

3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

○ 新種の不正送金ウイルスを国内で初めて確認

警視庁は3月16日、インターネットバンキングで不正送金する新種のコンピュータウイルス「ドリームボット」を国内で初めて確認したと発表した。

このウイルスは、迷惑メールに添付されたファイルを開いたり、ウイルスが仕掛けられたサイトを閲覧したりすると感染する。

感染したパソコンなどの端末でインターネットバンキングを利用すると、使い捨てで安全性が高い「ワンタイムパスワード」の入力を求める偽画面が表示され、そこに銀行から付与されたパスワードを入力すると、自動で第三者の口座に不正送金される。

日本サイバー犯罪対策センターは、ホームページで、端末のウイルス感染をワンクリックで確認できるサイト (<https://www.jc3.or.jp/info/dgcheck.html>) を開設した。



○ USBストレージのデータを盗み取るマルウェアを発見

3月31日、JPCERT/CC (JPCERT コーディネーションセンター) は、USBストレージ内のデータを盗み取って外部に送信するマルウェアの情報を公開し、注意を呼びかけた。

マルウェアは、ネットワーク接続された端末に侵入して常駐し、端末にUSBストレージが接続されると、「interad.log」、「slog.log」等の名前で、そこに保存されたファイルの一覧をPC内に生成する。攻撃者は、ここから標的とするファイルを選んでリスト化し、これを基にストレージ内のファイルを圧縮して別の感染端末から細分化した上で外部へ送信するというもの。

JPCERT/CC は、クローズドネットワーク内で情報を管理している環境でも、同手法が悪用されれば、ストレージ内のデータが窃取されるとして、ストレージ管理ツールの見直し等の対策を挙げて注意喚起している。