ホワイト ペーパー:

ファイルレス攻撃解説

ファイルレス攻撃解説

ファイルレス攻撃はサイバー攻撃の分野で「次の新たな脅威」として最近出現し、大きな注目を集めています。しかし実際には、この形態の不正攻撃は長い間存在していました。ファイルレス攻撃が今話題になっているのは、急増していることと、攻撃対象のエンドポイントの上位にも被害を拡大させる一連の攻撃で使用されていることが分かってきたためです。

現在ニュースになっているのは、ほとんどがランサムウェアですが、その一方で、昨年、ファイルレス攻撃数が過去最大になりました。Verizonによると、2017年のセキュリティ侵害のうちマルウェアによるものは51%のみで[1]、またPonemon Instituteの「2017年エンドポイント セキュリティ リスク状況」によると、2017年のサイバー攻撃のうち29%がファイルレスでした。Ponemonは、2018年には35%まで増加すると予測しています。[2] ファイルレス攻撃は潜行性が高く、そのため、より効果的です。ファイルレス攻撃は実行可能ペイロードを隠し、痕跡も残さないので、アンチウィルス、ホワイトリスト、そしてその他の従来のエンドポイント セキュリティ ソリューションでは検知できません。Ponemon Instituteは、ファイルレス攻撃はファイルベースの攻撃の10倍効果的であると断言しています。

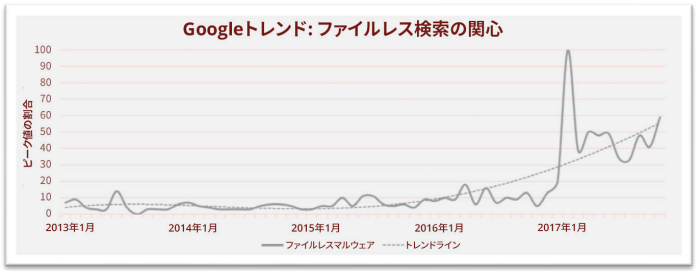

図1.ファイルレス攻撃への注目増加を示すGoogleトレンドチャート

ファイルレス攻撃とは

通常とは違った形態であるものの、実行可能ファイルが含まれていますので、「ファイルレス マルウェア」という用語は正しくはありません。より正しく説明し、かつ分かりやすい言葉は、「ファイルレス攻撃」です。ファイルレス攻撃は低観測性 (LOC) 攻撃のカテゴリーに分類される、ほとんどのセキュリティ ソリューションで検知できないステルス攻撃の一種であり、フォレンジック分析もうまく働きません。

空き巣を例として考えてみましょう。人の歩みを検知する圧力センサーが床に埋め込まれたスマートホームに、ハイテクな空き巣が侵入したとします。この非常に賢い空き巣はドローンを持っていて、センサーを踏まずに飛んでいくことができます。空き巣が去った後の現場で鑑識官は困り果てて、侵入者の

マカフィーとの連携

足跡が見つからない、と警察署長に報告します。この例では、家主の防犯対策技術も警察の鑑識も、侵入者の技術に敗北しています。認識可能な痕跡を残さないLOCやファイルレス攻撃では、これと同じような状況が起こるのです。

このステルス性のLOCはマルウェアとは異なり、オブジェクト（マルウェア）を使うのではなくプロセスを操作して攻撃をしかけます。通常LOCは、信頼されているアプリケーションやプロセスの脆弱性を悪用して不正なコードを配信し、それをディスクではなくメモリ（RAM）に保存させます。多くのLOC攻撃では、Microsoft Windows PowerShell が悪用されています。PowerShellは、管理者がタスク自動化および構成管理に使用する、正当かつ有益なツールです。PowerShell はコマンドライン シェルとそれに対応するスクリプト言語で構成されており、これを使用すると、攻撃者はWindows内のほぼすべてにアクセスできるようになります。

典型的なファイルレス攻撃は、ネットワーク (ウェブサイト)を経由するか、またはワード文書のような無害なメール添付文書を装って、不正なスクリプト、コードおよびコマンドを配布します。ファイルレス攻撃は一旦侵入すると様々なプロセスを開始します。まずは予備調査を行って認証情報を盗み、これを使って実際のマルウェアのダウンロードを行います。

典型的なLOC戦略には以下が含まれます。

- 「Living off the land (環境寄生)」：攻撃対象のシステムにすでに存在しているツール、ユーティリティ、OSコンポーネントを利用して、検出を免れるよう設計された攻撃。
- 「マルウェア レス」：攻撃対象にインストールされていない正当なツールを使用した攻撃。
- 「Clean up after yourself (自己後処理)」：一般的なWindowsユーティリティを活用して、攻撃中に使用したファイルすべてをゼロで上書きする。

ファイルレス攻撃は非常に高い柔軟性を持っています。異なる技術の組み合わせ、またはランサムウェアなどの他の攻撃との組み合わせを用いて、複数のペイロードを作り出したり、現在のマルウェア検知技術の裏をかくための複雑性を高めています。

ファイルレス攻撃のアタック キルチェーン

手順1：不正アクセスの開始

ファイルレス攻撃は最近の多くの先進的攻撃と同様に、ソーシャルエンジニアリングを用いて、ユーザーにフィッシングメールのリンクや添付をクリックさせます。不正なスクリプトは、ウェブサイトのフラッシュや公認アプリケーションが生成した文書に隠されています。そしてアンチウィルスの署名スキャンで検知されることを避けるため、目立たない方法でダウンロードされ、ディスクではなくメモリに書き込まれます。

時間と労力の節約のため、メモリから平文パスワードを抽出できる、認証情報読取りツールのMimikatzのような回避キットや難読化キットが使用されることが多くあります。WannaCryやPetyaランサムウェア攻撃では、侵入時にこの有名なハッキングツールを使用しています。ファイルレス攻撃は通常水平移動します。つまり、予備調査または企業ネットワーク上の重要なデータへのアクセス権限の入手のため、またはサイバースパイの実行のために、デバイスからデバイスへと移動していくのです。

「多くのサイバー攻撃は今後も基礎的なセキュリティ脆弱性、露出、ユーザー行動を悪用しますが、ファイルレス攻撃はみなさんのシステムの機能を利用します。攻撃者は、信頼されたアプリケーションを利用したり、PowerShellやJavaScriptといった本来持っているシステム オペレーティング ツールにアクセスすることで、攻撃の初期段階では実行可能ファイルをダウンロードすることなくコンピューターの不正操作を可能にするツールの開発に大きな進展をもたらしました。」

—Steve Grobman (McAfee, LLC シニア バイス プレジデント兼CTO)

手順2:ファイルレスでの実行

この段階では攻撃者は、従来のセキュリティ監視技術によってファイルやアクテビティが検査されないように配慮します。このステップでは、不正なプロセスを起動するために、信頼された、ホワイトリストのアプリケーションやOSの奥深くに入り込みます。ここでは2つの主な戦略がとられます:

- **メモリにダウンロードして実行:**この方法では、ディスクにダウンロードすると検知されてしまうような署名を持つファイルの内容をダウンロードできます。攻撃者がPowerShellベースのマルウェアを好む理由の一つは、メモリベースのダウンロードおよび実行をサポートしているからです。McAfee Labsによると、PowerShellマルウェアは2017年第2四半期から第3四半期にかけて倍増し、計28,000件以上になっています。[3]
- **信頼されているアプリケーションを使用:**このケースでは、通常は不正なコンテンツをダウンロードしないような承認済みのホワイトリストのアプリケーションを活用して、セキュリティ ソフトウェアによる検査を回避します。

問題は、ほとんどの自動化センサーではコマンドラインの改ざんを検知できないことにあります。熟練した分析者であればこういったスクリプトを識別できますが、しかし多くの場合、そもそもどこを探せばよいのかがわかりません。

手順3:ファイルレスの持続性

攻撃対象のシステムが再起動されたとき、ファイルレス攻撃はどうなるでしょうか?単純な答えは、RAM上の不正なコードは消去される、です。ファイルレス技術はほとんどが短命であるというのが事実ですが、持続的攻撃を狙う攻撃者は複数の回避技術を使ってこれに持続性を持たせることがあります。この方法は以下の通りです:

- 不正なコードを、OSやコモン ユーティリティに関係する一般的でない場所、例えばWindows レジストリ、WMIストア、SQLテーブル、タスクスケジューラーなどに埋め込む
- 検査を回避できるようにシステムプロセスにコードを埋め込んで、アクティビティが正規プロセスから発生しているように見せかける

手順4:目的の達成

予備調査、認証情報取得、データ抜き出し、サイバースパイ、または損害を与えるなど、攻撃目的は様々ですが、上記の手順がすべて実行された時点でファイルレス攻撃は成功したとみなされます。ファイルレス攻撃はアクテビティを巧妙に隠すことができ、また検知にファイルベースのアプローチをするほとんどのセキュリティ ソリューションは動作監視をしていたとしてもファイルレス攻撃を検知できないからです。攻撃者は、ホワイトリストのプログラムは監視しないという、セキュリティアプリケーションの信頼モデルを悪用して、それらの機能やプロセスを用いて目的を果たします。

図2.F117A ステルス機

低観測性 (LOC) および軍事ステルス技術

低観測性という用語はもともと軍事用語で、人、飛行機、船舶、潜水艦、ミサイル、衛星の存在を、レーダー、赤外線、音波、およびその他の検知方法から見えにくく、または全く見えなくするために使用される技術のことをいいます。

サイバーセキュリティの世界では、LOC攻撃は、F-117a　ナイトホーク攻撃機やB-2ステルス爆撃機に匹敵するものです。LOC攻撃はカモフラージュ技術を使っており、もっとも広く採用されているサイバー攻撃防御メカニズムでは検知できません。

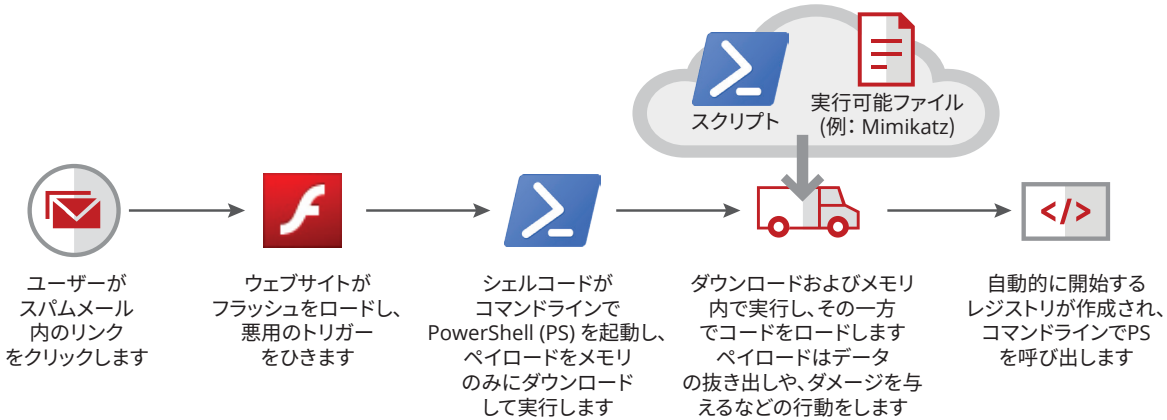

図3.ファイルレス攻撃アタック チェーンの例

ファイルレス攻撃の今後の傾向

その他の多くのサイバー攻撃と同様に、ファイルレス攻撃も今後、より洗練され複雑に進化すると言っても過言ではないでしょう。攻撃者の技術開発に影響するファクターはいくつかあります:

- Windows OS固有の脆弱性は、攻撃者の技術開発の可能性を広げています。消費者は、OSに組み込まれたプロセスや技術から派生する脆弱性を悪用するファイルレス攻撃への対策を、OSベンダーに一任できません。
- 完璧ではないものの、スクリプトの動作はMicrosoft Antimalware Scan Interface (AMSI) である程度確認できます。これにより、多くのベンダーはある一定のLOCの検知率を向上させることができます。将来は、AMSIとサードパーティの機械学習機能を統合することで、ファイルレス攻撃の可視化を進めることができるでしょう。
- 攻撃的動作阻止 (またはプロセス エンベロープ) やコマンド ライン ベースのプロテクションといった防御策が成熟し始めるにしたがって、いくつかのLOC技術はすたれていく可能性があります。攻撃的動作阻止では、プロセスに関する属性データをキャプチャーし、動作主体が処理しターゲットにするイベント チェーンを作ります。その後イベントを精査して、その動作チェーンが不正なものかどうか、またそのイベントは許可されるべきかどうかを判断します。

こういった技術は正当なものですが、その一方で、攻撃者が目標を達成するために潜行性を深める方法を開発する手助けともなってしまいます。しかし、ほとんどのセキュリティ専門家が十分認識しているように、攻撃者はたいてい、最も弱いパスを狙います。これを念頭に置けば、セキュリティ ベンダーと企業は、この戦いで優位に立てる可能性が出てきます。

ヘッドラインニュースとなったファイルレス マルウェア

Emotet バンキング型トロイの木馬
金融機関を対象としたこのサイバー攻撃は、大規模なスパム作戦を行い世界中に蔓延しました。だまされたユーザーはマイクロソフトのワード文書をダウンロードさせられ、これがPowerShellマクロを起動して、システム上にマルウェアをダウンロードしインストールします。[4]

Golden Dragon
これは、2018年冬季オリンピックに関係した組織を対象としたファイルレス攻撃です。この攻撃は、Golden Dragonという名前で知られるPowerShell「インプラント」を介して起動し、その後継続的に活動します。このインプラントは最初は予備調査ツールとして活動して、対象システムの分析をします。そして基礎的なシステムデータを暗号化して不正なコントロールサーバーに送信します。PowerShellコードは一度実行されると、攻撃を継続させるために、コントロールサーバーからペイロードをダウンロードし続けます。またこの攻撃は、マルウェア対策製品のプロセスを確認してそのプロセスを終了させてしまうので、追跡が困難です。[5]

ファイルレス マルウェアとの攻防:先を見越した対策

ファイルレス攻撃への効果的な防御には、2つ必要なものがあります:

- **状況を把握し計測する能力:**攻撃に使用された技術を識別し、PowerShellまたはその他のスクリプト エンジンでのアクテビティを監視し、集合的脅威データにアクセスし、ユーザー アクテビティを可視化します
- **標的となったシステムの状況をコントロールする能力:**任意のプロセスを停止し、攻撃の一部となっているプロセスを修正し、感染したデバイスを隔離します

従来のほとんどのエンドポイント セキュリティ技術ではこういったエリアに対応しきれず、また「特効薬」のような一点集中の製品は全体の動きを考慮に入れていません。ファイルレス攻撃は、より大きな一連の活動に組み込まれた戦術、技術、手順 (TTP) です。ファイルレス攻撃への有効な対策のカギとなるのは、脅威ライフサイクル全体 (攻撃のすべての段階) に対応する、保護、検知、修正の統合的アプローチを、攻撃前、攻撃中、攻撃後も継続して実行することです。防御戦略は、大まかに言うと、以下に集中させるべきです:

- 攻撃され得る入り口を減らす
- 不正な動作を可視化する
- 迅速かつ柔軟な方法で大規模な対処を実施する

先進的なサードパーティのセキュリティ　ベンダーは、ほとんどのOSプロバイダーより優位に立っていて、安定した抑制と均衡を提供して顧客のセキュリティ方針を改善させています。ファイルレス攻撃に対応する機能を持つ回復力の高いエンドポイント セキュリティ アーキテクチャを作るには、様々な機能が必要になります。

- **エンドポイント強化:**ファイルレス攻撃はエンドポイントを起点としているので、脆弱性評価、セキュリティ上の弱点やメモリの保護、デスクトップ ファイアウォール、URLフィルタリングなどの重要な防御策を採用することによって、攻撃される入口を最小化し、まず第一に攻撃を受けないようにします。
- **属性強化:**適応能力の高い「バルクヘッド」は、アプリケーションが認証されホワイトリストのものであったとしても、攻撃対象となったアプリケーションのプロセスを上書きし、実行を防ぐ属性を有効化します。
- **機械学習:**人による分析には限界があるので、機械学習を活用して、カスタムビルドのペイロードの実行前後に分析を行い、二次的なゼロデイ ペイロードの実行を防ぎます。
- **アプリケーション隔離:**アクセス保護ルールを用いて、攻撃対象となったアプリケーションによる他システムの乗っ取りを防ぎ、侵入地点のセキュリティ上の弱点が拡大しないようにします。
- **動作監視:**正しいアプリケーションで発生した問題を検知することは非常に重要です。これにはプロセス インジェクションや水平方向へのネットワーク操作などといったTTPの識別を含みます。
- **インタラクティブ脅威ハンティング:**エンドポイント検出・対応ツール(EDR)は、自動的かつプロアクティブにエンドポイントの異常動作の調査と対応をし、ファイルレス攻撃の足掛かりとなっているものを探すことができます。このタイプの先進技術を用いると、数秒で結果が出せ、また、対象となったシステムだけでなくインフラストラクチャ全体の大規模な調査が可能になります。

- **フレキシブルな対応:**リアルタイムに何千ものエンドポイントにわたって対応できる能力が不可欠です。敏速かつ適応力のある対応メカニズムには、エンドポイントの封鎖と検疫機能があり、攻撃を食い止め、ファイル、ネットワーク、およびプロセスの復旧をサポートします。
- **早期検知と復旧:**EDRおよびその他の脅威探索ツールは、セキュリティ情報およびイベント管理(SIEM)、ユーザー／エンティティ挙動分析(UEBA)、および機械学習などの、セキュリティ オペレーション センター (SOC) をサポートする技術と組み合わせると、ファイルレス攻撃にあった場合に発見を早め、迅速な是正処置ができるようになります。
- **単一コンソールの集中管理:**統一プラットフォームでセキュリティ管理をして効率化することで、企業全体で何百、何千もあるノードのコントロール、可視化、レポーティング、実用的ダッシュボードの利用が可能になり、防御上の抜け穴を最小化でき、プロセスが合理化され、対応時間は短くなります。
- **パートナー技術との統合:**セキュリティ　ベンダーは、エンドポイント セキュリティを越えた先進技術を持つサードパーティパートナーとの密接な統合をし、侵入者に打ち勝つための優位性を提供します。セキュリティ エコシステム全体が幅広く、よりよく連携されていればいるほど、ファイルレス攻撃に対抗する能力が高くなります。

まとめ

ファイルレス攻撃を効果的に遮断するには、脅威ライフサイクル全体をカバーする、複数の層にわたった統合アプローチが必要になります。ファイルレス攻撃との闘いは困難に見えるかもしれませんが、ファイルレス攻撃とは、より大きな、より複雑な一連の攻撃の一部である戦術カテゴリーの一つであるということを覚えておいてください。一つの対策だけでは不十分です。真に効果的な防御には、包括的かつ総体的なアプローチが必要です。これには、規模拡大が可能なこと、また求められた時と場所で適切な措置を迅速に実施することが求められます。

1. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
2. http://www.zdnet.com/article/fileless-attacks-surge-in-2017-and-security-solutions-are-not-stopping-them/
3. 2017年12月 McAfee Labs 脅威報告:https://www.mcafee.com/jp/about/newsroom/press-releases/press-release.aspx?news_id=20171217005042
4. https://securingtomorrow.mcafee.com/mcafee-labs/emotet-downloader-trojan-returns-in-force/
5. Golden Dragon https://securingtomorrow.mcafee.com/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/

マカフィーについて

マカフィーはデバイスからクラウドまでカバーする、サイバーセキュリティ企業です。協力から生まれるパワーに触発され、世界を安全な場所にするためにビジネスおよびコンシューマー向けのソリューションを創出しています。マカフィーは他社製品とコラボレーションするソリューションを提供し、お客様企業を脅威から保護し、その検知や是正を同時に、協力して行えるような、真に統合されたサイバー環境を構築するサポートをしています。コンシューマー向けではすべてのデバイスを保護して、ご自宅や出先での安全なデジタル　ライフスタイルをサポートしています。他のセキュリティ企業と協業し、マカフィーはすべての人の利益のために、団結してサイバー犯罪者に対抗する取り組みを牽引しています。

www.mcafee.com/ja.

McAfee™
Together is power.

〒150-0043
東京都渋谷区道玄坂1-12-1
渋谷マークシティウエスト20F
www.mcafee.com/ja