フィッシング対策協議会

月次報告書（２００６年９月分）

APWG Phishing Activity Trends Report (July 2006)
日本語版

２００６年１０月２０日

目次

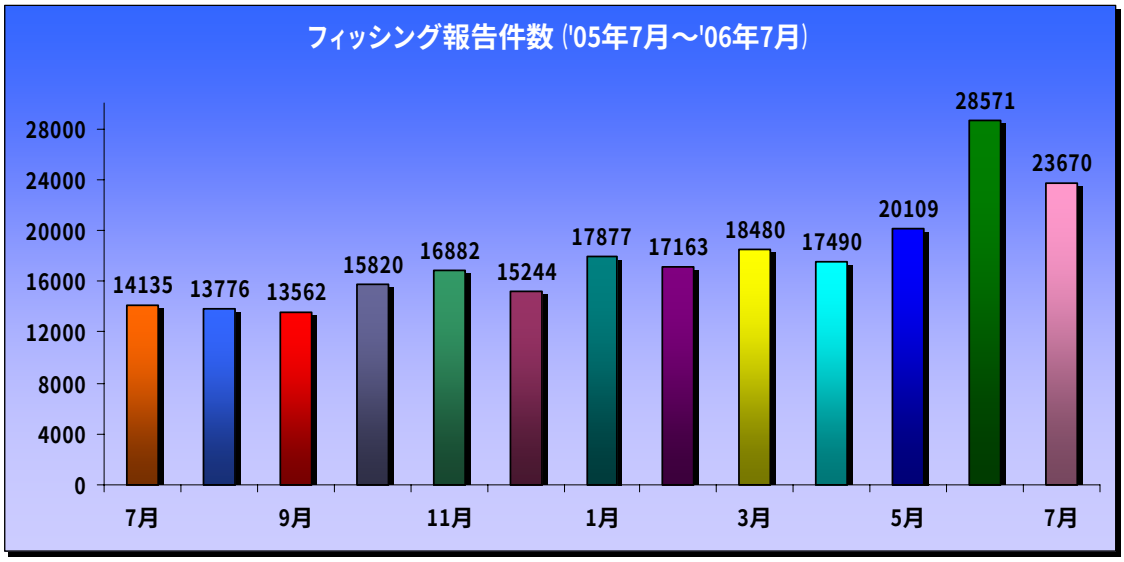
1. APWG Phishing Activity Trends Report 2006年7月　日本語版

『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、ソーシャルエンジニアリングや悪意のあるプログラムを使い、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。ソーシャルエンジニアリングでは偽装した電子メールが使われ、受信者を騙して、ユーザーネームやパスワードなどの情報を盗むために用意した偽装Webサイトへ誘導します。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。また、悪意のあるプログラム（Crimeware：クライムウェア）をPCに仕掛けて個人情報を盗む場合には、キーロガーがしばしば使われています。さらに、インターネット接続時の経由するルートを不正に改ざんし、偽装Webサイトへ誘導するような手法もあります。

『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電子メール 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ています。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。加えてAPWGでは、会員企業によるCrimeware（クライムウェア）の傾向（タイプ、発生数、拡散の仕方）について調査した結果をまとめています。

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	**23,670**
・7 月期に報告されたフィッシング・サイト数	**14,191**
・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	**154**
・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	**15**
・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	**42%**
・ポート 80 を使用しないサイトの割合	**8.9%**
・サイトのオンライン上の平均残存期間	**4.8 日間**
・サイトの最長オンライン残存期間	**31 日間**

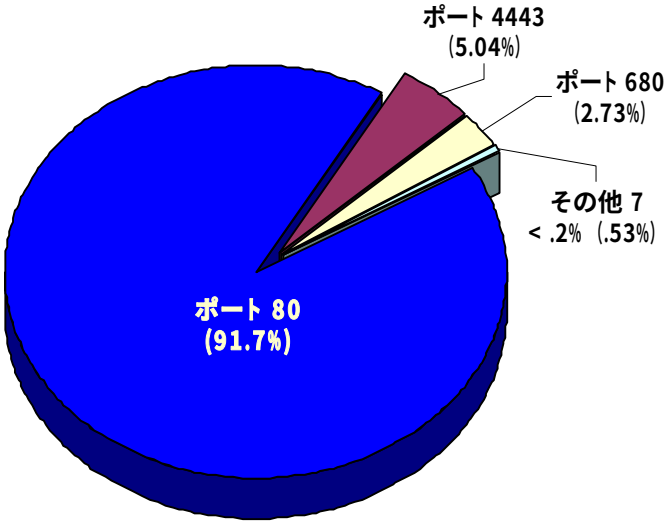


フィッシング行為報告件数（月単位／2005 年7月～2006 年7月）

『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HTTPポート 80 が最も頻繁に使用されるポートとなる傾向が続き、報告された全フィッシング用サイトの 91.7%に上りました。

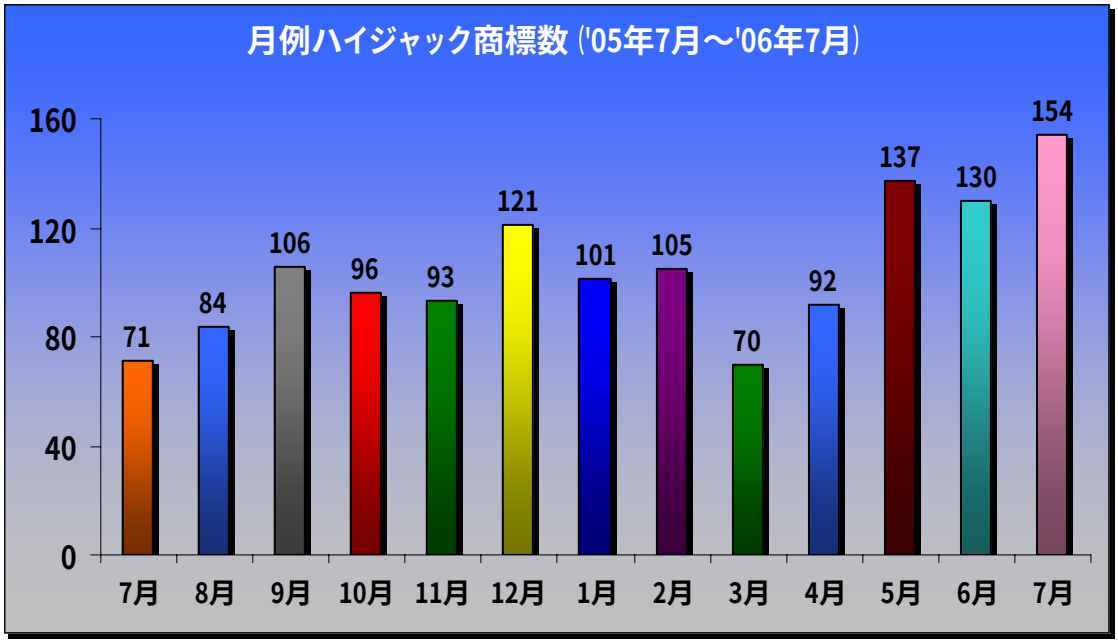


フィッシング・サイトとして最も使用された HTTP ポート

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

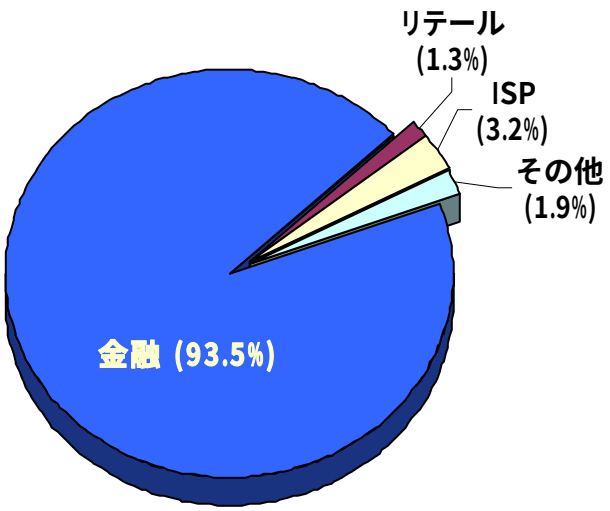
2006 年 7 月期にフィッシング攻撃の標的にされた商標数は、APWG がこれまで記録してきたなかで最も多い数となりました。



ハイジャック商標数（2005 年 7 月～2006 年 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標的となった産業分野となり、7月期は全攻撃の93.5%に上りました。

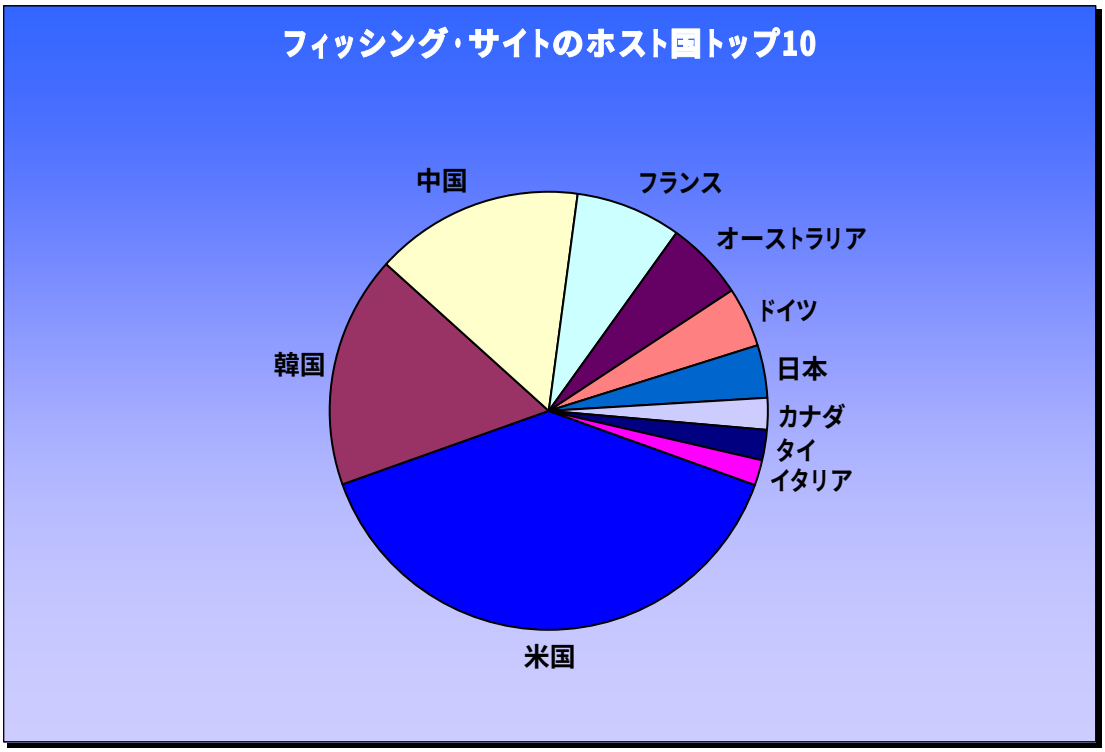


最も標的となった産業分野

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、トップ 3 のフィッシング用サイトのホスト国に変動がないことを確認しました。アメリカは全体の 29.85%で引き続きトップとなりました。その他 2 位以降の国は、韓国 13.34%、中国 12%、フランス 5.87%、オーストラリア 4.56%、ドイツ 3.32%、日本 3.04%、カナダ 1.78%、タイ 1.59%、イタリア 1.52%でした。

下記チャートはフィッシング・サイトのホスト国全体の中から、トップ１０の国に対する比率を示しています。



フィッシング・サイトのホスト国

プロジェクト：クライムウェア

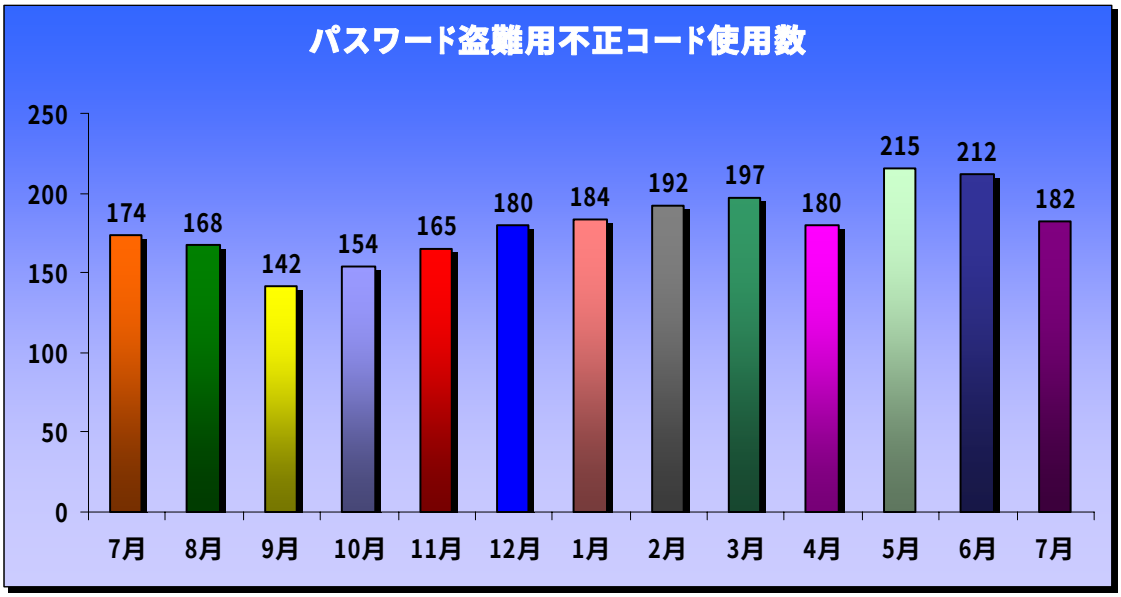
「クライムウェア」用語および７月期の分類による実例

「プロジェクト：クライムウェア」では、クライムウェアによる攻撃を以下のように分類しますが、今後新たな攻撃手法が出現してきた場合使用する用語を追加していきます。

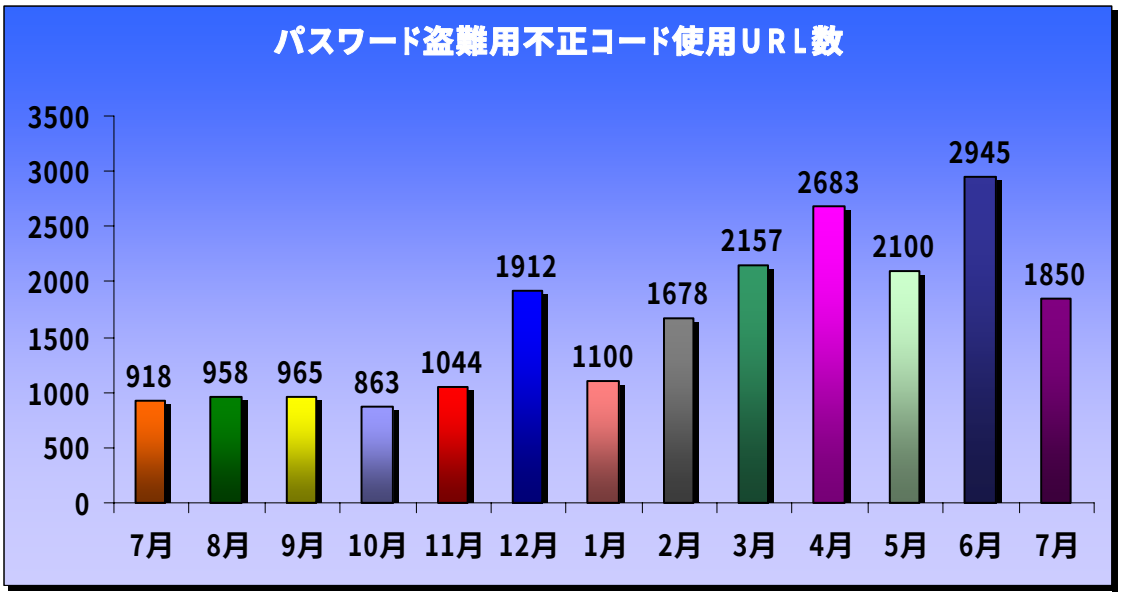
「フィッシング用トロイの木馬－キーロガー」

定義：エンドユーザーの個人情報をこれらのユーザーの信用証明を奪う目的で収集することを意図して設計されたクライムウェアのコード。フィッシングを目的としたキーロガーの場合、一般的なキーロガーとは異なり、金融機関、Eコマースやウェブをベースとしたメールサイトへのアクセスによる特定の情報獲得を目的とした特定の入力操作（そして特定の組織、最も重要なのは金融機関、オンライン小売業者、Eコマース商社）のみをモニターする追跡モニター・コンポーネントを備える。

フィッシング用トロイの木馬－キーロガー等－



フィッシング用トロイの木馬ーキーロガーのホストとなったウェブサイト



7 月期 Websense Security Labs は、新しい悪質な Web サイトを発見しました。そのサイトは、トロイの木馬をインストールする悪意のあるコードを配布しており、ユーザーが何も行わなくてもユーザーの PC にダウンロードする可能性がありました。

同サイトは 2006 年 FIFA ワールドカップの Web サイトを装っており、有名なワールドカップ決勝イタリア戦のジネディーヌ･ジダン選手の頭突き事件に関するトップニュースを扱っているという点以外は本物と同じように作られていました。

ユーザーは、同サイト上のどのページを訪れてもトロイの木馬型ダウンローダに感染する恐れがありました。このトロイの木馬はさらに、同サイトから別の悪意のあるコードをダウンロードするようになっていました。同サイトは、非合法な「Web Attacker」ツールキット（以前のアラートを参照 http://www.websense.com/securitylabs/alerts/alert.php?AlertID=472）を使用していました。

「Web Attacker」ツールキットはロシアの Web サイトで 20 ドルから 300 ドルの価格で販売されています。このツールキットを使用すると、ユーザーのブラウザの種類に応じて攻撃を行うコードをインストールさせることができるようになります。インストールされるコードには、5 つの異なる亜種のうちの 1 つが含まれています。（新旧の脆弱性を突くエクスプロイトを含む）

同サイトは米国でホスティングされていました。

サイトのスクリーンショット:

「フィッシング用トロイの木馬－リダイレクター」

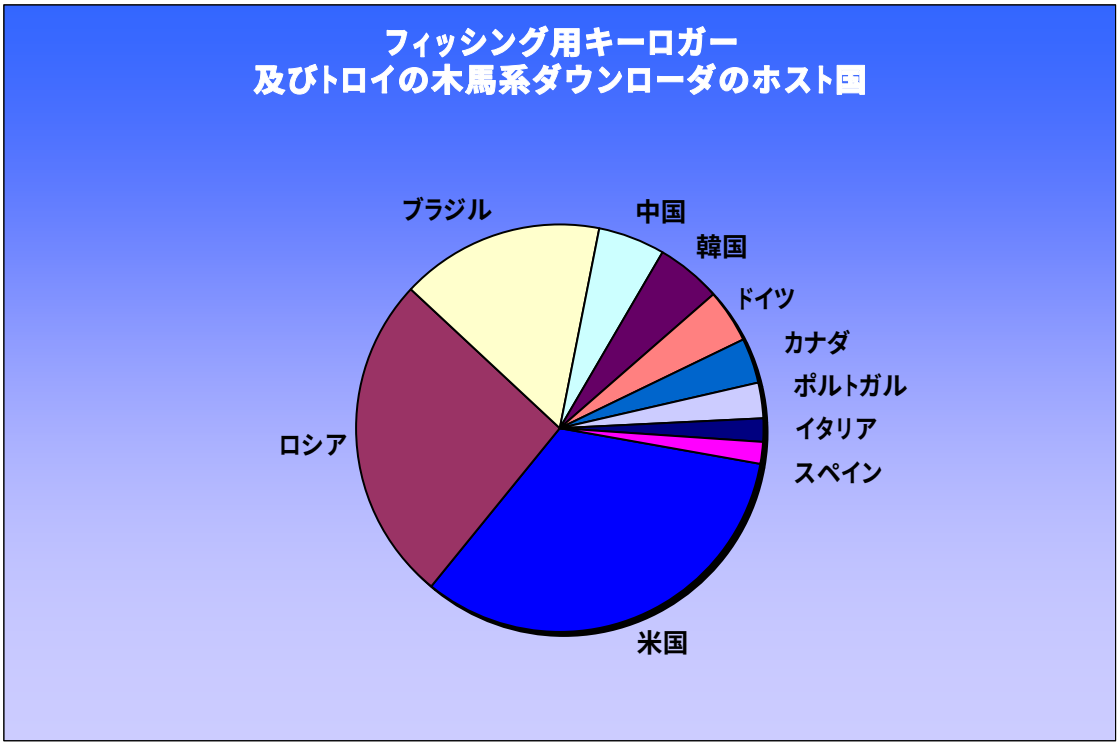
定義：エンドユーザーをネットワーク上で本来意図されていない場所に誘い出すことを目的として設計されたクライムウェアのコード。これにはホストファイルや他のＤＮＳ特有の情報を改ざんするようなクライムウェア、詐欺サイトへ情報を誘導するようなブラウザー・ヘルパー、詐欺地点への誘導を行うネットワーク・レベルでのドライバーやフィルターのインストールを行うクライムウェアを含む。これらは全て個人情報の略取やその他の信用情報の不正獲得という犯罪目的のためにインストールされる。

フィッシング用キーロガーの使用と共に、情報の行先を変えてしまうトラフィック・リダイレクタの使用も顕著に増加しているようです。特に、単純に PC ユーザーの DNS サーバやホストファイルのセッティングを部分的に変更することにより、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）するという不正コードの使用が最も多く見受けられます。詐欺用サーバはほとんどのドメインに対して有効なレスポンスを応答します。しかしながら、フィッシング犯達が消費者を銀行のサイトに似せた詐欺用サイトに誘導したいと考えた場合、単にネーム・サーバーの応答をその特定のドメイン向けに変更します。これはフィッシング犯達がユーザー側からのいつどのような入力操作についても、ユーザーにこのような不正な行為が行われていることを知られることなくリダイレクトするための特に有効な手段と考えられます。ユーザーが自分で目的のサイトのアドレスを打ち込み、メール本文や「インスタント・メッセージ」中のリンク先に入るという行為を行わなかったとしてもフィッシングに巻き込まれてしまうのです。

フィッシング用トロイの木馬とダウンローダのホスト国 (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の形態をとる不正コードのホストとして 7 月期中に分類されたウェブサイトの内訳を示しています。米国は依然として地理的所在地のトップで全体の 27.77%を占めました。その他 2 位以降の内訳は、ロシア 19.17%、ブラジル 6.1%、中国 5.98%、韓国 4.6%、ドイツ 3.74%、カナダ 3.24%、ポルトガル 3.11%、イタリア 2.86%、スペイン 2.74%でした。

下記のチャートは、フィッシング用キーロガー及びトロイの木馬系ダウンローダのホスト国全体の中から、トップ１０の国に対する比率を示しています。



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。