フィッシング対策協議会

月次報告書（２００７年３月分）

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

２００７年４月２０日

目次

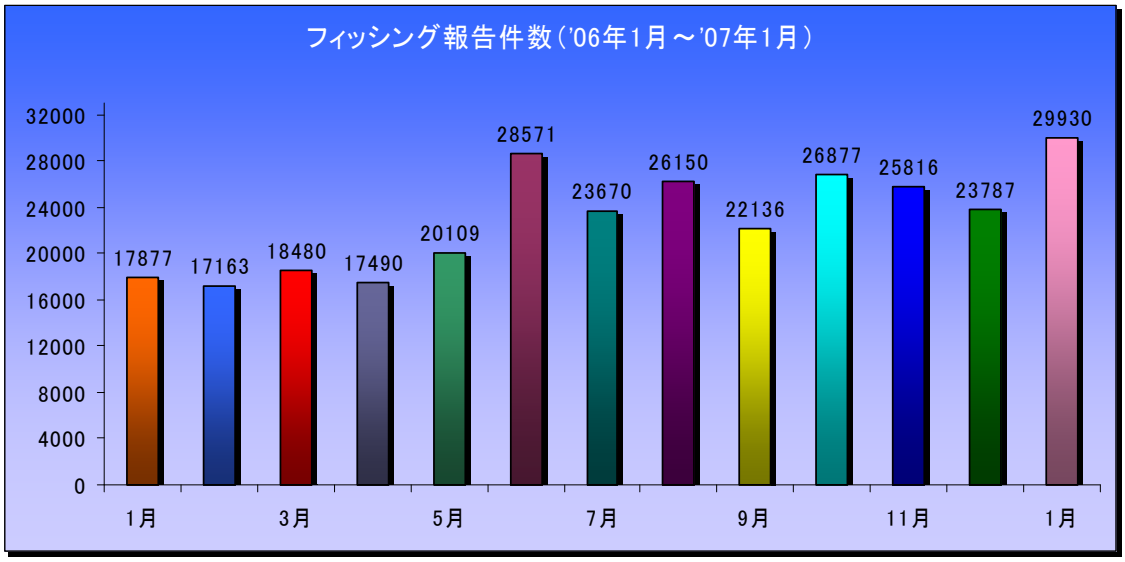
1. APWG Phishing Activity Trends Report 2007年1月　日本語版

『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

・1 月期のフィッシングに関する報告件数	**29,930**
・1 月期に報告されたフィッシング・サイト数	**27,221**
・1 月中にフィッシングによりハイジャックされた商標数	**135**
・1 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	**10**
・1 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	**24.5%**
・IPアドレスのみでホストネームなし	**18%**
・ポート 80 を使用しないサイトの割合	**3.0%**
・サイトのオンライン上の平均残存期間	**4.0 日間**
・サイトの最長オンライン残存期間	**30 日間**



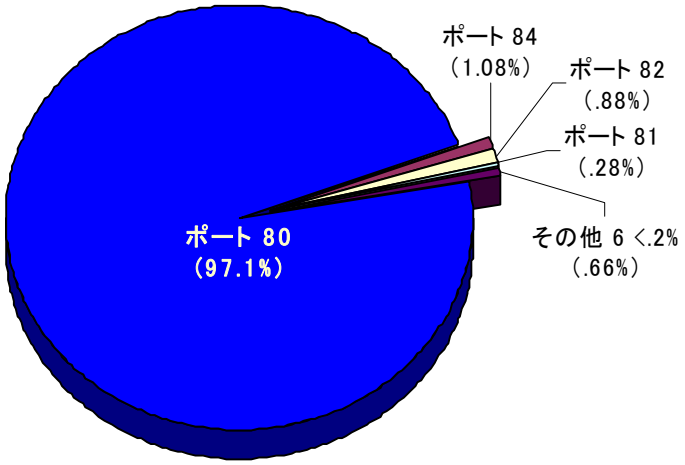
フィッシング行為報告件数（月単位／2006 年1月～2007 年1月）

『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

1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97.1%に上りました。

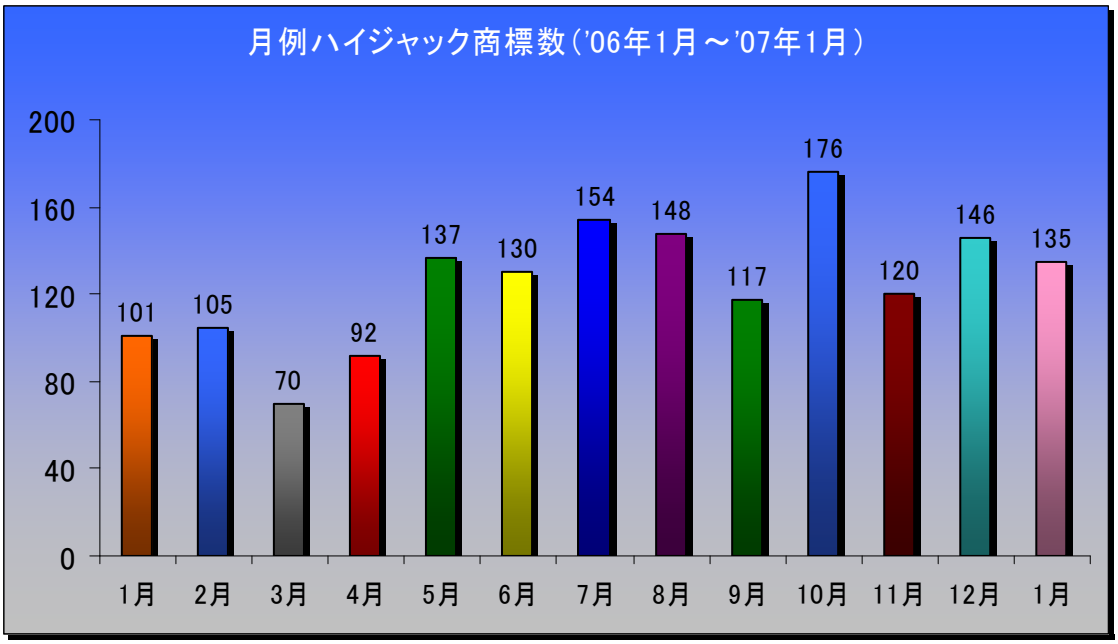


フィッシング・サイトとして最も使用されたHTTPポート

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

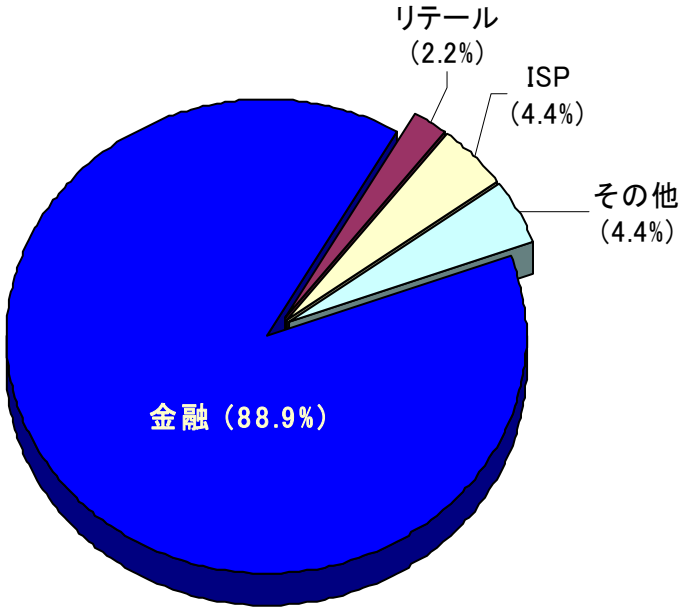
2007 年 1 月期は、前月期と同じくらいの数の商標がハイジャックされました。注目すべき点は、ソーシャルネットワーキングサイトや賭博サイトのような今まであまり被害に遭っていなかった Web サイトが多数ハイジャックされたことです。



ハイジャック商標数（2006 年 1 月～2007 年 1 月）

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

1 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 88.9%に上りました。また、より多くの証券サイトと、さらに多くの国際的な銀行、商標が詐称され、ハイジャックされました。



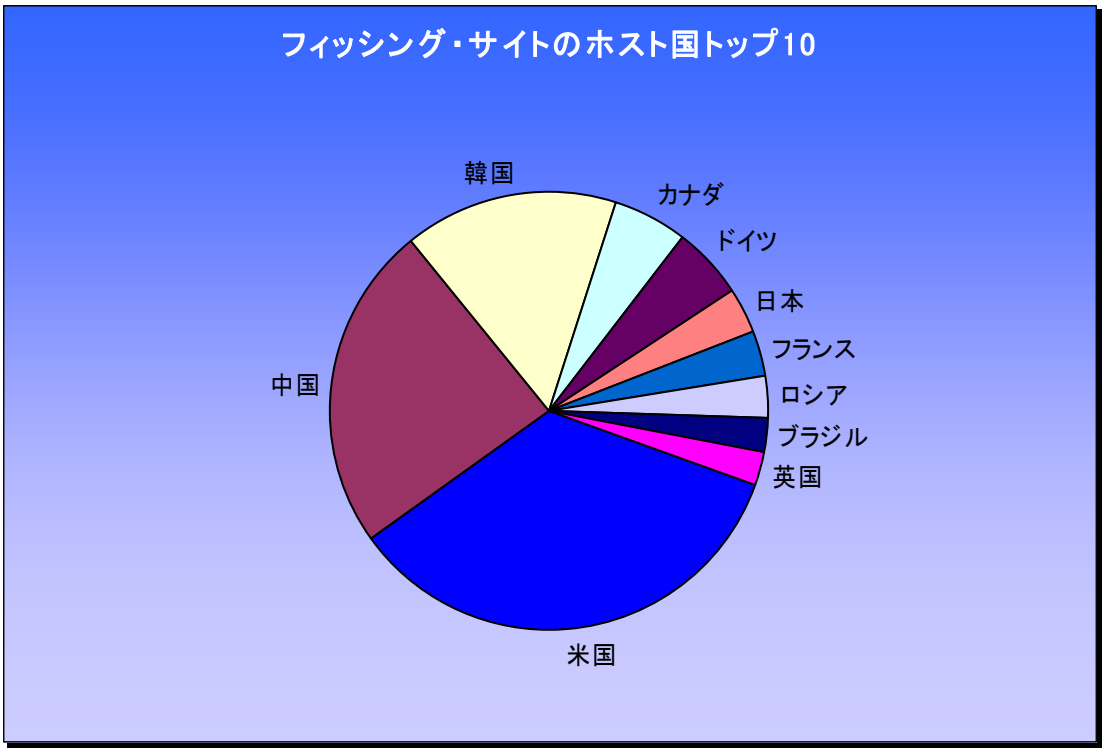
最も標的となった産業分野

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

1 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 24.27%で引き続きトップとなりました。その他 2 位以降の国は、中国 17.23%、韓国 11%、カナダ 4.05%、ドイツ 3.64%、日本 2.41%、フランス 2.33%、ロシア 2.15%、ブラジル 1.9%、英国 1.67%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

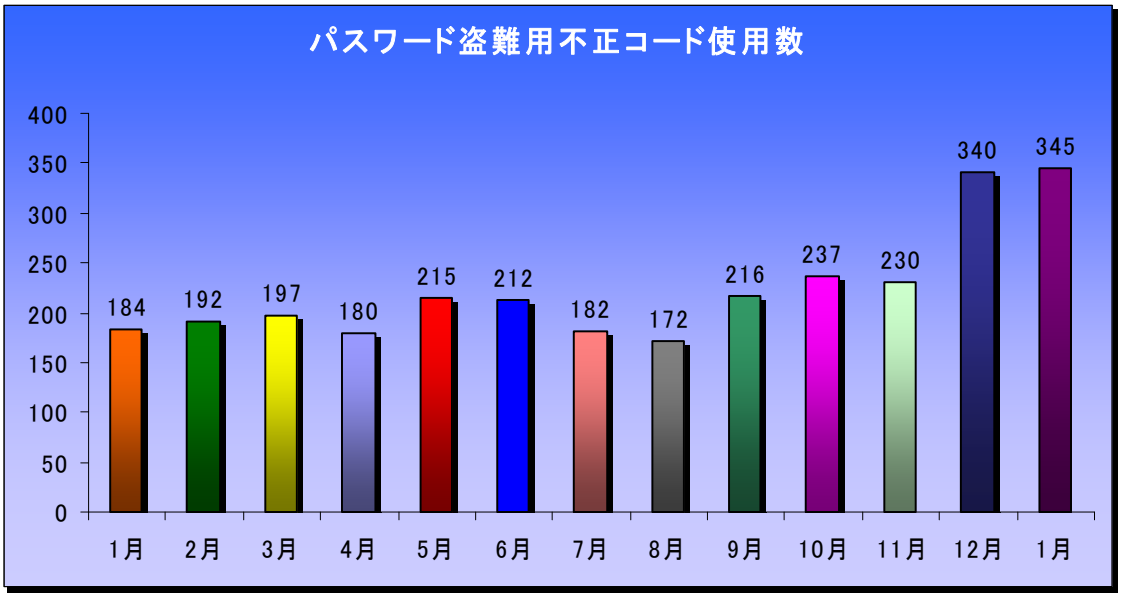
「クライムウェア」用語および 1 月期の分類による実例

「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。

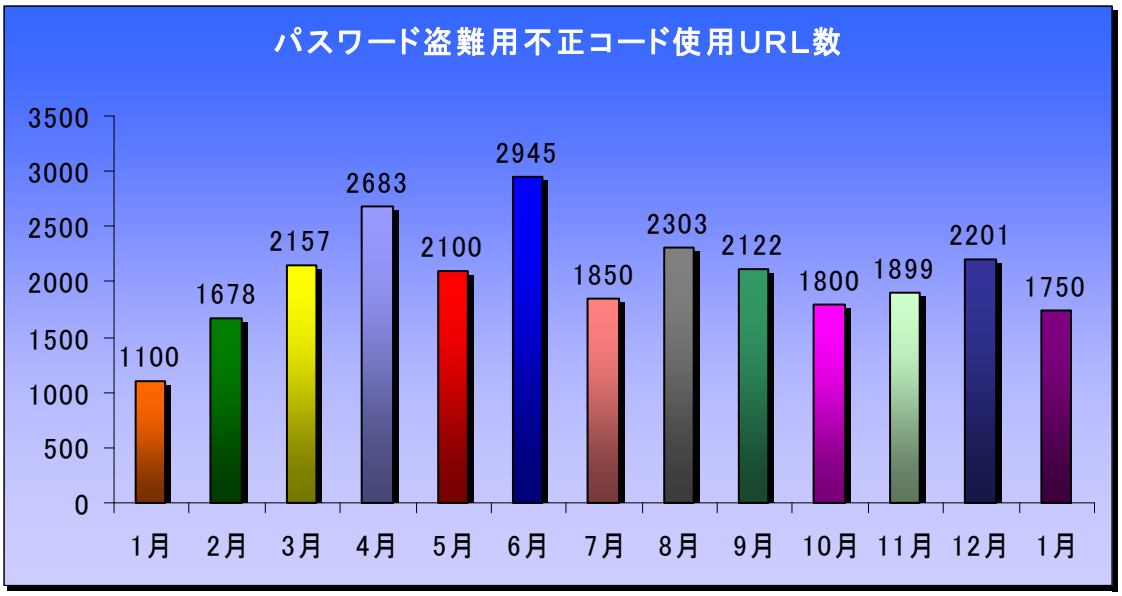
「フィッシング用トロイの木馬－キーロガー」

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



プロジェクト クライムウェア実地観測結果: ブラジル、ロシア人サイバー犯罪組織の共謀

1月期 Websense Security Labsは、ブラジル人の悪意のあるコード作者がロシア製の有名なWeb攻撃ツールを利用していることを突き止めました。複数のグループが連携して活動するような例はこれまでには見られなかったことから今回のような協力関係には重要な意味があります。Web Attackerというツールキットを使用することによって、攻撃者は自分のWebサイトにコードを仕掛けてサイトを訪れたユーザーに感染させることができるのです。このツールキットは現在Web上で最も広く使用されている攻撃ツールです。

かねてからブラジル人の攻撃は、ユーザーにコードを実行させる手段として主に騙しによる手法をとってきました。このような攻撃は大規模に行われ、毎日のように新たな攻撃例が確認されました。

我々が確認した攻撃例の中の一つに、犯人逮捕に対して巨額の懸賞金を支払うとする強盗事件に関する偽のニュース記事がありました。また別の攻撃は電子メールで画像を閲覧するように促すものでした。攻撃者はどちらのケースでもユーザーを彼らのサイトに誘導する手段として電子メールを用いていました。そしてどちらのサイトにも、パッチが完全に適用されていない PC で訪問した場合に情報窃盗型の悪意のあるコードをダウンロードしてインストールするソースコードが仕掛けられていたのです。

攻撃例のスクリーンショット 1

You forwarded this message on 1/15/2007 7:48 AM.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: eduboate@portal.com.br
To: [redacted]
Cc: eduboate@portal.com.br
Subject: Olha as foto da boate.

Olá! lembra daquela foto?

Agora que eu consegui seu email, sempre mandarei fotos legais! Espero que não percamos o contato...
Bom, eu consegui a foto da galera reunida tudo chapado hehe! Impressionante ficou muito legal! eehehe

Quando vi a foto me impressionei... Você precisa ver! Voce ta morto de bebo naquele lugar..!
Pelo que vi, você está no meio encostado com uma mina...

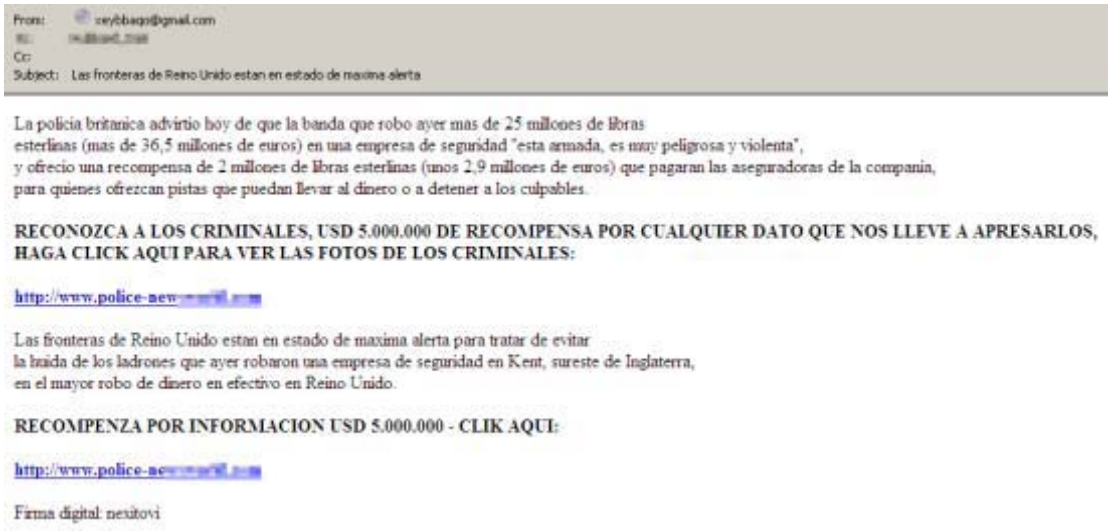
Passei a foto para o computador para poder estar passando para o pessoal.. Para ver ela, só clicar no link que eu salvei, junto tem mais algumas fotos:
http://kissboate.net/recentes/fotos/[redacted]

Estou com mais fotos ta aqui comigo.. Se quiser dar umas olhadas nela, só pedir.. Assim que eu tiver um tempo,
passarei elas para o computador e também enviarei..

ah! Me liga pra confirmar da festa porque eu perdi seu telefone que o Diego passou. Dê um sinal de vida pelo menos...

Vou ficando por aqui... Depois a gente 'conversa' mais!
Abraços. edu

攻撃例のスクリーンショット 2



From: [redacted]@gmail.com
To: [redacted]
Cc:
Subject: Las fronteras de Reino Unido estan en estado de maxima alerta

La policia britanica advirtio hoy de que la banda que robo ayer mas de 25 millones de libras
esterlinas (mas de 36,5 millones de euros) en una empresa de seguridad "esta armada, es muy peligrosa y violenta",
y ofrecio una recompensa de 2 millones de libras esterlinas (unos 2,9 millones de euros) que pagaran las aseguradoras de la compania,
para quienes ofrezcan pistas que puedan llevar al dinero o a detener a los culpables.

RECONOZCA A LOS CRIMINALES, USD 5.000.000 DE RECOMPENSA POR CUALQUIER DATO QUE NOS LLEVE A APRESARLOS, HAGA CLICK AQUI PARA VER LAS FOTOS DE LOS CRIMINALES:

http://www.police-[redacted]

Las fronteras de Reino Unido estan en estado de maxima alerta para tratar de evitar
la huida de los ladrones que ayer robaron una empresa de seguridad en Kent, sureste de Inglaterra,
en el mayor robo de dinero en efectivo en Reino Unido.

RECOMPENZA POR INFORMACION USD 5.000.000 - CLIK AQUI:

http://www.police-[redacted]

Firma digital: nexitovi

「フィッシング用トロイの木馬－リダイレクター」

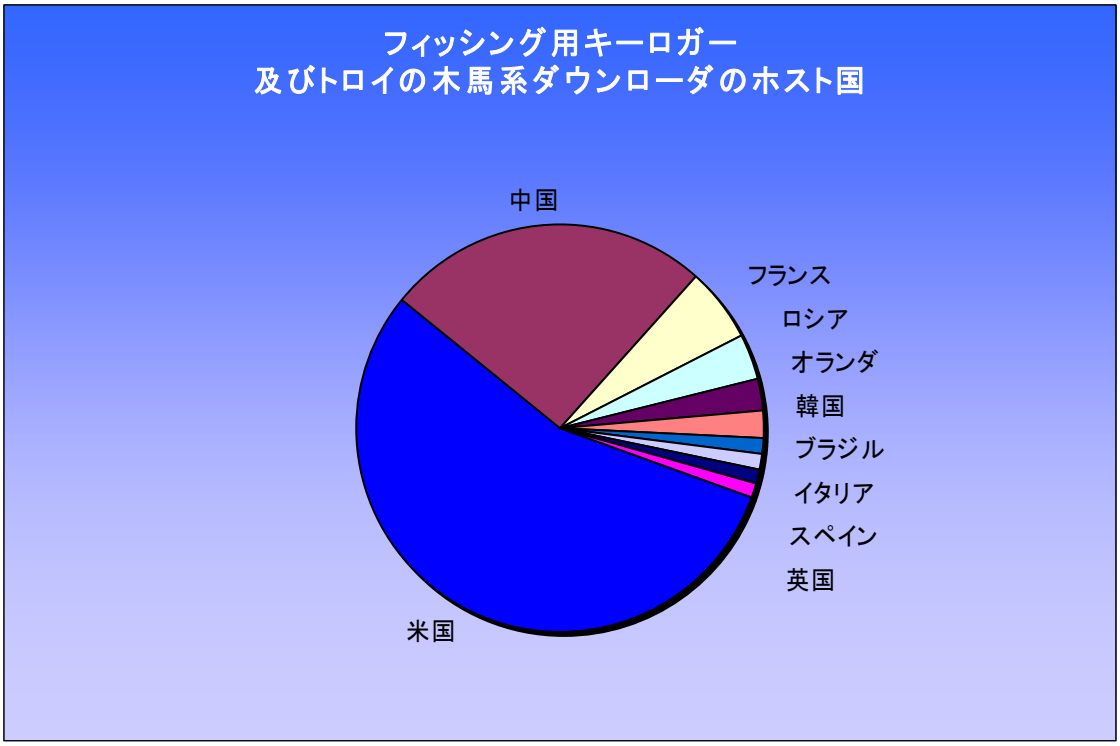
定義:エンドユーザーをネットワーク上で本来意図されていない場所に誘い出すことを目的として設計されたクライムウェアのコード。これにはホストファイルや他のDNS特有の情報を改ざんするようなクライムウェア、詐欺サイトへ情報を誘導するようなブラウザー・ヘルパー、詐欺地点への誘導を行うネットワーク・レベルでのドライバーやフィルターのインストールを行うクライムウェアを含む。これらは全て個人情報の略取やその他の信用情報の不正獲得という犯罪目的のためにインストールされる。

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 1 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。米国が 47%で地理的所在地のトップとなりました。その他 2 位以降の内訳は、中国 22%、フランス 5%、ロシア 3%、オランダ 2%、韓国 2%、ブラジル 1%、イタリア 1%、スペイン 1%、英国 1%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。