News Release

2016 年 8 月 1 日

「WideAngle」のマネージドセキュリティサービス運用基盤に
搭載した人工知能を拡充し、サイバー攻撃分析ロジックを大幅強化
～機械学習により、未知の脅威を検知～

NTT コミュニケーションズ株式会社(略称：NTT Com)は、総合リスクマネジメントサービス「WideAngle」のマネージドセキュリティサービス（MSS）において、2015 年 10 月に搭載した人工知能によるサイバー攻撃の検知能力を更に強化し、標的型サイバー攻撃や Web サイトへの攻撃などにおける未知の攻撃手法も検知できる独自開発のロジックを 2016 年 8 月から順次導入します。

1.背景

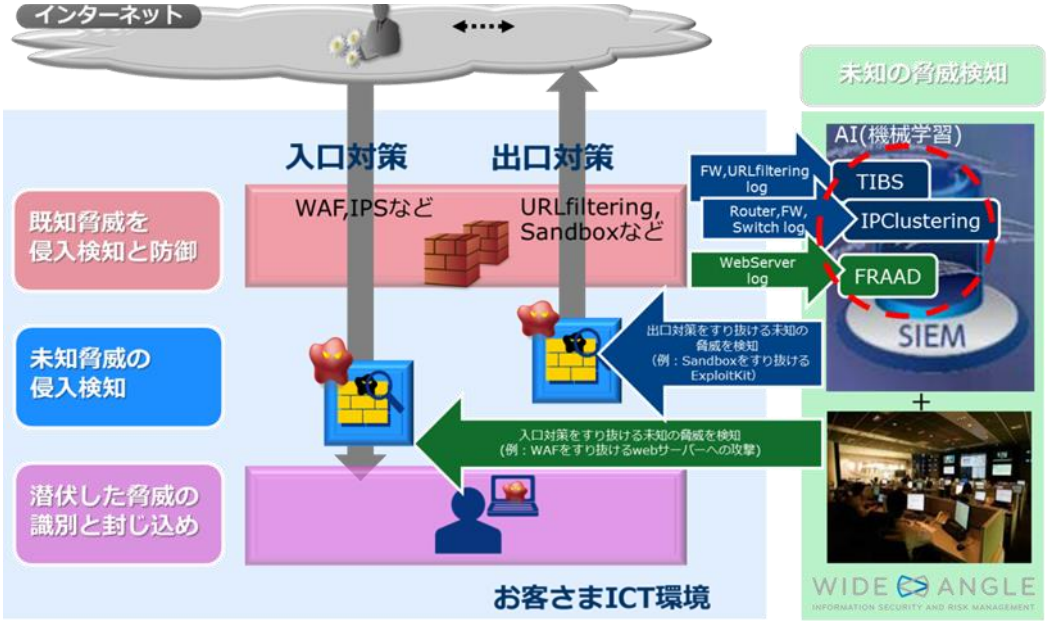
企業の機密情報などを詐取する標的型攻撃や Web サイトへの攻撃は、新種のマルウェアや新しい攻撃手法などにより、日々、高度化しています。そうした未知のセキュリティ脅威を防御するには、過去の攻撃手法を基にしたパターンマッチングやブラックリスト方式による検知・遮断などの従来対策では不十分な状況です。

こうした中、企業の情報資産を守るためには、未知の攻撃手法を用いるサイバー攻撃を、リアルタイムに検知・判別し、迅速に遮断する仕組みが重要となってきました。

2.概要

NTT Com は、数多の未知のセキュリティ脅威をリアルタイムに検知・判別する仕組みとして、NTT セキュリティ株式会社および NTT セキュアプラットフォーム研究所が開発した人工知能の要素技術である機械学習を活用したロジックを、「WideAngle」の MSS の運用基盤(SIEM)に組み込み、グローバルに提供します。このため、既に「WideAngle 」の MSS を利用しているお客さまは、新規申込をすることなく、脅威検知能力が強化されたサービスを利用可能です。なお、2015 年 10 月 7 日に報道発表した機械学習機能を活用した DGA[*1] 検知ロジックによる未知の悪性 URL の検知割合は、お客さま環境によっては Critical Alert 全体の 6 割を占めるまでに至っております。

NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation　Public Relations Office
〒100-8019　東京都千代田区内幸町 1-1-6
1-1-6 Uchisaiwai-cho, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010



(1)標的型サイバー攻撃などにおける未知の攻撃手法の検知

更なる出口対策として機械学習を活用し、新種の ExploitKit[*2] の活動やマルウェアコールバックを検知・分析する仕組み[*3] を導入しました。これにより従来攻撃者がコードの一部の僅かな文字列の変更等により従来のパターンマッチングによる検出対策をすり抜ける ExploitKit やマルウェアによる被害を最小限に抑えることが可能となります。

また、Proxy/IPS などのセキュリティアプライアンスを保有しない場合にも、L2 スイッチ・ルーター・ファイアウォールなどの通信ログから、機械学習したマルウェア挙動と合致したケースを検出し、未知のマルウェア感染を検知する技術[*4] も導入します。

(2)Web サイト向けの未知の攻撃手法の検知

お客さまの Web サーバーの正常な利用状況を学習し、外部からの未知の脅威を検知・分析する仕組み[*5] を導入しました。これにより、WAF の検出を掻い潜るパラメータ変更やパスコードの一部変更などによるインジェクション攻撃も検出することが可能となります。

3.今後の予定

NTT Com は、2016 年 8 月 1 日より事業を開始する NTT セキュリティ株式会社と共に、企業の ICT 環境をサイバー攻撃から守る手段として、上記に加えて、人工知能に関わる研究・開発活動を継続していきます。また、IoT セキュリティの脅威への対策にも取り組んでいきます。

*1 DGA（Domain Generating Algorithm）： URL アドレスであるドメインネームを自動で生成するための計算手法であり、生成手法をカスタマイズ可能で、多くのマルウェアで活用されている。

*2 ExploitKit：インターネットに接続された PC など、様々な脆弱性に対し、臨機応変に攻撃が出来る様、キット・パッケージ化されたプログラム群を指す。PC への潜入に成功すると Adobe Flash や Java などの通常使用されている技術のバージョンチェックなどを行い、その脆弱性を利用する攻撃用プログラムをダウンロードし、攻撃に繋げる。

*3 TIBS (Time Isolated Behavior Structure)：機械学習を活用し、マルウェアや ExploitKit における一定時間(勤務時間内など)におけるユーザーの振る舞い（どのような Web サイトへどのくらいアクセスしているか、その Web サイトの特徴は何かなど）を学習することで、通常アンチウィルスやＵＲＬフィルタリング、サンドボックスなどでは検知できない未知の感染後の活動を検出することが可能となります。

*4 IP Clustering：感染端末は正常通信も織り交ぜつつ、複数の不審な通信を発生させるという特徴から、マルウェアが利用する上記通信時のプロトコル・ポート・組織などの組み合わせを学習することで、ネットワーク機器の通信ログだけで未知のマルウェア感染を検知することが可能となります。これにより、http 通信以外の TCP/UDP 通信を行うマルウェアも検出できます。

*5 FRAAD(Frequent Resource Access Anomaly Detection)：お客さまの Web サーバーログから正常利用におけるページシーケンスや URL パラメータなどを自動学習することで、WAF などの既存の入口対策さえもすり抜けてしまう攻撃を検知することが可能となります。