SOPHOS
Security made simple.

Intercept X のディープラーニング

Intercept X は、ディープラーニングと、ベストインクラスのエクスプロイト対策、CyptoGuard ランサムウェア対策、根本原因解析などの機能を統合することにより、業界で最も包括的なエンドポイント保護を実現します。ソフォスならではの機能を結集した Intercept X は、エンドポイントに対するさまざまな種類の脅威を阻止できます。

主な特長

- 業界トップのパフォーマンスを誇るマルウェア検出エンジン
- 既知と未知のマルウェアを阻止
- マルウェアの動作を未然にブロック
- シグネチャのみに依存しない
- オフライン状態のホストも保護
- およそ 20 ミリ秒でマルウェアを検出
- 数億件のサンプルを使って学習
- 2016 年 8 月から VirusTotal で実証済み
- 有害ファイル、不要と思われるアプリケーション（PUA）、無害ファイルに分類
- すぐに使用開始でき、トレーニングは不要
- 最小限のメモリフットプリント（20 MB 未満）
- Windows PE (Portable Executable) を重点的に保護

今日のセキュリティソリューションの多くはリアクティブ（事後対策）であり、その処理もあまりに低速です。巧妙なエンドポイント攻撃が急増している今、従来のアプローチではとても太刀打ちできません。たとえば、SophosLabs が新たに解析するマルウェアサンプルの数は、1 日あたり 40 万件を超えています。その 75% は特定の組織を標的にしたマルウェアが占めているため、対策はますます難しくなっています。

ディープラーニングは、機械学習の高度な手法の 1 つです。エンドポイントセキュリティのアプローチに変革をもたらしつつあり、Intercept X はその先端を行くソリューションとなっています。ディープラーニングが統合された Intercept X は、エンドポイントセキュリティを事後的なアプローチから予測的なアプローチへと転換し、未知の脅威に対抗します。

ディープラーニングと、他の機械学習モデルの相違点

「Intercept X は、人間の脳に似た仕組みを持つディープラーニングニューラルネットワークを使用します。その結果、既知のマルウェアとゼロデイ攻撃の両方を高い精度で検知でき、誤検知率の低減に成功しています」

ESG Lab Report (2017 年 12 月)

機械学習を採用した製品が多数登場していますが、機械学習にはさまざまなタイプが存在し、どれも同じというわけではありません。ソフォスは、マルウェアの検出にディープラーニングを活用しています。ディープラーニングは、「ディープラーニングニューラルネットワーク」や「神経回路網」と呼ばれるように、人間の脳の仕組みからヒントを得て開発された技術です。これと同じタイプの機械学習には、顔認識、自然言語処理、自動運転などがあり、高度なコンピュータサイエンスおよび調査研究分野で活用されています。

機械学習には、ランダムフォレスト、K-meansクラスタリング、ベイジアンネットワークなど、さまざまなモデルが存在します。その中でもディープラーニングのパフォーマンスは群を抜いていますが、有効なモデルの作成には膨大な量のデータと高度な計算処理能力が必要になるという難点もあります。ソフォスは、有効なモデルをシンプルな方法で構築するために、SophosLabs が過去 30 年以上にわたって蓄積してきたマルウェアおよび解析データと、1 億を超えるエンドポイントから日々収集するテレメトリを活用しています。

エンドポイントセキュリティで一般的に使用されている他の機械学習モデルに比べて、ディープラーニングには次のような優位性があります。

スマートな機能：ディープラーニングモデルは、脳の神経細胞のような複数の階層で分析を行います。これによってモデルの強度が大幅に向上し、さまざまな入力特徴量の間に存在する複雑な関係を解析します。また、最適な入力の組み合わせと操作を自動的に見つけ出すことができ、人間の認識能力では不可能な処理を可能にします。このようなディープラーニングを活用したソフォスのマルウェア検出モデルは、他の機械学習エンジンでは検知できないマルウェアも検出できます。

優れた拡張性：ディープラーニングは、何億ものサンプルのトレーニングにも対応できる拡張性を備えています。この拡張性は、毎週 280 万件ものマルウェアサンプルを新たに解析する SophosLabs において、重要な役割を果たしています。まず、大量のトレーニングデータを継続して取り込むことで、目に見える脅威全体をモデルに「記憶」させることが可能になります。また、膨大な入力データを処理できるので、脅威予測の精度が上がるだけでなく、常に最新の状態を維持できます。

動作が軽い：これまでの機械学習では、モデルのサイズが巨大になることが多く、何ギガバイトにも達するモデルも存在します。ソフォスのディープラーニングでは、モデルのサイズを大幅に圧縮しています。20 MB 未満という極めて小さいサイズなので、エンドポイントのパフォーマンスに影響を与えることはありません。

ソフォスのディープラーニング機能

ソフォスは、ディープラーニングに関する豊富な知識をもとに、業界トップクラスの性能を誇るマルウェア検知エンジンを提供しています。

豊富な経験：ソフォスは、サイバーセキュリティ分野の機械学習に長年取り組んできたエキスパートであり、競合他社と一線を画しています。また、ディープラーニングを活用したマルウェア検知モデルについても、何年にもわたる導入実績を持っています。ソフォスのマルウェア検知モデルは、DARPA のテクノロジーをベースに、ソフォスのデータサイエンティストチームによって開発されました。2010 年、米国防高等研究計画局 (DARPA) がマルウェアをはじめとするサイバー攻撃の「DNA」解明を目的に行った Cyber Genome プログラムで開発されたモデルが、現在 Intercept X に組み込まれているアルゴリズムの原型です。

実証済み：ソフォスのモデルの特長は、オープン性と透明性です。Black Hat などのセキュリティカンファレンスにおいて独自の手法を開示するだけでなく、独立系サードパーティによるテストにも積極的に参加しています。ソフォスのモデルは、2016 年 8 月に VirusTotal において実証されており、NSS Labs などのサードパーティテスト組織から高い評価を得ています。いずれのテストにおいても、抜群の効果と低い誤検知率を両立している点が実証されています。

「過去最高スコアを獲得したソリューションの1つ」

Maik Morgenstern氏、AV-TESTのCTO

パフォーマンス：ソフォスのディープラーニングテクノロジーは、極めて高速です。ファイルから数百万の特徴量の抽出、深層分析の実行、有害かどうかの判別という一連の処理を 20 ミリ秒以下で実行します。しかも、この処理はすべてファイルの実行前に完了します。

SophosLabs：どの機械学習モデルにおいても、トレーニング用の学習データが非常に重要な役割を果たします。ソフォスのデータサイエンティストチームは、SophosLabsに数億のサンプルへのアクセスを提供し、最適なモデルの開発を支援しています。この 2 つのグループのコラボレーションは、データラベリングの精度向上（さらには、モデリングの品質向上）にも貢献しています。データサイエンティストと脅威研究者のチームが相互に脅威インテリジェンスを共有しフィードバックを行うことで、モデルの精度が継続的に向上しています。

「Intercept X は、複雑で巧妙な攻撃を次々にブロックした」

ESG Lab Report（2017年12月）

無償評価版

無償評価版の登録 (30日間)
sophos.com/interceptx

ソフォス株式会社
partnersales@sophos.co.jp
03-3568-7550

18-01-02 DS NA (2897-DD)