

フィッシング対策協議会

月次報告書（2005年11月分）

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

2006年1月4日

目次

1.	APWG PHISHING ACTIVITY TRENDS REPORT 2005 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

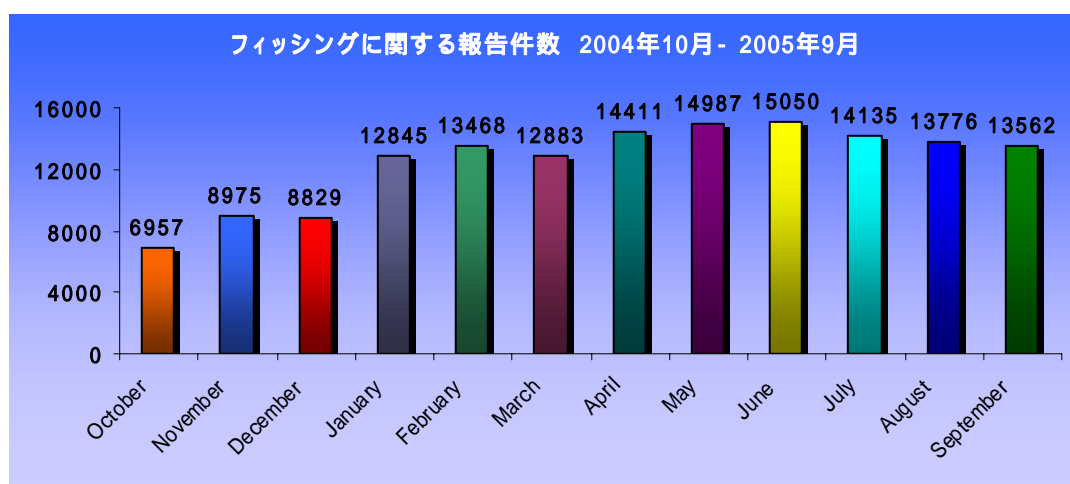
1. APWG Phishing Activity Trends Report 2005年9月 日本語版

『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、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へ誘い出し、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い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での 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

・9月期のフィッシングに関する報告件数	13,562
・9月月に報告されたフィッシング・サイト数	5,259
・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	106
・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	50%
・IPアドレスのみでホストネームなし	34%
・ポート80を使用しないサイトの割合	8%
・サイトのオンライン上の平均残存期間	5.5日間
・サイトの最長オンライン残存期間	31日間

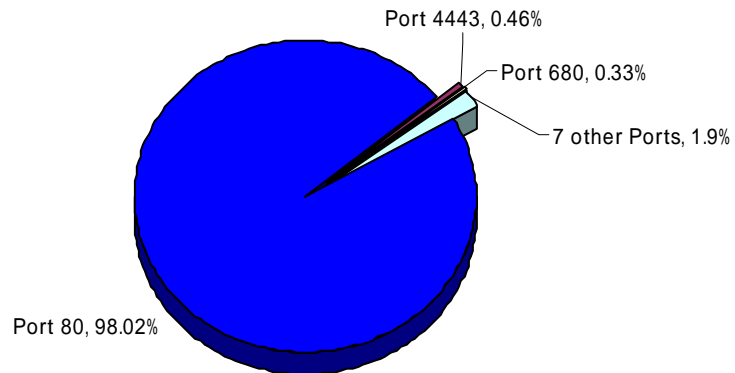


フィッシング行為報告件数(月単位 / 2004年10月 ~ 2005年9月)

『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

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 98.02%にまで増加しました。



フィッシング・サイトとして最も使用された HTTP ポート

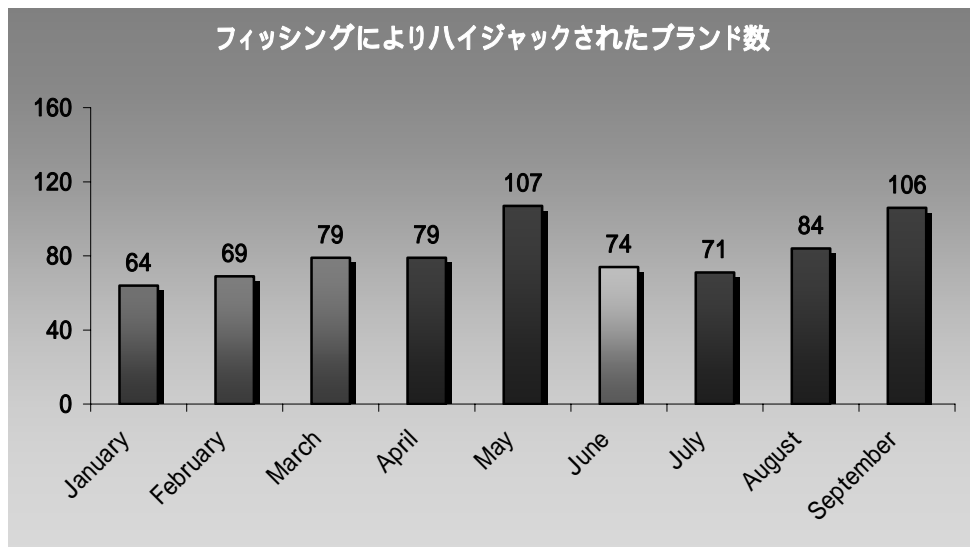
1.3. 【Brands and Legitimate Entities Hijacked By Email Phishing Attacks】

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月期にフィッシング被害を被った商標の報告件数は106件に増加しました。9月期にフィッシングされた商標数は前月と比べ大幅な増加となりました。

特筆すべきは信用組合に対する攻撃の多さであり、この傾向は現在まで数ヶ月に渡り続いています。予想に反して、より大規模な銀行が狙われた件数も増加しました。

9月期はより多くのヨーロッパおよびカナダの金融機関が報告されました。

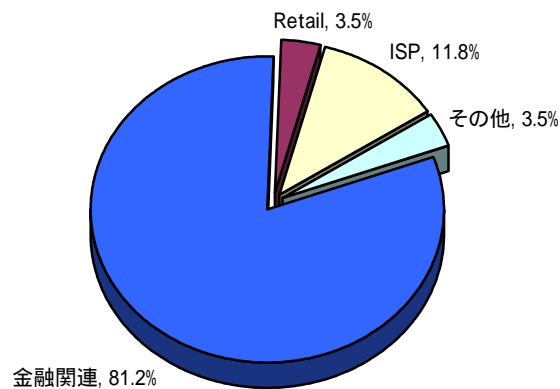


ハイジャック商標数 (2005年1月~9月)

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、全攻撃の 81.2%を占め安定しています。

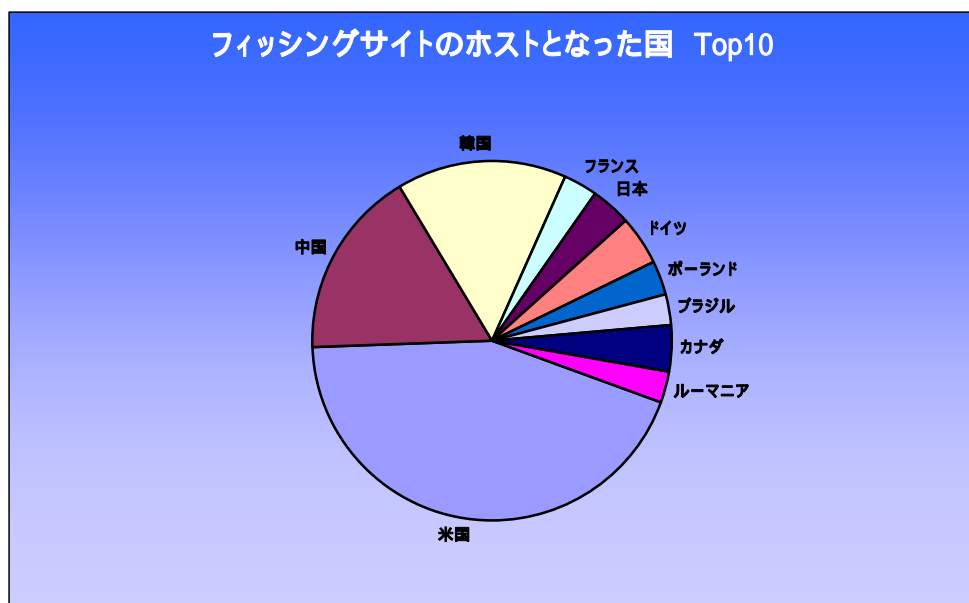
2005年9月はISPがフィッシングされた件数が劇的に増加しました。また、赤十字社を含む災害被害救済組織の名を騙ったフィッシング詐欺が急増しました。



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

9 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 31.22% でリストのトップに留まっています。トップ 10 のその他は、中国 12.13%、韓国 10.91%、ドイツ 3.16%、カナダ 2.97%、日本 2.44%、フランス 2.31%、ポーランド 2.24%、ブラジル 1.98%、ルーマニア 1.98% でした。



フィッシング・サイトのホスト国

9月期の特殊事例と新しい標的 救援募金とフォト・フィッシング攻撃

9月期 APWG は、絶望のふちにある人々を救済するという人間の善意に付け込んだフィッシング攻撃のいくつかの新事例を観測しました。今回の嘆かわしい攻撃は、自然災害の被災者への救援募金に寄付を行う人々の善意を食いものにする行為でした。様々な攻撃目標と案件を対象にした攻撃があり、それらの中には、赤十字社、救世軍、ハリケーン「カタリナ」募金およびハリケーン「リタ」募金が含まれていました。中でも攻撃件数が最も多かったのが、ハリケーン「カタリナ」に関連した事例で、大抵の場合は赤十字社の名を騙った詐欺行為でした。ハリケーン呼び名が発表されるや否や、詐欺工作者達は先ず救援と募金を募るサイトを反映するドメイン名を登録し、ハリケーンが上陸した直後から詐欺用の餌を爆発的勢いでばら撒き始めました。

ハリケーン「カタリナ」での詐欺行為事例

Websense Security Labs では、ユーザーを詐欺用サイトに誘い出す行為を行う新しいeメール詐欺について複数の報告を受けました。eメールでは先ずハリケーン「カタリナ」についての最新情報を手短かに述べ、詳細な情報を提供するサイトへのリンクを提供します。このウェブサイトが暗号化されたJavaScript を包含しており、それが HTML Help の二つの脆弱性に付け込んでいきます。Microsoft ではこれらの脆弱性について、<http://www.microsoft.com/technet/security/bulletin/MS05-001.msp> で公表しています。二つの内どちらかの脆弱性に付け込むことに成功した場合、トロイの木馬系ダウンロードがワークステーションに設置されることとなります。トロイの木馬は第2の不正ファイル(これもトロイの木馬)を取り込み始めます。第2のトロイは「裏口機能」を持ち、フィッシング工作者がそのワークステーションを完全に制御することを可能にしてしまいます。

ここで利用されたテクニックおよびトロイの木馬は、8月初めより出回り始めたイラクのニュースeメール詐欺事件 (Iraqi News Email Scam) と酷似しています。

不正工作の最初のウェブサイトのホスト国はメキシコ、第2のウェブサイトのホスト国はアメリカでした。

Websense Security Labs ではまた、数百件に上る新しいウェブサイトがハリケーン「カタリナ」被害者救援のための募金を呼びかけていることを観測しています。これらのサイトの多くは詐欺であると思われる。

Sample email text:

Just before daybreak Tuesday, Katrina, now a tropical storm, was 35 miles northeast of Tupelo, Miss., moving north-northeast with winds of 50 mph.

Forecasters at the National Hurricane Center said the amount of rainfall has been adjusted downward Monday. Mississippi Gov. Haley Barbour said Tuesday that Hurricane Katrina killed as many as 80 people in his state and burst levees in Louisiana flooded New Orleans.

Katrina killed as many as 80 people.

NEW ORLEANS, United States (UPI) -- Mississippi Gov. Haley Barbour said Tuesday that Hurricane Katrina killed as many as 80 people in his state and burst levees in Louisiana flooded New Orleans.

Just before daybreak Tuesday, Katrina, now a tropical storm, was 35 miles northeast of Tupelo, Miss., moving north-northeast with winds of 50 mph. Forecasters at the National Hurricane Center said the amount of rainfall has been adjusted downward Monday.

Thirty storm-related deaths in Mississippi's Harrison County were at an apartment complex, near the beach in Biloxi, Kally Jakubic with the county's Emergency Operations Center told CNN.


Louisiana Gov. Kathleen Babineaux Blanco said there was no official death tally in Louisiana, but said she expected that to change.

Meanwhile, New Orleans Mayor Ray Nagin said a levee holding back the waters of Lake Pontchartrain breached, forcing the air evacuation of 90 patients from a hospital.

"The city of New Orleans is in a state of devastation," Nagin told WWL-TV. "We probably have 80 percent of our city underwater. With some sections of our city, the water is as deep as 20 feet."



next article
Zotob worm exploits Windows



Exploit code for recently patched Windows flaws has swiftly evolved into a new series of worms...

[Read more...](#)

事例その2

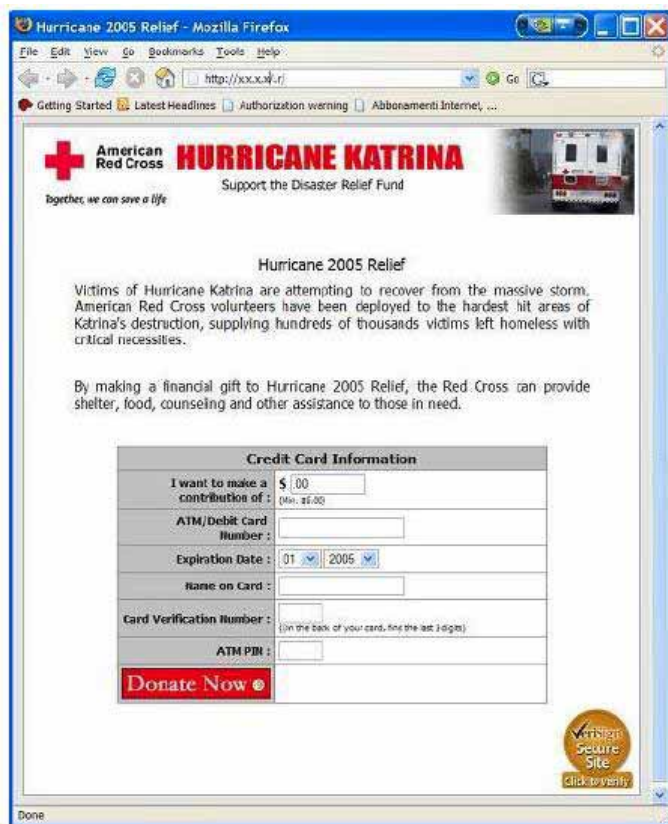
Websense Security Labs では、ハリケーン「カタリナ」の被災者救援努力を支えるために募金をする人々を標的とする新しいフィッシング攻撃についての報告を受けました。詐欺メールは HTML で書かれ、あたかも赤十字社からのメールであるかのように装っていました。このメールはまた、ベリサイン社 (Verisign) の安全サイト (Secure Site) の認証ロゴを付けており、エンド・ユーザーを騙して合法的なメールであるかのように信じ込ませる試みでした。そのメールに書かれたリンクに接続すると、ユーザーは (本警告の発表時点では) ブラジルにあった詐欺用のウェブサイトに誘導されました。このサイトは他のコンテンツのホストにもなっており、互譲性があるようでした。ユーザーのクレジットカード番号、有効期限、PIN コードをオンライン・フォームで入力するよう求められ、その後、本物の赤十字社のウェブサイトに転送される仕組みでした。

Phishing email body:

Victims of Hurricane Katrina are attempting to recover from the massive storm. American Red Cross volunteers have been deployed to the hardest hit areas of Katrina's destruction, supplying hundreds of thousands victims left homeless with critical necessities.

By making a financial gift to Hurricane 2005 Relief, the Red Cross can provide shelter, food, counseling and other assistance to those in need.

Phishing website screenshot



APWG では、これらの事例に加え、一般に普及しているオンライン・サービスやオンライン・ゲームをターゲットとしたフィッシング攻撃の出現を察知し始めました。ほとんどの場合、エンド・ユーザーの信用情報を取得し、そのアカウントで接続できる他のサービスに接続したり、ログオン信用情報を得るためのキーロガーをインストールしたり、または、オンライン・ゲームのトークンを得るためにログオン信用情報を獲得するということが目的でした。

Yahoo! Photos での事例(警告)

Websense Security Labs では、フィッシング攻撃で使用される手法の変化を観察しました。これは Yahoo! のユーザーを狙ったもので、偽の Yahoo! のサイン・インのページを表示することによりユーザーの Yahoo! ID とパスワードを獲得しようとするもので、ここしばらく出回っていました。ところが最近これらのフィッシング用サイトが、今までとは異なる Yahoo! Photos などの Yahoo! サイン・インのページを使用するようになってきました。

Yahoo! Photos の事例では、ユーザーが友達だと名乗る差出人からの e メールまたはインスタント・

メッセージを受け取り、最近撮った休暇や誕生日パーティーの写真を見てほしいと告げられます。このメッセージにはフィッシング用サイトへのリンクがあり、ここでユーザーの Yahoo! ID とパスワードが記録されます。その後、この ID とパスワードは本物の Yahoo! Photos のサイトに転送されます。

これらのフィッシング用サイトのほとんどは、アメリカの Yahoo! Geocities が提供するフリー・ウェブスペース上に存在します。



プロジェクト:クライムウェア

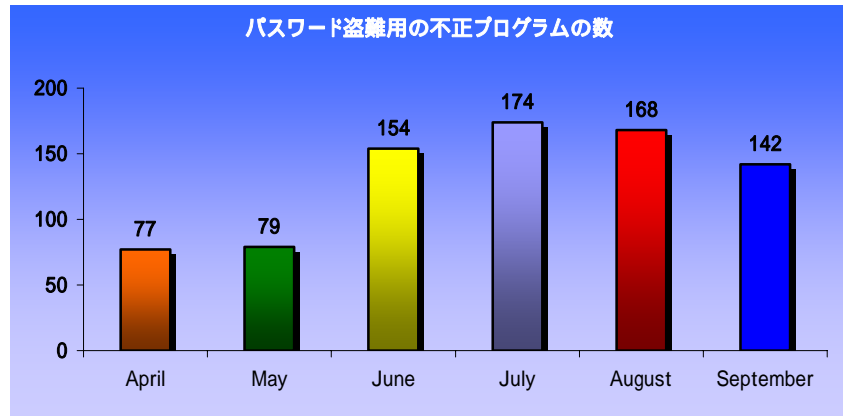
「クライムウェア」分類詳細

「プロジェクト:クライムウェア」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。

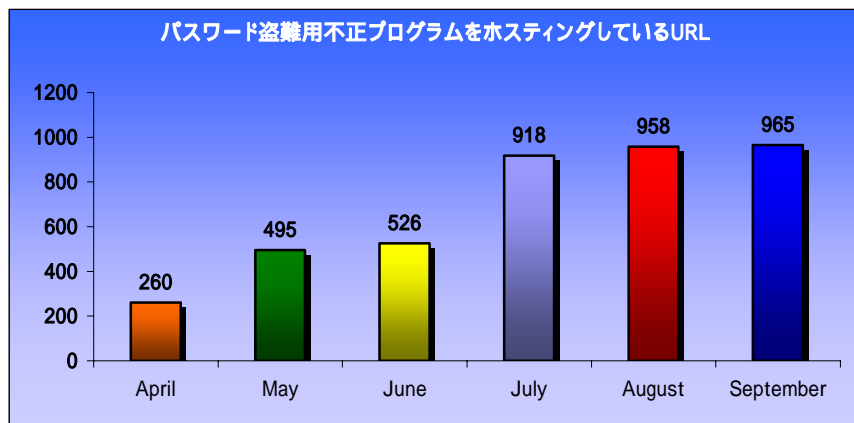
「フィッシング用トロイの木馬 - キーロガー」

9 月期 Websense Security Labs では、キーロガーの変種の出現件数は若干減少したにもかかわらず、パスワード盗難用の不正コードを使用した URL の増加は顕著であったことを確認しました。

フィッシング用トロイの木馬 - キーロガー



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)

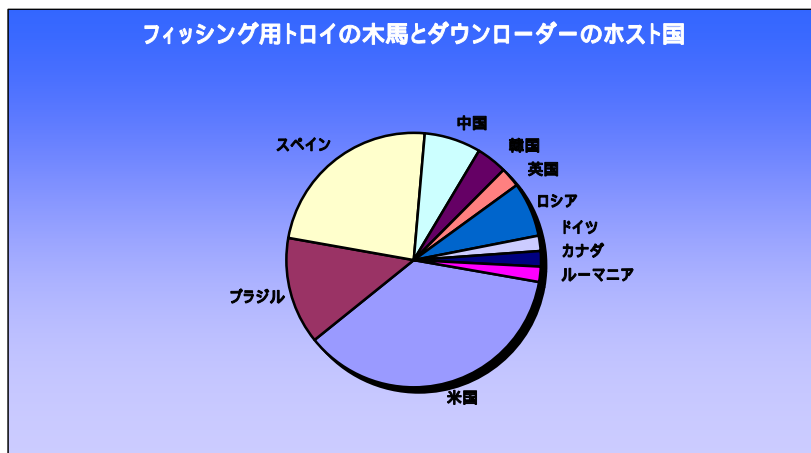


フィッシング用トロイの木馬とダウンローダーのホスト国 (IP アドレスによる)

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 9 月中に分類されたウェブサイトの内訳を示すものです。

アメリカは依然として地理的所在地のトップで33%を占め、スペインが急速に増加し21.4%となり、ブラジルの12.5%を抜き第2位となりました。

その他の内訳は、中国 6.5%、韓国 3.62%、イギリス 2.37%、ロシア 6.25%、ドイツ 1.75%、ルーマニア 1.75%、カナダ 1.75%でした。



より高度なトロイの木馬とその感染メソッド

9 月期 Websense Security Labs では、GUI のステップ・スルー・ウィザードや複雑なエラー・チェック機能を持つ完全なアプリケーションとしてのフィッシング用キーロガーのサンプルを目撃しました。以前の、大抵はバックグラウンドで走り、表面に現れず、サイズも小さかった不正コードの実行アプリケーションとは異なり、今回のものは大規模な Visual Basic で書かれたアプリケーションであり、ユーザーが GUI に情報を入力するよう誘導されるものでした。

以下は、Websense Security Labs が 2005 年 9 月 21 日付けで発信した警告事例です。

Websense Security Labs では、AOL の顧客をターゲットとした新しい攻撃事例についての報告を受けました。ユーザーは AOL のセキュリティー担当部署から詐欺メールを受信します。そのメールには、先週末 AOL のセキュリティーが突破され、機密情報が漏洩した可能性があると書かれています。そこでユーザーは、あるウェブサイトへ接続し、顧客情報を保護するための新しいセキュリティー・パッチをダウンロードの上インストールするよう求められます。

ユーザーがリンクをクリックすると、スコットランドがホスト国となっている偽のウェブサイトに誘導されます。このサイトには patch.scr という Visual Basic で書かれ、Yoda Crypt を使用する不正コードが仕込まれています。このファイルが走ると、あるウィザードが開き、ユーザーは支払い限度額を含めた口座と代金請求に関わる機密情報を暴露してしまうことになります。

獲得した情報はテキストファイル形式で FTP を経由してホストのアカウントに送られます。

Email Body:

mandatoryupdate@aol.com

Valued AOL Member:

Over this past weekend America Online fell victim to attacks from hackers. Thousands of people were affected as personal and private information was illegally stolen from them off of our servers. We are still unable to identify everyone who was affected by these attacks.

To prevent this from happening to you or to correct the problem if you have fallen victim to such an attack, we have created a new Security Patch_ <URL removed> - a new, required update for members of all versions of America Online Software.

Failure to download_ <URL Removed> this Security Patch_ <URL Removed> the next 48 hours will result in the temporary suspension of your America Online account. At this point we will send you a Security Patch CD in the mail. Upon installing it, your account will be reactivated. Instead of that, you can download our Security Patch right here_ <URL Removed>, or by visiting the following URL:

After logging in you will be prompted to 'Run' the above Security Patch.
We thank you for your cooperation and look forward to continue to serve you.



Safety, Security & Privacy
Helping you have a more safe and secure online experience.

Attention AOL Member!

The billing information you currently have on file with us is out of date. We require our members to update and confirm their billing information with us on a regular basis. We do this so that we can offer you and your account the highest level of security possible.

Please take this time to update your account information with us right now by completing the fields to the right and clicking the 'Next' button. Failure to update your account with us right now will result in the possible suspension of your account.

Thank you!



Please fill out the fields above!

Please complete all the fields below with your CHECKING ACCOUNT information.

First Name: M.I.: Last Name:

Street Address: City:

State: ZipCode: Country: Phone Number:

Card Number: [Help](#) CVN: [Help](#) Expiration Date:

PIN: [Help](#) Most Recent Balance: US Dollars
\$\$\$\$\$\$

[Next click here](#) 



Safety, Security & Privacy
Helping you have a more safe and secure online experience.

Please complete all the fields below with your CHECKING ACCOUNT information.

Attention AOL Member!

The billing information you currently have on file with us is out of date. We require our members to update and confirm their billing information with us on a regular basis. We do this so that we can offer you and your account the highest level of security possible.

Please take this time to update your account information with us right now by completing the fields to the right and clicking the 'Next' button. Failure to update your account with us right now will result in the possible suspension of your account.



Thank you!

Please fill out the fields above!

First Name: M.I. Last Name:

Street Address: City:

State: Zip Code: Country: Phone Number:

Card Number: [Help](#) CVN: [Help](#) Expiration Date:

PIN: [Help](#) Most Recent Balance: US Dollars

Last 3-4 digits on the back of your card:

ON THE BACK OF YOUR CARD:



Next 




Safety, Security & Privacy
Helping you have a more safe and secure online experience.

Please complete all the fields below with your CHECKING ACCOUNT information.

Attention AOL Member!

The billing information you currently have on file with us is out of date. We require our members to update and confirm their billing information with us on a regular basis. We do this so that we can offer you and your account the highest level of security possible.

Please take this time to update your account information with us right now by completing the fields to the right and clicking the 'Next' button. Failure to update your account with us right now will result in the possible suspension of your account.



Thank you!

Please wait...!

First Name: M.I. Last Name:

Street Address: City:

State: Zip Code: Country: Phone Number:

Card Number: [Help](#) CVN: [Help](#) Expiration Date:

PIN: [Help](#) Most Recent Balance: US Dollars

The PIN number you use at ATMs!

Next 

OK

AOL Update

Your information has been successfully submitted to America Online for review. Our Secure Billing Team will verify and update the information you have submitted to us. We will contact you within 24 hours regarding the status of your AOL Update. Thank you!

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머스・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。