

## 第10回 パスワード・スティーラー

フィッシングは様々な手法を用いて個人情報を搾取することを目的としていますが、クライムウェア（悪意を持った、犯罪目的のプログラム）を利用してログイン時のパスワードを盗む事を目的としているものもあり、総称して「パスワード・スティーラー」と呼ばれています。今回はスペイン語圏の銀行を標的としたパスワード・スティーラーの事例についてご紹介いたします。

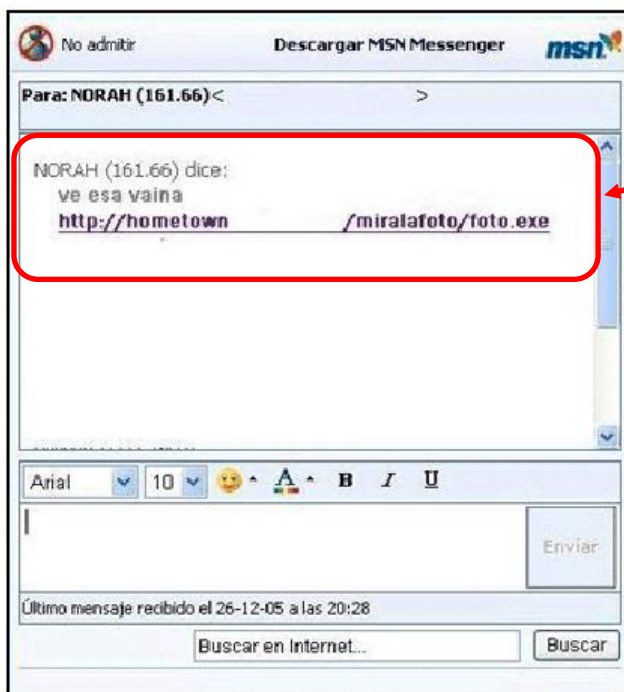
- - - 「APWG Phishing Activity Trends Report 2005年12月 日本語版」より - - -

### 事例：スペイン語圏の銀行を狙ったパスワード・スティーラー（Panda Labs による報告）

「Banker.BSX」と呼ばれるクライムウェアは、銀行口座のパスワードを盗み出すトロイの木馬で、ポート 1106 を開いた上でスペイン語圏にある特定の銀行サイトにユーザがアクセスするのを監視し、パスワードを盗み取るというものです。「Banker.BSX」はそのウェブサイトで実行されるバーチャル・キーボードでのログインやパスワードのタイピング行為を含むユーザー操作を掌握します。次に、そのクライムウェアは収集したデータを特定のEメールアドレス宛てに送信します。

「Banker.BSX」は、MSN メッセンジャーを介して流布する「Nabload.U」と呼ばれる別のトロイによって被害にあったPCにダウンロードされていました。

サンプルメッセージ画面：



「Nabload.U」により MSN メッセンジャーを介して「Baker.BSX」が流布されている状態。