Acronis データをセキュアに保つマシンラーニング（機械学習）

2017年1月にリリースされたAcronis Active Protectionは、洗練された分析を使用してシステムでランサムウェアのような振る舞いが行われていないかをモニターし、迅速に遮断します。独立系調査機関による試験でも良好な結果を示し、メディアから称賛が寄せられましたが、それでもなお、アクロニスはこのソリューションをさらに強力にすべく研究を重ね、ML（機械学習）とAI（人工知能）テクノロジーを活用することで、一層強力な機能となりました。

マシンラーニング（機械学習）活用の仕組み

マシンラーニングはビッグデータに関連して使用されることが多々あります:　膨大な量のデータを分析し、実施可能な結果を導くために使用されます。マシンラーニングはデータ量と選択されたアルゴリズムに基づくため、データサンプルが大量であればあるほど、より良い結果につながります。

アクロニスはこのテクノロジーをどう使用するのか？最初の手順は、プログラムのサブルーチン上でレポートされるスタックトレース分析を実行することです。このテクニックはある種のデバッグを実行する際に使用されることが一般的で、ソフトウェアエンジニアが問題個所を把握し、さまざまなサブルーチンが実行時に一緒に機能する方法を知るために役立ちます。

アクロニスはこのアプローチをランサムウェア攻撃に適用し、不正コードの注入を検知するためにマシンラーニングを使用します。

マシンラーニングの仕組み

アクロニスは多数の正規プロセスを実行するWindowsシステムを使用して、これまでに膨大な量のクリーンデータを分析してきました。その後、数百万の正規のスタックトレースをこれらのプロセスから取得し、ディシジョンツリー学習を使用して「適正な」振る舞いのさまざまなモデルを構築しました。また、真逆の例を提供するために、多様な情報源から不正なスタックトレースも収集しました。

これら数百万にのぼる学習サンプルに基づき、振る舞いパターンが特定されます。

ディシジョンツリー学習において、アイテムの観察からその目標値に関する結論を導き、特定可能な要素に基づき新しいアイテムの値を正確に予測します。このモデルにより、アクロニスは目標値に対する適切な応答を構築することができます。データを収集し、分析のために送信することで、クライアントマシンをスローダウンさせず、一定のレベルの保護を効率的に提供します。

マシンラーニングが有効化されるのはいつか？

上記の通り、Acronis Active Protectionはヒューリスティック（振る舞い）に基づきます。バージョン2.0では、正規のプロセスを探す複数の新しいヒューリスティックを追加しました。Acronis Active Protectionが正規プロセスの中に不審な振る舞いを検知した場合には、スタックトレースを取得し、Acronisのマシンラーニングモジュールに送信します。そこで振る舞いが既存のクリーンモデルおよび感染したスタックトレースと比較され、脅威であるかどうかが判断されます。

振る舞いが不正な性質のものであると判断された場合には、ユーザーには、プロセスをブロックするよう提案するアラートが表示されます。

アンチランサムウェア防御の新しいレベル

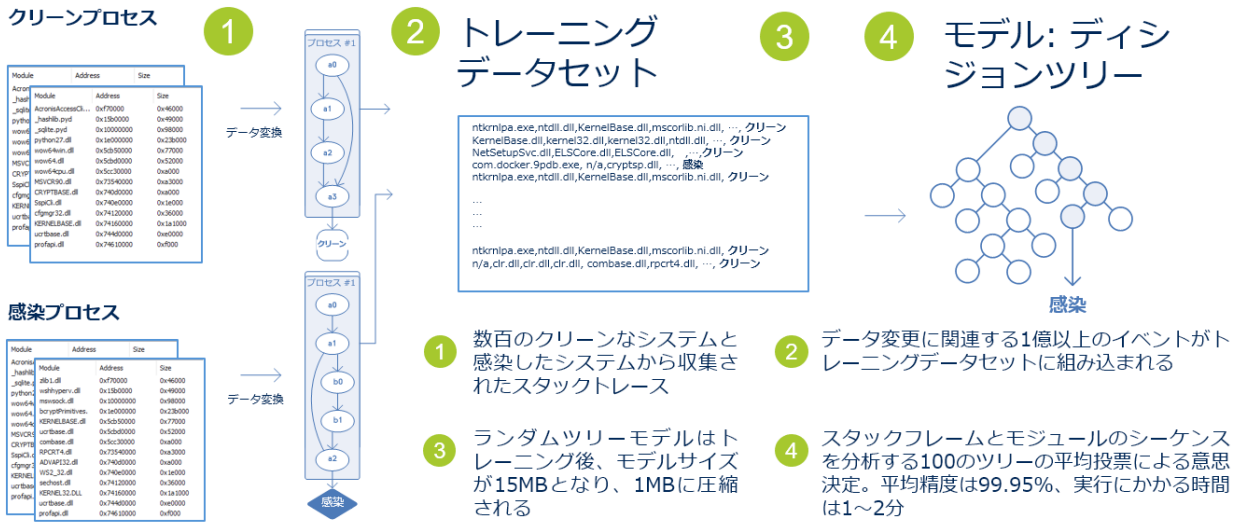
マシンラーニングが発展する中、こうしたテクノロジーはすべて、Acronis Active Protectionを新しいレベルへと導きます。特に、ゼロデイ脅威と戦う場合にその効力を発揮します。正規プロセスのモデルを作成するため、犯罪者が新しい脆弱性やシステムに侵入する方法を見つけた場合でも、マシンラーニングがランサムウェアのプロセスを検知して遮断します。

Acronisのマシンラーニングインフラは新しい、匿名化されたプログラムデータが分析のために定期的にアップロードされるよう構築されています。このインフラは数百万のリクエストを同時に管理することができます。そして、一定の情報のフローがあるため、新しい振る舞いモデルが迅速に利用可能となります。また、製品のヒューリスティックの定期的なアップデートがセキュリティをさらに高めます。背後で行われるこうした数秒の処理は、ユーザーに気づかれることなく実行されるため、Acronis Active Protectionをオンにするだけで、あとは何もする必要はありません。

次に何が行われるのか

Acronisは静的コード分析にマシンラーニングを活用することで、このテクノロジーの使用を拡大し続けます。分析は実行前の段階で完了するため、ファイルをダウンロードしたり、ハードドライブにコピーしたりする場合には、コードに異常がないことを瞬時にチェックされます。不審なものがあった場合には、プロセスがユーザーや自動スクリプトによって開始される前にブロックされます。

マシンラーニングモデルはスクリプトの分析にも使用できるため、アクロニスは既にその方向で研究を始めています。実際、NioGuard Security Labが実施した試験では、ほとんどのアンチウイルスソリューションがスクリプトベースの攻撃を検知できない中、Acronis Active Protectionは優れた結果を残しました。この成功に気を緩めず、アクロニスはアンチランサムウェアテクノロジーをより一層改良していきます。



詳細は、www.acronis.comをご覧ください。