— AUS（アルテミス・ユーザ・サポート）便り 2017/02/27号 —
http://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●IoTマルウェア「Mirai」に新たな亜種、Windowsに感染して拡散攻撃

http://www.itmedia.co.jp/enterprise/articles/1702/15/news086.html
http://blog.trendmicro.co.jp/archives/14455

このニュースをザックリ言うと・・・

- 2月14日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、IoT機器に感染し、大規模なDDoS攻撃を行うマルウェア「Mirai」に新たな亜種が確認されたとして警告が出されています。

- これまでのMiraiはOSにLinuxを搭載したIoT機器（以下Linux機器）に感染するものでしたが、今回確認された亜種「BKDR_MIRAI.A」は、Windows PCにも感染するのが大きな特徴とされている（厳密には、感染する機器によってLinux用とWindows用の2種類のマルウェアを作成する）とのことです。

- また、これまでのMiraiよりも侵入しようとするサービスポートの範囲が広く、例えばWindows PC上のMicrosoft SQL Serverに侵入し、データベースの管理者権限を持つユーザアカウントの作成を行うとされています。

AUS便りからの所感等

- BKDR_MIRAI.Aは、Linuxの実行形式だったこれまでのMiraiと異なり、Windowsの実行形式（exeファイル）となっており、また、ポートスキャンを行うサービスポートとして、従来の22(SSH) や 23(Telnet) の 他 、 135(DCE/RPC) ・ 445(Active Directory) ・ 1433(SQL Server)・3306(MySQL)・3389(リモートデスクトップ)と、WindowsやWindows上の製品が用いる(MySQLを除く)サービスポートが多く追加されています。

- SQL Serverを狙ったマルウェアと言えば2003年の「SQL Slammer」が知られており、当時もこのマルウェアによる大量のパケットにより全世界でネットワーク障害が発生する事態となりました。

- 通常、ルータやUTMを隔てたNAT内にある機器に対し、外部から上記のようなサービスポートへアクセスされることはありませんが、外部あるいはリモートからサーバを管理する目的でポートを開ける設定を行っている場合や、一旦内部に侵入したマルウェアからNAT内で無防備にしている機器が攻撃を受ける場合等が考えられます。

- Windows PCもLinux機器も、各々がOSのファイアウォール機能やアンチウイルス等により確実に防御しているか、またデフォルトのパスワードのままになっているユーザアカウントが存在しないか、十分に確認を行うことが重要となります。

ITmedia エンタープライズ

2017年02月15日 12時48分 更新

IoTマルウェア「Mirai」に新たな亜種、Windowsに感染して拡散攻撃

IoT機器をボット化してしまうマルウェアの「Mirai」の新たな亜種は、感染したWindowsマシンを踏み台にして、ボット化できるIoT機器を探索できてしまうという。

[ITmedia]

印刷/PDF 90 ツイート 128 いいね！ 128 シェア 10 B! Bookmark 25 Pocket 4 G+1 共有する 通知

トレンドマイクロは2月14日、IoT機器をボット化してサイバー攻撃の踏み台に悪用するマルウェア「Mirai」の新たな亜種を確認したと発表した。Windowsに感染し、ボット化させるIoT機器の探索などができるという。

同社が発見した「BKDR_MIRAI.A」は、感染先のマシンから攻撃者の設置するコマンド＆コントロールサーバ（C&Cサーバ、C2サーバ）に接続し、スキャンするIPアドレスのリストを受信する。感染先がLinux機器だった場合は、これまでと同様にマルウェアのMiraiを作成して機器をボット化する。Windows機器だった場合は自身のコピーを作成して、新たな感染先となるLinux機器を探索するという。

TREND MICRO トレンドマイクロ セキュリティブログ POWERED BY TrendLabs

ポートスキャン機能を増強した「Mirai」、Windowsも踏み台に追加

投稿日: 2017年2月14日
脅威カテゴリ: 不正プログラム、サイバー攻撃、脆弱性、TrendLabs Report
執筆: TrendLabs フィリピン

2016年末、Linux を搭載した IoT機器を狙う「Mirai」（「ELF_MIRAI」ファミリとして検出）による、大規模な「分散型サービス拒否（DDoS）」攻撃が数々の被害を発生させました。これらの事例は、「モノのインターネット（Internet of Things、IoT）」のエコシステムが、機能していない事実を明らかにしました。Mirai は、さらに拡散範囲を拡大するべく、今度は Windows PC を踏み台とするための機能を取り入れ、再び注目を集めています。

トレンドマイクロは、2017年脅威予測において、「Mirai と同様のマルウェアを利用した DDoS攻撃の増加」を指摘していますが、今回入手したWindows版マルウェア（「BKDR_MIRAI.A」として検出）は、Mirai同様の機能を持つものではありません。Mirai の感染対象である Linux機器を探し、Mirai 本体を拡散させ、最終的にMirai のボットネットを拡大させることを目的としたものです。これまでMiraiは特定範囲のIPアドレスに対しブルートフォース（総当り）攻撃を行い、自身のボットネットを拡大していました。今後はこの「BKDR_MIRAI.A」により、Windows環境からも「Mirai」のボットネットが拡大されることになります。

「BKDR_MIRAI.A」は、コマンド＆コントロール（C&C）サーバに接続し、スキャンする IPアドレスリストを受信します。システムにログインできた場合、感染端末および機器のオペレーティングシステム（OS）を確認します。Linux機器であった場合は、そこにマルウェアMirai を作成し、新しいボットとして利用します。機器の OS が Windows であった場合、マルウェアは、そこに自身のコピーを作成し、Linux機器の探索を継続します。マルウェアは、Linux用と Windows用の2種類のマルウェアを作成します。

●「Googleアカウントが変更されました」突然の強制ログアウト続出

http://www.itmedia.co.jp/news/articles/1702/24/news097.html

このニュースをザックリ言うと・・・

- 2月24日朝（日本時間）、Googleアカウントの利用者の一部より、突如アカウントの強制ログアウトが発生したという報告が相次ぎました。

- Googleアカウントでログイン済みのスマホアプリなどにアクセスした際、「Googleアカウントが変更されました。セキュリティ保護のため、もう一度ログインしてください」という通知が出た、というものです。

- 当初は大規模な不正ログインやパスワードの変更などの発生が懸念されていましたが、Googleの説明によるとそういったものは発生しておらず、実際には従来のパスワードを入力して再度ログインすることにより、元通りGoogleアカウントが利用できている模様です。


ITmedia NEWS

速報

2017年02月24日 14時02分 更新

「Googleアカウントが変更されました」突然の強制ログアウト続出　Google「フィッシングではない」

「Googleアカウントが変更されました」――Googleのサービスから強制ログアウトされたユーザーが続出。Googleによると「フィッシングなどではない」という。

[ITmedia]

Googleアカウントでログイン済みのサービスを利用しようとすると、「Googleアカウントが変更されました」と告知が出て、強制ログアウトされた――こんなユーザーが2月24日に続出した。

Googleは「調査の結果、フィッシングやアカウントのセキュリティに影響するものではない」と発表。再ログインを行うよう促している。

AUS便りからの所感等

- スマートフォン、特に通常はGoogleアカウントとの紐付けが重要となるAndroidスマホにおいて、購入時にGoogleアカウントを作成してログインしたきりのユーザの場合、今回の事態に遭遇したときにパスワードを覚えていないというケースもあると思われ、Googleではこのような場合にパスワードを再取得する手段を提供していますが、重要なアカウントについては必ずパスワードを記憶または記録しておき、また第三者に悪用されないよう、二段階認証等アカウントを保護する機能を有効にしておきましょう。

- Googleアカウントに対しセキュリティ上の問題が発生したわけではないようですが、大手サービス等にまたがる連鎖的な不正ログインが度々発生していることから不安になっていたユーザも少なくないと見られ、そしてそういった不安を狙い、アカウントを詐取しようとスパムメール等からフィッシングサイトへ誘導する攻撃も発生する恐れは十分考えられます。

- 表示されたメッセージで検索し、他のユーザが同じようなトラブルや不審な攻撃に遭遇していないか等について十分に情報収集を行い、万が一、偽のWebサイトに誘導されても決してアカウント情報の入力をしないことに注意してください。

●2月度のMSセキュリティパッチは延期、その後定例外でFlash Playerアップデートがリリース

https://technet.microsoft.com/ja-jp/library/security/ms17-005

このニュースをザックリ言うと・・・

- 2月15日（日本時間）、マイクロソフト社（以下MS）より、当日リリース予定だった定例のセキュリティパッチについて、一部ユーザに問題が生じる可能性があるため、リリースを延期することが発表されました。

- 同日にはAdobe社からFlash Playerの脆弱性を修正した最新バージョン24.0.0.221がリリースされていますが、Windows 8.1以降のIE・Edge用のFlash Playerについては、1週間後となる2月22日に、MSより定例外のセキュリティパッチ「MS17-005」としてリリースされています。

- 今回リリースされなかったとみられるセキュリティパッチは、次の定例のリリース日となる3月15日に改めてリリースされる予定です。

AUS便りからの所感等

- Flash Playerは、JavaやAdobe Readerと並び依然として脆弱性を狙われる確率が高いソフトウェアであり、必ずアップデートを行い、また実際に最新のバージョンとなっているかAdobe社のサイトで忘れずに確認を行いましょう。

- Windows 8.1以降のIE・Edge用のFlash Playerはセキュリティアップデートが Adobeからではなく MSから配布されることになっているためか、稀に通常のFlash Playerよりもリリースが遅れる場合があり、IEやEdgeの設定で無効化する、あるいはChrome等最新のFlash Playerを使用可能な他のブラウザに乗り換えることを検討するのもある意味有効な手段と言えます。


Microsoft | TechNet

マイクロソフト セキュリティ情報 MS17-005 - 緊急

Adobe Flash Player のセキュリティ更新プログラム (4010250)

公開日: 2017 年 2 月 22 日

バージョン: 1.0

概要

このページのトピック

概要
脆弱性の情報
影響を受けるソフトウェア
よく寄せられる質問
問題を緩和する要素

このセキュリティ更新プログラムは、すべてのサポートされているエディションの Windows 8.1、Windows Server 2012、Windows Server 2012 R2、Windows RT 8.1、Windows 10、および Windows Server 2016 にインストールすることで Adobe Flash Player の脆弱性を解決します。

このセキュリティ更新プログラムは、深刻度が「緊急」と評価されています。この更新プログラムは Internet Explorer 10、Internet Explorer 11、および Microsoft Edge に含まれる、影響を受ける Adobe Flash ライブラリを更新することにより、Adobe Flash Player の脆弱性を解決します。詳細については、「影響を受けるソフトウェア」のセクションを参照してください。

- なお、Windowsにおいてファイルやプリンタ等の共有を行うプロトコルである「SMB」には脆弱性が報告されており、今回のパッチで修正されるものとみられましたが、こちらも延期のため修正されないままとなり、こういった脆弱性が修正されるまでに悪用される可能性を抑止するため、アンチウイルスやUTMの導入は決して欠かせないものとなります。