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

○　JTB への攻撃に用いられた①マルウェア「PlugX」

ITmedia ニュース等は６月 17 日、セキュリティ企業のファイア・アイが国内の大手旅行会社 JTB へのサイバー攻撃に用いられた遠隔操作マルウェア「PlugX」に関する記者説明会を実施したと報じた。

PlugX は中国製のマルウェアで、コンピュータを遠隔操作するための②RAT（Remote Administration Tool）」の一種。

ファイア・アイの分析官によれば、以前は「Poisonlvy」という別のマルウェアが日本への攻撃に用いられていたが、2012 年ごろから、PlugX が日本国内の③APT（Advanced Persistent Threat）攻撃に使われているという。また、攻撃の対象国は日本だけでなく、米国、韓国、香港、台湾等にも及んでおり、最近はベトナムを対象とした攻撃も増えている。産業でいえば、ハイテク、航空宇宙、メディア、通信、政府、軍需産業等が標的となっており、技術関連情報等の知的財産が狙われている。

記者説明会では、中国語の OS とマルウェアを作成するための PlugX のツールキットを用意した上で、マルウェアの作成と遠隔操作を実演した。マルウェアの作成は④GUI 画面から、⑤C&C サーバ等を設定することで簡単に行うことができ、実際に PC をマルウェアに感染させてから、遠隔で様々な操作を行うのもさほど難しくはないことが示された。

○　新型⑥ランサムウェア「Bart」、ZIP パスワードでファイルを人質に

ITmedia ニュースは６月 28 日、被害者のファイルを ZIP で圧縮してパスワードをかけ、身代金を要求する新手のランサムウェア「Bart」が出現したと報じた。日本を含む世界各国で急速に感染を広げているという。

従来のランサムウェアは、感染すると外部の制御用サーバに接続して命令を受け取り、公開鍵と非公開鍵を使用する暗号アルゴリズムを使って被害者のファイルを暗号化するのが常套手段だった。これに対して、Bart は外部の制御サーバは使わず、被害者のファイルを ZIP で圧縮してパスワードをかけてしまうという。

圧縮された ZIP ファイルを開こうとするとパスワードの入力を促され、パスワードが分からなければ解凍はできない。ZIP 化されたファイルと同じディレクトリには、復元方法について説明する「recover.txt」「recover.bmp」というファイルが残されていて、リンク先の決済サイトから身代金を支払うよう要求する。

Bart はフィッシング詐欺メールを通じて出回っているダウンローダー型マルウェア「RockLoader」を通じて感染する。この手口や身代金要求画面などは、これまで出回っていた別のランサムウェア「Locky」と酷似しているという。ただし、Bart が要求する身代金は３ビットコイン（約 2,000 ドル相当）で、Locky が要求していた 0.5 ビットコインに比べて金額がつり上がっている。

被害は既に各国に広がっており、日本でも６月 24 日の時点で 75 件の被害が出ているという。

---

① 不正かつ有害に動作させる目的で作成された悪意のあるソフトウェア
② 遠隔操作を可能にするツール
③ 標的型攻撃の一種
④ Graphical User Interface の略でマウス等のポインティングデバイスを用いて、直感的な操作を可能にする操作方法
⑤ 指令サーバともいい、インターネットから PC のマルウェアに対して、コマンドを送り遠隔操作するサーバ
⑥ 感染した PC をロックしたり、ファイルを暗号化し使用不能にした後、元に戻すことと引き換えに金銭を要求するマルウェア