

月次報告書（2007年11月分）

APWG Phishing Activity Trends Report (September 2007)
日本語版

2007年12月20日

目次

1.	APWG PHISHING ACTIVITY TRENDS REPORT 2007 年 9 月 日本語版.....	2
1.1.	【HIGHLIGHTS】ハイライト.....	3
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	4
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	5
1.4.	【MOST TARGETED INDUSTRY SECTORS】最も標的となった産業分野	6
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

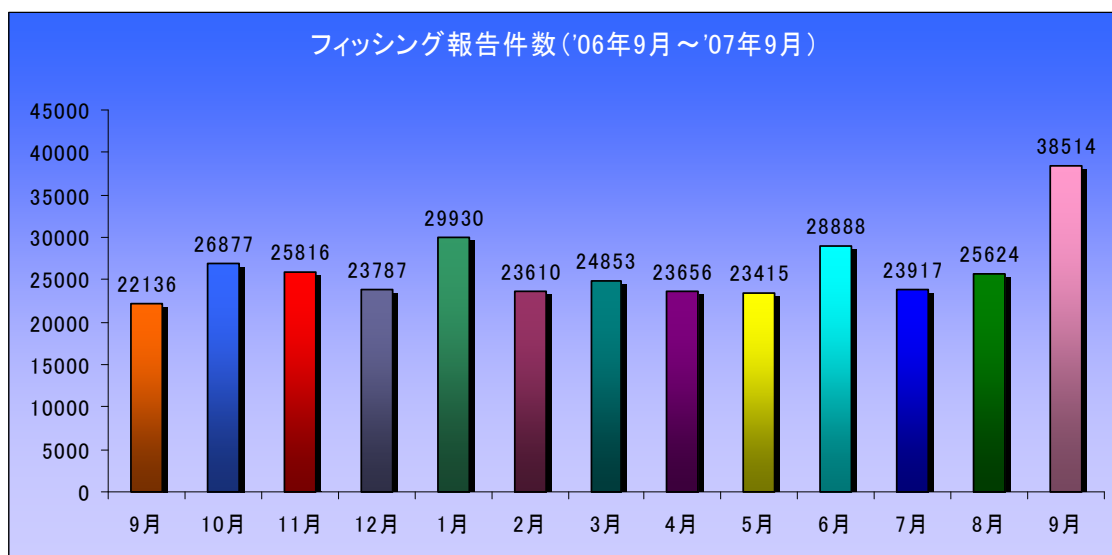
1. APWG Phishing Activity Trends Report 2007年9月 日本語版

『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ウェブ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、偽装ウェブ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

・9 月期のフィッシングに関する報告件数	38,514
・9 月期に報告されたフィッシング・サイト数	28,015
・9 月中にフィッシングによりハイジャックされた商標数	92
・9 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
・9 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	23.6%
・IPアドレスのみでホストネームなし	9%
・ポート 80 を使用しないサイトの割合	0.82%
・サイトのオンライン上の平均残存期間	3.2 日間
・サイトの最長オンライン残存期間	31 日間



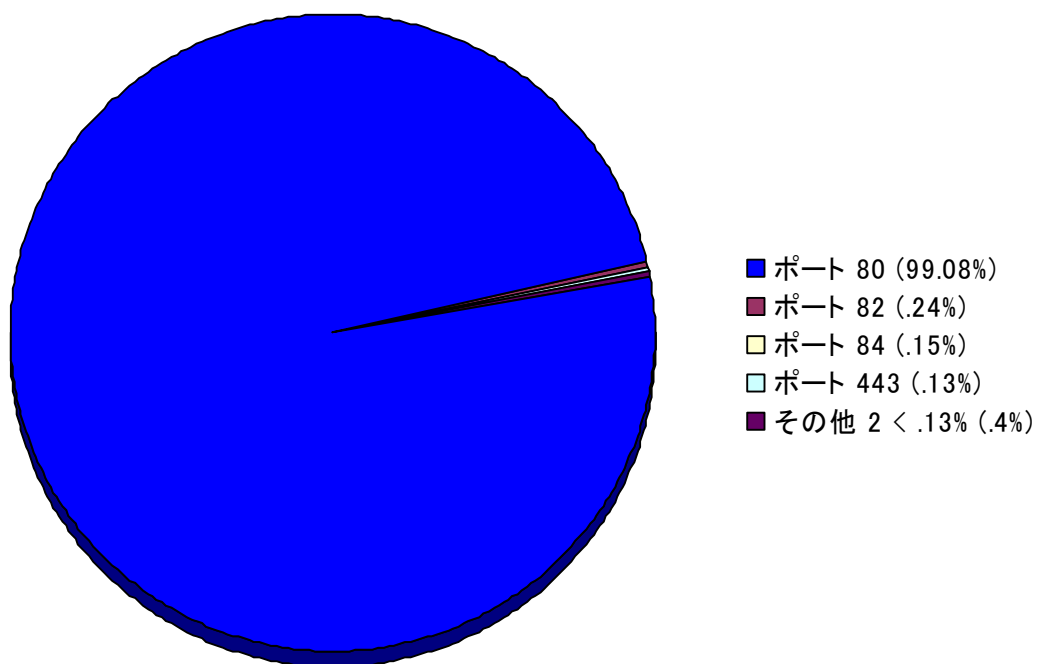
フィッシング行為報告件数(月単位/2006 年9 月～2007 年9 月)

『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 APWG 事務次長 Foy Shiver(電話 404-434-7282)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

9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99.08%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

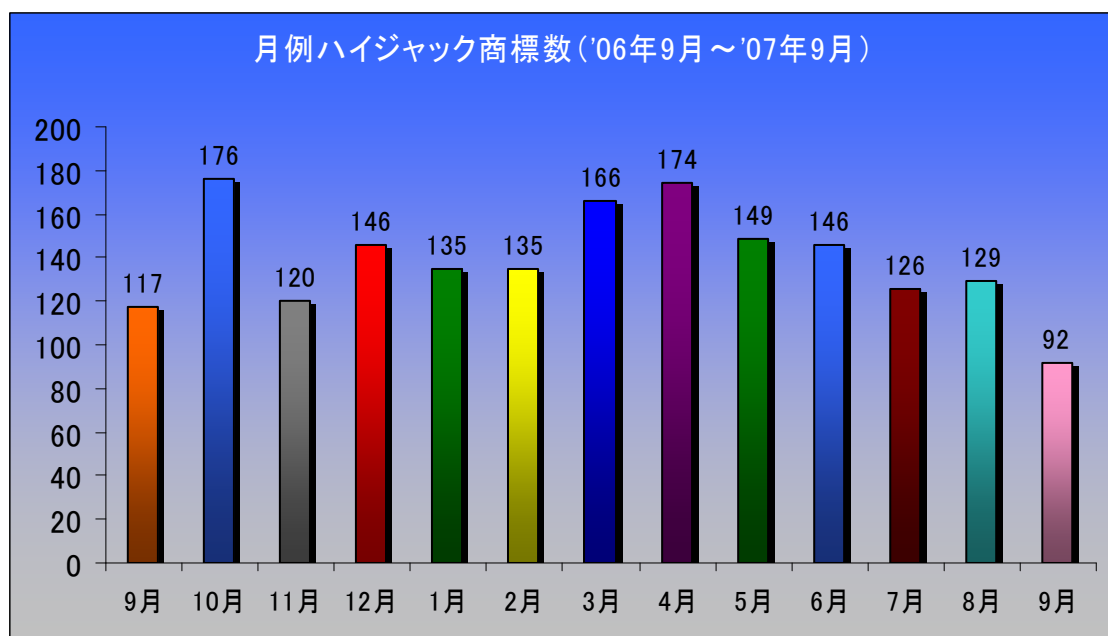
1.3. 【Brands and Legitimate Entities Hijacked By Email Phishing Attacks】

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

9月期は、ハイジャックされた商標数が大きく減少して92となりました。

銀行系ではない大手の商標の一部は、フィッシング対策およびユーザー認証技術を著しく改善しました。それらの対策は有効に機能しているとみられ、該当の商標のいくつかに関するフィッシングの報告数が減少していることを観測しています。

しかしながら、しばらくの間それほど標的にされていなかった有名な銀行に対する大規模な攻撃を確認しています。



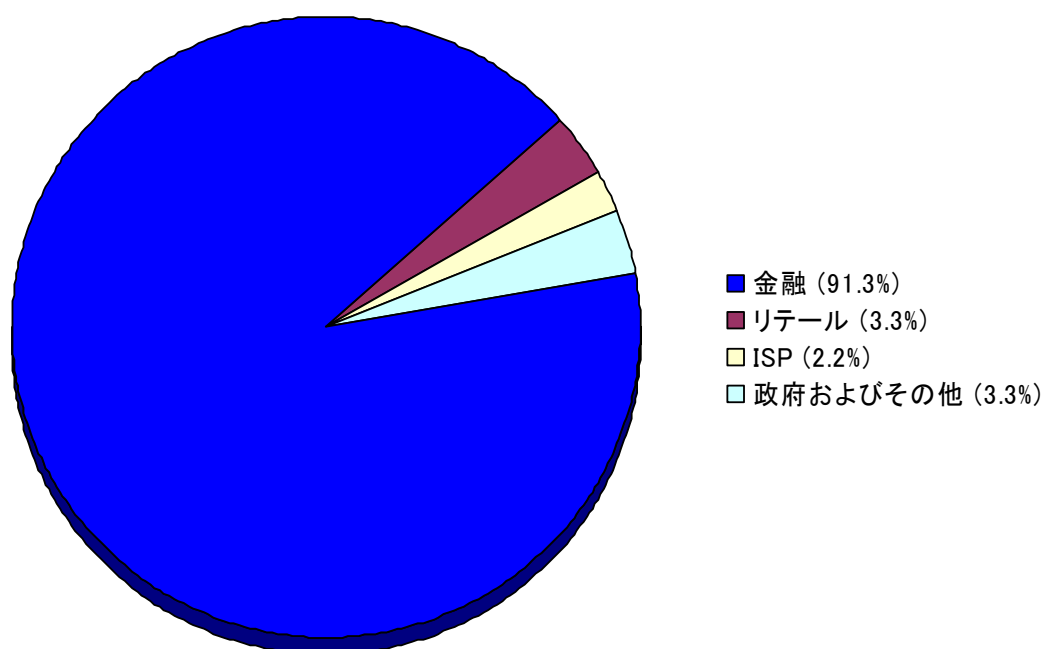
ハイジャック商標数 (2006年9月～2007年9月)

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

9 月期は、金融サービスが引き続き最も標的となった産業分野となり、全攻撃の 91.3%を占めました。

APWG は、大手インターネット小売業者およびオンライン求人サイトの一部に対するフィッシングの増加を確認しています。オンライン求人サイトが狙われているのは、ここ数か月の間にそれらのサイトが被害を受けた個人情報窃盗事件と関係があると思われます。

米国および英国の税務当局が引き続き、消費者に対するフィッシング攻撃において組織名を悪用されました。

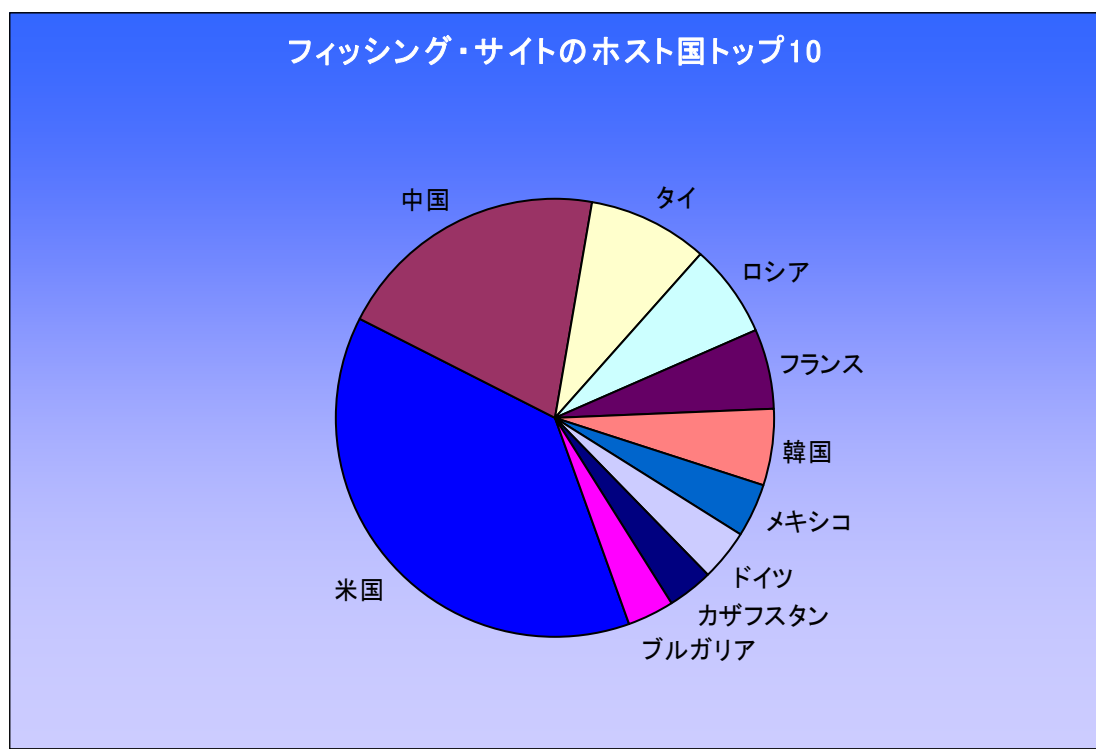


最も標的となった産業分野

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

9 月期 Websense Security Labs は、アメリカが 28.43% で引き続きフィッシング用サイトのホスト国のトップとなったことを確認しました。その他 2 位以降の国は、中国 15.22%、タイ 6.68%、ロシア 5.17%、フランス 4.41%、韓国 4.08%、メキシコ 2.97%、ドイツ 2.89%、カザフスタン 2.53%、ブルガリア 2.46% 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

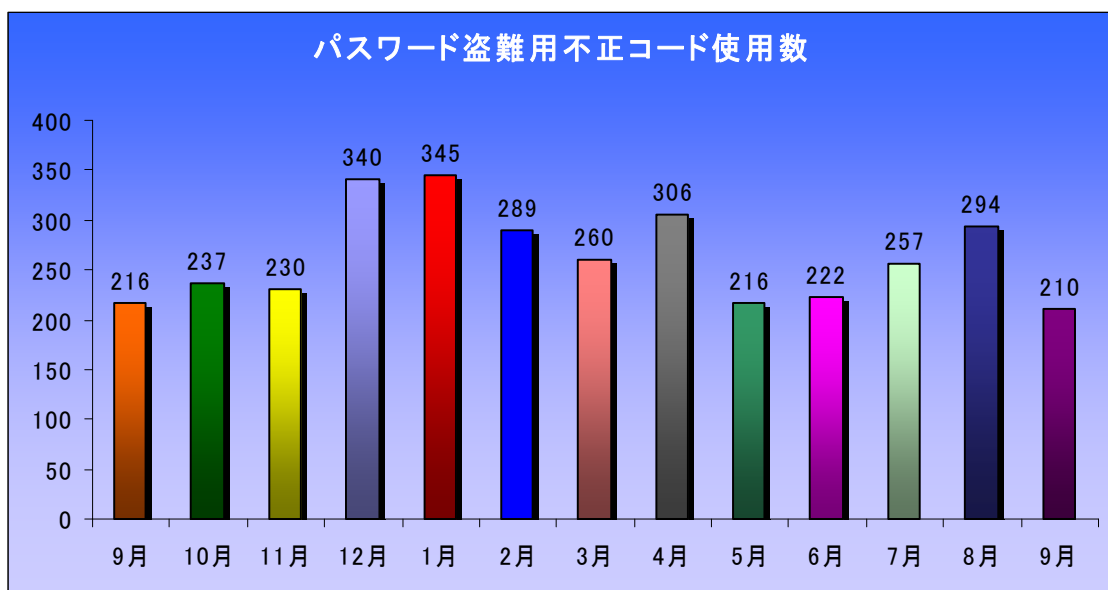
「クライムウェア」用語および 2007 年 9 月期の分類による実例

「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。

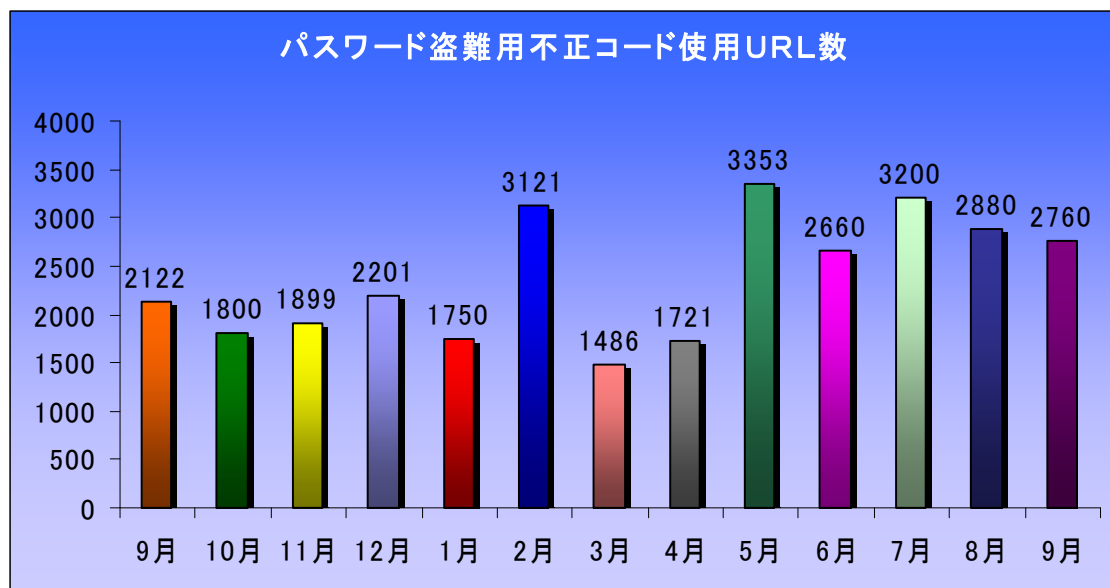
「フィッシング用トロイの木馬ーキーロガー」

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ーキーロガー等



フィッシング用トロイの木馬－キーロガーのホストとなったウェブサイト



「フィッシング用トロイの木馬－リダイレクタ」

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・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。

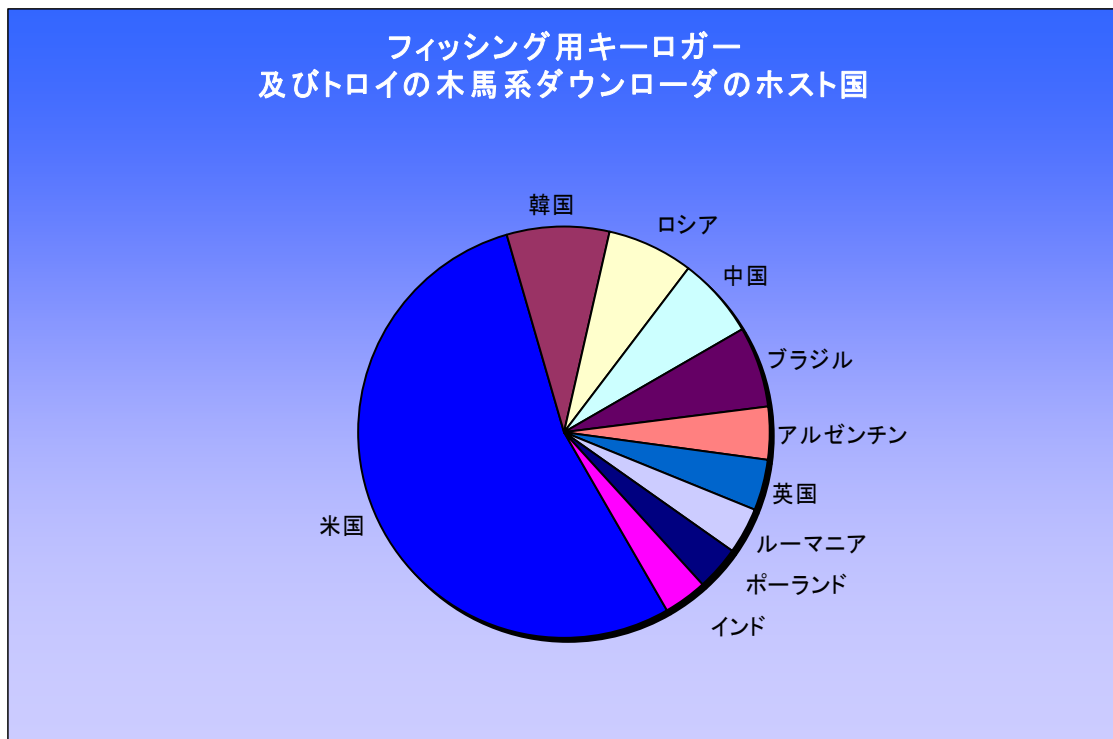
フィッシング用キーロガーの使用と共に、情報の行先を変えてしまうトラフィック・リダイレクタの使用も顕著に増加しているようです。特に、単純にPCユーザーのDNSサーバやホストファイルのセッティングを部分的に変更することにより、特定の、あるいは全てのDNSルックアップを詐欺用のDNSサーバに再誘導(リダイレクト)するという不正コードの使用が最も多く見受けられます。詐欺用サーバはほとんどのドメインに対して有効なレスポンスを応答します。しかしながら、フィッシング犯達が消費者を銀行のサイトに似せた詐欺用サイトに誘導したいと考えた場合、単にネーム・サーバーの応答をその特定のドメイン向けに変更します。これはフ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」¹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。

¹ 訳注 ネットワークを利用して直接メッセージのやり取りが可能になるソフトウェア。IM とも呼ばれる。

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9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、53.82%で引き続きホスト国のトップとなりました。その他2位以降の内訳は、韓国8.20%、ロシア6.51%、中国6.49%、ブラジル6.33%、アルゼンチン4.11%、英国3.95%、ルーマニア3.64%、ポーランド3.56%、インド3.39%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1,700以上の企業および政府機関が加入しており、会員数は3,000名以上に上ります。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。