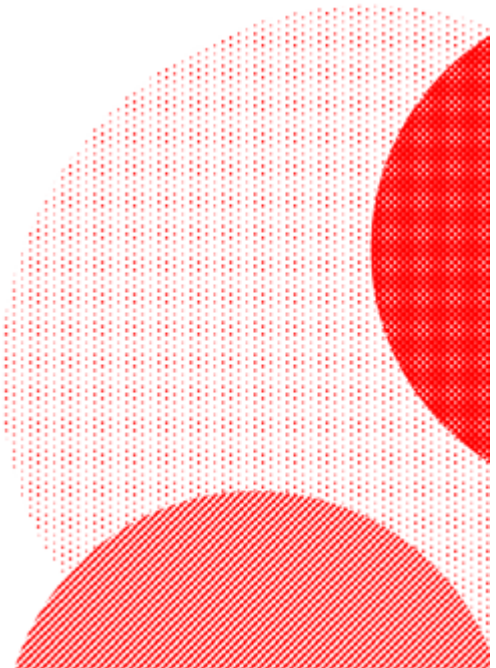
高度なマルウェアに対抗する
次世代アンチウイルスソフト

2017年8月

FFRI North America, Inc.
株式会社ＦＦＲＩ



高度なマルウェアとファイルレスマルウェア

高度なマルウェアとは、感染、制御、データの流出、ペイロードの実行をするための高い機能性を備えた、持続的なマルウェアのことです。クライアント側での攻撃として最大の脅威となるのが高度なマルウェアです。

ファイルレスマルウェアは、個人レベルの攻撃で、攻撃対象のPCに秘密裏に侵入および感染します。これにより、攻撃者は従来のシグネチャベースのセキュリティツールやフォレンジックツールをかいくぐり、システムを操作できるようになります。ファイルレス攻撃は、近いうちに従来型の「ディスクへの書き込み」を行う攻撃にとって代わり、従来のアンチウイルスソリューションを効果がなく、役に立たないものにするでしょう。

「現在、ファイルレスマルウェアは、最大のリスクであると考えます」と、
Moor Insights & Strategy社のパトリック・ムーアヘッド氏は述べています。「これまで、ファイルレスマルウェアによって攻撃者たちはすでに大きな成功を収めています。また、ファイルレスマルウェアへの感染は非常に検知しにくく、現在大流行しています。ファイルレスマルウェアによる被害は今後ますます増大するでしょう。」

高度なマルウェアの脅威が増大

2017年、ファイルレスマルウェアは世界の主要なネットワークにおいて最大の脅威となっています。1月と2月だけでも、さまざまな分野のグローバル企業140社がファイルレスマルウェアの被害を受けました。

「現在のマルウェア対策ソリューションの多くは、このような新しいタイプの攻撃を検知したり、攻撃に対応したりすることができないため、これらの攻撃は重大なリスクをもたらします」と、TIRIAS Research社のジム・マクレガー氏は述べています。「社内のIT部門は、ソリューションをすぐにはアップグレードしないため、新しいタイプの攻撃にさらされやすいことを覚えておく必要があります。また、顧客データ、財務情報、メールなどの貴重な情報を保持している可能性が高い、規模の大きな企業が先に狙われやすくなっています。」

企業は、増大する脅威を認識し、あらゆるタイプの高度なマルウェア攻撃にさらされる機会を減らし、防止することで、自社を守る必要があります。しかし、企業の多くは、高度なマルウェアをほとんど検知できない古いアンチウイルスソフトにいまだに頼っています。高度なマルウェア攻撃への対策ができていない企業は危険にさらされており、甚大な損失と損害を発生させる侵入の被害を受けやすい状態になっています。

ファイルレスマルウェア攻撃に対する警告

報道によると、2016年の大統領選挙期間中にロシアが米国の民主党全国委員会に対してハッキングを行っています。この攻撃では、ファイルレスマルウェアおよびフィッシングメールが使用され、特定の人物や組織を標的とした機密情報の入手や不正アクセスが目的となっていました。

米国国土安全保障省およびニュージャージー州サイバーセキュリティ・通信統合対策グループ（以下、NJ対策G）は、このような攻撃に対して警告しています。

(https://ics-cert.us-cert.gov/s tes/default/files/documents/NCCIC_ICS-CERT_AAL_Malware_Trends_Paper_S508C.pdf)

(https://www.cyber.nj.gov/threat-analysis/fileless-evasive-intrusion-tactics-pose-challenge-for-network-defense)

2017年3月の報告書では、「ファイルレスおよび非マルウェア型の侵入手法が、公的組織および民間組織の両方のリスクを高め、進行中のスパイ行為や将来的な妨害行為を支援するためにデータを盗んだり、ネットワーク上にパーシスタンスを設定したりする、脅威となりうる攻撃者によって使用されることが増えるとNJ対策Gは確信している」と記載されています。

またNJ対策Gは、現在ほとんどの組織が、ファイルレス攻撃に対する防御策を講じていないとも報告しています。

このような高度なマルウェア攻撃は勢いを増していますが、サイバーセキュリティ業界においては新しいものではありません。

ファイルレスマルウェアは21世紀よりも前に存在していました。しかし、実際にセキュリティ業界やメディアの注目を得たのは、2001年にCode Red、2003年にSQL Slammerが発生し、サービス妨害攻撃（DoS攻撃）の原因となってからです。

Code RedとSQL Slammerは、どちらもファイルレスマルウェアであり、どちらも甚大な被害をもたらしメディアを騒がせました。

ファイルレスマルウェアは定期的に姿を現していましたが、最近、攻撃者たちの間でこれまで以上に人気となり始めました。

「ファイルレスマルウェアはいまだに比較的新しく、残念ながら我々はほとんどの場合、対策できていません」と、独立系テクノロジー業界アナリストのジェフ・カーガン氏は述べています。

「問題は、今、ファイルレスマルウェアが急速に成長し、広がり始めているということです。ファイルレスマルウェア攻撃はフィッシングメールや
Word文書の形式であることも多いため、企業は危険にさらされています。一度ファイルを開くと、感染してしまうのです。」

ファイルレスマルウェアはこれまでも存在していましたが、なぜいまだに防御が困難なのでしょうか。

FFRI yaraiで見えない敵と戦う

見えない敵と戦うことは不可能に見えますが、FFRI yaraiなどの次世代のエンドポイントソリューションは、クライアントごとに挙動を分析するヒューリスティック検出技術により、それを可能にしています。ランサムウェアなどの、特定のタイプの高度なマルウェアには、すべての感染において共通する特徴的な挙動が存在します。FFRI yaraiは、ヒューリスティックベースのエンドポイントセキュリティによってこれらのパターンを識別し、挙動ベースの脅威を阻止することで、エンドユーザーが手動でプロセスを承認する時間を確保します。つまりFFRI yaraiなら、ペイロードがすべて送られる前に脅威を効果的に阻止できるのです。

「攻撃は著しく増大し、拡大しています」とFFRI North America, Inc.のCEO、パブロ・ガルシア氏は述べます。

またガルシア氏は、「高度なマルウェアを検知するには、マルウェアについて詳しく知る必要があります」と述べています。「マルウェアの防御を行うには、新たなアプローチが必要となるため、このような高度な攻撃に対応するソフトウェアを提供するセキュリティベンダーは非常に少ないのが現状です。」

従来のアンチウイルスソフトは、予防するというよりは、問題が起きてから対応するタイプのソフトウェアです。それらは、ハードドライブに書き込まれた既知の特徴やシグネチャのデータベースに依存しています。

FFRI yarai（http://www.ffri.jp/）は独自の方法を採用しており、プログレッシブ・ヒューリスティック技術および機械学習などの高度な手法により、典型的なマルウェアのシグネチャを探すのではなく、挙動を分析します。

「FFRI yaraiは、攻撃が始まる前に自動的に攻撃を阻止します」と、パブロ・ガルシア氏は述べています。「FFRI yaraiは機械学習を使用して攻撃の予兆となる挙動の変化を検知します。これにより、出回っているマルウェアのうち、まだ識別されていないマルウェアの攻撃さえも検知することができます。FFRI yaraiは、悪意ある攻撃の挙動と特徴を見極めることができます。FFRI yaraiのプラットフォームは、サードパーティーがその情報を一般に公開するよりもずっと前に、100件を超えるゼロデイ攻撃を阻止しています。これは、企業のセキュリティを維持するために非常に重要です。」

「FFRI yaraiのエージェントは、五つの目的別検知エンジンを使用して、最先端のサイバー攻撃を特定、阻止、および隔離します。FFRI yaraiの多層構造の先読み防御技術は、高度な脅威の特定と阻止を実現する上で重要です。」

「FFRI yaraiは、シグネチャに依存しません。脅威は常に姿を変え、変化しているからです」とガルシア氏は述べます。「マルウェアの名前も攻撃も変化するのです。現代において、マルウェアは常に懸念事項となっています。高度な攻撃の『襲来がくるか、どうか』の問題ではなく、『いつ発生するか』の問題なのです。攻撃を仕掛けてくる攻撃者にとって、高度な攻撃は純粋に的当てゲームなのです。世界には高度な攻撃を行う狡猾な人間が存在するため、常に用心する必要があります。」

FFRI yaraiの顧客事例

エマーソン・スタンプ氏は、先進技術、システムおよびコンポーネントを誇る世界最大級の自動車部品メーカーの1つであるDENSO Products and Services America, Inc.社（米国カリフォルニア州、ロングビーチ）のネットワークアシスタントマネージャーです。

迫り来る脅威の一歩先をいくため、スタンプ氏はFFRI yaraiのセキュリティソフトウェアを検討していました。また、IT部門の時間と労力を減らしたいと考えていました。

「高度なマルウェアは、しばらくの間問題になっていましたが、この2、3年で、本当にビジネスに影響を与える問題となりました」と、自動車部品会社で過去17年間勤務してきたスタンプ氏は述べています。「弊社の標準的なウイルス対策パッケージでは十分ではありませんでした。」

スタンプ氏は、同社は従来のアンチウイルスソフトを使用しており、まだ特に高度なマルウェアの攻撃は受けていないものの、それは2人のネットワーク管理者が毎日3～4時間かけてネットワークを保護しているからであると話しました。

「弊社では、阻止しなければならない驚異の一歩先を歩み続けるために、ネットワーク管理者に長時間にわたって調査してもらっていました」と、スタンプ氏は言います。「添付ファイルやメールにも対応していました。ネットワーク管理者は、これらの作業で頭がいっぱいでした。ウイルス対策パッケージでは十分ではないのです」と、スタンプ氏は付け加えました。

FFRI yaraiを導入する前は、DENSO Products and Services America社のネットワーク管理者は、高度なマルウェア攻撃からシステムを保護するために貴重な時間を費やしていました。FFRI yaraiの導入後は、ヘルプデスクへのお問い合わせ対応や、トレーニング、品質検査を行う時間が増えました。

製品テストでは、DENSO Products and Services America社のITチームはマルウェアとランサムウェアをローカルエリアネットワーク（LAN）上で動作させ、FFRI yaraiにより新製品のリリーステスト中に動作した25のペイロードをすべて阻止しました。

「FFRI yaraiは私たちにとって最適なソフトウェアです」と、2016年10月からFFRI yaraiを使用しているスタンプ氏は言いました。「FFRI yaraiは、弊社で使用しているウイルス対策パッケージとともに問題なく動作しています。また、ほかのプログラムと競合することもありません。FFRI yaraiは、実際に問題が発生するリスクを減らしています。」

これにより、ネットワーク管理者の時間と労力も節約できています。

「現在、弊社では1人のネットワーク管理者だけで、何が起こっているかを監視しています」と、スタンプ氏は述べます。「日常業務の邪魔になることはありません。何か異常があればレポートが作成されます。本当に、本当に素晴らしいです。FFRI yaraiは、間違いなく弊社の頭痛の種と、マルウェア攻撃への対応に必要だった工数を減らしてくれました。」

「FFRI yaraiのおかげで、より強固なセキュリティが手に入りました」

FFRI yaraiの導入事例、防御実績、販売パートナーはホームページからご確認いただけます。

http://www.ffri.jp/products/yarai/index.htm

FFRI North America, Inc.
65 Enterprise 3rd Floor
Aliso Viejo, CA 92656
Email:sales@ffri-inc.com

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/