フィッシング対策協議会

月次報告書（２００６年５月分）

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

２００６年6月２０日

目次

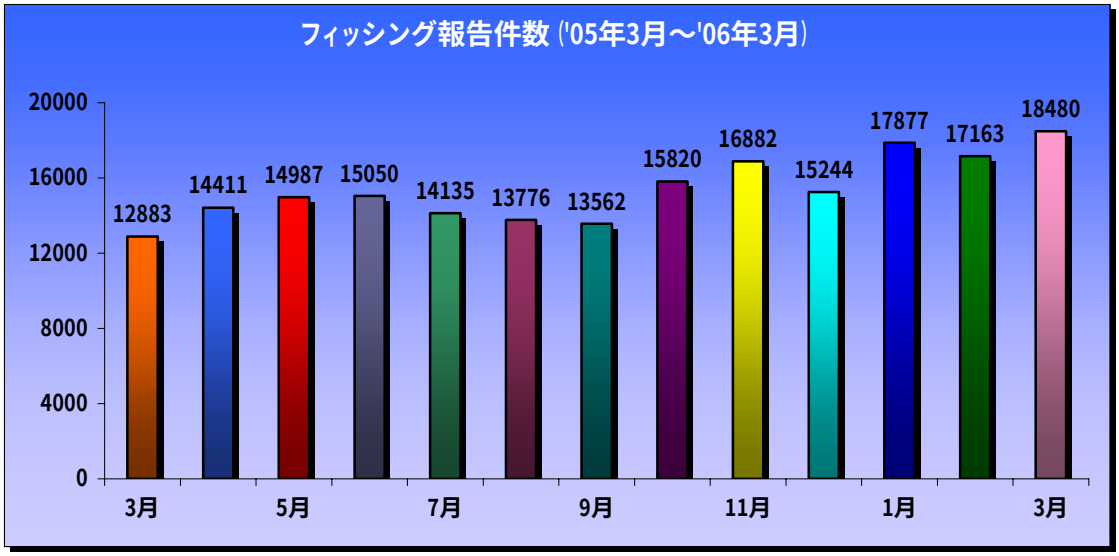
1. APWG Phishing Activity Trends Report 2006年3月　日本語版

『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

・3 月期のフィッシングに関する報告件数	**18,480**
・3 月期に報告されたフィッシング・サイト数	**9,666**
・3 月中にフィッシングによりハイジャックされた商標数	**70**
・3 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	**3**
・3 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	**48.05%**
・IP アドレスのみでホストネームなし	**32%**
・ポート 80 を使用しないサイトの割合	**3.9%**
・サイトのオンライン上の平均残存期間	**5 日間**
・サイトの最長オンライン残存期間	**31 日間**

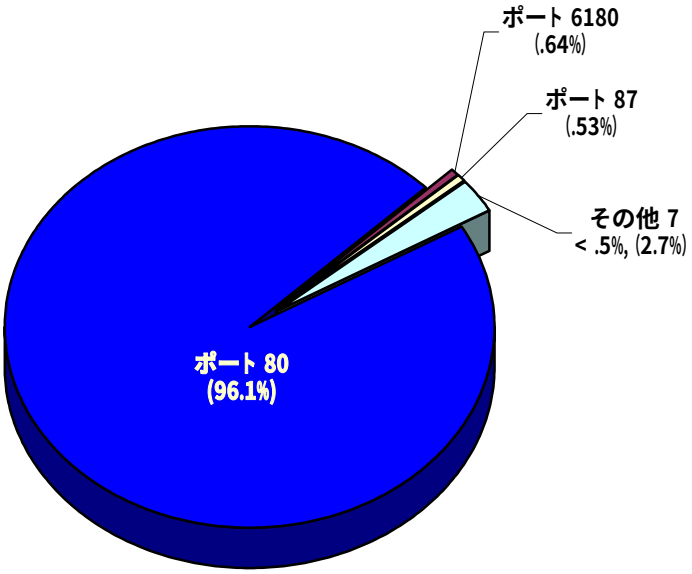


フィッシング行為報告件数（月単位／2005 年3 月～2006 年3 月）

『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

2006 年 3 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 96.1%に上りました。



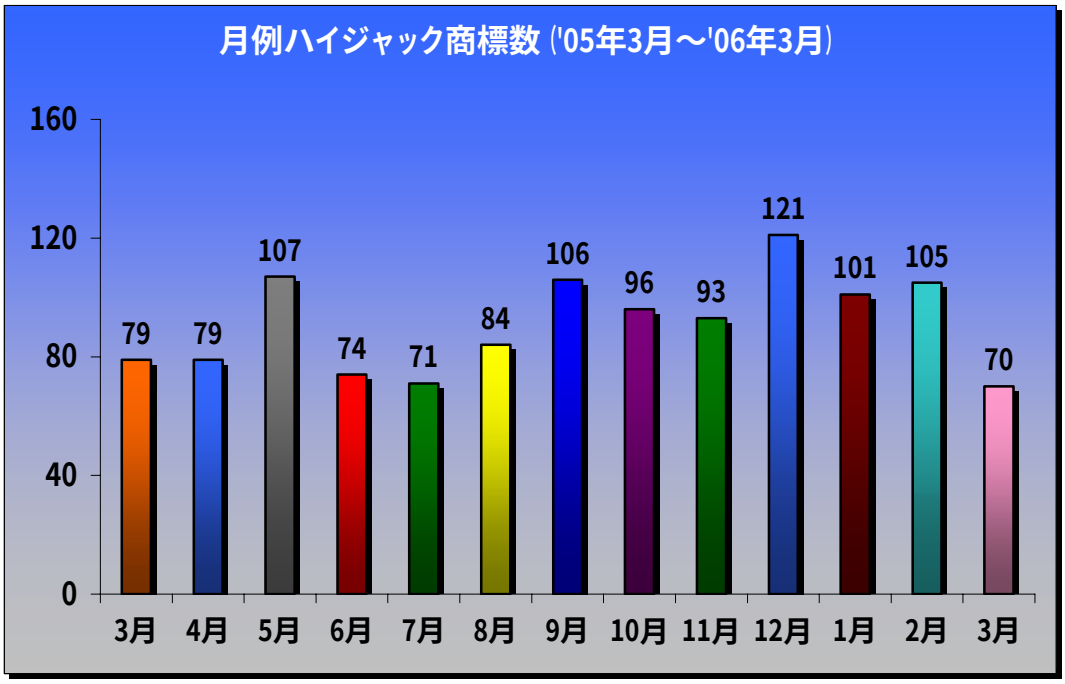
フィッシング・サイトとして最も使用された HTTP ポート

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

2006 年 3 月期は、ハイジャックされた商標数が前月期 (2006 年 2 月期) に比べて大幅に減少しました。

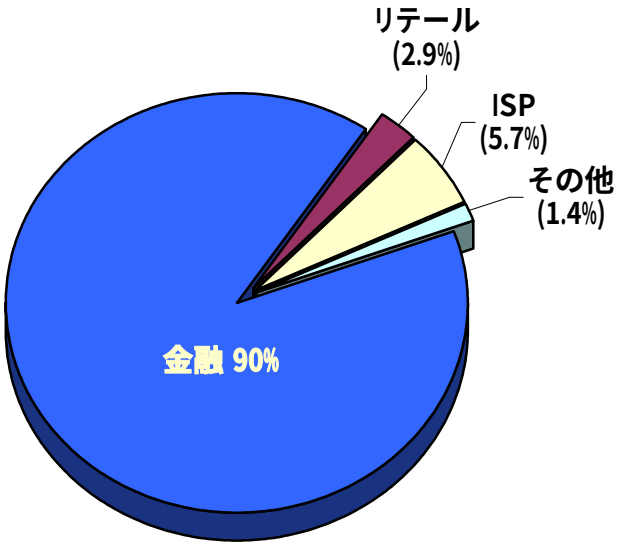
しかしながら、ある銀行に関しては、圧倒的に多くのフィッシングの標的となっていました。このことは、フィッシング詐欺師たちがこの金融機関の信用証明情報を簡単に現金化する方法を見つけ出したということを意味している可能性があります。この銀行がトラック 2 の問題(トラック2に記録されている PIN のオフセット値や CVV(Card Verification Value)といったセキュリティコードを利用したセキュアな認証を行っていない問題)を抱えているために、フィッシング詐欺師に偽造 ATM カードを作成された可能性があります。



ハイジャック商標数（2005 年 3 月～2006 年 3 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であり、3 月期は全攻撃の 90%に上りました。



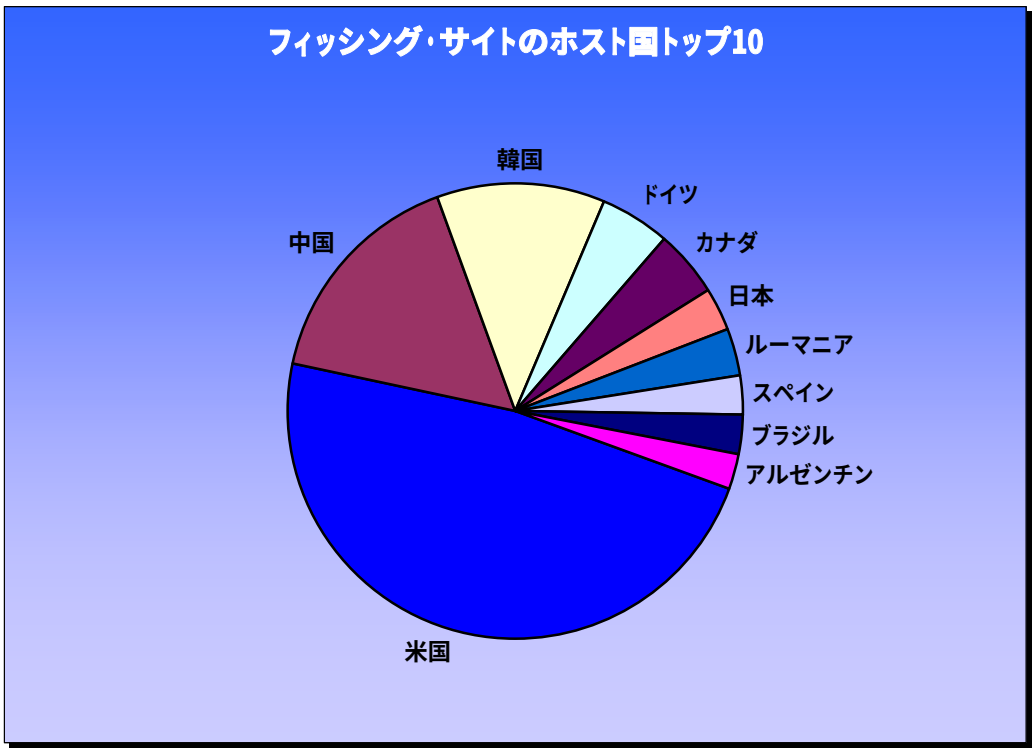
最も標的となった産業分野

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

3 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 35.13%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 11.93%、韓国 8.85%、ドイツ 3.57%、カナダ 3.52%、日本 2.39%、ルーマニア 2.29%、スペイン 2.13%、ブラジル 1.97%、アルゼンチン 1.92%と続きます。

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 3 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。

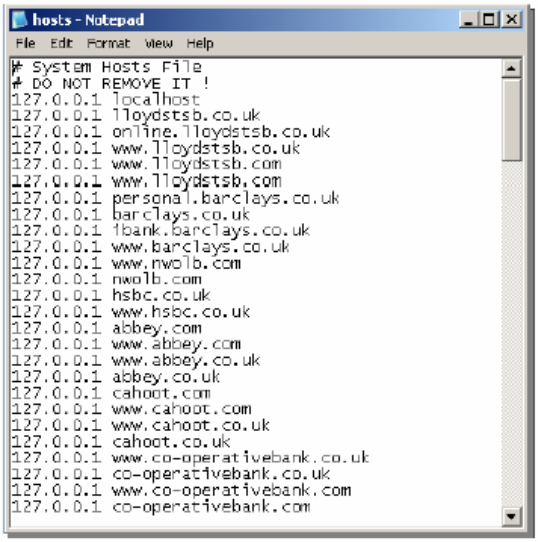
金融機関に対するトロイの木馬攻撃

Websense Security Labs は 3 月期に、米国およびヨーロッパにある 100 以上の金融機関の利用者を標的にしたトロイの木馬に関する報告を受けました。その悪意あるコードは一旦利用者のマシンにインストールされると、マイコンピュータか Internet Explorer のどちらかが開いているかをチェックします。どちらのアプリケーションも開かれていない場合、その悪意あるコードは、標的サイトの商標リストをもとに、ローカルマシン上の hosts ファイルをすべて localhost (127.0.0.1)を指すように書き換えます。

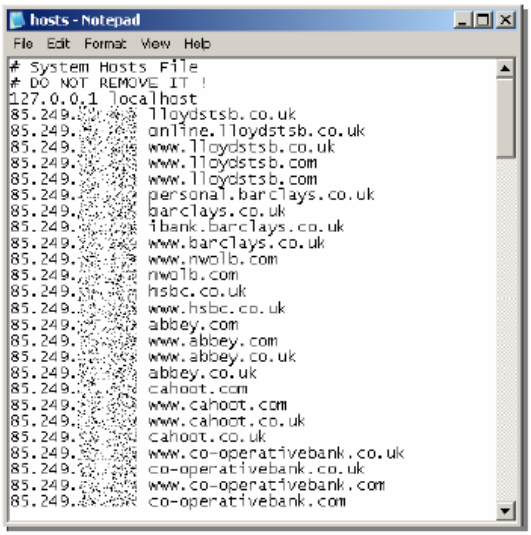
マイコンピュータまたは Internet Explorer のどちらかのアプリケーションが開かれている場合は動作が異なり、悪意あるコードはロシアの DNS サーバに DNS 検索を行い、Web サイトのアドレスを受け取ります。そして、DNS サーバから返されたアドレスを標的サイトの商標リストとともに hosts ファイルに書き加えます。hosts ファイルを改変されたマシンが標的のサイトに訪れると、そのマシンはロシアにある偽の Web サイトにリダイレクトされます。このような仕組みのために、フィッシング詐欺犯は、いずれかの標的サイトのサーバがオフラインであるときに、DNS を介して宛先アドレスを変更することができました。

ロシアに準備された Web サーバは、標的の偽サイトのために用意されたホスト名を使用していました。その Web サーバには 100 以上の異なるフィッシング詐欺用商標が登録され、すべてが個々の攻撃のための独自のページを備えていました。

スクリーンショット 1：アクティブウィンドウが開いていない場合の hosts ファイル



スクリーンショット 2：アクティブウィンドウが開いている場合の hosts ファイル



確認された Microsoft Internet Explorer のゼロデイエクスプロイト

さらに 3 月期に APWG は、エンドユーザーの同意なしに悪意あるコードが実行される、新たな Internet Explorer の「ゼロデイ」脆弱性に関する報告を受けました。この脆弱性は、パッチが未公開で、IE を悪用してユーザーの同意なしにコードを実行することが可能、というものでした。

TextRange の脆弱性を悪用するために Web サイトが特別に作成され、それは SDbot の亜種をダウンロードさせます。この SDbot の亜種はいくつかの動作を行った後に、IRC サーバへ接続してさらなるコマンドを待ち受けるというものでした。

Websense Security Labs は、honey クライアントを使ってこの脆弱性を追跡することによって、脆弱性を悪用してエクスプロイト･コードを実行する 200 以上の固有の URL を確認しました。最も一般的なものは、シェルコードを使用してトロイの木馬系ダウンローダーを実行し、HTTP 経由で追加のペイロードをダウンロードするものでした。そのペイロードとは、様々な形態のボット、スパイウェア、バックドア、などのトロイの木馬系ダウンローダーでした。

3 月の終わり、フィッシング詐欺犯は、IE の脆弱性を攻撃する悪質な Web サイトにユーザーを誘導する目的で、電子メールの送信を始めました。この電子メールには本物の BBC の記事から抜粋した文章が使われており、「Read More (続きを読む)」というリンクが貼られていました。このリンクをクリックしたユーザーは電子メールの BBC の記事をコピーした偽の Web サイトに誘導されます。その Web サイトでは、未パッチの createTextRange の脆弱性が悪用され、キーロガーがダウンロードされ、インストールさ

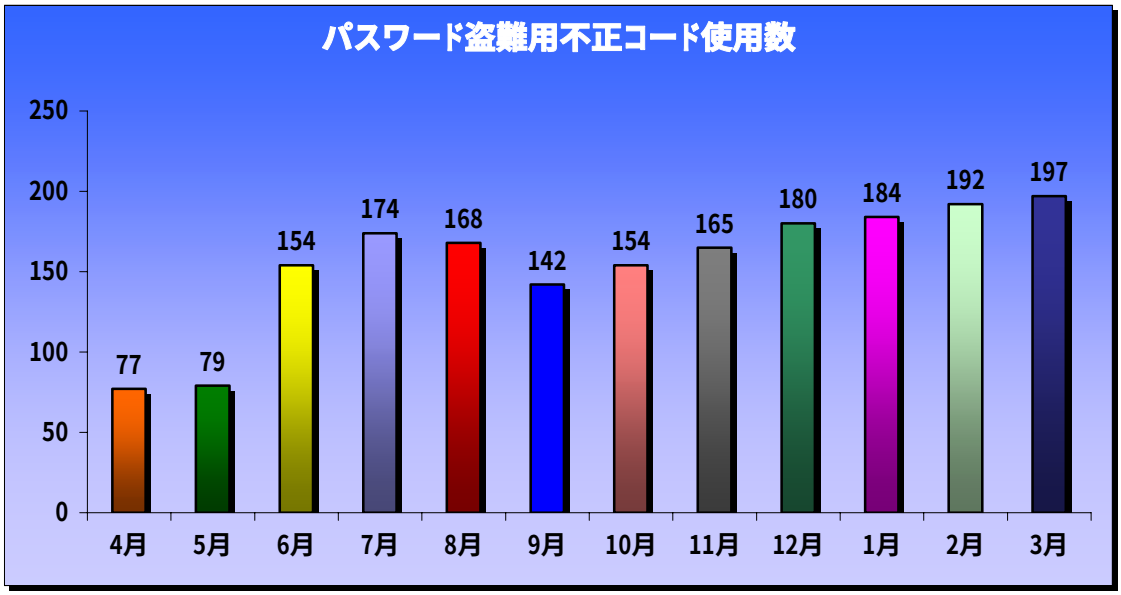
せられます。このキーロガーは、様々な金融機関の Web サイトを監視し、収集した情報をフィッシング詐欺犯に送信するというものでした。

悪質なWeb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－キーロガー」

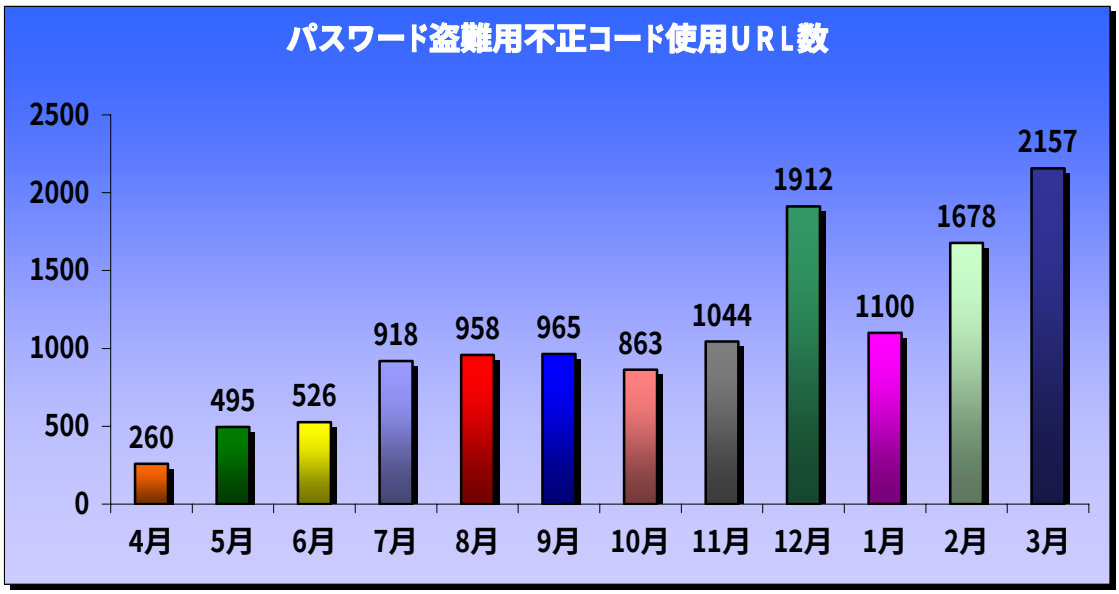
定義：エンドユーザーの個人情報をこれらのユーザーの信用証明を奪う目的で収集することを意図して設計されたクライムウェアのコード。フィッシングを目的としたキーロガーの場合、一般的なキーロガーとは異なり、金融機関、Eコマースやウェブをベースとしたメールサイトへのアクセスによる特定の情報獲得を目的とした特定の入力操作（そして特定の組織、最も重要なのは金融機関、オンライン小売業者、Eコマース商社）のみをモニターする追跡モニター・コンポーネントを備える。

フィッシング用トロイの木馬－キーロガー等



3 月期ＡＰＷＧでは、過去最多となる 197 件のフィッシング用トロイの木馬を発見・記録しました。

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」

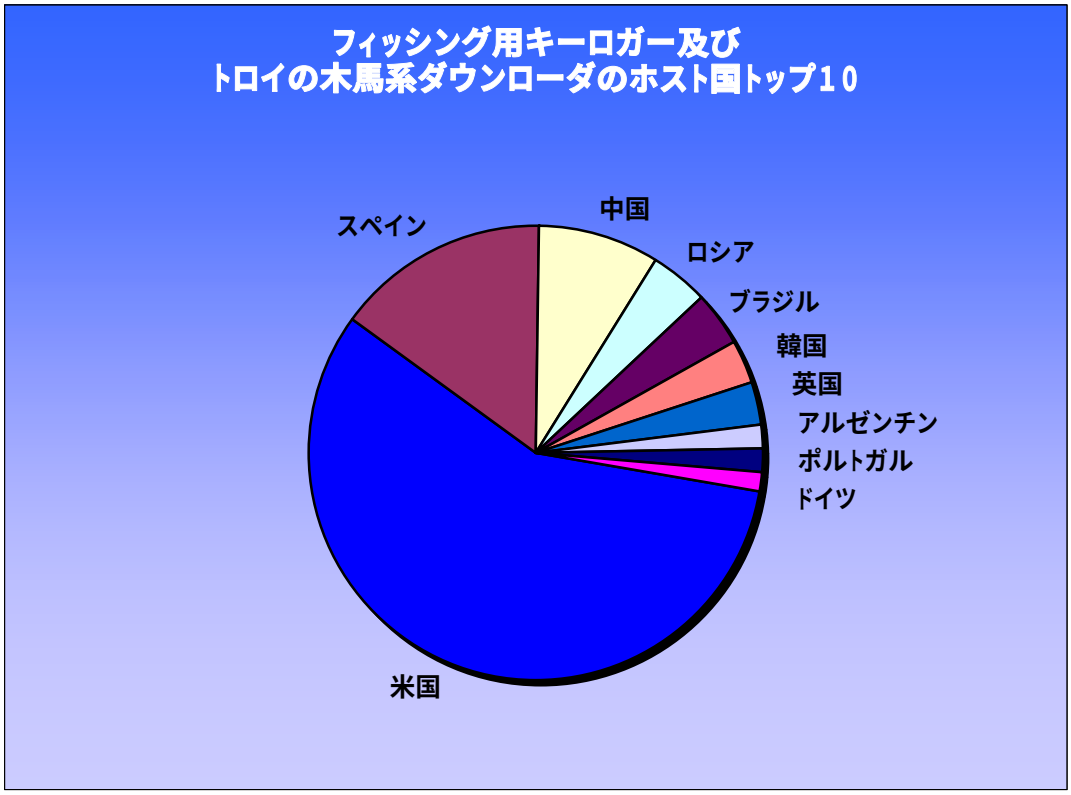
定義：エンドユーザーをネットワーク上で本来意図されていない場所に誘い出すことを目的として設計されたクライムウェアのコード。これにはホストファイルや他のＤＮＳ特有の情報を改ざんするようなクライムウェア、詐欺サイトへ情報を誘導するようなブラウザー・ヘルパー、詐欺地点への誘導を行うネットワーク・レベルでのドライバーやフィルターのインストールを行うクライムウェアを含む。これらは全て個人情報の略取やその他の信用情報の不正獲得という犯罪目的のためにインストールされる。

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ーのホスト国 (IP アドレスによる)

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とる不正コードのホストとして 3 月期中に分類されたウェブサイトの中で、米国は依然として地理的所在地のトップで全体の 39.87%を占めました。その他、2 位以降の内訳は、スペイン 10.7%、中国 6.02%、ロシア 2.94%、ブラジル 2.67%、韓国 2.2%、英国 2.09%、アルゼンチン 1.26%、ポルトガル 1.1%、ドイツ 0.94%と続きます。

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。