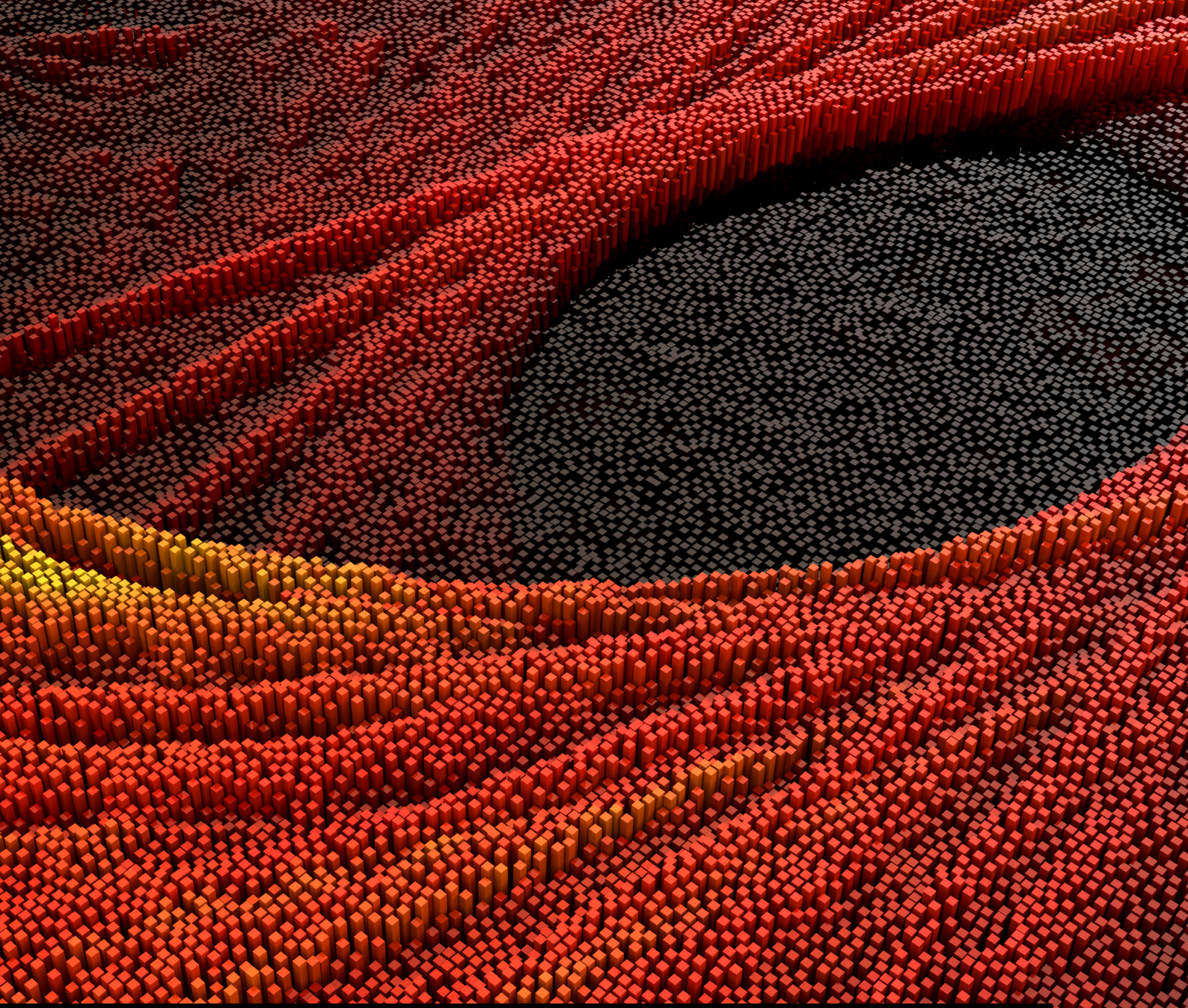


ファイルレス攻撃と闘う

ファイルレスマルウェアに対抗するための第一線の防御を実現

CYLANCE

2017 年にはファイルレス攻撃が急増しましたが、これは攻撃者と従来型アンチウイルスソリューションの攻防において攻撃者が優勢に立ったことが大きな原因です。昨年は、いくつかのファイルレスマルウェアが勝利を収めました。OceanLotus Group は、オペレーション「コバルトキティ」でアジアの複数の企業に侵入し、検出されるまでの約 6 ヶ月間、ファイルレスでの活動を続けました。悪名高いランサムウェアの Petya と WannaCry は、いずれもキルチェーン内にファイルレスの手法を取り入れていました。情報セキュリティに従事している主要な担当者は皆、ファイルレス攻撃をくい止めるのは難しく、脅威を取り巻く状況はますます悪化しているという認識で一致しています。

従来型のアンチウイルスソリューションはファイルと署名に基づくブラックリストをあまりにも重視しすぎているため、ファイルを捨て去るということは、そうした既存のセキュリティソリューションに対抗するための理にかなった方法だと言えます。検出対象の感染ファイルが存在しない場合、セキュリティソリューションは何ができるでしょうか？正当なシステムリソースのみを使用する攻撃者をブラックリストでくい止めることは可能でしょうか？セキュリティの状況は変化しており、従来型のアンチウイルス製品と次世代セキュリティソリューションの差は日々広がっています。

Cylance® は、人工知能と機械学習を活用したセキュリティで評価されており、ファイルレスマルウェアに対する第一線の防御を実現します。この文書では、サイランスがどのようにして組織を保護するかを詳しく説明します。

ファイルレス攻撃とは何か

ファイルレス攻撃とは、その名前が示すように、ホストシステムにファイルを書き込むことなくインフラストラクチャやデータを侵害する攻撃のことです。ファイルレスマルウェアは、正当なシステムリソースを悪意のある目的に利用することによって（そのため「環境寄生型」と呼ばれることがあります）、ほとんどの従来型の脅威検出方法から巧みに隠れることができます。この種類の攻撃は、以下のような特徴に基づいて識別することができます。

- マルウェアはディスクではなく、メモリに常駐する
- スクリプトを多用するマルウェアは、Jscript/JavaScript を使用して最初の感染を引き起こし、攻撃の踏み台とする
- マルウェアは PowerShell、WMI などの正当な Windows の管理ツールのリソースを悪用して活動を行う
- マルウェアはシステムレジストリを変更することにより永続性を獲得する

エクスプロイトキットは
この攻撃にどのように関連しているか

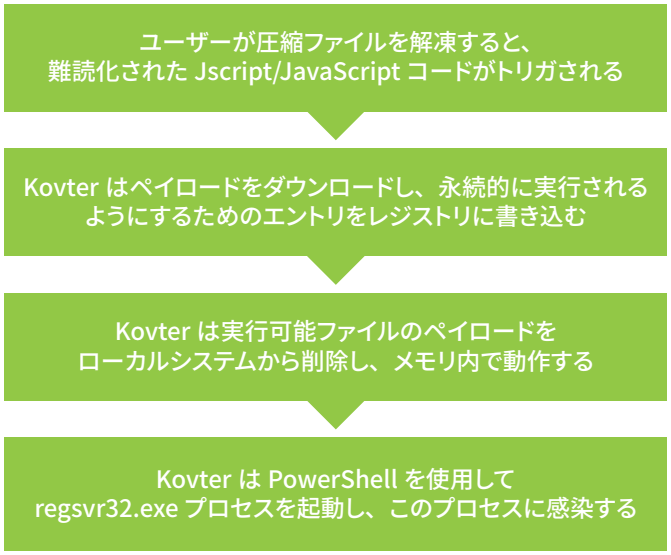
エクスプロイトキットとは、既知のソフトウェアエクスプロイトとシステム分析やペイロード配布のためのツールをパッケージ化したものであり、ファイルレス攻撃の重要なコンポーネントです。エクスプロイトキットはしばしば、悪意のある広告リダイレクトを使用してユーザーのブラウザーをひそかにスキャンします。ブラウザーにセキュリティ上の欠陥が検出されると、ユーザーはランディングページにリダイレクトされ、そのページでより大規模なシステムスキャンが実行されます。システムの脆弱性が特定されると、エクスプロイトキットはシステムにマルウェアを送り込めるようになります。このすべてのプロセスはエンドユーザーからは見えません。

ファイルレスの例：Kovter

Kovter はクリック詐欺を行うトロイの木馬型のマルウェアであり、2016 年にファイルレスの手法を活用し始めました。元々のバージョンの Kovter は、アクティブユーザーのプロファイルの下にフォルダを作成し、そこに KB9162892.exe という名前のペイロードを保存していました。

ユーザーが悪意のあるウェブサイト広告をクリックする → ユーザーは別のウェブサイトにリダイレクトされ、そこでブラウザーの脆弱性がスキャンされる → 脆弱性のあるブラウザーはエクスプロイトキットのランディングページにリダイレクトされる → 広範なシステムスキャンが実行され、OS や他のソフトウェアの脆弱性が特定される → エクスプロイトキットが、特定された脆弱性を突いてペイロードをユーザーのシステムに送り込む

しかし、ファイルレス化した Kovter は新しい手法により感染するようになりました。難読化された Jscript/JavaScript を起動して、Kovter の実行可能ファイルを %TEMP%（Windows の一時フォルダ）にダウンロードするのです。次に、再起動後に毎回このファイルが実行され、感染の次の段階に進めるようにするためのエントリを Windows のレジストリに書き込みます。そして、マルウェアは PowerShell を使用して regsvr32.exe プロセスを起動し、このプロセスに感染します。最後に、Kovter はそれ自体の実行可能ファイルを %TEMP% ディレクトリから削除します。これによって、署名ベースでは何も検出されなくなります。



新しい Kovter は、正当なものとして認識されているシステムプロセスに常駐し、メモリ内で動作します。問題となるファイルも、検出すべき悪意のあるプロセスも存在しないため、従来型のアンチウイルスの検出手法の多くは回避されてしまいます。

サイランスのアプローチ

サイランスは、CylancePROTECT® と CylanceOPTICS™で提供されているツールの組み合わせによってファイルレスマルウェアをくい止めます。

実行前防御

CylancePROTECT では数理モデルを用いて実行される前のペイロードを予測判定し、悪意のあるコードを検知およびブロックすることでマルウェア感染を予防することができます。先に紹介した Kovter のケースをみても分かるとおり、ファイルレスマルウェアと呼ばれるものでも、感染動作の段階では実行可能ファイルのペイロードが利用されているケースも多く、CylancePROTECT はこれらを数理モデルを使って予測防御することができます。

次にファイルレスマルウェアを防御するための鍵となるのが、ファイルレスマルウェアにシステムリソースを使わせないようにすることです。ファイルレスマルウェアの存在を検出することは困難であることが実証されていますが、ファイルレスマルウェアからツールを奪うことは困難なことではありません。サイランスでは、スクリプト制御、メモリ防御、コンテキスト分析エンジン（CAE）を使用して、ファイルレス攻撃による損害を事前にくい止めます。

スクリプト管理

システム管理者は、CylancePROTECT のスクリプト制御によって、環境内でスクリプトを使用するタイミング、場所、方法を決められるようになります。CylancePROTECT スクリプト制御は、それ自体をスクリプトのインタープリタに注入することによって、スクリプトの活動やスクリプトのパスを実行前に把握します。疑わしいスクリプトの活動が検出された場合は、その活動がブロックされるか、システム管理者にアラートが送信されます。

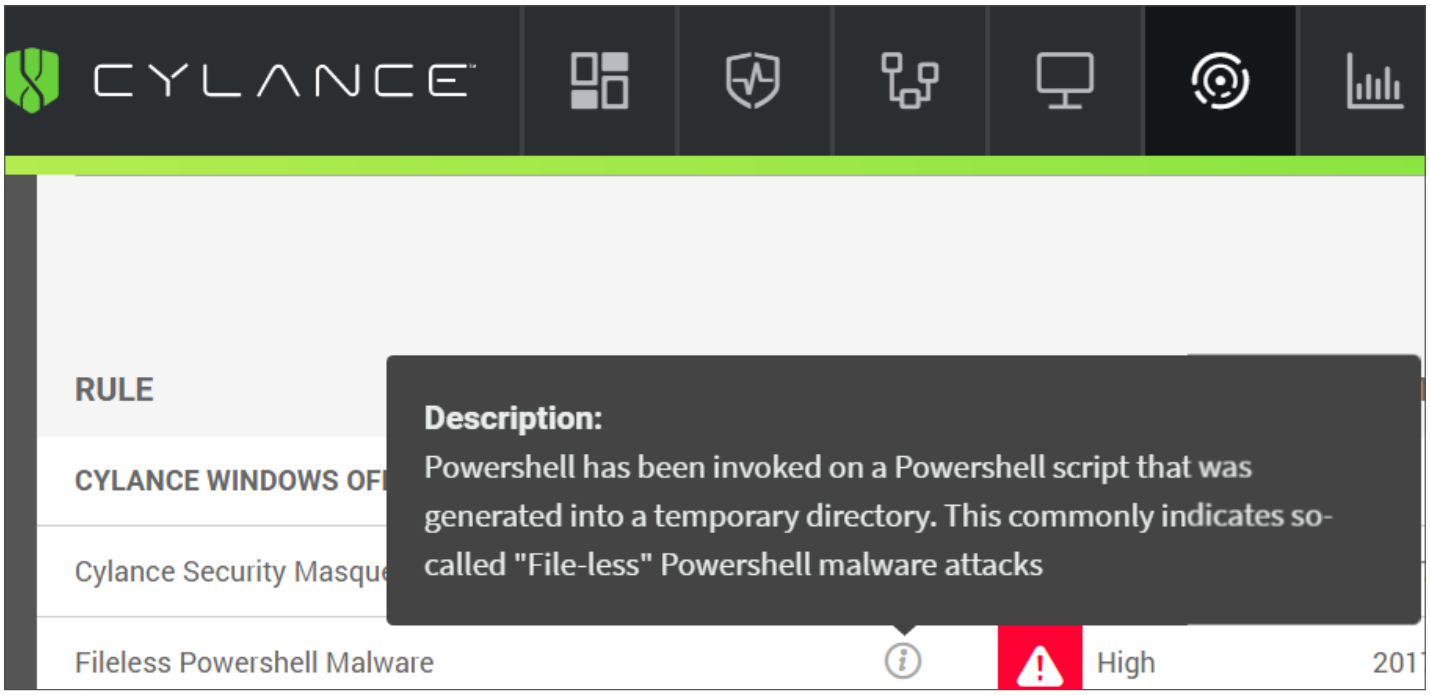
サイランスは、PowerShell、Active Script（Jscript と VBScript）、Microsoft Office マクロのスクリプト制御機能と検出機能を提供しています。PowerShell をブロックすると、PowerShell コンソールの起動も防止されます。これにより、PowerShell ワンライナーの実行が阻止され、システムが保護されます。PowerShell をブロックした場合でも、明示的に承認されたスクリプトの実行は可能です。

メモリのエクスプロイトの検出と防止

CylancePROTECT のメモリ防御は、ファイルレス攻撃の動作に必要な空間を与えないようにします。このメモリ防御エージェントは、保護対象の各プロセスにロードされる DLL と、管理機能を提供するサービスコンポーネントで構成されています。このエージェントは、ユーザーモードの API 関数にフックして、セキュリティ侵害の兆候を監視します。API の内部でこうした兆候が検出されると、疑わしい関数は中断させられます。また、その後の動作を以下から選択することができます。

- 違反を無視し、プロセスを続行する
- 違反に関するアラートを送信するが、プロセスは続行する
- 違反をブロックし、アラートを送信する
- プロセスを完全に終了させる

CylancePROTECT のメモリ防御は、32 ビットと 64 ビットのいずれのプロセスでも動作し、システムのパフォーマンスに大きな影響を与えることはありません。CylancePROTECT の管理者はメモリに関するポリシーを簡単に設定することができ、現代的で複雑なホスト侵入防止システムと同等の保護を実現できます。



コンテキスト分析エンジン（CAE）

CylanceOPTICS のコンテキスト分析エンジンは、脅威検出と対処の機能を通じて各エンドポイントのセキュリティを高めます。このアプローチによって、各エンドポイントは仮想 SOC として機能することができ、事前に設定されたプロセスによって脅威に対処できます。つまり、人間による操作を必要とせずに週 7 日 24 時間動作する自動化されたエンドポイント保護が提供されます。クラウドに接続するのではなく、エンドポイント上で CAE により脅威の分析が実行されるため、遅延が短縮され時間が節約されます。

CAE は、システムの動作のカタログに対してルールを適用する手段を提供します。これらの動作には、ファイルレス攻撃の動作時に使用される、PowerShell、JavaScript、ブラウザのそれぞれに固有の動作が含まれます。また、それぞれの環境に固有の懸念事項に対処するためのカスタムルールを作成することもできます。ファイルレスマルウェアが必要なリソースにアクセスできないようにすることは、ファイルレス攻撃に対抗するための非常に効果的な方法です。

まとめ

ファイルレスマルウェアは、脅威の標準的な検出方法ではほとんどの場合に感知することのできない目立たない方法で、従来型のアンチウイルスソリューションを使用している製品に深刻な脅威をもたらします。ファイルレスマルウェアは、ホストシステムを攻撃するために正当なリソースをハイジャックすることによって、それ自体の存在をカムフラージュして、気づかれずに動作することができます。

サイランスは、ファイルレスの脅威が存在し続けるために必要なリソースをそれらの脅威から奪いとるための高度なツールを提供します。サイランスの製品は、スクリプトの実行、メモリ空間、エンドポイントの改変を制御することによって、ファイルレス攻撃をくい止めてインフラストラクチャを安全に保ちます。

Cylance Japan 株式会社
〒100-6510
東京都千代田区丸の内 1-5-1　新丸の内ビルディング 10F
www.cylance.co.jp
03-6386-0061 (代表)

201812-WP007