「先読みする防御」が見据える次の脅威

ファイルレスマルウェアから守るセキュリティ技術

2017 年 9 月

株式会社ＦＦＲＩ

OS の進化による便利な機能は、サイバー犯罪者にも狙われる

OS のバージョンアップにより追加される新機能の多くは、ユーザーの利便性を向上させます。しかし、こうした新機能はサイバー犯罪者も研究しており、マルウェア感染などに悪用できないか模索しています。

例えば以前の Windows に付属していたメールソフト「Outlook Express」では、本文のプレビュー機能が搭載されていました。確認したいメールを開かなくても内容が表示される便利な機能でしたが、この機能はウイルスを自動実行するワームに悪用され、世界的に感染が拡大したため、現在ではなくなっています。このように、OS の新機能はユーザーだけでなく、サイバー犯罪者にも有益となるケースもあるのです。

Windows では近年、PowerShell が標準化されました。これはコマンドラインツールを拡張したもので、1000 以上のコマンドに対応します。つまり、Windows のほとんどの操作を PowerShell で行うことができます。2016 年には PowerShell のオープンソース化と Linux、Mac OS 対応が発表されています。しかし、PowerShell の OS 標準化は、まさに攻撃者にとっても便利なツールとなってきており、マルウェアとして利用されるケースも増えてきました。

PowerShell スクリプトを利用したファイルレスマルウェア

PowerShell を悪用してマルウェアに感染させようとする攻撃は、2016 年頃から急激な増加傾向が見られています。2017 年初頭には標的型攻撃メールで確認され、その後はいわゆる「ばらまき型」メールでも確認されており、実際に FFRI にも届いています。メールの件名には「請求書」など日本語が使用され、本文の日本語もかなり正確なものになっています。明らかに日本を狙った攻撃といえるでしょう。

こうした攻撃は日本だけでなく、世界規模で発生しています。例えば、米国、フランス、エクアドルなど 40 カ国の銀行、政府機関、電気通信会社をはじめとする 140 社以上の企業や組織が影響を受けたとカスペルスキーが伝えています。このうち銀行のケースでは、ソフトウェアと PowerShell を組み合わせることでシステム管理者のパスワードを盗み出していました。

（関連記事：Fileless Memory-Based Malware Plagues 140 Banks, Enterprises : https://threatpost.com/fileless-memory-based-malware-plagues-140-banks-enterprises/123652/）

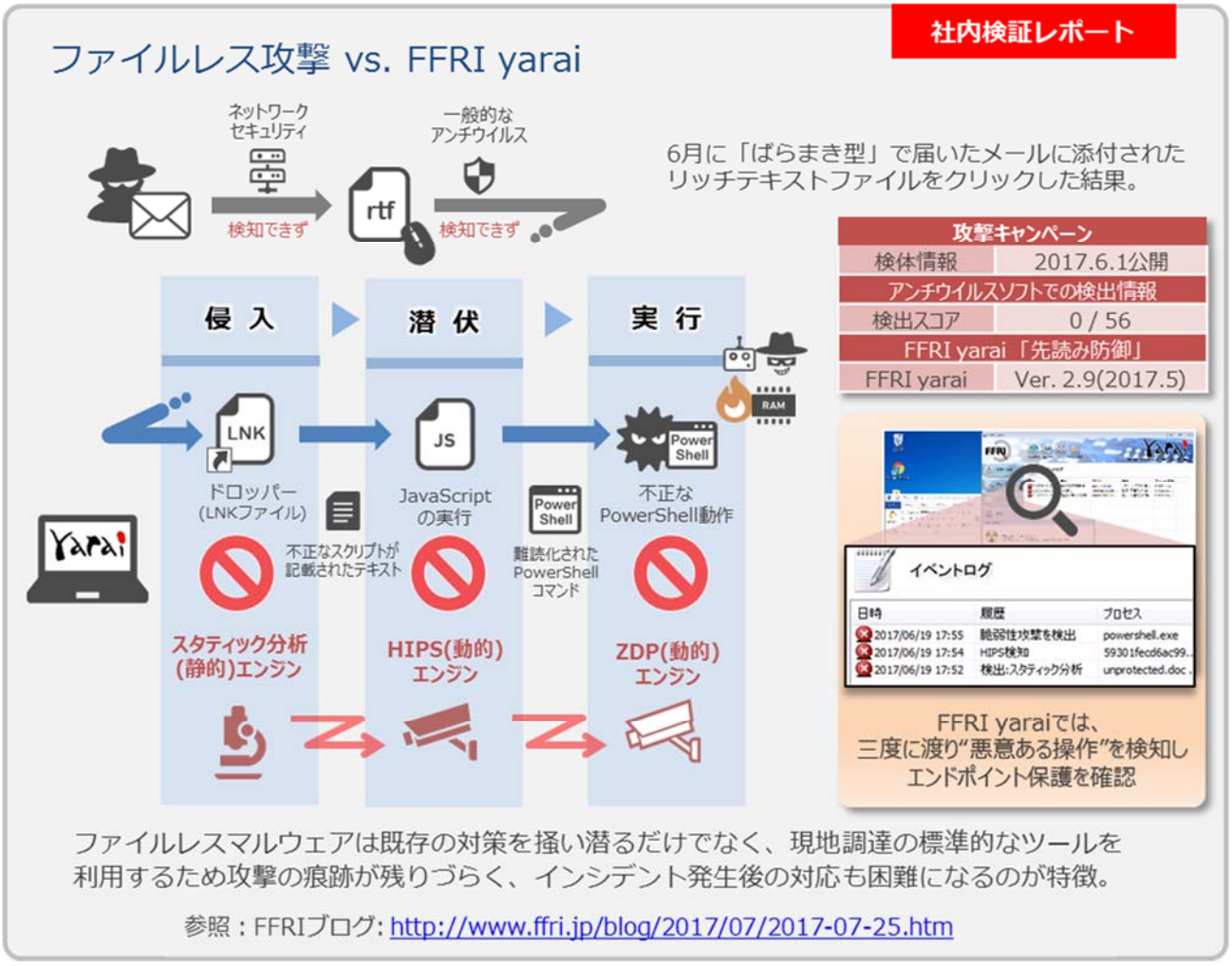
日本で実際に行われた標的型攻撃では、リンクファイル（拡張子.lnk）を起点として PowerShell スクリプトを呼び出すというものでした。実行ファイル（拡張子.exe）を使用しないため、「ファイルレスマルウェア」と呼ばれています。

ファイルレスマルウェアに対して、セキュリティ対策ベンダーは非常に重大な問題として受け止めています。ファイルレスマルウェアは、現時点では一般的なウイルス対策ソフトでは検知が難しくなっています。リンクファイルに記載されるスクリプトの場合も亜種の作成が行い易く、一般的なウイルス対策ソフトのパターンマッチング技術では検知が困難です。

リンクファイルには、OS 標準の PowerShell コマンドと、エンコードされた引数が設定されており、このエンコードされた引数こそが PowerShell にて悪意ある動作を行うためのスクリプト本体となっていました。また、その後のプロセスそのものは正規のものとして扱われ、マルウェアはその正規プロセス内のメモリ上で動作します。これにより、ディスク上にマルウェアを生成することなく、PC にマルウェアを感染させることができるわけです。

PowerShell は非常に強力なツールであるがゆえに、攻撃にも有用であり、従来の実行ファイル型マルウェアと同等の機能を実現できてしまいます。また、前述のように実行ファイルを使わないため、従来型のアンチウイルス製品に検知される可能性を下げる効果も期待できます。さらには、ファイルレスマルウェアはディスク上に痕跡が残りづらいため、検体の入手が困難です。ファイルレスマルウェアによる被害はすでに世界中で発生しているので、早急な対策、対応が求められています。

現状、ファイルレスマルウェアとしては JScript（拡張子.js）ファイルや Office マクロ（拡張子.docx）等のファイルを使ったものや、リンクファイルを使ったものなど多種多様なものがあります。また、今後、さらに増加する可能性があります。



今後想定される、ファイレスマルウェアのさらなる進化

現時点では、ファイルレスマルウェアといっても、アタックベクタとして実行ファイル型のドロッパーを介するものや、JScript、マクロ、リンクファイルといった、何かしらのファイルを実体として持っているケースが多くなっています。そのため、それらをファイルとして検知することで、対応できる可能性があります。

これに脆弱性攻撃を組み合わせた場合、完全に実体を持たないマルウェアとなります。Windows や Office、あるいは Adobe Flash Player、Adobe Acrobat といった Adobe 製品、Java SE、ブラウザやそのプラグインなどの脆弱性は毎月のように公開されています。これらの脆弱性を悪用した攻撃が成功した場合、任意のプロセスを起動することが可能となるでしょう。

このとき、PowerShell に悪意ある引数（スクリプト本体）を指定することで、脆弱性を持つブラウザや OS 標準プロセスから、悪意あるスクリプトを直接起動できます。このような攻撃が成功してしまった場合、ファイルとしての実体がないゆえに検体が残らず、インシデント対応としてのフォレンジックの難易度も格段に上昇します。非常に厄介な攻撃が実現することになってしまうのです。

また、サーバーソフトウェアを狙われたり、外部の Web サイトを改ざんしてスクリプトを埋め込むことで、フィッシングメールを介さず、正規サイトへのブラウザアクセスを行っただけで、ファイルレスマルウェアに感染させることができる可能性もあります。

攻撃シーケンス上流でのブロックが重要

では、このようなファイルレスマルウェア、あるいは今後登場すると思われる新たな攻撃手法に対し、どのような対策をすればいいのでしょう。

マルウェアを利用した攻撃では、様々なアタックベクタがあります。それは、スクリプトのメール添付であったり、インターネット上からブラウザの脆弱性を突くものなど、多岐にわたります。このとき、可能な限り入口に近い、攻撃シーケンスの上流でマルウェアをブロックすることが望ましいとされています。東京電機大学から「イベントツリーとディフェンスツリーを併用した標的型攻撃に対するリスク分析手法の提案と適用（相原遼，石井亮平，佐々木良一 東京電機大学）」という論文が公開されています。

この論文によると、対策コストとリスクのバランスを考慮した場合、トータルコストでは攻撃シーケンスの上流でのブロックに重点を置いたエンドポイント型セキュリティ対策が最も費用対効果が高いことが判明しています。攻撃シーケンスが進むほど、発見した後のコストは増大する傾向があり、フォレンジックが必要になるというレベルから、損害賠償に発展するレベルにまで影響が及ぶ場合があります。

つまり、サイバー攻撃が次の段階に進む前のできる限り早期に発見し、対処を行うことが必要としています。そのためには、入口対策・内部対策・出口対策のいずれか一種類のみでは対応できませんし、結果的にコストを大きく削減することはできません。論文では、攻撃の初期段階で防御する可能性を高める入口対策は、かけられる対策コストに関わらず有効な対策となること。そして、エンドポイント型のセキュリティソフト等の入口対策は、費用対効果が高い選択肢であると結論づけています。

ファイルレスマルウェアなど新たな攻撃も検知する「FFRI yarai」

PowerShell を悪用するファイルレスマルウェアは、一般的なウイルス対策ソフトでは検出できません。では、「FFRI yarai」はどうでしょう。FFRI では、2009 年から標的型攻撃に特化したエンドポイント型セキュリティ対策製品を出荷しており、多くの官公庁や企業で利用が広がっています。

一般的なウイルス対策ソフトは、定義ファイルによるパターンマッチングを主軸にマルウェアを検知しています。定義ファイルは実際のマルウェアを分析して作成されるので、新種のマルウェアには対処できません。

さらに、最近では AI 等の学習機能を搭載した次世代型のウイルス対策ソフトも登場していますが、これらも実行ファイルに特化していますし、ファイルレスマルウェアに対応するには膨大なファイルレスマルウェアのデータを与えて学習させる必要などいくつかの課題があり、早急な対策には間に合わないでしょう。　一方、「FFRI yarai」は、5 つの振る舞い防御エンジンを搭載しています。まず「ZDP エンジン」は、メールや Web ページ閲覧時の攻撃など、既知・未知の脆弱性を狙ったウイルス攻撃を防御します。「Static 分析エンジン」は、複数の分析機能によって、プログラムを実行させることなくマルウェアを検知します。「Sandbox エンジン」は、PC を再現した仮想環境上でプログラムを実行することでマルウェアを検知します。「HIPS エンジン」は、実行中のプログラムを監視し、悪意ある挙動を検知します。「機械学習エンジン」は、FFRI が収集したマルウェアに関するビッグデータをもとに、実行中のプログラムを監視し、機械学習で分析した特徴から悪意ある挙動を検知します。

最新版の「FFRI yarai v.2.9」では、ファイルレスマルウェアへの対策をさらに強化しています。例えば PowerShell マルウェアの場合、「Static 分析エンジン」によりリンクファイル自体の検知も可能であり、リンクファイルを使わずに PowerShell が動作した場合であっても、「HIPS エンジン」によって、その動作をリアルタイムに監視することで、不正なスクリプトの実行をブロックできます。

また、アタックベクタが脆弱性攻撃に進化したとしても、「FFRI yarai」には未知の脆弱性攻撃をブロックできる「ZDP エンジン」がもともと備わっています。

「FFRI yarai」により強化された入口対策では、多様なアタックベクタに対応し、攻撃シーケンスの上流で攻撃を食い止め、実被害を最小限に留めることが可能となっているのです。

株式会社ＦＦＲＩ
〒150-0013　東京都渋谷区恵比寿 1-18-18
東急不動産恵比寿ビル 4 階
TEL:03-6277-1811　E-mail：sales@ffri.jp
http://www.ffri.jp/

FFRI yarai の導入事例、防御実績は、ホームページからご確認いただけます。

http://www.hitachi-systems.com/solution/s105/yarai/