平成２９年３月６日

２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

○　ウェブ改ざん攻撃に変化、ランサムウェア配付等の温床に

ITmedia ニュースは２月２日、日本サイバー犯罪対策センター（ＪＣ３）とセキュリティ各社が、ウェブサイト閲覧者をマルウェアに感染させるサイバー攻撃の国内での状況について発表したと報じた。

攻撃者が使うツールや閲覧者が感染するマルウェアの種類等に大きな変化がみられるという。

この種の攻撃で攻撃者は、攻撃を実行するために①「エクスプロイトキット」と呼ばれるツールを使用する。攻撃者は脆弱性を抱えるウェブサイトのシステムに不正侵入し、マルウェア配付サイトへのリンクを埋め込むといったコンテンツ改ざんなどの行為に及ぶ。攻撃されたウェブサイトを閲覧すると、閲覧者のコンピュータがマルウェア配布サイトに接続（誘導）されてしまう。その際、コンピュータに脆弱性が存在するとマルウェアが送り込まれて感染する。ユーザーはその後、攻撃者によって不正にコンピュータを操作され、金銭を詐取されるなどの被害に遭うおそれがある。

ＪＣ３によれば、国内では 2016 年後半から「RIG-EK」というツールによる攻撃が増加しており、全国の警察やセキュリティ企業らと連携して、改ざんサイトの無害化に取り組んでいるという。改ざんされた 298 サイトの管理者等に対して、38 の都道府県警察から状況確認や修復依頼等を行っている。

○　IoT マルウェア「Mirai」の新たな亜種を確認

ITmedia ニュースは２月 15 日、IoT 機器を②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トレンドマイクロが発表したと報じた。Windows に感染し、ボット化させる IoT 機器の探索等ができるという。

トレンドマイクロが発見した「BKDR_MIRAI.A」は、感染先のマシンから攻撃者の設置する C&C サーバ（指令制御サーバ）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。

BKDR_MIRAI.A は、初期の Mirai よりも多くのポートが追加され、広範囲に感染先候補の機器を探索できるとしている。このマルウェアはまず、探索先のポートがオープンであるかを確認。③MySQL や Microsoft SQL Server で使用されているソフトウェアを識別する役割も果たしているとみられる。

また、BKDR_MIRAI.A は、感染機器が接続するネットワーク内の IoT 機器への侵入にも利用される恐れがあるという。特に、家庭用ルータでは「192.168.x.x」の IP アドレス空間が一般的に使われていることから推測が容易で、攻撃者がこの IP アドレス空間をスキャンすれば、家庭内ネットワークの機器を簡単に探索できる。感染対象となる機器のパスワードが初期設定のまま使用されていればさらに感染は容易で、ボット化させられてしまう危険性が高い。

トレンドマイクロは、このような拡大した機能により、Mirai 以外の別のマルウェアの拡散にも使われる可能性があると指摘している。

---

① 攻撃者がＰＣやデバイスの脆弱性を利用する際に用いるハッキングツール
② 外部から遠隔操作可能な状態になっていること
③ 世界中で最もよく利用されているオープンソースのデータベースの一つ