フィッシング対策協議会

月次報告書（２００５年９月分）

APWG Phishing Activity Trends Report (July 2005)
日本語版

２００５年１０月２０日

目次

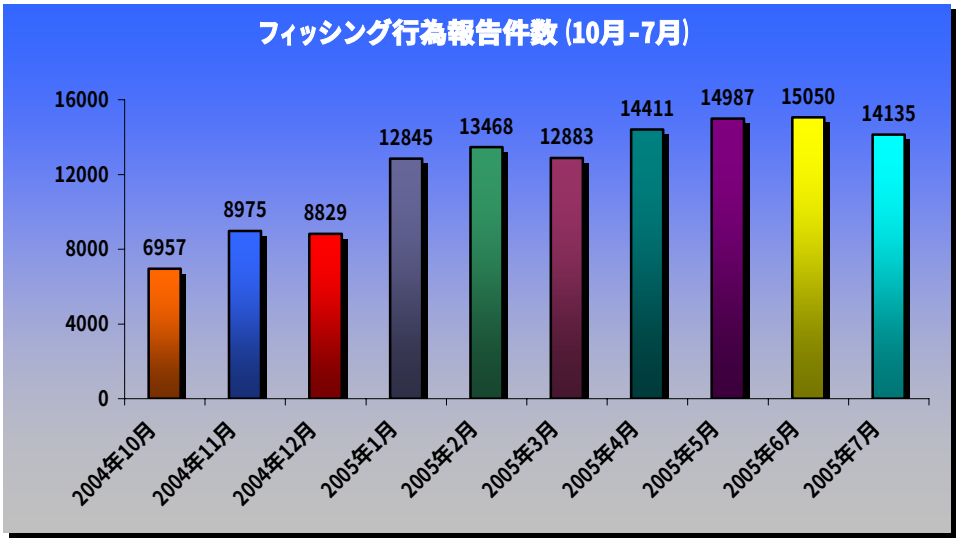
1. APWG Phishing Activity Trends Report 2005年 7月　日本語版

『フィッシング(phishing)』とはオンライン上での個人情報の窃盗行為のことを指し、巧詐eメールを用いて、その受信者を詐欺目的の偽装ウェブサイトに誘い出し、被害者のクレジットカード番号や口座のユーザーネーム・パスワード、社会保障番号等を巧みに暴き出すものです。社会的信用が確立している大手の銀行やオンライン小売業者、クレジットカード会社の商標をハイジャックすることにより、フィッシング犯は被害者を信用させ個人情報を盗み出すことに成功しています。このような詐欺行為によりクレジットカードが詐欺被害に遭ったり個人情報が盗み取られる等して経済的損失を被る被害が消費者の間で増加しています。

『フィッシング行為最新事情レポート』では、フィッシング対策実務者グループ（ＡＰＷＧ）がそのウェブサイト http://www.antiphishing.org 上あるいはグループ宛ての e メール reportphishing@antiphishing.org で報告を受けたフィッシング攻撃の事例を分析します。ＡＰＷＧが保有するフィッシング攻撃の事例に関する情報データベースは、eメール詐欺およびフィッシング行為についての最も包括的なインターネット・アーカイブです。

1.1. 【Highlights】ハイライト

・7 月期のフィッシングに関する報告件数	**14,135**
・7 月中にフィッシングによりハイジャックされた商標数	**71**
・7 月中にフィッシング行為を受けた上位 80%に属する商標数	**6**
・7 月期最も多くのフィッシング・ウェブサイトのホストとなった国	**米国**
・標的となりうる名称がなんらかの形で含まれているＵＲＬ	**46%**
・IP アドレスのみでホストネームなし	**41%**
・ポート 80 を使用しないサイトの割合	**9%**
・サイトのオンライン上の平均残存期間	**5.9 日間**
・サイトの最長オンライン残存期間	**30 日間**



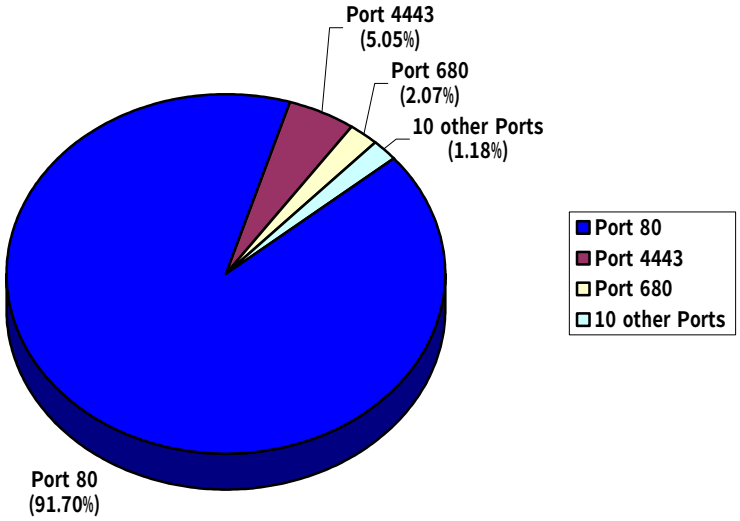
フィッシング行為報告件数（月単位／2004 年10 月～2005 年7月）

『フィッシング行為最新事情レポート』(The Phishing Attack Trends Report)は、顕著な問題となりつつあるフィッシングあるいは e メール詐欺（スプーフィング）に起因する個人情報の盗難および詐欺行為の撲滅を目指す産業界連合団体「フィッシング対策実務者グループ」(Anti-Phishing Working Group)が月例発行しています。詳細はロニー・マニング manning@websense.com（電話 858-320-9274）、または APWG 事務局長ピーター・キャシディ（電話 617-669-1123）までお問い合わせください。『フィッシング行為最新事情レポート』(The Phishing Attack Trends Report)の分析研究は、次の企業からの提供によるものです。

1.2. 【Top Used Ports Hosting Phishing Data Collection Servers】

フィッシングしたデータの集積サーバのホストとして最も使用されたポート

7 月期はフィッシング用ホスト・サイトにカズン（類似）ドメイン名を使用する傾向が続きました。その結果、代替ポートの使用は減少し、標準的なHTTPポート 80 の使用が報告を受けた全フィッシング・サイトの 91.7%に上りました。

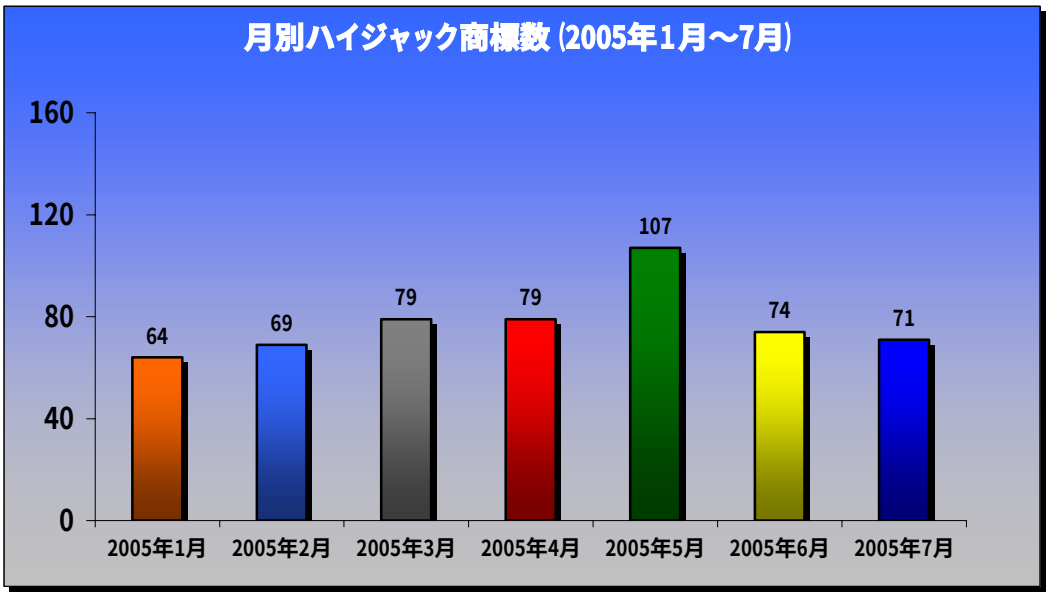


フィッシング・サイトとして最も使用された HTTP ポート

1.3. 【Brands and Legitimate Entities Hijacked By Email Phishing Attacks】

e メール・フィッシング攻撃によってハイジャックされた商標および合法的法人組織、報告された商標数

７月期にフィッシング被害を被った商標の報告件数は再び減少し 71 件となりました。しかしながらフィッシング犯（フィッシャー）は標的の網をより広範囲に拡げ、従来からの大企業を標的とすることからより小規模の金融機関を広範囲に渡って攻撃するようになってきています。

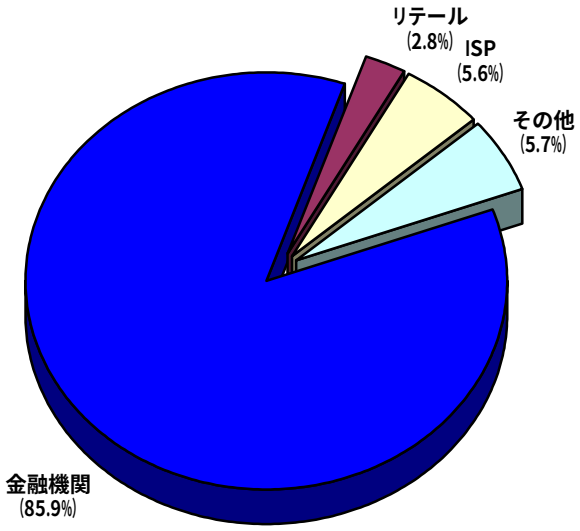


ハイジャック商標数（2005 年 1 月～7 月）

1.4. 【Most Targeted Industry Sectors】最も標的となった産業分野

金融サービス分野が引き続き最もフィッシングの標的となった産業分野であり、全攻撃の 86%に上るまで増加しました。APWG は保険、信用組合、支払サービス事業及び ATM のネットワークを含む金融サービス分野での新しい標的を確認しています。

また、ヨーロッパの金融機関と ISP を標的とした攻撃についての報告が増加していることに加え、カナダの機関に関する攻撃報告も増加しました。

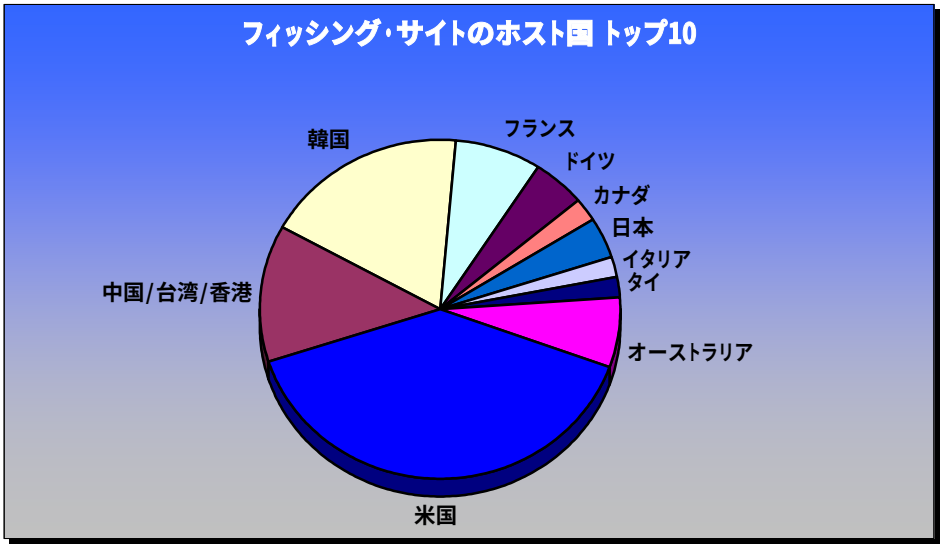


最も標的となった産業分野

1.5. 【Web Phishing Attack Trends】ウェブに対するフィッシング攻撃事情
フィッシング・サイトのホストとなった国

7 月期 Websense Security Labs は、オーストラリアがホスト国であるフィッシング･サイト数の激増を確認しました。アメリカは全フィッシング･サイトの 30%のホストとなり第一位に留まっています。トップ 10 のその他は、韓国 14%、中国 10%、フランス 6%、オーストラリア 5%、ドイツ 3.5%、日本 3%、カナダ 1.7%、タイ 1.5%、イタリア 1.5%でした。

イギリスあるいはアメリカに拠点を置かない商標に対するフィッシング攻撃が益々頻繁になってきています。アメリカ及びイギリスは依然として最も攻撃されやすいのですが、Websense Security Labs では英語以外の言語による攻撃の増加傾向を確認しており、イタリア、スペイン、日本、韓国、ドイツといった国のユーザーからの信用情報獲得を目指した試みとなっています。



フィッシング・サイトのホスト国

攻撃方法最新事情

プロジェクト：クライムウェア

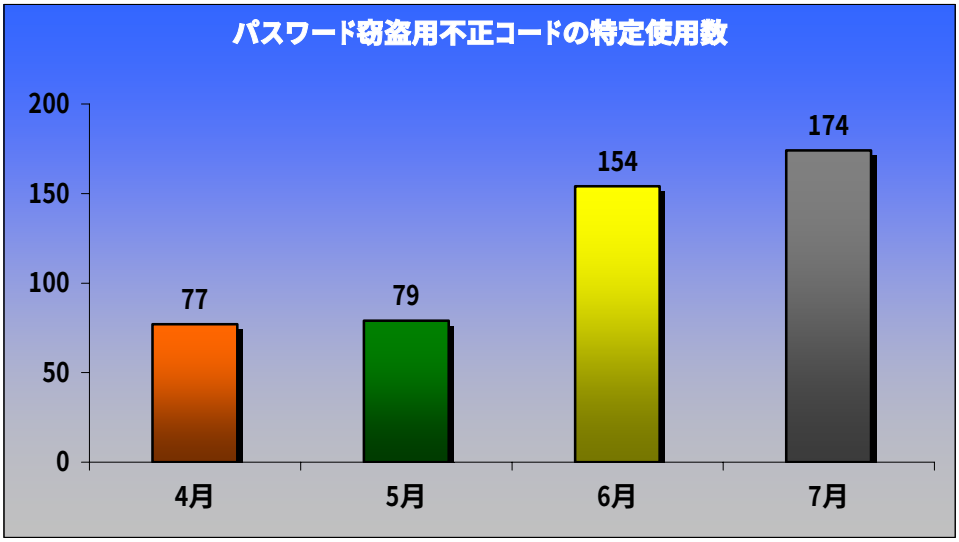
「クライムウェア」分類詳細

「プロジェクト：クライムウェア」は、月例報告においてクライムウェアによる攻撃の区分体系を整理分類して報告します。

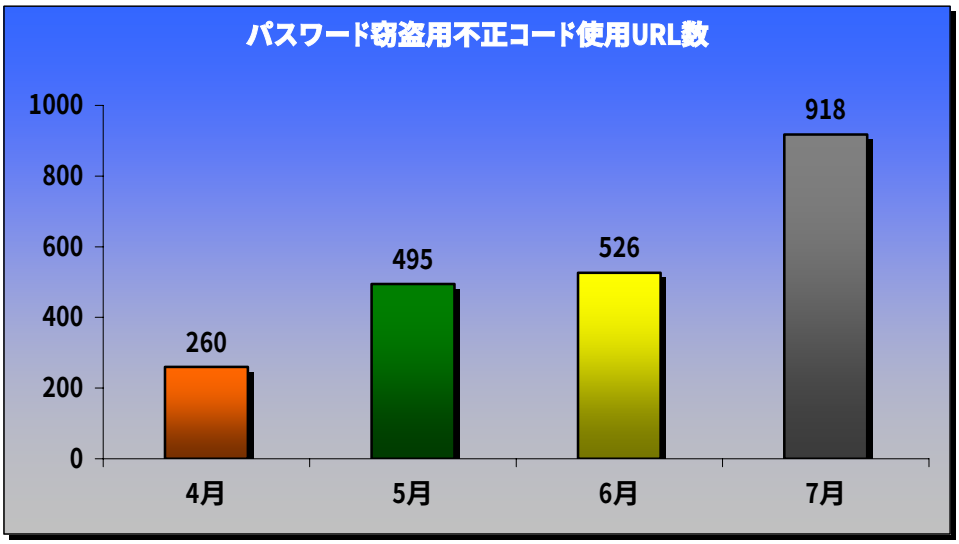
「フィッシング用トロイの木馬－キーロガー」

Websense Security Labs は 7 月期再びキーロガーに分類されるクライムウェア及び銀行を標的とした新種のキーロガーの増加を確認しました。このようなキーロガーをホストするウェブサイト件数の増加については更に目を見張るものがあり 100%に近い増加率となっています。トロイの木馬系キーロガーの全ホスト・サイトの 70%近くが米国とブラジルにあり、主にオンライン・ジャーナル、ブログや個人用情報貯蔵（パーソナル・ストレージ）に使用される個人用ウェブサイトがホストとなっています。

フィッシング用トロイの木馬－キーロガー（特定変種）



フィッシング用トロイの木馬－キーロガー（キーロガーのホストとなった特定ウェブサイト）

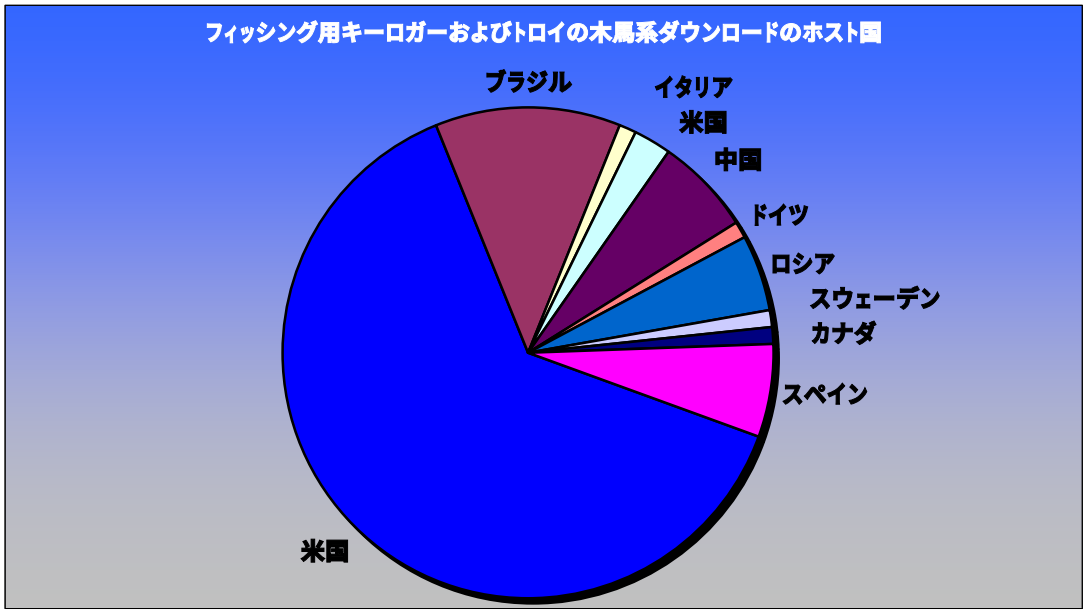


フィッシング用トロイの木馬とダウンローダーのホスト国 (IP アドレスによる)

下記のチャートは、フィッシング用キーロガーまたはキーロガーをダウンロードさせるトロイの木馬系ダウンローダーの形態を取る不正コードのホストとして 7 月中に分類されたウェブサイトの内訳を示すものです。

米国は依然として地理的所在地のトップで 57%以上を占め、ブラジルが第 2 位で 11%です。先月の報告に引き続きブラジルは依然としてブラジルの金融機関をターゲットとしたポルトガル語で書かれた詐欺技術を用いたフィッシング用キーロガーの最も高い集積率を示しています。

その他の内訳は、中国 5.7%、スペイン 5.4%、ロシア 4.4%、イギリス 2.4%、カナダ 1.2%、ドイツ 1%、スウェーデン 1%、イタリア 1%でした。

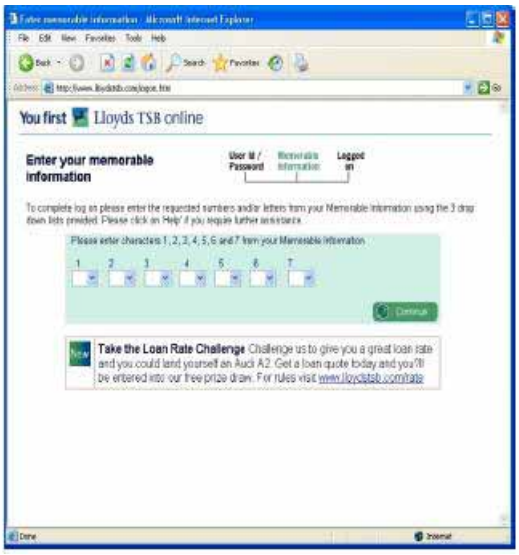


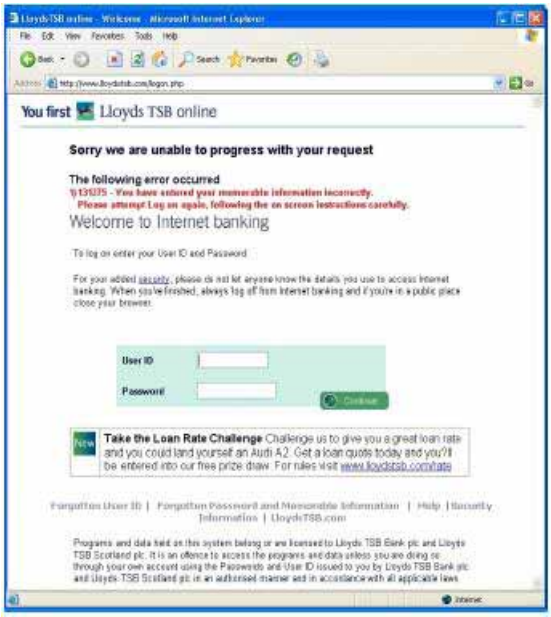
「フィッシング用トロイの木馬ーリディレクター」

7 月期は、実在するサイトの URL を入力すると詐欺サイトに誘導（リディレクト）されてしまうように個人のパソコンのシステムを改造してしまうよう設計されたトロイの木馬の出現数が増加しました。中でも最も多いのが個人のパソコン上でホスト・ファイルを改ざんしてしまうというものです。

Websense Security Labs では、ユーザーに対するフィッシング攻撃を行うトロイの木馬の新変種を検知しました。このトロイの木馬は感染したマシン上でホスト・ファイルの改ざんを行い、ある銀行の本物のアドレスが入力されるとそれをフィッシング用サイトの IP アドレスにマッピングしてしまうというものでした。このマッピングにより、ユーザーが自分の銀行口座へのアクセスを試みた場合、フィッシング用サイトへ誘導（リディレクト）されてしまうのです。

例えば次に示す画面では、ブラウザはスクリーン上では正しいウェブアドレスを表示していますが、実際はフィッシング用サイトを取り込んでしまっています。ユーザーがログオン情報を偽ウェブサイトに入力すると、この銀行の本物のウェブサイトにリディレクトされます。このトロイの木馬はキーロガーとしても機能し、ユーザーのオンライン銀行へのアクセスを一旦検知すると、そのキー・ストロークを捕捉し始めます。次にこのトロイは捕捉したキー・ストローク情報をアタッカーにアップロードします。

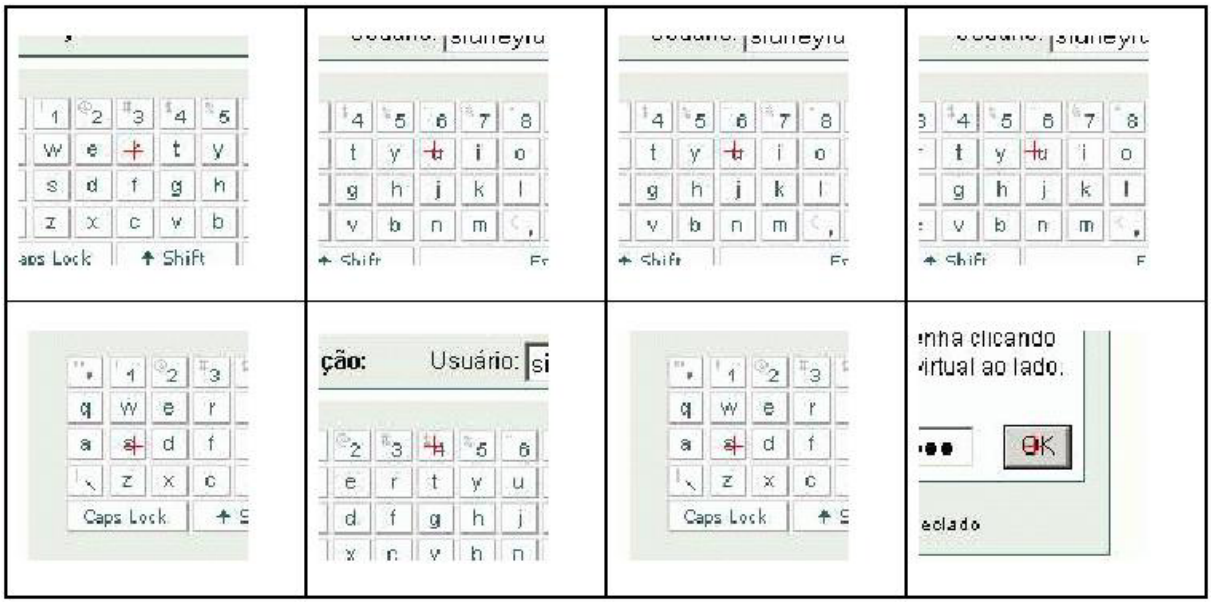




「スクリーン・スクレーパー」

7 月期の後半、我々は以前よりも頻繁にもう一つのトロイ系詐欺テクニックが使用され始めていることを察知しました。これらはエンドユーザーの信用情報を獲得するために、標的となったパソコンのモニター画面（スクリーン・ショット）そのものを捕捉するよう設計されたトロイの木馬です。キーロガーによるフィッシング被害の増加に伴い、いくつかの銀行ではウェブサイト内に於けるユーザーの本人確認の方法を変更してきました。この場合、ユーザーはブラウザのポップアップ・ウィンドウの数字キーパッドをクリックすることによりログオンすることが求められます。

詐欺コードは、アクティブになったウィンドウが情報をモニターしたいウィンドウになるまで待機します。そして一旦そのプログラムにアクセスすると、マウスでのクリック操作を行う画面そのものの「削り取り（スクレープ）」を行い、得られた情報を詐欺サイトにアップロードすることにより信用情報を奪取します。下の例はウェブサイトで「スクリーン・スクレーパー」が実行される場合のイメージです。



Anti-Phishing Working Group について

フィッシング対策実務者グループ（APWG）は、顕著になりつつあるフィッシングや e メール・スプーフィングの問題に起因する個人情報の窃盗および詐欺行為の撲滅対策を中心課題として活動する産業界連合団体です。この連合団体では、フィッシング問題について討議し、ハードおよびソフトのコスト面からフィッシング問題の問題範囲を定義し、問題解決のための情報と最良の実践例を共有するためのフォーラムを提供します。また、適当と判断される場合には、APWG はこれらの情報を司法当局と共有する意思があります。

グループへの加入は、一定条件を満たす金融機関、オンライン小売業者、インターネット・サービス・プロバイダーと司法機関およびソリューション・プロバイダーに公開しています。APWG には 900 近くの企業および政府機関が加入しており、会員数は 1,400 名近くに上ります。フィッシング攻撃および e メール詐欺は、オンライン上でビジネスを行う多くの組織にとって組織の機密にかかわる問題であるため、APWG の方針として会員組織についての情報は公開していません。

フィッシング対策実務者グループのウェブサイトは、 http//:www.antiphishing.org です。
公共および産業界のためのフィッシングと e メール詐欺問題に関する情報の供給源としての機能を担っており、これにはフィッシング攻撃に対して即効性があり有用で実用に即した技術的な解決方法の特定と普及促進を含みます。フィッシング攻撃に関する問題分析、法的手段の行使、記録保持作業は現在タンブルウィード・コミュニケーションズ (Tumbleweed Communications) のメッセージ保護研究所により提供されています。

APWG はタンブルウィード・コミュニケーションズおよび数社の会員銀行と金融機関、e コマース・プロバイダーによって設立されました。2003 年 11 月にサン・フランシスコにおいて最初の会合が開かれ、その後 2004 年 6 月には、グループの運営委員会と理事会および執行委員会により運営が管理される独立法人となりました。