掲載日時： 2020-06-05 06:30

サイバーセキュリティにおけるAI活用の最先端

人工知能は隠れたパターンや高度な攻撃を駆使する脅威を発見することは得意だが、まだ人間が不要な状況にはなっていない。

著者 : Allen Bernard （Special to ZDNet.com） 翻訳校正： 石橋啓一郎

URL : https://japan.zdnet.com/article/35152705/

脅威の数は毎日増えているが、セキュリティツールや人間のセキュリティチームの能力はそのペースについていけず、マルウェアの大波に飲み込まれそうになっている。

Capgeminiのレポート「2019 Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security」によれば、調査に回答したサイバーセキュリティアナリストの56%は攻撃の頻度の増加と高度化についていけてないと答えている。また、23%は組織に影響を与えるすべてのインシデントを適切に調査することはできていないと述べており、42%は自動車や航空機の制御システムなどの「応答時間が重要な」アプリケーションに対する攻撃が増加していると回答していた。

レポートでは「ハッカーがリモートから窃盗を行ったり、被害を与えたりする能力を持つインターネット時代には、被害を与えようとする者から資産や業務を守ることはこれまでにないほど困難になっている」と述べている。「その数は驚くほど多い。Ciscoは、2018年中に同社だけで顧客を標的とした脅威を7兆件ブロックしたと述べている。これほど脅威が増え続けている状況では、組織には支援が必要になる。一部の組織はAI（人工知能）について検討しているが、これは（今のところは）完全に問題を解決するためではなく、守りを強化するためだ」

AIと機械学習は、以前から、無数にあるサイバーセキュリティツールやセキュリティプラットフォームが発生させるノイズを減らすために使われてきているが、一見したところでは、最先端のAIでも、基本的なものに見える機能からそれほど大きく進歩しているようには見受けられない。これらの技術は、今でも誤検知の削減や、不要なアラートのフィルタリングなどをはじめとする、サイバーセキュリティチームがもたらす効果の妨げとなるものを減らすことに焦点を当てている。

Forrester Researchのセキュリティ&リスク担当バイスプレジデント兼主席アナリストChase Cunningham氏は、「まだその水準に達していない段階であるにも関わらず、人々がAIとサイバーセキュリティについて話しているのは少々皮肉だ」と述べている。「AIは大量のデータを分析して、どのような異常があるかを調べ、その異常に対してどのような対応を取ったらいいかを提案することを得意としている。全体として見みれば、それが一番重要なことだ」

IDCのセキュリティ&トラスト担当プログラムバイスプレジデントFrank Dickson氏は、この10年ほどで一番変わったのは、一見単純そうに見えるこの作業が膨大な量になったことだと話す。

「この作業の複雑さは過小評価されている」とDickson氏は言う。「何か特定のインフラストラクチャーを思い浮かべてもらいたい。そのインフラには1000万くらいのエンドポイントがあっても不思議ではない。アプリケーションも数千種類に及び、SaaS、PaaS、IaaSなどのさまざまな環境が入り交じっていることも珍しくない。あらゆる場所にIoT（モノのインターネット）デバイスが散らばっている。また、受託業者がやってきて、自分が管理しているネットワーク上で作業をすることもある。それに加えて、事業部門の人々が、自分がよく知らない新しいサービスを立ち上げる。とにかく恐ろしく複雑であり、目の前にあるその作業をやらなければならない」

毎日100万種類の新しいマルウェアサンプルが生まれている

Symantec（Broadcomが2019年8月にSymantecのエンタープライズ向けセキュリティ事業の買収を発表し、1月にはAccentureがBroadcomから買収すると発表している）のフェローであるEric Chien氏によれば、毎日100万種類もの新しいマルウェアサンプルが生まれているという。人間がそれだけの数の悪質なコードを分析して、自分の組織にリスクがあるかどうかを評価することは不可能だ。しかし幸いなことに、今日のAIはこれを得意としている。AIは、これらの脅威のほとんどを検出し、止めるのを支援できる。これは、その多くが既存のマルウェアから派生したものであるためだ。

これによって、人間のアナリストが残るわずかなマルウェアに集中する余裕を作ることができる。これらはまったく新しいもので、非常に大きなダメージを与えるものであったり、より大規模で、あまり目立たず、混乱を引き起こす多層的な攻撃の一部であったり、高度に標的を絞った攻撃であったり、それらすべての要素の組み合わせであったりする可能性がある。

「本当の進歩は、最後に残った隙間をどう見つけるかにある」とChien氏は言う。「この最後に残った隙間は、非常に影響が大きい脅威である傾向がある。つまり、非常に大きなダメージを与えるものだ」

サイバーセキュリティにAIが有効な3つの応用例

Chien氏は、サイバーリスク管理市場に入ってきている最新のAI製品には、主に3つの高度な応用例があると述べている。

1つ目は、機器やアプリケーションの振る舞いの分析に機械学習を適用し、通常の振る舞いと比べて疑わしい振る舞いのパターンを検出して、人間が分析できるようにフラグを付けるというものだ。この仕組みは一般に、UEBA（ユーザーおよびエンティティの振る舞い分析）と呼ばれている。

「こうした他の種類の属性を持ち込む際には、例えばファイルの性質などだけではなく、このマシンは午後5時、朝9時、夜中の12時にどんな振る舞いをしているかということも考慮に入れる」とChien氏は言う。「その種の振る舞いに関する属性を多く取り込むのが最新のやり方だ」

2番目の応用例は、AI技術を使ってネットワーク全体を監視し、高度で持続的な標的型攻撃（APT攻撃）を見つけることだ。攻撃を準備している攻撃者は、事前にネットワーク内に潜伏し、ユーザーの行動を探ったり、脆弱性を探したりすることが多い。攻撃者はネットワーク内を動き回り、認証情報を盗んで特権を昇格しようとするが、一般に、それらの行動を総合的に見ていくと、侵入者の存在を示す活動のパターンが見えてくる。

「私たちは標的型攻撃分析と呼ばれる手法を持っている。これは基本的に、それらすべての制御ポイントの相互関係を示すことのできる機械学習を使用したものだ」とChien氏は言う。「この仕組みは、環境内で何か不審なことが起こっているときには、それを見分けることができる。1つ1つは、このマシンで疑わしい行動がある、こちらで少しおかしな行動がある、といった内容だが、それが広範にみられる。この手法は、環境の中で何かが起こっており調査が必要だと知らせるだけだ」

3つ目の応用例は、Symantecが「適応型セキュリティ」と呼んでいるものだ。同じ組織は2つとないためサイバーセキュリティに対するニーズやサイバーセキュリティ戦略も組織によって異なっているのが普通だ。

「もし私が100%（のセキュリティ）を求めているなら、自分が関わっているすべての環境に適応する必要がある」とChen氏は言う。「実際、私たちが機械学習を使用し始めているのは、私たちが置かれている環境について学習して理解し、その環境やマシンやユーザーだけに特化した自己学習モデルを導入するためだ」

よくある例は、AIを使って、内容に「機密」という言葉が含まれているすべての文書にフラグをつけて報告させることだろう。このやり方は、あまり多くの機密情報を扱っていない組織ではうまくいくかもしれない。しかし政府機関では、その種の文書は珍しくないため、AIでそれらの文書すべてに「疑わしい」というフラグを付けても意味がない。この種のAIは、それらの文書の動きを検知しても、警告を出さないことを学ぶだろう。

しかし、その逆のこともできるかもしれない。組織が突然多くの「機密」文書を作成し始めた場合に、AIが環境の変化に適応できるように用意された機械学習アルゴリズムが、変化が起こっていることをつかんで、ネットワーク内の機密文書の動きを「疑わしい」とフラグ付けしないようにさせることも可能だ。

AIが近い将来にマルウェアの脅威をなくしてくれると期待する人もいるが、それはまだかなり先のことになるだろう。これは、攻撃者側もマルウェアの開発にAIを導入しており、軍拡競争の様相を呈しているためだ。

幸い、AIは守り手がその一歩先を行くのに役立っている。その一方で、攻撃者側は、未知の脆弱性を悪用する手段や、パッチが適用されていないサーバーが1つあればよく、ネットワーク上にある無数のエンドポイントの中で、感染させられるものを1つ見つければ済む。あるいは、簡単にだ

まされて感染した文書をダウンロードしてしまったり、あるいはフィッシング詐欺に引っかかって認証情報を渡してしまったりする従業員が1人いれば、最高の防御も簡単に破られてしまう。

「私は、あるCISO（最高情報セキュリティ責任者）から、『機械学習はPythonで書かれているが、AIはPowerPointに書かれているだけだ』と言われたことがある。これは、機械学習はパターン認識を得意といるため、非常に成熟した科学になっているが、AIは現時点では概念的なものでしかないということだ。AIは既知のパターンを利用し、既知のポリシーに基づいて動作する。しかし自己学習機能や自己回復機能については、現時点では、まだ難しいことが多いと言わざるを得ない」（Chien氏）

この記事は海外CBS Interactive発の記事を朝日インタラクティブが日本向けに編集したものです。
