平成２８年１１月１８日

１０月中の不正プログラム関連情報

※　ニュースの内容は、各種報道、インターネット等で公表されている情報に基づくもので、県警が事実を確認したものではありません。

鳥取県警察本部サイバー犯罪対策室

○　史上最大級の DDoS 攻撃に使われたマルウェア「Mirai」

ITmedia ニュースは 10 月４日、米情報セキュリティサイトの「Krebs on Security」が史上最大級の①分散型サービス妨害（DDoS）攻撃を仕掛けられた問題で、この攻撃に使われたマルウェアの②ソースコードが公開されたと報じた。

Krebs on Security が 10 月１日に伝えたところでは、この攻撃に使われたマルウェアの名称は「Mirai」、投稿者は「Anna-senpai」。英語のハッカーフォーラムにソースコードが掲載されたという。

Krebs on Security は９月下旬、620Gbps にも達する DDoS 攻撃を受けてダウンした。同サイトの運営者は、モノのインターネット（IoT）デバイスを踏み台にした③ボットネットのネットワークから攻撃が仕掛けられていると伝えていた。

Mirai はルータや防犯カメラといった IoT デバイスに感染してボットネットを形成し、DDoS 攻撃を仕掛ける２大マルウェアのうちの１つで、もう一つのマルウェア「Bashlight」と競合しながら勢力を広げているとされる。攻撃の踏み台にされているのは出荷時のデフォルトのパスワードとユーザー名がそのまま使われているルータや防犯カメラ、プリンタ等の IoT デバイス。Mirai はそうしたデバイスを継続的にスキャンして感染を広げる。デフォルトのパスワードの変更が感染を防ぐ手段と指摘されている。

○　ネット接続テレビを標的としたウイルスを検知

産経新聞は 10 月 31 日、インターネットへの接続機能を持つ市販の「④スマートテレビ」の画面を停止させ、不正に金銭を要求する脅迫文を表示させる新種のウイルスが、日本国内で今年に入り、300 件以上検出され、複数の感染被害も出ていることが分かったと報じた。

これまでのサイバー攻撃では PC が主な標的だったが、IoT の導入が進み、家電にも攻撃の手が及んできていることが明らかになっており、セキュリティ企業等は注意を呼び掛けている。

トレンドマイクロでは、スマートテレビ等で利用されている同社の対策ソフトが、新種ウイルスを約 320 件検出したとしている。ほとんどは感染を免れたが、複数の被害が同社に報告された。

テレビ上で音楽やゲームなどのアプリをダウンロードした際に感染する恐れが高く、感染すると、正常に動いていたテレビの画面が急に停止する。代わりに、画面上には日本語や英語で、法務省や米国土安全保障省などを装い「ブロックを解除するためには、１万円を支払ってください」

「あなたは違法なことをした」などという虚偽のメッセージが表示される。視聴者には米アップル社が提供するプリペイドカード「iTunes カード」の購入を求め、金銭と同じ価値のあるカード裏面のコード番号を打ち込むように促す。また、72 時間の制限時間を示し、時間内に支払えなければブロックは解除できないと脅迫する。

ウイルスに感染すると約 30 分後にプログラムが発動し、テレビ画面が停止する仕組みになっている。脅迫画面が表示されると、コントローラーを操作したり電源を入れ直したりしても元には戻らず、復旧するためにはテレビの基本ソフト（OS）を初期化しなければならない。

電子情報技術産業協会（JEITA）によると、平成 26 年以降の薄型スマートテレビの国内出荷台数は累計 760 万台以上。トレンドマイクロは、感染しても絶対に支払わないよう呼び掛けている。

---

① 標的となるコンピュータに対して、複数のコンピュータから大量の処理負荷を与えることで、サービスを機能停止状態に追い込む手法

② コンピュータプログラム（動作のすべて）を記述したテキストファイル

③ ウイルスなどによって、遠隔操作できる攻撃用プログラムを送り込み、外部からの指令で一斉に攻撃を行わせるネットワーク

④ 地上波以外の番組を好きなときに見ることができたり、ＳＮＳ機能でチャットを行うことができる