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。

●Miraiの亜種、新たなIoTマルウェア「Satori」がアジアで感染拡大

https://japan.zdnet.com/article/35111546/
https://cybersecurity-jp.com/news/19623

このニュースをザックリ言うと・・・

- 12月5日（現地時間）、中国のセキュリティ企業Qihoo 360（奇虎360）より、新たなIoTマルウェア「Satori」がアジアで感染を拡大しているとするレポートが発表されました。

- Satoriは以前に猛威を振るった「Mirai」の亜種とされ、数ヶ月前から活動が観測されていましたが、今回これによるとみられるポートスキャン（TCPポート37215および52869）の発生が確認されたことから、警告が出されています。

- 同社では11月下旬にも、Miraiの亜種とされるマルウェアによるポートスキャン（TCPポート23および2323）の発生について警告していますが、これが今回のSatoriによる攻撃の一部であると推測しています。

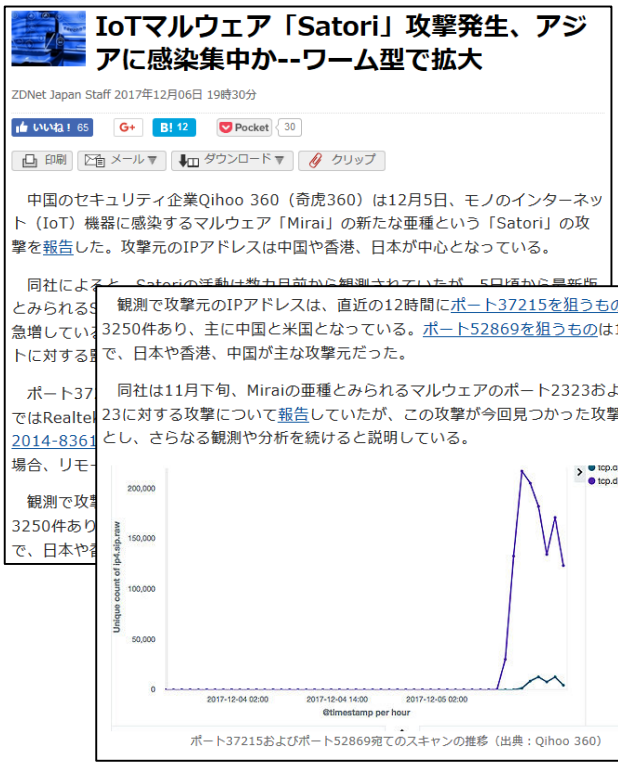
AUS便りからの所感等

- PCのように自身でファイアウォール機能等を持っているとは限らないIoT機器については、決してインターネット上から直接アクセスされるようなむき出しの状態にしないことが重要です。

- 機器の意図しないポートにアクセスされないよう、必ずルータ・UTMのポートフィルタリング機能等により、防御を行ってください。

- IoT機器と社内LANの任意のPC等とで自由に通信可能な状態であれば、やはりどちらかに侵入したマルウェアが底を踏み台としてもう一方へ感染する恐れがあり、機器の管理者からのみアクセスできるようUTM等で適切にネットワークの分割を行うことも欠かせません。

ZDNet Japan



IoTマルウェア「Satori」攻撃発生、アジアに感染集中か--ワーム型で拡大

ZDNet Japan Staff 2017年12月06日 19時30分

中国のセキュリティ企業Qihoo 360（奇虎360）は12月5日、モノのインターネット（IoT）機器に感染するマルウェア「Mirai」の新たな亜種という「Satori」の攻撃を報告した。攻撃元のIPアドレスは中国や香港、日本が中心となっている。

同社によると、Satoriの活動は数ヶ月前から観測されていたが、5日頃から最新版とみられるS…急増してい…トに対する…

ポート37…ではRealtek…2014-8361…場合、リモー…

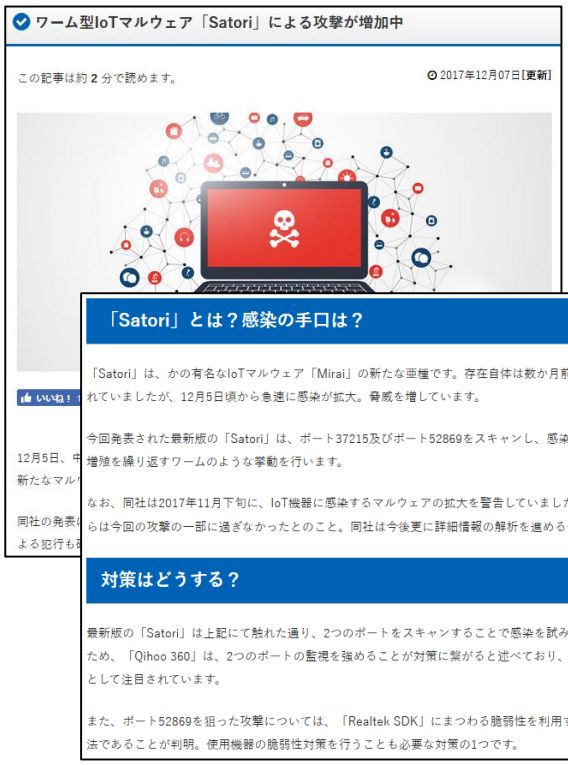
観測で攻撃…3250件あり…で、日本や…

観測で攻撃元のIPアドレスは、直近の12時間にポート37215を狙うものが26万3250件あり、主に中国と米国となっている。ポート52869を狙うものは1万9403件で、日本や香港、中国が主な攻撃元だった。

同社は11月下旬、Miraiの亜種とみられるマルウェアのポート2323およびポート23に対する攻撃について報告していたが、この攻撃が今回見つかった攻撃の一部だとし、さらなる観測や分析を続けると説明している。

ポート37215およびポート52869宛てのスキャンの推移（出典：Qihoo 360）

サイバーセキュリティ.com



ワーム型IoTマルウェア「Satori」による攻撃が増加中

この記事は約 2 分で読めます。

2017年12月07日[更新]

「Satori」とは？感染の手口は？

「Satori」は、かの有名なIoTマルウェア「Mirai」の新たな亜種です。存在自体は数か月前から確認されていましたが、12月5日頃から急速に感染が拡大。脅威を増しています。

今回発表された最新版の「Satori」は、ポート37215及びポート52869をスキャンし、感染すると自ら増殖を繰り返すワームのような挙動を行います。

なお、同社は2017年11月下旬に、IoT機器に感染するマルウェアの拡大を警告していましたが、それらは今回の攻撃の一部に過ぎなかったとのこと。同社は今後更に詳細情報の解析を進める予定です。

対策はどうする？

最新版の「Satori」は上記にて触れた通り、2つのポートをスキャンすることで感染を試みます。そのため、「Qihoo 360」は、2つのポートの監視を強めることが対策に繋がると述べており、有効な対策として注目されています。

また、ポート52869を狙った攻撃については、「Realtek SDK」にまつわる脆弱性を利用する攻撃方法であることが判明。使用機器の脆弱性対策を行うことも必要な対策の1つです。

●日本で流通する迷惑メールの4つのパターン…ラック社が解説

https://japan.zdnet.com/article/35110995/

このニュースをザックリ言うと・・・

- 11月24日（日本時間）、国内大手セキュリティベンダーのラック社より、「サイバー救急センターレポート」第1号が公開されました。

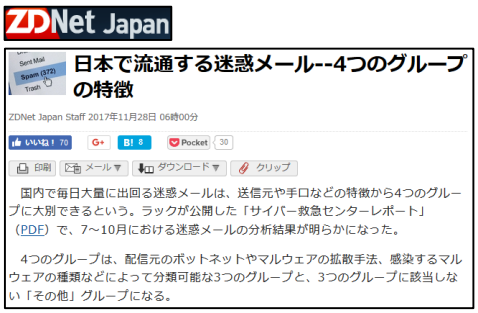
- 同レポートに掲載されている、7～10月における迷惑メールの分析結果では、国内で大量に出回る迷惑メールが送信元や手口などの特徴から、大きく4つのグループに分類されています。

A）日本語文章と実在する組織になりすまし、ネットバンキングを狙うマルウェア「DreamBot(別名URSNIF, gozi)」に感染させようとするグループ
B）件名が「Invoice」「Voice Message」など、短い英単語からなり、ランサムウェア「Locky」等に感染させようとするグループ
C）添付ファイルではなく、本文中のリンク先から不正なマクロを含むWord等のファイルを、さらに「Pony」「Zeus」の亜種などをダウンロードさせるグループ
D）件名や本文中に文字が含まれておらず、主にランサムウェアの拡散を行うグループ

AUS便りからの所感等

- 上記のうち特にAグループは様々な組織をかたって日本語のメールを送信しており、それ以外にも頻繁に目に付く迷惑メールがある程度のパターンに絞られる傾向にあることは確かですが、そこに注意をそらされているうちにこれまでにないパターンの迷惑メールに引っかかり、マルウェアに感染してしまうようでは本末転倒です。

- アンチウイルス・UTMによるメールチェック機能を必ず有効にするとともに、迷惑メールの大量拡散について注意喚起を行っている複数の情報源を常時巡回し、マルウェアに感染させようとする攻撃へ怠りなく警戒を行うようにしてください。


ZDNet Japan

日本で流通する迷惑メール--4つのグループの特徴

ZDNet Japan Staff 2017年11月28日 06時00分

国内で毎日大量に出回る迷惑メールは、送信元や手口などの特徴から4つのグループに大別できるという。ラックが公開した「サイバー救急センターレポート」（PDF）で、7～10月における迷惑メールの分析結果が明らかになった。

4つのグループは、配信元のボットネットやマルウェアの拡散手法、感染するマルウェアの種類などによって分類可能な3つのグループと、3つのグループに該当しない「その他」グループになる。

●Google Playプロテクトでは検出されない…Google Playでアプリを配布し、マルウェアをタイマーで作動させる攻撃が発生

http://www.atmarkit.co.jp/ait/articles/1711/27/news062.html

このニュースをザックリ言うと・・・

- 11月21日（現地時間）、アンチウイルスソフト等を提供するスロバキアのESET社より、公式Androidアプリストア「Google Play」の自動検査をかいくぐる不正なアプリの手口についての調査結果が発表されました。

- 同社が同業のAvastおよびSfyLabsと連携して行った調査結果によれば、10月と11月、「不正コードを含まないアプリがマルウェアをダウンロードし、そのマルウェアがタイマーに従って悪意ある挙動をする」という攻撃手法により、オンラインバンキングアプリを狙う不正なアプリがインストールされるケースが確認されたとしています。

- このとき確認された不正なアプリはGoogle Playからは削除されたものの、それ以外の場所からのインストールに対し現時点で「Google Play Protect」による検査を通過してしまうとしており、同社では、自分が何を行っているかを明確に理解している場合以外は「提供元がPlayストアではないアプリのインストール」を無効にすること等を推奨しています。

AUS便りからの所感等

- 今回確認されたケースでは、アプリは「管理者権限」を要求し、権限を取得した2時間後に別のアプリのダウンロードを実行、さらに「提供元がPlayストアではないアプリのインストール」を許可されている場合にインストールの続行を要求し、ユーザがこれを承諾することにより、最終目的となるアプリがインストールされるという手順になっていたとのことで、ユーザがこの過程のどこかで不審に思えばインストールを拒否できる類のものでしたが、言葉巧みに誘導され、まんまとインストールを許すことも十分考えられます。

- あらゆるセキュリティを侵害する攻撃に共通することですが、「どういった攻撃が行われるか」を知り（あるいは啓発し）、そしてある権限を引き渡すなどの行為がどういった結果をもたらすか、熟知していることが慎重な行動の為には必須と言えます。

- うっかり不正なアプリをインストールしてしまうことがないよう、レビューやネット上の情報を十分考慮すること、またセキュリティベンダーが提供するアンチウイルスアプリをPCと同様にインストールしておくことも検討に値します。