ソリューション概要

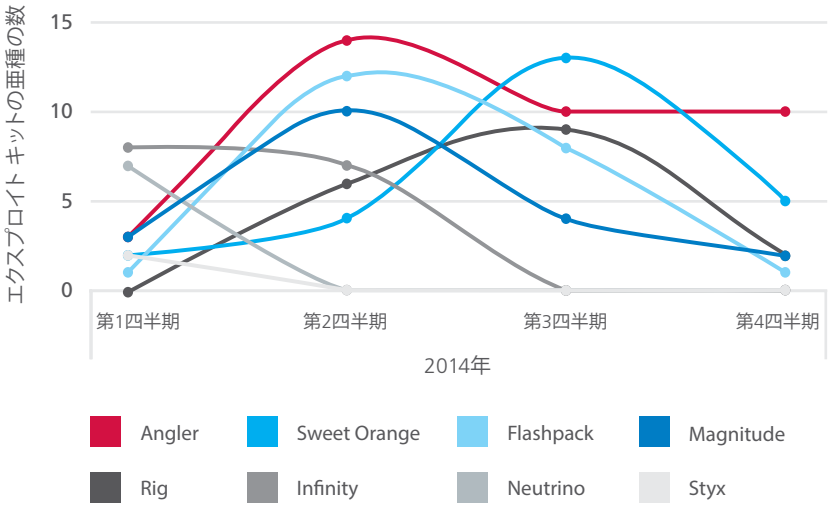
Anglerエクスプロイト キットに対する対策

エクスプロイト キットはすぐに使用できるソフトウェア パッケージで、既知の脆弱性や未知（ゼロデイ）の脆弱性を簡単に攻撃することができます。これらのツールキットはクライアント側の脆弱性を攻撃し、主にWebブラウザーやブラウザーからアクセス可能なプログラムを狙います。エクスプロイト キットは感染状況を確認したり、感染先のマシンを自由に操作する可能性もあります。

Anglerエクスプロイト キットとは

Anglerエクスプロイトについては、『**McAfee® Labs脅威レポート: 2015年2月**』に詳しい解説があります。Anglerが注目を集め始めたのは2014年の後半です。このキットはファイルレスの感染（メモリー インジェクション）、仮想マシン、セキュリティ製品の検出回避などの機能を搭載し、配布するペイロードも、オンラインバンキングを狙うトロイの木馬、ルートキット、ランサムウェア、CryptoLocker、バックドアなど多岐にわたっています。Anglerは熟練した技術がなくても使用できます。オンラインの闇市場で簡単に入手できるため、マルウェア送信の手段としてよく利用されています。

エクスプロイト キットの亜種 (2014年)



出典: McAfee Labs, 2015

intel Security

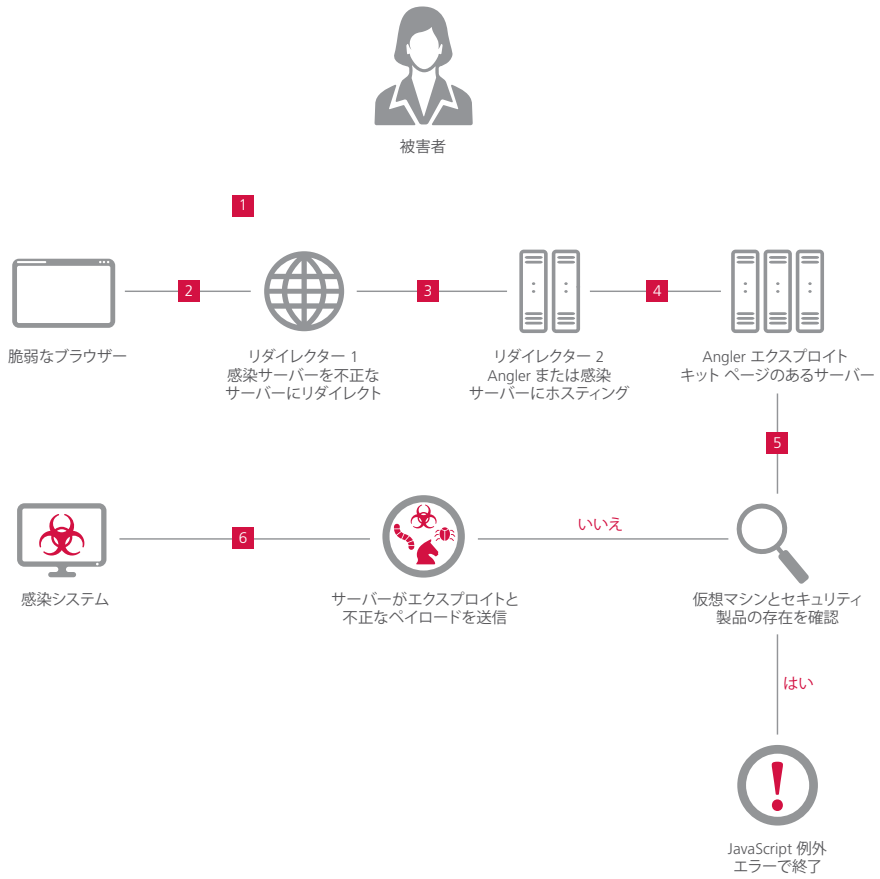
Anglerは、セキュリティ製品から自身の存在を隠すため、そのパターンとペイロードを頻繁に変えています。Anglerの主な特徴は次のとおりです。

- ランディング ページに到達する前にリダイレクトを2段階で行う。
- ランディング ページのあるWebサーバーには、1つのIPから1回しかアクセスできない。攻撃者はホストの監視を積極的に行っています。
- システムで仮想マシンとセキュリティ製品の存在を確認する。
- ガベージとジャンク コールのリバース エンジニアリングを難しくしている。
- ダウンロード時にすべてのペイロードを暗号化し、感染先のマシンで復号する。
- ファイルレスで感染する（メモリーに直接配備する）。

Anglerエクスプロイト キットがシステムに感染するまでの流れは次のとおりです。

- 被害者が、感染したWebサーバーに脆弱なブラウザーからアクセスします。
- 感染サーバーから中間サーバーに誘導されます。
- エクスプロイト キットのランディング ページのある不正なサーバーに移動します。
- このページで脆弱なプラグイン（Java、Flash、Silverlight）の存在とバージョンが確認されます。
- 脆弱なブラウザーまたはプラグインが見つかると、ホストがペイロードを送信し、マシンに感染します。

Angler エクスプロイト キットの感染チェーン



Anglerエクスプロイト キットを阻止する保護対策

Anglerエクスプロイト キットからシステムを保護する方法として、推奨事項をいくつか挙げておきます。

- 強力なスパム対策とフィッシング詐欺対策を実施しているセキュリティ意識の高いインターネット サービス プロバイダーを利用する。
- オペレーティング システムの自動更新を有効にするか、更新を定期的にダウンロードし、オペレーティング システムにパッチを適用して既知の脆弱性を解決する。ソフトウェア ベンダーが公開したパッチを速やかに適用する。トロイの木馬やスパイウェアの攻撃を防ぐには、すべてのパッチを適用したコンピューターをファイアウォールで保護する必要があります。
- 添付ファイルを開くときには十分に注意する。メールやインスタント メッセージの添付ファイルを自動的にスキャンするように、ウイルス対策ソフトウェアを設定しましょう。また、メール プログラムで添付ファイルを自動的に開いたり、画像を自動的に表示しないように設定し、プレビュー ウィンドウを非表示にしてください。未請求メールや予期しない添付ファイルは絶対に開かないでください。知人からのメールも例外ではありません。
- スパムを利用したフィッシング詐欺に注意する。メールやインスタントメッセージにあるリンクをクリックしない。
- ブラウザー プラグインを使用してスクリプトとiframeの実行をブロックする。

Anglerエクスプロイト キットから保護するIntel Securityのソリューション

McAfee Web Gateway

マルバタイジング、ドライブバイ ダウンロード、信頼されたWebサイトに埋め込まれた不正なURLは、Anglerエクスプロイト キットを配布する手口の一例に過ぎません。**McAfee Web Gateway**は、このような脅威を阻止し、会社の保護対策を強化する強力な製品です。

- **ゲートウェイを保護するマルウェア対策エンジン**: シグネチャを使用しない意図解析により、Webトラフィックから不正なコンテンツをリアルタイムで排除します。プロアクティブなエミュレーションと動作分析により、ゼロデイ攻撃や標的型攻撃を阻止します。McAfee Gateway Anti-Malware Engineはファイルを検査し、不正なファイルのダウンロードをブロックします。
- **McAfee Global Threat Intelligence（McAfee GTI）との統合**: McAfee Web Gatewayは、McAfee GTIからリアルタイムで提供されるファイル レピュテーション、Webレピュテーション、Webカテゴライゼーションにより、最新の脅威を阻止します。既知の不正なサイトに対する接続だけでなく、不正な広告ネットワークを使用しているサイトへの接続も拒否します。

McAfee VirusScan® Enterprise

McAfee VirusScan Enterpriseを使用すると、Anglerが散布するマルウェアを検出し、簡単に駆除することができます。McAfee VirusScan Enterpriseは、実績豊富なマカフィーのスキャン エンジンを搭載し、ウイルス、ワーム、ルートキット、トロイの木馬などの高度な脅威を阻止します。

- **攻撃からプロアクティブに保護**: マルウェア対策と侵入防止機能が統合され、アプリケーションのバッファー オーバーフローの脆弱性を攻撃するエクスプロイトを阻止します。
- **非常に強力なマルウェア検出・駆除機能**: 高度な動作分析により、ルートキットやトロイの木馬などの脅威を阻止します。ポート ブロック、ファイル名でのブロック、フォルダー/ディレクトリのロック、ファイル共有のロック、感染の追跡/ブロックなどの技術により、マルウェアの侵入を阻止します。
- **McAfee GTIの統合でリアルタイムのセキュリティを実現**: 市場で最も包括的な脅威情報プラットフォームにより、ファイル、Web、メール、ネットワークを介して侵入する脅威を検出します。既知の脅威だけでなく、新たに発生する脅威も阻止します。

McAfee Advanced Threat Defense

McAfee Advanced Threat Defenseは、複数の検出エンジンを統合し、多層型のマルウェア検出ソリューションを提供します。McAfee Advanced Threat Defenseは、シグネチャ ベースの複数の検査エンジン、レピュテーション ベースの検査、リアルタイムのエミュレーション、コードの完全な静的分析、動的サンドボックスを搭載し、Anglerなどのエクスプロイト キットとそれによって配備されるマルウェアを阻止します。

- **シグネチャ ベースの検出**: ウイルス、ワーム、スパイウェア、ボット、トロイの木馬、バッファー オーバーフロー、複合型の攻撃を検出します。McAfee Labsでは、豊富な経験と知識に基づき、1億5千万件を超えるシグネチャ（Anglerとその亜種も含む）を登録しています。
- **レピュテーション ベースの検出**: McAfee GTIネットワークからファイルのレピュテーションを取得し、新たに発生した脅威を検出します。
- **リアルタイムの静的分析とエミュレーション**: リアルタイムの静的分析とエミュレーション機能により、シグネチャベースの技術やレピュテーションでは識別できないマルウェアやゼロデイ脅威を迅速に検出します。
- **完全な静的コード分析**: リバース エンジニアリングでファイルのコードを解析し、その属性と命令セットを特定します。ファイルを実行せずにソース コードを分析します。包括的な解凍機能により、様々な圧縮ファイルを開いてコードの分析とマルウェアの分類を行い、特定のマルウェアがもたらす脅威を把握することができます。
- **動的なサンドボックス分析**: 仮想のランタイム環境でファイルのコードを実行し、動作を検証します。仮想環境は会社のホスト環境に合わせて設定できます。Windows 7（32/64ビット）、Windows XP、Windows Server 2003、Windows Server 2008（64ビット）、AndroidのカスタムOSイメージを使用できます。

McAfee Network Security Platform

McAfee Network Security Platformは、ネットワーク トラフィックを詳細に検査します。McAfee Network Security Platformは、完全なプロトコル分析、脅威レピュテーション、動作分析、高度なマルウェア分析などの高度な調査技術を搭載し、ネットワーク上の既知の脅威とゼロデイ攻撃を阻止します。

- **包括的なマルウェア対策**: McAfee GTIのファイル レピュテーション、JavaScriptの検査を含む詳細なファイル分析、シグネチャを使用しない高度なマルウェア解析により、ゼロデイ脅威、カスタム マルウェア、ステルス攻撃を阻止します。
- **高度な調査技術を使用**: 完全なプロトコル分析、脅威レピュテーション、動作分析機能を搭載し、ネットワーク上の既知の脅威とゼロデイ攻撃を阻止します。
- **McAfee GTIとの統合**: リアルタイムのファイル レピュテーション、IP レピュテーション、位置情報を組み合わせ、ユーザー、デバイス、アプリケーションに関するコンテキスト データを提供します。これにより、ネットワーク攻撃を正確に特定し、迅速に対応することができます。
- **Security Connected**: McAfee Network Security PlatformはMcAfee Advanced Threat Defenseと統合されています。監視対象のトラフィックで不審なファイルを検出すると、McAfee Advanced Threat Defenseに送信して分析を行い、その結果に基づいてトラフィックを拒否または許可します。

McAfee Threat Intelligence Exchange
情報プラットフォームは環境要件に合わせて拡張していく必要があります。**McAfee Threat Intelligence Exchange**を使用すると、環境内で実行される不明なファイルやアプリケーションなど、組織の脅威状況を正確に把握できます。これにより、攻撃のリスクを劇的に減らすことができます。

- **包括的な脅威情報**: グローバルなソースから総合的な脅威情報を収集できます。これらの情報ソースは簡単に調整できます。McAfee GTIだけでなく、サードパーティのソースも利用できます。エンドポイント、ゲートウェイ、その他のセキュリティ コンポーネントからリアルタイムで受信したローカルのイベント データや履歴データも使用できます。
- **実行防止と修復**: McAfee Threat Intelligence Exchangeは、環境内で不明なアプリケーションの実行を防止します。実行が許可されたアプリケーションが後で不正なプログラムと認識された場合、McAfee Threat Intelligence Exchangeは、強力な一元管理機能とポリシー施行機能により、アプリケーションに関連する実行中のプロセスを無効にします。
- **可視性**: McAfee Threat Intelligence Exchangeは、圧縮された実行ファイルを追跡し、環境内での最初の実行だけでなく、以降の動作も監視します。インストール後のアプリケーションやプロセスをすべて追跡するので、対応と修復を迅速に行うことができます。
- **侵害の兆候(IoC)**: 既知の不正ファイル ハッシュをMcAfee Threat Intelligence Exchangeにインポートしてポリシーを施行することで、これらの既知の不正ファイルから環境を保護できます。環境でIoCを確認すると、McAfee Threat Intelligence ExchangeがIoCに関係するすべてのプロセスとアプリケーションを終了します。

Anglerのように簡単に使えるエクスプロイト キットが増えています。脅威状況は常に変化しています。Intel Securityのテクノロジは Anglerエクスプロイト キットのような脅威からエンドポイントとネットワークの両方をプロアクティブに保護します。

McAfee. Part of Intel Security.
東京本社 〒150-0043 東京都渋谷区道玄坂 1- 12- 1 渋谷マークシティウェスト 20F TEL 03-5428-1100（代）FAX 03-5428-1480
西日本支店 〒530- 0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所 〒460-0002 愛知県名古屋市中区丸の内 3-20-17 中外東京海上ビルディング 3F TEL 052-954-9551（代）FAX 052-954-9552
福岡営業所 〒810- 0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674（代）
www.intelsecurity.com