

フィッシング対策協議会

月次報告書（2005年10月分）

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

2005年11月18日

目次

1.	APWG PHISHING ACTIVITY TRENDS REPORT 2005 年 8 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

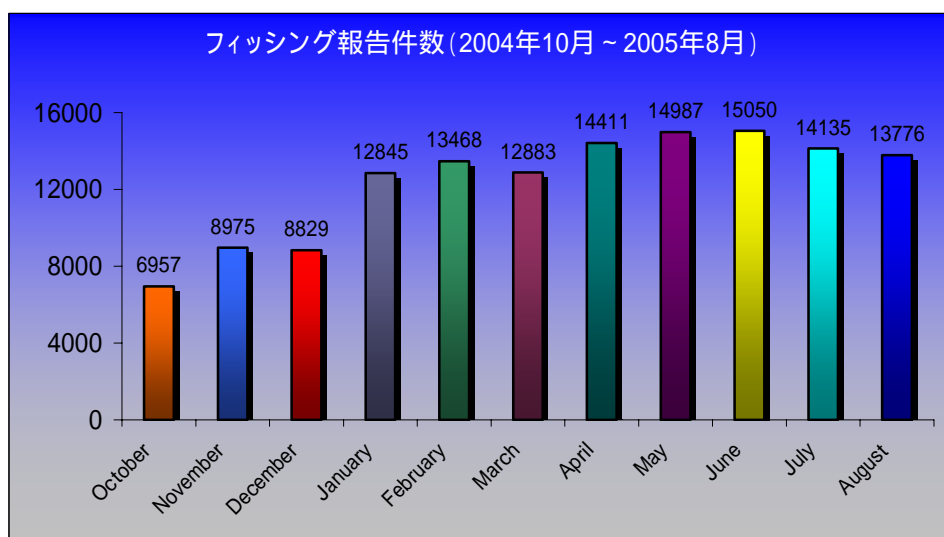
1. APWG Phishing Activity Trends Report 2005年8月 日本語版

『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に誘い出し、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ったり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

・8月期のフィッシングに関する報告件数	13,776
・8月月に報告されたフィッシング・サイト数	5259
・8月中にフィッシングによりハイジャックされた商標数	84
・8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
・8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	49%
・IPアドレスのみでホストネームなし	36%
・ポート80を使用しないサイトの割合	6%
・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

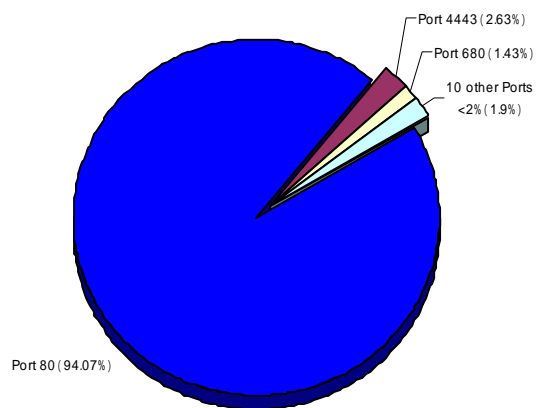


フィッシング行為報告件数(月単位 / 2004年10月～2005年8月)

『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・キャッシュディ(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

8 月期はフィッシング用ホスト・サイトにカズン(類似)ドメイン名を使用する傾向が続きました。その結果、代替ポートの使用は減少し、標準的なHTTPポート 80 の使用が報告を受けた全フィッシング・サイトの 94.07% 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

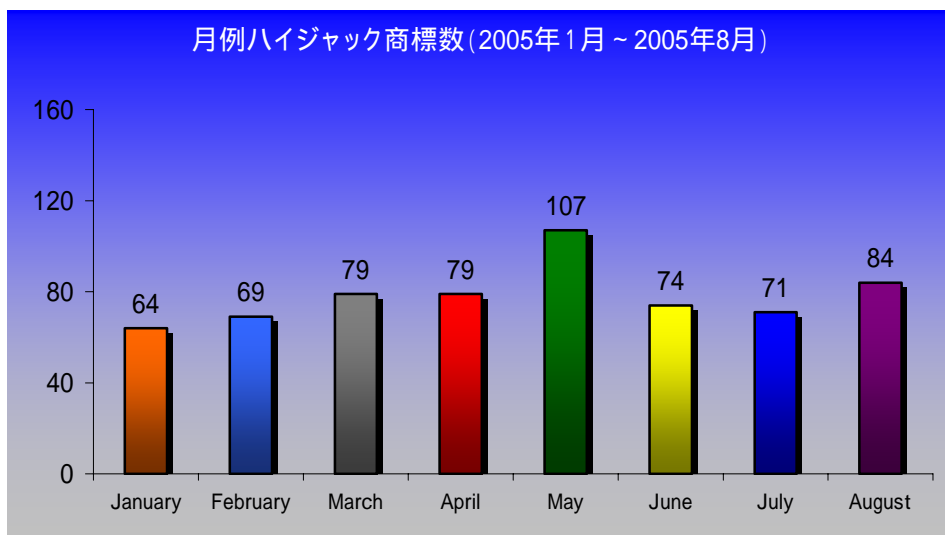
1.3. 【Brands and Legitimate Entities Hijacked By Email Phishing Attacks】

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

8月期にフィッシング被害を被った商標の報告件数は84件に増加しました。APWGでは多種に渡る商標が被害に遭い、特に北アメリカ全土および西ヨーロッパの極小金融機関の被害が顕著に現れていることを観測しています。

消費者がクレジットカードやその他の個人情報を入力しなければインターネット上でのサービスが停止してしまうと見せかけて騙すISPフィッシングの件数が増加しています。

7月期同様、保険会社への被害が観測されました。



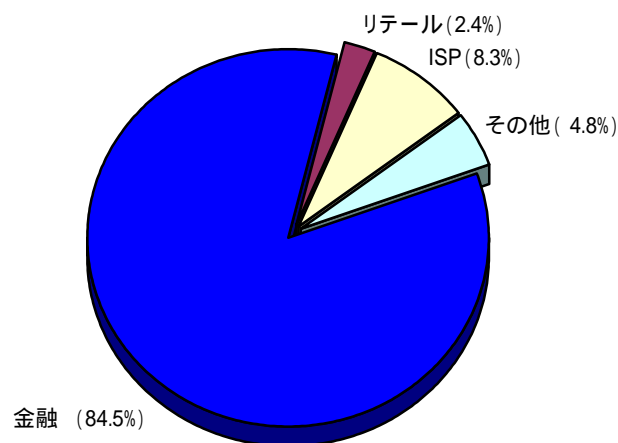
ハイジャック商標数(2005年1月～8月)

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85%近くを占め変動がありません。

8月期APWGでは、複数の合法企業より自社のサイトが何らかの理由でフィッシング用サイトのホストであるというレッテルを貼られてしまったとの報告を受けました。ある事例では、フィッシング対策用ツールバーがその会社のサイトへのアクセスをブロックしてしまい、消費者がそこに到達できなくなりました。

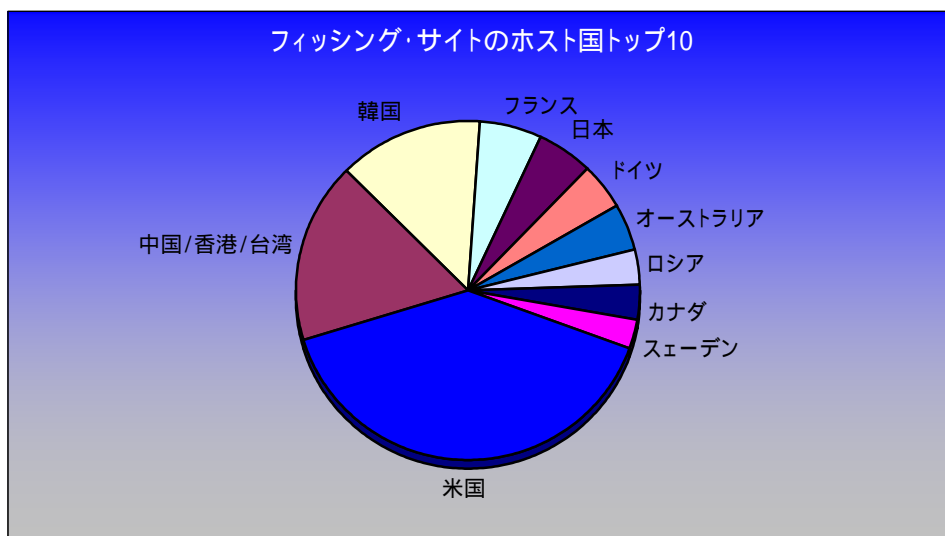
他の事例では、ドメイン名の登録レジストラがドメイン名を保持してしまい、それがDNS内で機能できなくなりました。このことは、あるサイトがフィッシング対策用のブラックリストに加えられたり、ドメイン名のレジストラが保持行為を発動する前に、そのサイトが本当に詐欺用サイトであるかどうかをしっかりと見極めることへの注意の必要性を喚起しています。



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

8 月期 Websense Security Labs は、中国と韓国の順序が入れ替わりはしたものの、依然として同じフィッシング用サイトのホスト国がトップ 3 を占めていることを観測しました。アメリカは 27.9% 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 12.15%、韓国 9.6%、フランス 4.07%、日本 3.65%、ドイツ 3.23%、オーストラリア 3.05%、ロシア 2.4%、カナダ 2.21%、スウェーデン 2.04% でした。



フィッシング・サイトのホスト国

攻撃方法最新事情

プロジェクト: クライムウェア

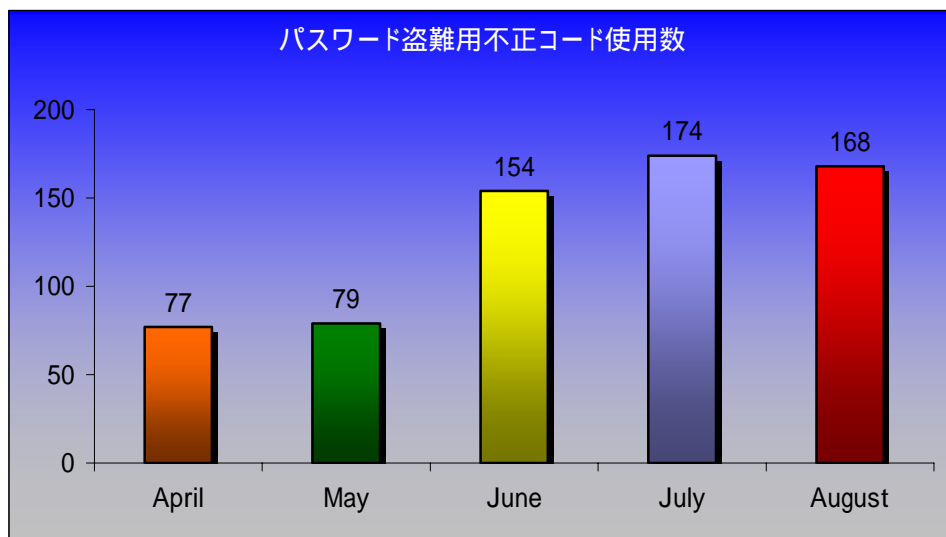
「クライムウェア」分類詳細

「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。

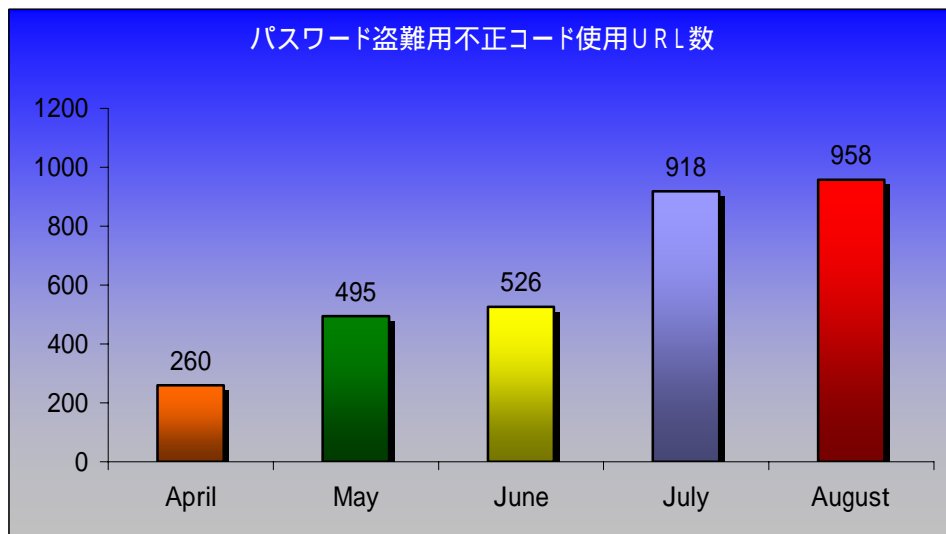
「フィッシング用トロイの木馬 - キーロガー」

8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)



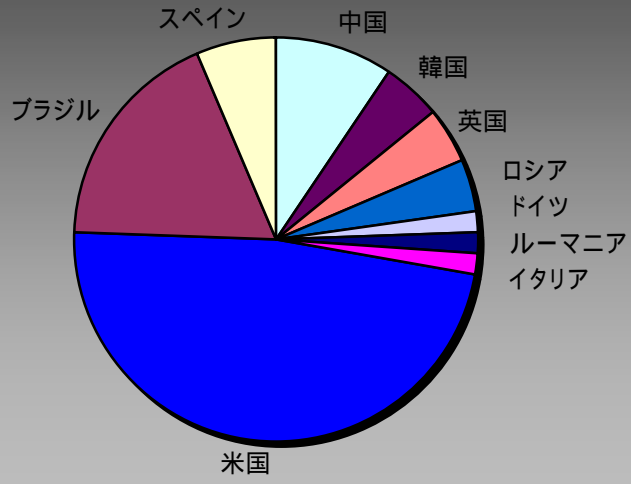
フィッシング用トロイの木馬とダウンローダーのホスト国(IP アドレスによる)

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 8 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 40% を占め、ブラジルが引き続き 2 位の座を占め先月の 11% から 15% に増加。増加率ではスペインが最も大きく、先月の 5.4% から 8 月は 12.5% 近くの倍以上跳ね上がりました。

その他の内訳は、中国 7.82%、韓国 3.9%、イギリス 3.6%、ロシア 3.5%、ドイツ 1.5%、ルーマニア 1.38%、イタリアも 1.38% でした。

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ーのホスト国



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。