ソリューション概要

パスワード盗用型マルウェアを阻止する

スマートフォンやタブレットが普及し、このような電子機器への依存度が高まっています。このため、サイバー犯罪者にとって認証情報は非常に重要な要素となっています。ほとんどの高度な持続型攻撃では、攻撃の早い段階でパスワードを盗み出しています。

パスワード盗用型マルウェアは、ネットワークやシステムのセキュリティを回避し、認証情報を取得しようとします。現在、パスワード盗用型マルウェアとして使用頻度の高いFareitを初めて確認したの5年前です。2012年に出現して以来、最新のサイバーセキュリティを回避するため、Fareitは進化を続けています。

当初、FareitはWebブラウザーからログイン情報を盗み出し、オンラインバンキングなどのアプリケーションにアクセスしたり、メール アカウントを乗っ取り、なりすましを行いました。その後、Fareitはより積極的に情報を盗み出すようになり、攻撃ごとにハッシュを変えるなど、高度な技術で自身の存在を隠すようになりました。2016年に確認されたFareitは、感染したネットワーク資産を悪用して分散型サービス攻撃を実行しました。現在、Fareitはサービスとして提供されるようになり、サイバー犯罪者はマルウェアの配布で金銭を稼いでいます。感染数が増えるほど、報酬が増える仕組みです。

この10年間で初期攻撃として最も多く実行されているのが、Fareitなどのパスワード盗用型マルウェアを配布するフィッシング詐欺です。

パスワード盗用型マルウェアを阻止するポリシーと手順

McAfeeでは、パスワード盗用型マルウェアの脅威から保護するために、次のことを推奨します。

- パスワード盗用型マルウェアは、マルウェアによって配布されています。マルウェア対策製品を常に最新の状態にしておくことが重要です。
- 警戒心の低いユーザーが閲覧中にマルウェアをダウンロードしてしまう可能性があります。Webブラウザーとアドオンを常に最新の状態にし、多層型の防御手段を講じる必要があります。

McAfee
Together is power.

- 管理者権限ではなく、権限が制限されているユーザーとしてアプリケーションを実行しましょう。
- ネットワークの境界を保護しましょう。攻撃者は、パスワード盗用型マルウェアに感染したアプリケーションに外部から接続を試みます。ファイアウォールを利用して、このようなアクセスを阻止しましょう。
- 会社の認証情報（インターネット閲覧時のWebプロキシ、データベース アプリケーション、共有フォルダーの認証情報）は、会社の資産にのみ使用しましょう。信頼されたネットワーク システムで、企業のITセキュリティ グループが承認していないシステムを使用してはなりません。
- 正規のソフトウェアをトロイの木馬に変え、パスワード盗用型マルウェアを埋め込む攻撃も発生しています。このような攻撃を阻止するため、ソフトウェアの配布方法を厳重に管理する必要があります。どの環境でも、企業のアプリケーションをリポジトリで一元管理し、そこから承認済みのソフトウェアをダウンロードするようにすると効果的です。
- ITセキュリティ グループで検証されていないアプリケーションのインストールをユーザーに許可する場合には、既知のベンダーが署名した信頼できるアプリケーションだけをインストールするように指示しましょう。オンライン上で無害に見えるアプリケーションにパスワード盗用型マルウェアが埋め込まれていることも少なくありません。
- Web以外の場所からアプリケーションをダウンロードしないようにしましょう。Usenetグループ、IRCチャネル、インスタント メッセージ クライアント、ピアツーピア システムは、マルウェアをダウンロードする可能性の高い経路です。また、IRCやインスタントメッセージに貼り付けられたWebサイトのリンクも、感染したダウンロードに誘導される危険性があります。
- フィッシング詐欺対策の研修を実施しましょう。パスワード盗用型マルウェアは、フィッシング詐欺攻撃で配布されます。

システムがパスワード盗用型マルウェアに感染した可能性がある場合には、次のようなベストプラクティスを実施して感染の拡大を防ぎましょう。

- アプリケーションが二要素認証に対応している場合には、二要素要素を有効にする。パスワードが盗まれても、侵入は防ぐことができます。
- エンドポイント ファイアウォールを使用する。ファイアウォール ルールで受信/送信トラフィックを制限することで、盗まれたパスワードを使った感染の拡大を防ぐことがっできます。

パスワード盗用型マルウェアを阻止するMcAfee製品

McAfee VirusScan® Enterprise 8.8またはMcAfee Endpoint Security 10

- 最新のパッチ、DAT、スキャン エンジンが使用されるように、エンドポイントのマルウェア対策を常に最新の状態に保ちましょう。McAfee Global Threat Intelligence（McAfee GTI）が使用されていることを確認しましょう。
- アクセス保護ルールを作成して、ランサムウェアのインストールを阻止します。次のKnowledgeBaseの記事を参照してください。
  - アクセス保護ルール: KB81095、KB54812
  - McAfee VirusScan Enterprise 8.8の設定に関するベストプラクティス: PD22940
  - McAfee Endpoint Security の設定に関するベストクラクティス: KB86704

McAfee Host Intrusion Prevention

侵入防止ツールだけではパスワード盗用型マルウェアの被害を防ぐことはできません。McAfee Host Intrusion Preventionを使用すると、パスワード盗用型マルウェアが潜むペイロードの拡散を防ぐことができます。

- IPSカスタム シグネチャを使用してルールを作成し、マルウェアによるファイル操作（作成、書き込み、不正なコードなど）を阻止します。
- svchost.exeがWindows以外の実行ファイルを実行しないように、McAfee Host Intrusion Preventionのシグネチャ3894を有効にします。
- McAfee Host Intrusion Preventionシグネチャ6010と6011を有効にし、インジェクションをすぐにブロックします。
- サブルールには次の2種類あります。
  1. Filesエンジンと次の条件のサブルールを使用してIPSカスタム シグネチャを作成します。
     - Name: <名前を挿入>
     - Rule type: Files
     - Operations: Create, Execute, Read, Write
     - Parameters: Include - Files - <マルウェアのパス/ファイル名>
       - ファイル名はパスにする必要があります。パスにワイルドカードを使用する場合には、ファイル名を “**\” または “?:\” で始めます。ドライブ名にワイルドカードを使用する場合には、“**\<ファイル名>.exe”、“?:\<ファイル名>.exe” のように使用します。
       - FilesパラメーターではMD5ハッシュを使用できません。使用できるのはパス/ファイル名だけです。
       - ドライブの種類を指定すると、特定のドライブへのパスに限定できます（例: ハードディスク、CD、USB、ネットワーク、フロッピーなど）。
     - Executables: ファイル操作を実行する特定のプロセス（explorer.exe、cmd.exeなど）にシグネチャを制限する場合を除き、何も指定する必要はありません。
  2. Programエンジンと次の条件のサブルールを使用して、IPSカスタム シグネチャを作成します。
     - Nama: <名前を挿入>
     - Rule type: Program
     - Operations: Run target executable
     - Parameters: <空白にします>
     - Executables: ソースの実行ファイルとして特定のプロセスにシグネチャを制限する場合を除き、何も指定する必要はありません。たとえば、explorer.exeがTarget Executable（notepad.exeなど）を実行しないように設定します。
     - Target Executables: ブロックする実行ファイルのプロパティを定義します。たとえば、notepad.exeの実行をブロックする場合には、この実行ファイルのパスとファイル名を指定します。1 つ以上の条件（ファイルの説明、ファイル名、フィンガープリント、署名者）を使用して、実行ファイルを定義します。

McAfee SiteAdvisor® EnterpriseまたはMcAfee Web Protection

- Webサイトのレピュテーションを使用して、パスワード盗用型マルウェアを配布するサイトの利用を阻止または警告します。

McAfee Threat Intelligence ExchangeとMcAfee Advanced Threat Defense

- McAfee Threat Intelligence Exchangeのポリシー設定:
  - 監視モードを開始します。エンドポイントで不審なプロセスを検出したときに、システム タグを使用してMcAfee TIE施行ポリシーを適用します。
  - 駆除: 既知の不正な項目
  - ブロック: 不正である可能性が非常に高い項目。レピュテーションが不明なファイルをブロックすると、保護対策は強化されますが、初期の管理作業が増えます。
  - レピュテーション レベルが不明以下の場合: Advanced Threat Defenseにファイルを送信します。
  - McAfee Threat Intelligence Exchangeサーバーのポリシー: McAfee Threat Intelligence Exchangeが送信していないファイル場合には、McAfee Advanced Threat Defenseのレピュテーションを使用します。
- Threat Intelligence Exchangeの手動操作:
  - ファイル レピュテーションの施行（動作モードによる）。不正な可能性が非常に高い: 駆除/削除
  - 不正な可能性がある。ブロック
- エンタープライズ レピュテーションでMcAfee GTIのレピュテーションを上書きできます。
  - たとえば、非対応または脆弱なアプリケーションの不要なプロセスをブロックします。
  - ファイルに「不正な可能性がある」というマークを付けます。
- テスト目的で不要なプロセスを許可します。
  - ファイルに「信頼できる可能性がある」というマークを付けます。

McAfee Advanced Threat Defense

- すぐに使える検出機能:
  - シグネチャ ベースの検出: McAfee Labsのデータベースに登録されたシグネチャ数は6億を超えています。
  - レピュテーション ベースの検出: McAfee GTI
  - リアルタイムの静的分析とエミュレーション: シグネチャ レスの検出で使用
  - カスタムYARAルール
  - 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、その属性と機能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。
  - 動的なサンドボックス分析。
- 分析用のプロファイルを作成し、パスワード盗用型マルウェアが実行される可能性が高い場所を特定します。
  - Windows 7、8、10などの一般的なオペレーティング システム.
  - Windowsアプリケーション（Word、Excel）をインストールして、マクロを有効にします。
- アナライザーを使用してインターネット アクセスを分類します。
  - サンプルの多くは、Microsoftドキュメントに含まれるスクリプトを実行し、外部に接続してマルウェアの攻撃を実行します。インターネットに接続する分析用プロファイルを作成すると、検出率が高くなります。

McAfee Network Security Platform

- McAfee Network Security Platformは、デフォルト ポリシーに定義されたシグネチャを使用して、パスワード盗用型マルウェア関連のファイル転送に使用されるTorネットワークを検出します。
- Advanced Threat Defenseとの統合で新しい亜種を検出します。
  - 詳細なマルウェア ポリシーでMcAfee Advanced Threat Defenseとの統合を設定します。
  - McAfee Network Security Platformが.exe、Microsoft Office、Java Archive、PDFファイルをMcAfee Advanced Threat Protectionに送信し、検査するように設定します。
  - McAfee Advanced Threat Defense Applianceの設定がセンサー レベルで適用されていることを確認します。
- コールバック検出ルール（ボットネット用）を更新します。

McAfee Web Gateway

- McAfee Web Gatewayのウイルス対策による検査を有効にします。
- McAfee GTIを有効にして、URLとファイルのレピュテーションを使用します。
- McAfee Advanced Threat Defenseと統合し、サンドボックスでゼロデイ脅威を分析します。

VirusTotal Convicter: 自動介入

- Convicterは、McAfee ePolicy Orchestrator®（McAfee ePO）の自動応答システムで実行されるPythonスクリプトです。McAfee Threat Intelligence Exchange脅威イベントを生成したファイルをVirusTotalで調査できます。
- GetSuspなど、他の脅威情報交換を参照するようにスクリプトを変更できます。
- コミュニティの信頼しきい値を満たしてれば、スクリプトはエンタープライズ レピュテーションを自動的に設定します。推奨のしきい値: ベンダーの30%と大手2社の同意が必要。
- フィルター:「Target file name does not contain: McAfeeTestSample.exe.」（対象のファイル名が次の項目を含まない: McAfeeTestSample.exe）
- これは無料のコミュニティ ツールです（McAfeeのサポートはありません）。

McAfee Active Response

- McAfee Active Responseは、高度な脅威を検出して対応します。McAfee Labs、Dell SecureWorks、ThreatConnectなどの脅威フィードと関連付けると、広範囲に拡散する前に新しい脅威を検出し、被害を未然に防ぐことができます。
- カスタム コレクターを使用すると、パスワード盗用型マルウェアの兆候を検出し、識別するツールを作成できます。
- トリガーや対応はユーザーが作成し、特定の条件下で実行されるアクションを定義します。たとえば、ハッシュまたはファイル名見つかったときに、削除アクションを自動的に実行します。

詳細情報

Phishing Attacks Employ Old but Effective Password Stealer（古いパスワード盗用型マルウェアを効果的に使うフィッシング詐欺）

Fareitウイルス プロファイル

Fareitウイルス プロファイル

McAfee Together is power.

マカフィー株式会社
〒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）
www.mcafee.com/jp