ソリューション概要

Pinkslipbotからの保護

W32/Pinkslipbotは、個人情報や銀行の口座情報を盗み出す自己増殖型のマルウェア ファミリです。このマルウェアは、制御サーバーを操作するコマンドベースのバックドアやVNCを利用するバックドアにより、感染先のコンピューターを完全に制御します。Pinkslipbotは、ネットワーク共有を介して環境内の他のシステムに拡散し、制御サーバーに接続して自身の更新をダウンロードします。

Pinkslipbotが最初に確認されたのは2007年ですが、このマルウェアの作成者は2、3か月ごとに更新を行い、新しいバージョンを公開してきました。

Pinkslipbotが盗み出した情報を利用すると、感染したシステムの場所を正確に特定できます。また、感染した組織や人物も特定が可能です。攻撃者はこの情報を第三者に売り渡し、支払いの確認後、標的型攻撃のマルウェアを感染先のシステムに配布する可能性もあります。特に、感染先が有名な組織や企業の場合、このような攻撃が実行される確率が高くなります。

Pinkslipbotの技術的な詳細については『McAfee Labs脅威レポート: 2016年6月』で解説しています。このレポートでは、初期の感染プロセス、拡散方法などの技術的な情報と防御策について説明します。

Pinkslipbotを阻止するポリシーと手順

以下では、Pinkslipbotを阻止するためのポリシーと手順について説明します。

境界を保護するには、ネットワークのすべての出口で未使用のポートを塞ぎ、不正であることが確認されているIPアドレスとの接続要求をブロックする必要があります。また、Pinkslipbotの移動を阻止するため、ネットワーク共有の使用を禁止する必要があります。さらに、Microsoft Windowsの自動実行機能を無効にする必要があります。Windows OSに最新のパッチを適用し、マルウェア対策を最新のバージョンに更新することも重要です。

システムにパッチを適用しないと脆弱性が悪用される可能性があります。どの環境でもパッチの管理を適切に行う必要があります。ベンダーパッチがリリースされたら、速やかにテストと検証を行い、実装しなければなりません。古いバージョンの依存関係でパッチが適用できない場所には別の対策を実装し、既知の脆弱性に対する攻撃を回避する必要があります。Pinkslipbotなどのマルウェアを効果的に防ぐには、積極的なパッチ管理が欠かせません。

intel Security

Pinkslipbotは主に、エクスプロイト キットが存在するWebサイトのドライブバイ ダウンロードで感染しますが、このようなサイトにはフィッシング詐欺メールから誘導されることが少なくありません。メールに「内部」、「外部」というタグを付けることで、偽装メールやフィッシング詐欺メールを区別しやすくなり、未知の不正リンクのクリックを未然に防ぐことができます。

Pinkslipbotの一部はメモリー内で実行されます。システムにパッチを適用するだけでは十分ではありません。フルスキャンを実行し、マルウェア駆除ツールを利用する必要があります。感染した場合には、システムを再起動してメモリーからマルウェアを駆除し、再度スキャンしてマルウェアが存在しないことを確認してください。また、辞書攻撃対策として強固なパスワードの使用し、自動実行を無効にして、高い権限を使用しないことをお勧めします。

Pinkslipbotは有名なZeusトロイの木馬の進化形で、非常に攻撃的です。Windowsシステムに脆弱なログイン パスワードが設定されているだけで、エクスプロイト キットを使用したり、ユーザーを騙して操作を実行させなくても、Pinkslipbotの感染に成功することができます。感染すると、システムで実行されたアクティビティが記録され、攻撃者に送信されます。制御サーバーと独自の方法で通信を行うため、Pinkslipbotの検出と分析は難しくなっています。これまでの経緯を見ても、成功を繰り返すたびに危険度を増していくのは間違いありません。環境をよく理解し、推奨のポリシーや手順を実施することで、Pinkslipbotによる被害を最小限に抑えることができます。

Pinkslipbotを阻止するIntel Securityのソリューション

McAfee VirusScan Enterprise (VSE) とMcAfee Endpoint Security (ENS) 10

McAfee VirusScan EnterpriseとMcAfee Endpoint Security 10は、エンドポイント システムを保護する高度なマルウェア対策を提供します。McAfee VirusScan Enterpriseは新たにMcAfee Endpoint Security 10となり、プラットフォームが最適化され、パフォーマンスが向上しています。McAfee VirusScan EnterpriseとMcAfee Endpoint Security 10のDATには、Pinkslipbotのコンポーネントを検出・駆除する機能が含まれています。McAfee VirusScan EnterpriseとMcAfee Endpoint Security 10は、メモリー検出、ルートキット対策、動作分析、静的解析など、多層的な保護対策を提供します。次のように、Pinkslipbotを阻止するアクセス保護ルールを実装することで、新しい亜種に対する保護層を追加できます。

- すべてのプロセスにC:\Users*\AppData\Roaming\Microsoft**.exeの実行と作成を禁止するアクセス保護ルールを作成し、テストする。
- %LOCALAPPDATA%\Microsoft\フォルダーでcscrpit.exeおよびwscript.exeによるWPLファイルの読み取り、実行、作成を禁止するアクセス保護ルールを作成してテストする。これは通常JavaScriptファイルです。これらのファイルをブロックすることで、新しいマルウェア バージョンのダウンロードを防ぐことができます。
- 可能であれば、%UserProfile%フォルダーでcscrpit.exeおよびwscript.exeによるファイルの読み取りと実行を禁止するアクセス保護ルールを作成してテストする。
- updates_*new.cb、upd_*.cb、updates*_new.cbによる新しいファイルの実行と作成を禁止するアクセス保護ルールを作成してテストする。これらはPinkslipbotの設定ファイルによって使用されます。これらのファイルをブロックすることで、マルウェアの更新を防ぐことができます。
- iexplorer.exeとexplorer.exeによるポート65200と65400の使用を禁止するアクセス保護ルールを作成し、テストする。Pinkslipbotは、これらのプロセスに自身のコードを挿入します。これらのポートをブロックすることで、Pinkslipbotと制御サーバーの通信を遮断できます。
- autorun.infファイルのリモート実行を禁止するアクセス保護ルールを実装し、テストする。

McAfee Host Intrusion Prevention (HIPS)
McAfee Host Intrusion Preventionは、シグネチャと動作分析による侵入防止と動的なステートフル ファイアウォールにより、ゼロデイ脅威からシステムを保護します。コンテンツのスケジュール更新により、パッチの公開前でもアプリケーションとオペレーティング システムの脆弱性に対する攻撃を阻止できます。次のようなシグネチャを有効にすることで、マルウェアがソフトウェアの攻撃によく使用する手段を阻止し、環境のセキュリティを強化できます。

- 組み込みのMcAfee HIPSシグネチャ6010（一般的なアプリケーションのフック保護）をテストし、有効にする。
- 組み込みのMcAfee HIPSシグネチャ6011（一般的なアプリケーションの起動保護）をテストし、有効にする。
- 管理ポート以外のすべてのポートをブロックするファイアウォール ルールをポリシーに追加し、Pinkslipbotに感染したシステムを隔離する。

McAfee Endpoint Security 10とMcAfee Host Intrusion Preventionは、McAfee Complete Endpoint Protectionに含まれています。

McAfee Web Gateway (MWG)
Pinkslipbotの主要な感染経路はドライブバイ ダウンロードとメールのリンクです。McAfee Web Gatewayは、高性能なWebセキュリティにより、不正なWebサイトからシステムを保護します。このソリューションは、専用のハードウェア アプライアンスに配備するだけでなく、仮想マシン イメージとして使用することもできます。次の対策を行ってください。

- McAfee Web Gatewayのスパム フィルタリングを設定する。
  - スパム フィルタリングで次のものを阻止できます。
    - 不正なIP
    - 不正なURL
    - スパム メール
- GAM検査を有効にする。
- 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する。
- McAfee Advanced Threat Defenseと統合し、サンドボックスでゼロデイ脅威を検出する。

McAfee Active Response (MAR)
McAfee Active Responseは、Pinkslipbotなどの高度脅威が狙うシステムを継続的に監視し、脅威の検出と対応を行います。イベントを自動的に監視することで感染の兆候を確認できます。次の対策を行ってください。

- DNSキャッシュに次のドメインが存在するかどうか確認する。存在する場合、Pinkslipbotの感染が疑われます。
  - gpfbvtuz.org
  - hsdmoyrkeqpcyrtw.biz
  - lgzmtkvnijeaj.biz
  - mfrlilcumtwieyzbfdmpdd.biz
  - hogfpicpoxnp.org
  - qrogmwmahgcwil.com
  - enwgzzthfwhdm.org
  - vksslxpxaoql.com
  - dxmhcvxcmdewthfbnaspnu.org
  - mwtfngzkadeviqtlfrrio.org

  - jynsrklhmaqirhjrtygjx.biz
  - uuwgdehizcuuucast.com
  - gyvwkxfxqdargdooqql.net
  - xwcjchzq.com
  - tqxllcfn.com
  - feqsrxswnumbkh.com
  - nykhliicqv.org
  - ivalhlotxdyvzyxrb.net
  - bbxrsgsuwksogpktqydlkh.net
  - rudjqypvucwwpfejdxqsv.org
- 次のDNSキャッシュ クエリーを実行して、上記の既知のPinkslipbotドメインとシステムが通信を行っていないかどうか確認する。
  - DNSCache where DNSCache hostname equals “[Pinkslipbotのドメイン]”
- このクエリーにより、環境内のシステムとPinkslipbotドメインの間で確立された接続のリストが戻されます。項目をクリックすると関連システムが表示されるので、これらのドメインに接続しているシステムを簡単に識別できます。
- McAfee ENS 10やMcAfee HIPSなどのローカル ファイアウォールを使用して、Pinkslipbotに感染したシステムを隔離する。システムを隔離するには、McAfee ePOでロックダウン ファイアウォール システムをポリシーに割り当てます。
- McAfee ePOでシステムにオンデマンド スキャン タスクを割り当て、McAfee ENS 10 またはMcAfee VSEのフルスキャンを実行する。エージェントをウェークアップしてスキャンを開始する。

詳細情報

McAfee Labs 脅威アドバイザリ: W32/Pinkslipbot
このアドバイザリには、Pinkslipbotの技術的な分析結果が記載されています。

Intel Securityマルウェアウェビナー シリーズ: Pinkslipbot
この動画では、Pinkslipbotの概要を紹介しています。地域、業界別の感染状況、特徴や感染の兆候、推奨される防御策などを説明します。

McAfee. Part of Intel Security.
マカフィー株式会社
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エスト 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　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F TEL 052-551-6233（代）FAX 052-551-6236
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