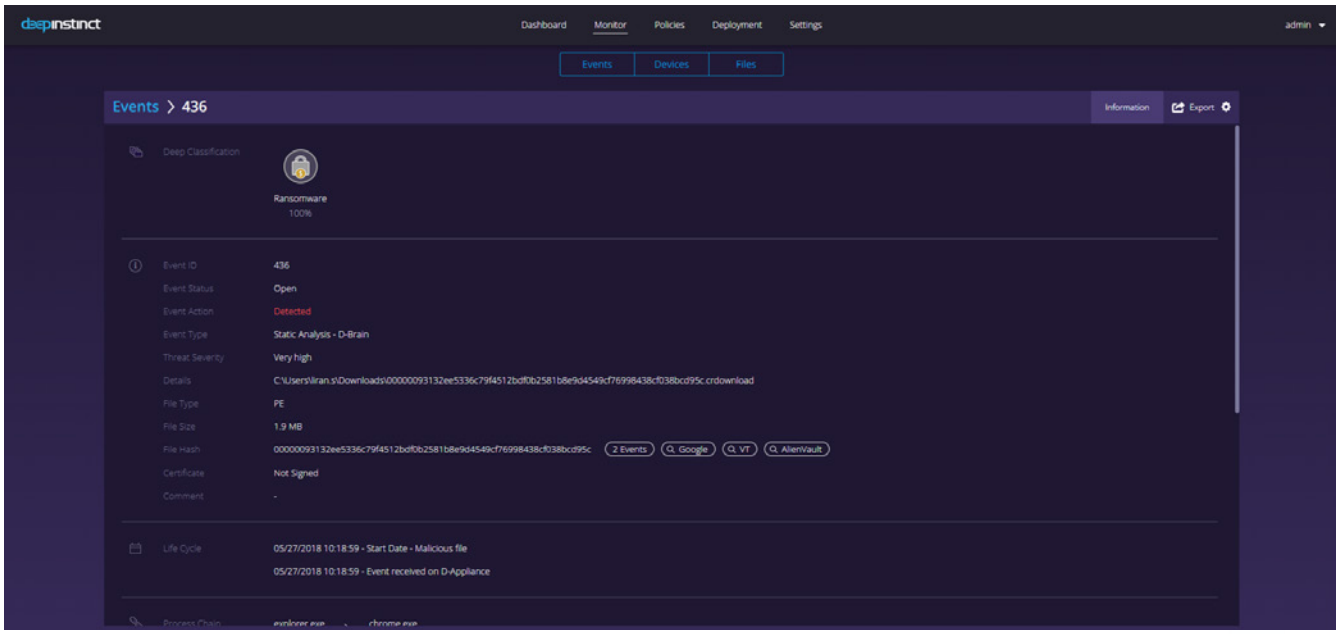
1. ラベル付け - 数百万個のマルウェアサンプルに対して、マルウェアタイプに応じて適切にラベル付けします。

2. 入力とトレーニング - ラベル付けされたサンプルがディープラーニングアルゴリズムに入力され、このアルゴリズムにより、特定されたパターンに基づいて、各マルウェアタイプが持つ特性が学習されます。このトレーニングの結果が、軽量の予測モデルです。



マルウェア分類トレーニング

Deep Instinct には、DNN に基づく新たな分類モデルが統合されています。このモデルは軽量であり、メモリ消費量は 30 MB 未満です。マルウェアとして検知されたファイルは、分類モデルにより再度スキャンされ、人の関与なしに、数ミリ秒でマルウェア種別を分類して、その結果を得ることができます。この分類モデルは、次の 7 つのマルウェアファミリータイプの分類が可能です : ランサムウェア、バックドア、ドロッパー、スパイウェア、ウイルス、ワーム、PUA (Potential Unwanted Application: 望ましくない可能性のあるアプリケーション)。Deep Instinct 管理コンソールのスクリーンショットである以下の図は、ランサムウェアの特性しかないマルウェアサンプルの分類結果を示しています。



Deep Instinct 管理コンソールのイベント詳細ページ

将来的には、セキュリティ管理者は、悪意度と分類されたファミリータイプの組み合わせに基づいて自動実行可能なルールを設定できる Deep Instinct ポリシーを定義できるようになります。

Deep Instinct について

Deep Instinct は、サイバーセキュリティにエンドツーエンドのディープラーニングを適用した初めての企業であり、唯一の企業です。攻撃を待ってから対処する検知と対応ベースのソリューションと異なり、Deep Instinct のソリューションは先制して動作します。予防的アプローチにより、ファイルやベクトルは実行前に自動的に解析され、お客様はゼロタイムで保護されます。これは、リアルタイムでは遅すぎる脅威ランドスケープでは不可欠です。

Deep Instinct は企業のサイバー脅威を根絶することを目的とし、SE Labs による試験で 100% の検知率と誤検知ゼロを達成するという比類のない精度で、最も捉えづらい既知および未知のマルウェア攻撃を防御します。エンドポイント、ネットワーク、サーバー、およびモバイルデバイスに保護を提供するこの軽量ソリューションは、ほとんどの OS とあらゆるファイルタイプに適用可能です。

Deep Instinct では、主要な MSSP や、HP、Tech Data などのフォーチュン 500 企業のお客様の保護にとどまらず、新たなパートナシップを日々構築し、拡張しています。当社を率いているのは、ディープラーニングの科学者や IDF のインテリジェンスサイバー部門の元メンバーから構成される経験豊富な学際的チームです。

デモを依頼

net one Partners
ネットワンパートナーズ株式会社

ネットワンパートナーズ株式会社
https://www.netone-pa.co.jp/
本 社 〒100-7026 東京都千代田区丸の内 2-7-2 JP タワー TEL 03-6256-0700（代表）
西日本営業部 〒532-0003 大阪府大阪市淀川区宮原 3-5-36 新大阪トラストタワー TEL 06-6105-0356（代表）

deepinstinct
BEFORE YOU KNOW IT
www.deepinstinct.com/ja/