平成２８年１２月８日

# １１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**

## ○　「マルウェア除去ツール」を偽装するランサムウェア

トレンドマイクロは11月10日、被害者に身代金を要求するランサムウェアに感染させることを目的とする日本語のメールがばらまかれているとして注意を呼び掛けた。

これまで、日本でのランサムウェアの拡散は主に英文メールによるものであり、今回のメールも日本国内で約30件しか確認されていないが、今回と同様の手口の日本語によるメールを10月以降繰り返し確認しており、トレンドマイクロではランサムウェアを使用するサイバー犯罪者が新たに日本を標的とし始めたことを示す兆候と見ている。

今回確認されたマルウェアスパムは、「【重要】総務省共同プロジェクト コンピューターウイルスの感染者に対する注意喚起及び除去ツールの配布について」という件名と本文で利用者をだまし、マルウェア除去ツールに偽装したランサムウェアをダウンロードさせて感染させようとするもの。メールは通信を匿名化する①Tor（トーア：The onion router）を利用する海外のフリーメールサービス「SIGAINT」で送られている。

メール本文は、受信者が「オンライン銀行詐欺ツールのマルウェア『VAWTRAK』に感染しているため、その除去ツールを配布する」という内容になっており、ZIPファイルが添付されている。ZIPファイルを解凍すると２つのPDFファイルが現れ、除去ツールのダウンロード方法や設定手順が記載されている。

設定手順では、メールの受信者にセキュリティソフトの機能オフを求め、海外のクラウドストレージサービスである「MEGA」からデータをダウンロードするように指示している。実際にダウンロードされるのは除去ツールではなくランサムウェアであり、最近流行しているLOCKYとは異なるマルウェアであることが確認されている。

## ○　オンライン銀行ユーザーを狙うマルウェアが急増

セキュリティ企業ESET等は11月21日、10月までのマルウェア動向を発表した。発表によると、10月までの直近１年間の国内マルウェア検出状況は、７月～９月期の総検出数が４月～６月期に比べて80%増加したという。10月だけでも既に前年の10月～12月期を上回るペースにあるとしている。

検出増加の背景には、オンライン銀行ユーザーを狙うマルウェアやランサムウェアへの感染を狙う攻撃の増加があるという。特にオンライン銀行ユーザーを狙うマルウェア「Bebloh（別名：URLZONE）」

の 10 月の検出割合は、８月の 5.0%から約４倍に増加した。攻撃では巧妙な日本語メールが使われ、アイコンや拡張子が細工された不正なファイルが添付されているケースが多い。受信者がマルウェアに感染してしまうと、オンライン銀行サービスの利用時に情報が盗み取られ、不正送金の被害に巻き込まれるなどのおそれがある。

また、ランサムウェア感染を狙う攻撃では、メールに不正な[②]スクリプトを添付して送り付けるケースが目立つ。５月以降は JavaScript の検出割合が 50～60%台で高止まりしている状況にあるが、10 月に入ってからは[③]PowerShell を使う手口が急増。PowerShell を使う手口は米国で多く検出されてきたが、攻撃者が日本も標的に加えた可能性があると関係者はみている。

---

① 仮想回線接続により、通信を複数のノードを経由させることにより、接続経路の匿名性を高めている
② コンピュータプログラムの種類のひとつで、決まった条件のもとで動く簡易式プログラム
③ Windows に組み込まれている拡張可能なコマンドラインインターフェース（CLI）シェル及びスクリプト言語