SOPHOS
Security made simple.

ソフォスが実現するサイバーセキュリティ向けの効果的な機械学習

長い間、サイバーセキュリティは防御側よりも攻撃側が圧倒的に優位であると考えられてきました。「防御側は毎回的を射なければならないが、攻撃側は一度的中させるだけでよい」と言われることにも表れています。これまでは先んじてきた防御側も、攻撃の波に追い上げられています。形勢を逆転させるうえで役立つと考えられるのが、最近進歩を遂げている機械学習です。

ソフォスは、2017 年 2 月に機械学習によるセキュリティソリューションを提供する Invincea 社を買収して以来、同社のテクノロジーと専門知識を SophosLabs とソフォス製品に統合してきました。その過程で、機械学習、特にディープラーニングについて仕組みを明らかにし、これがどのようにソフォス製品に統合され、お客様の保護に役立つかについて、ソフォスの複数のデータサイエンティストが記事を執筆しています。

この統合がほぼ完了した今、現状を考察し、今後を展望する段階を迎えています。

これまで、セキュリティ業界は秘密主義と専門用語で機械学習をけむに巻く。しかし、ソフォスは透明性、説明、情報提供を重視しています。

このガイドでは、ソフォスが一年間公開してきた機械学習についての記事をまとめてご紹介します。

関連記事はさらにあります。どうぞお役立てください。

ソフォス CTO、Joe Levy

機械学習の重要性

ソフォスが Invincea を買収した当初、それがお客様にとってどのような意味を持つのかについて説明を提供することが求められました。当時ソフォスが発表したメッセージはこちら (英語) です。

この後、ソフォスは RSA Conference 2017 でもこのメッセージについて説明しています。

RSA Conference 2017 からのレポート：マルウェア対策での機械学習の活用 (英語)

ソフォスの製品管理ディレクター、Russell Humphries は、マルウェアとの戦いが機械学習によってどのように変わるのかについて述べています。

機械学習の仕組み

次に、機械学習がどのように機能し、これをどのように応用できるかについて、できるだけ詳細に説明しました。

従来の機械学習からの目覚ましい躍進 (英語)

機械学習は、すでに多くのセキュリティベンダーが使用しています。では、ソフォスのディープラーニングのアプローチはどのような点で異なり、またどれだけ優れたものなのでしょうか。

機械学習についての 5 つの質問 (英語)

機械学習は、何も理解せずに製品に追加して魔法のように効くわけではありません。機械学習の基本と課題を検討し、アプローチを吟味する必要があります。

ディープラーニングの解明：ソフォスによる機械学習モデルの構築方法 (英語)

ディープラーニングモデルの開発に向けてソフォスが採用しているプロセスの概要について紹介しています。

機械学習の潜在的リスク

さらに、目的に合わせて機械学習を機能させるためには適切な専門知識が必要です。Black Hat USA 2017 および BSidesLV では、ソフォスのデータサイエンティストが機械学習のリスクについて述べました。また、Naked Security でも紹介しています。

機械学習：ダメなデータからはダメな結果しか生まれない

機械学習に関して注意すべきなのは、マルウェアを非常に正確かつ効率的に根絶するためには適切なデータセットを使用しなければならないという点です。しかし、機械学習の処理対象はモデルです。不確かな偏ったデータを投入しても、もたらされるのは役に立たない結果でしかありません。このことについて、ソフォスのデータサイエンティスト、Hillary Sanders は「だめなデータはだめな結果しか生まない：優れているはずの機械学習がだめなデータで台無しに」というテーマで説明しています。

機械学習のセキュリティ上の課題とは

あらゆる善意の技術的進歩について言えることですが、機械学習アルゴリズムも悪意による利用が可能です。ソフォスのチーフデータサイエンティスト、Joshua Saxe は、このような悪用に対する警告を概説し、ソフォスの防御について説明しています。

マシンベースのマルウェア分析を向上させるツール「LIME」

ソフォスの主席データサイエンティスト、Richard Harang は、機械学習からもたらされる結果の精度を高めるうえで効果的な LIME (Local Interpretable Model-Agnostic Explanations) について説明しています。

真実の定義：機械学習における不確かなラベルの克服 (英語)

機械学習をサイバーセキュリティに応用するうえでは、不確かなラベルの問題を解決する必要があります。この障害を克服するためにソフォスが採用している方策を紹介します。

人類滅亡の危機？

さらにソフォスは、「機械学習および人工知能全般が進歩しすぎると、いずれ人間に牙を剥けることになるのではないか」という、科学分野とハリウッド映画の両方で取り上げられている疑問にも向き合いました。

人間対機械：人工と生物のニューラルネットワークを比較 (英語)

生物の学習と人工知能を比較・対比させることで、より安全なインフラストラクチャの構築が可能になります。

人工知能が将来スカイネット化しない理由 (英語)

映画『ターミネーター』では、スカイネットという高度なコンピュータが人類の敵として描かれています。しかし、機械学習はあくまでも強力なツールであり、私たち人間の存在を脅かすものではありません。

今後も多くの記事を公開予定ですので、このガイドも随時更新していきます。

ソフォス株式会社営業部
Tel: 03-3568-7550
Email: sales@sophos.co.jp

2017-10-25 (NP)