IoTデバイスを攻撃から保護する

2016年10月、DynのDNSインフラが分散型サービス拒否攻撃（DDoS）を受けました。この攻撃の詳細は、『McAfee Labs脅威レポート: 2017年4月』で報告されています。

この攻撃ではDNSプロトコルが悪用されましたが、現在のセキュリティ技術では正規のトラフィックと不正なトラフィックを見分けるのは簡単なことではありません。さらに厄介なことに、攻撃用のトラフィックも正規のトラフィックも、世界中の数百万のIPアドレスから送信されています。

保護対策が不十分なIoTインフラが多いため、このようなDDoS攻撃が急増しています。Dynに対する攻撃で使用されたMiraiマルウェアは、ビデオ レコーダー、プリンター、防犯カメラ、冷蔵庫、サーモスタットなど、セキュリティ対策に不備がある様々なIoTデバイスを攻撃しました。IoTデバイスに感染すると、このマルウェアは他のIoTデバイスに感染してボットネットを形成し、DDoS攻撃を実行しています。

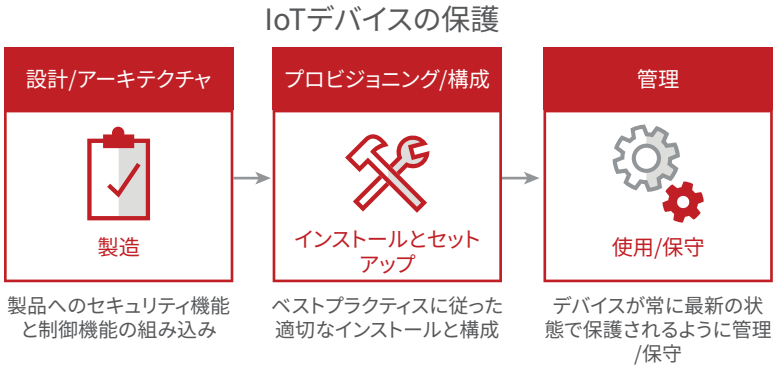
Dynのセキュリティ担当チームによると、Miraiのボットネットには数千万の不正なIoTデバイスが関係していました。

ネットワーク デバイスの感染の有無や感染の状況を簡単に識別する方法はありません。大規模感染の初期段階の場合もあれば、文字どおりの単なる移動や、DDoS攻撃に参加するボットネットの募集の場合もあります。しかし、IoTデバイスとネットワークを保護するための推奨事項もあります。

IoTデバイスの保護方法

攻撃者は、IoTデバイスを乗っ取るために最も簡単な方法を選択します。通常、脆弱な認証情報が狙われます。これに対しては、堅牢な認証情報や他のセキュリティ統制を使用することで対処できます。多くの攻撃経路には一定のパターンがあります。

McAfeeでは、既知のエクスプロイトだけでなく、将来的な攻撃もブロックできる対策の導入を推奨しています。製造から廃棄までの次の3つの段階でIoTデバイスを保護する必要があります。



1. セキュリティを意識してIoTデバイスを設計する。

IoTの製造元は、製品のアーキテクチャ、インターフェース、設計でセキュリティを考慮する必要があります。基本的なセキュリティ概念と機能（データとコードの分類、信用できるパートナー間での情報交換、使用中と保存中のデータ保護、ユーザー認証など）を実装し、テストする必要があります。将来の製品は、現在よりも保護機能が強化され、保存されるデータの量や機能も増えていきます。セキュリティ更新、機能のロック、ビルドの検証、ソフトウェアの審査などの機能や、業界のベストプラクティスに準拠したデフォルトの構成などが必要になります。これらはすべてメーカーの責任になり、すべての保証の基盤となります。ハードウェア、ファームウェア、オペレーティング　システム、ソフトウェアは厳しい環境でも耐えられるように設計しなければなりません。IoTデバイスを購入する場合には、メーカーがセキュリティに配慮しているかどうか十分に注意する必要があります。

2. プロビジョニングと構成を安全に行う。

大半のIoTデバイスは、設置時に何らかのセットアップやプロビジョニングが必要になります。ここではデバイスの識別と認証が重要なプロセスとなります。セキュリティのベストプラクティスに従ってデフォルトの構成を行うことが重要であり、ユーザーが簡単に理解できるようにルールを設定する必要があります。たとえば、デフォルトのパスワードを禁止し、パッチや更新への署名やデータの暗号化を義務付けるルールを作成する必要があります。保護されていないWeb接続も禁止するべきです。IoTデバイスを保護するには、ネットワーク アクセスを制限し、適切なタイミングでパッチを適用する必要があります。また、承認されたソフトウェアにのみ実行を許可する必要があります。ガジェットに対応する場合には、ウイルス対策、侵入防止などのセキュリティ ソフトウェアやローカルのファイアウォールを実装し、デバイスの保護機能を強化するべきです。システムが攻撃を受けたり、予期しない動作を行ったときに検知できるように、検出機能や利用統計情報の設定も必要です。プライバシー、データの保存期間、リモート アクセス、セキュリティ、失効手順の設定も不可欠です。

3. 適切な管理を行う。

消費者が所有するデバイスの場合、デバイスの管理方法は所有者が決めなければなりません。メーカーやオンライン サービス プロバイダーはプロビジョニングを行いますが、デバイスで何を実行するのかを決めるのは所有者です。プロビジョニングと管理は異なります。たとえば、ネットワーク カメラを設置するときに、メーカーのサイトに接続して最新のパッチを取得したり、クラウド ストレージの設定を行う場合があります。しかし、メーカーにカメラを管理されたくない人もいます。自分の意思に関係なくデバイスを動作させないようにするには、電源のオン/オフも、接続するオンライン サービスの選択も自分で行う必要があります。そのためには、ユーザーの識別と認証を適切に行わなければなりません。デフォルトのパスワードでは誰もが管理者機能を利用できるため、このようなパスワードは好ましくありません。たとえば、すべての Microsoft Windows システムでデフォルトのログイン パスワードが設定されて出荷されたらどうなるでしょうか。多くのユーザーはパスワードを変更しないため、攻撃者はいとも簡単にシステムにログインできてしまいます。

IoTシステムでは、デバイスの所有者を正しく認証できなければなりません。また、所有者がデータ ポリシーやプライバシー パラメーターを使用し、ベンダーよりも厳しい制限を設定できるように管理機能を拡張する必要があります。セキュリティの更新が利用可能になったときに、署名付きの更新が自動的に適用されるようにする必要もあります。セキュリティに詳しい所有者であれば、送受信接続、データの種類、ポート、セキュリティ設定に制限を設定するかもしれません。エラーや予期しない動作をログに記録して、信用済みのシステムに送信したり、ローカルで確認することもできます。デバイスによっては、電子メールやSMSで警告を送信するシステムをリモートに用意しておくことも必要でしょう。復旧不能な侵害の発生や所有権の譲渡に備えてリセット機能を用意しておくことも重要です。

IoTデバイスの保護に有効なポリシーと手順

- **IoTデバイスのセキュリティ状態を調査する。**IoTデバイスを購入する前に、デバイスやその供給元に問題が起きていないか確認する必要があります。インターネットで調べてみましょう。米連邦取引委員会のサイトを見ると、以前に執行された行政処置を確認できます。基本的な検索を行うだけでも、他社はプロアクティブである一方で、セキュリティに関して無視した会社も見られます。
- **すべてのIoTデバイスのソフトウェアを最新の状態にする。**これは簡単なベストプラクティスです。これにより、脆弱性、特に最近見つかり注目を集めた脆弱性を解決できます。パッチ適用の手順を決め、パッチが正常にインストールされていることを確認してください。
- **パッチすることのできないIoTデバイスについては、リスクを検出する。**システムをロックダウンし、未承認プログラムの実行を阻止するホワイトリストアプリケーションを利用することで実現することができます。
- ファイアウォールや侵入防止システムを使用して、**IoTデバイスをネットワークの他の部分から分離**しましょう。これらのシステムで不要なサービスやポートを無効にすると、侵入の可能性があるポイントの露出を減らすことができます。Miraiは未使用のポートを悪用しています。
- **デフォルトの設定を変更し、強固なパスワードを使用する。**デフォルトの脆弱なパスワードをそのまま放置すると、IoTデバイスは危険な状態になります。長いフレーズを使用する、特殊文字を使用する、大文字小文字と数字を組み合わせるなど、適切なパスワードを設定しましょう。強固で簡単に推測できないパスワードが必要です。
- **IoTのセキュリティ設定を利用する。**IoTデバイスによっては、詳細な機能を設定できる場合があります。このような機能は有効に活用しましょう。ゲストWi-Fiネットワークに類似した別個のネットワーキング機能を提供するIoT製品もあります。これは一例に過ぎません。より多くの機能を提供する製品があるかもしれません。
- **保護されたWi-Fi経由でIoTデバイスに接続する。**強固なパスワードを作成し、WPA2などの最新のセキュリティプロトコルを使用しましょう。
- **IoTデバイスに対する物理的なアクセスを制限する。**IoTデバイスが直接操作され、ハッキングされる場合もあります。
- **ユニバーサル プラグ アンド プレイ（UPnP）を無効にする。**多くのIoTデバイスは、インターネット上で検出できるようにUPnPに対応していますが、これがマルウェア感染の原因となる可能性があります。可能であれば、この機能を無効にしましょう。
- **IoTデバイスの電源を定期的に入れ直す。**マルウェアは通常、揮発性メモリーに存在しています。デバイスをシャットダウンして再起動することで、これらのマルウェアを消去できます。

McAfeeがIoTデバイスの攻撃からシステムおよびネットワークを保護する方法

これらのIoTデバイスのベストプラクティスを実施する以外にも、McAfeeの製品を利用すると、IoTデバイスへのマルウェア感染を防ぎ、ボットネットの不正な活動を阻止することができます。以下のMcAfee製品と構成を利用することで、IoTデバイスを保護し、IoTデバイスに対する攻撃からシステムとネットワークを保護できます。

McAfee VirusScan® Enterprise 8.8またはMcAfee Endpoint Security 10

- 常に最新のDATファイルを使用します。
- **McAfee Global Threat Intelligence** (McAfee GTI) を使用します。McAfee GTIは600万を超えるランサムウェアのシグネチャを保持しています。
- 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。
  - アクセス保護ルールの詳細は、次のKnowledgeBaseの記事を参照してください。**KB81095、KB54812**
  - McAfee VirusScan 8.8 Enterpriseで設定のベストプラクティスを参照してください。**PD22940**
  - McAfee Endpoint Security の設定に関するベストクラクティスを参考してください。**KB86704**

McAfee Host Intrusion Prevention

- McAfee Host Intrusion Preventionは、マルウェアの拡散阻止に役立ちます。IPSカスタム　シグネチャを使用してルールを作成すると、マルウェアが生成するファイル操作 (作成、書き込み、不正なコードなど) を阻止できます。
- McAfee Host Intrusion Preventionのシグネチャ3894: Access Protection—Prevent svchost.exe executing non-Windows executables (アクセス保護ーsvchost.exe によるWindows以外の実行ファイルの実行阻止) を有効にします。
- McAfee Host Intrusion Preventionシグネチャ6010と6011を有効にして、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) ファイル 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、「**\」または「?:\」というファイル名で始めます。ドライブ文字をワイルドカードで表すこともできます (例: **\<ファイル名>.exe、?:\<ファイル名>.exe)。
      - Filesパラメーターで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して、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) プログラム 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: 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が対象の実行ファイル (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、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 Threat Intelligence Exchange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、McAfee 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。
- McAfee 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をブロックできます。
  - 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

- 検出機能:
  - シグネチャ ベースの検出: McAfee GTIは6億を超えるシグネチャを保持しています。
  - 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: シグネチャを使用しない検出
  - 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
- マルウェアが実行される可能性が高い場所分析世のプロファイルを作成します。
  - 一般的なOS、Windows 7、8、10
  - 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。アナライザーを使用することで、インターネット接続のプロファイリングを行い、検出率を向上させています。

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、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。
- McAfee 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 Protection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

- Web ゲートウェイ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: 自動処理

- 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: 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 Endpoint Threat Defense and Response

- McAfee Endpoint Threat Defense and Responseは、高度な脅威を検出し、問題に対応します。McAfee GTI、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 コレクターにより、マルウェアの侵害兆候を検出し、識別する特定の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

ホワイト ペーパー: ***More Confidence, Safety, and Security in the Digital World***（より安全で安心なデジタル世界を実現するセキュリティ）

Best Practices for how to use Host IPS rules for a malware outbreak（マルウェア大量発生時のMcAfee Host Intrusion Preventionルールの使用方法）: **KB84507**

SIEM Orchestration. How McAfee Enterprise Security Manager can drive action, automate remediation, and increase situational awareness（SIEMオーケストレーション ー McAfee Enterprise Security Managerでアクションの実行、修復を自動的に行い、状況認識を強化する方法）: **PD24830**

ホワイト ペーパー: ***Secure Beyond the Signature***（シグネチャを超えたセキュリティ）

FAQs for McAfee Network Security Platform. Advanced Malware Detection（McAfee Network Security PlatformのFAQ ー 高度なマルウェア検出）: **KB75269**

McAfee Web Gateway製品ガイド ー Webフィルタリング: **PD26339**

〒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（代表）
www.mcafee.com/jp