ホワイトペーパー

AIを使った悪意ある文書とスクリプトの検出

マシンインテリジェンスにより多層的保護を強化する

悪質なサイバー攻撃は増加の一途をたどっており、サイバー犯罪者はEメールや他の通信チャネル経由でソーシャルエンジニアリングを第1の攻撃ベクトルとして利用しています。怪しげなEメールの添付ファイルは、開くとマルウェアエクスプロイトが脆弱性を突いて実行され、攻撃が開始されます。悪意ある文書もユーザーが通信チャネルを通じて受信したリンクからダウンロードされる可能性があります。

アクロニスの専門家によると、2022年半ばの時点でMicrosoft OfficeファイルやAdobe PDFファイルなどを利用した攻撃または悪意ある文書が全攻撃の約3分の1で使用されています。業界他社も同様の報告をしています。マルウェアは実行の連鎖はさまざまですが、通常ファイルに組み込まれています。例えば、脆弱性が最初にエクスプロイトされ、次に特権が昇格され、マルウェアがダウンロードされ、実行されます。マクロ、シェルコード、Javaスクリプト、さらにはファイル全体にも組み込むことができるため、Microsoft OfficeとPDFのファイルが長年にわたってサイバー攻撃で使用されています。しかし、近年ハッカーが検索エンジン最適化（SEO）を使って悪意あるファイル、とりわけPDFが、検索結果の上位になるよう操作しているためこの問題は悪化しています。

他の類似した問題では、PowerShellのような正当なツールによって実行される悪意あるスクリプトが関与しています。悪意あるスクリプトを使用する攻撃数は、悪意ある文書と同様に前年比で増加しており、アクロニスの専門家は、このような攻撃が過去2年間でほぼ倍増したことを確認しています。悪意あるスクリプトの目標も同じで、システムに侵入し、権限を昇格させ、ダウンロードして、ペイロードを実行します。

サイバーセキュリティ会社にとっては、上述の2つの問題は文書やスクリプトの善悪を見抜く必要があるという点で同じものです。明るいニュースとしては、機械学習（ML）や人工知能（AI）、またはアクロニスのマシンインテリジェンス（MI）を使えばかなり効果的に同上の問題を解決できます。

脅威検出のためのマシンインテリジェンスの使用

アクロニスは2017年のActive Protectionランサムウェア技術を導入時から機械学習の利用を開始しました。その後すぐにAIベースの静的検出エンジンを作成し、これは現在アクロニスの主力製品であるAcronis Cyber Protectで使用されています。

このエンジンは常にアップデートされており、新しい機械学習モデルが導入されるたびにパフォーマンスと検出率が向上しています。例えば、最初は実行されたプロセスのスタックトレースを分析するために使用され、その後ファイルやライブラリ全体を分析して悪意あるプロセスを検知するようになりました。現在では、実行ファイルとプロセスイメージから抽出された文字列を分析できます。追加の特徴として抽出された文字列に含まれる数百の単語の出現頻度により、検出率が3%以上向上しました。

容易に想像される通り、悪意ある文書やスクリプトを検出するために同様のアプローチが使用されます。Microsoft Office文書から始めまてみましょう。Microsoftが最近発表したとおり、インターネット経由のドキュメントではマクロが既定で無効にされてきており、このアプローチを徐々に展開し始めましたが、残念ながら、すべての問題を解決できるわけではありません。マーク・オブ・ザ・ウェブ(MOTW)属性は、インターネットや制限付きゾーンなどの信頼できない場所(ブラウザのダウンロードやEメールの添付ファイルなど）のファイルにWindowsにより追加されます。要するに、この属性はNTFSファイルシステムに保存されたファイルのみに適用され、FAT32フォーマットのデバイスに保存されたファイルには適用されません。ファイルが正当なオフィスメールからのものだったらどうなるでしょうか？言うまでもなく、マクロに大きく依存する環境（例えば、会計部門など）ではうまくいきます。それにもかかわらず、このようなポリシー対応環境はより安全になり、Emotetキャンペーンで使用されたようなフィッシング攻撃の典型的なケースは防御に成功します。しかし、前述のように、多くのビジネスでは他の複雑な状況が発生します。そのため、アクロニスのAIスペシャリストは機械学習の力を借りて、検出エンジンを強化し悪意ある文書を特定できるようにしました。

悪意あるマクロスクリプトはどのようなものか？下記項目が1つでも当てはまるものは、可能性があります。

- プロセスを作成する
- PowerShell、VBAなどでスクリプトを実行する
- リモートサーバーからファイルをダウンロードする
- 他のOfficeファイルやOfficeテンプレートファイルに組み込まれる

しかし、他の要因も多数あるため、実際に検出するのはそれほど簡単ではありません。例えば、アクロニスの機械学習モデルでは、DOCXファイルの以下の属性をチェックして判断します。

- さまざまなテキストやVBA関数機能
- コメントやコードなどの比率機能
- マクロ自体、コード、コメントのエントロピー
- 難読化
- URLや実行ファイルなど既知のセキュリティ侵害インジケーター（IoC）パラメータ

もちろんこれは完全なリストではありませんが、大規模なデータセットで多数が分析され、常に改定、更新されるということを説明する助けになります。その結果、1MB以下に圧縮されたモデルサイズではすぐれた検出率を達成しています。AIとMLがなければ、こうした結果を達成することはほぼ不可能です。また、これは強固な多層防御の一部であり、脅威がEメールスキャニングエンジンやサンドボックス、URLフィルタリングのような他の技術で以前に検出されていない場合にのみ作動します。

サービスプロバイダー環境でよく使われる悪意あるAutoITスクリプトを検出する、非常に類似したアプローチが最近アクロニスの専門家によって始められました。アクロニスは、約0.6 MBという小さなモデルを使って、92%の検出率をすでに達成しており、DOCXとともに常に改善されています。

攻撃用に改ざんされたPDF脅威の排除

Microsoft Office Word文書の他にAdobeポータブルドキュメントフォーマット（PDF）はサイバー犯罪者がシステムに侵害したり、ユーザーマシンにマルウェアを植えつけたりするためによく使われるツールです。PostScript言語に基づくPDFには、テキストやハイパーリンク、マルチメディア、画像、添付、メタデータなど多くの情報を含められるため、非常に強力なフォーマットになっています。PDFフォーマットには「アクション」機能があり、JavaScriptコードを実行するWebリンクやファイルを開くことができます。そして、ご想像のとおり、不正な目的のために実行されるその他多数の操作があります。

PDF文書はブラウザやさまざまな読み込みソフトウェアで閲覧することができ、そのすべてに、任意コード実行、バッファオーバーフロー、メモリ破損、領域外読み取りなどサイバー犯罪者が悪用できる脆弱性があります。現在、PDFリーダー向けに何千ものCVEがあり、Adobe Acrobat Readerだけでおよそ300種類の脆弱性が知られており、セキュリティ研究者も、サイバー犯罪者も、ほぼ毎日新しいPDF関連のエクスプロイトを発見しています。

CVE-2021-28550脆弱性エクスプロイトの例：Acrobat Reader DCバージョン2021.001.20150以前、2020.001.30020以前および2017.011.30194以前に「Use After Free」脆弱性があります。未認証の攻撃者が、この脆弱性を利用して現行ユーザー環境で任意コード実行を行う可能性があります。この脆弱性の悪用には、被害者が不正なファイルを開くためのユーザーインターフェースが必要です。

PDFファイルに組み込まれた悪意あるリンクによるフィッシング例

アクロニスの機械学習ベースのPDF検出モデルでは、上記の他のファイルタイプと同じように、さまざまなパラメータをチェックして正しい判断を導きます。

- エントロピー
- 総文字数
- 特別キーワード数
- 行数、特別割り当て行
- その他

その結果、非常に効果的な検出率を達成します。

サイバーセキュリティ意識向上トレーニングの有益性

この種類の検出モデルを、すぐれたサイバープロテクションソリューションに統合することは不可欠です。しかし、ユーザーが脅威とその振る舞いを認識し、適切に対応した場合には、企業全体と個人のセキュリティポスチャにとって大きな利益となります。ほとんどの悪意ある文書やスクリプトがその目的を果たすために、ユーザーの関与を必要とするためです。つまり、ユーザーの関与がない場合は脅威もありません。

この意識向上トレーニングでは、基本に忠実で、よく知られたコミュニティルールに従う必要があります。

- Eメールやリンクの送信元を必ずチェックしてください。この人物を知っているか？このファイルを予期していたか？単に名前やエイリアスではなく、実際のメールアドレスを見て送信元を確認してください。
- ユーザーがすでにファイルをクリックし、不具合の兆候が出ていたり、何かの有効化を求められたり、リンクや偽のキャプチャが表示されたりしたら、直ちにページを閉じる、またはダウンロードしたファイルを削除するなどして、セキュリティチームに連絡してください。
- ファイルをクリックしても何も起こらない場合も、良くない徴候です。ファイルが開いて、予期しない事が起きた場合、既に被害を受けている可能性があるため、セキュリティチームにすぐ連絡してください。

最善策は、添付ファイルを開かないことであり、リンクをすぐにクリックしないことです。すべてを二重にチェックして、それでも安全性を確信できない場合は、セキュリティチームにお問い合わせください。注意を怠らず、安全を期してください。

Acronis

詳細情報はこちらをご覧ください：
www.acronis.com