フィッシング対策協議会

月次報告書（２００５年６月分）

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

２００５年7月２１日

目次

1. APWG Phishing Activity Trends Report 2005年 4月　日本語版

Anti-Phishing Working Group（APWG）がリリースした月次レポートを、翻訳したものです。

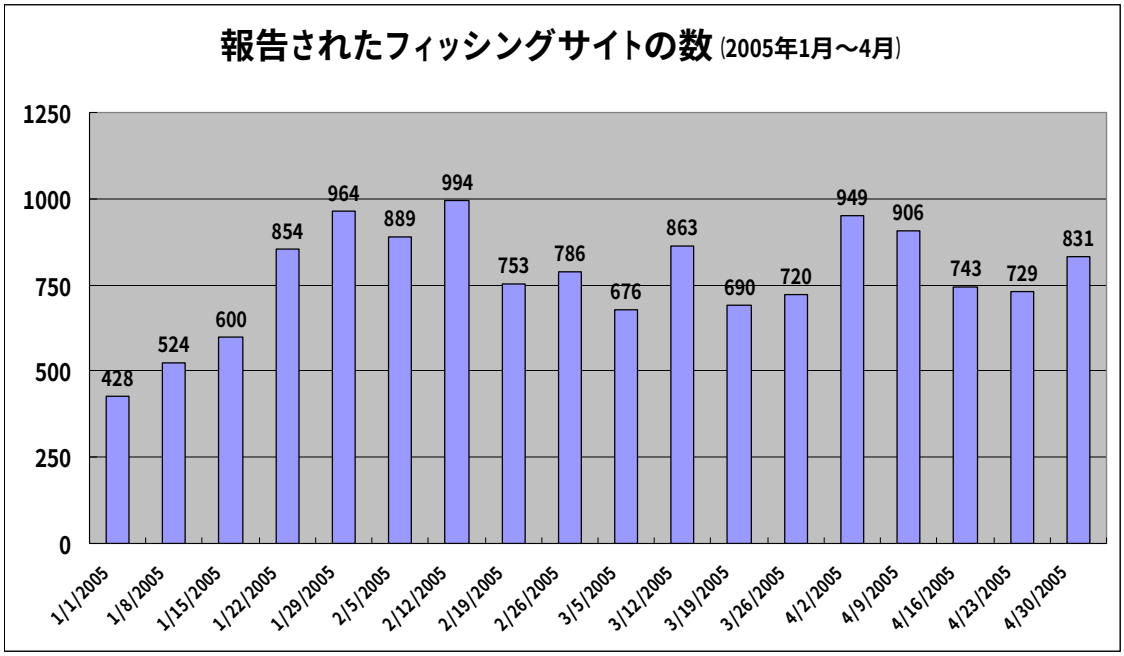
Phishing Activity Trends Report　April,2005
http://antiphishing.org/APWG_Phishing_Activity_Report_April_2005.pdf

「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。

「Phishing Activity Trends Report」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 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

- 4 月中に報告された稼動中のフィッシング・サイト数　2854
- フィッシング・サイトの月間平均増加率（2004 年 7 月～2005 年 4 月）15%
- 4 月中にフィッシング行為によりハイジャックされた商標数　79
- 4 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　7
- 4 月期最も多くのフィッシング・ウェブサイトが発見された国　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　33%
- IP アドレスのみでホストネームなし　37%
- ポート 80 を使用しないサイトの割合　5.5%
- サイトのオンライン上の平均残存期間　5.8 日間
- サイトの最長オンライン残存期間　30 日間



稼動中フィッシング・サイト報告件数（週単位／2005 年 1 月～2005 年 4 月）（サイト数）／（当該週の最終日付）

1.2. 【Phishing domains trends】フィッシング・ドメイン最新情報

「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「Anti-Phishing Working Group」が月例発行しています。詳細は Ronnie Manning, manning@websense.com（電話 858-320-9274）、または APWG 事務局長 Peter Cassidy （電話 617-669-1123）までお問い合わせください。「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。TUMBLEWEED COMMUNICATIONS、WEBSENSE

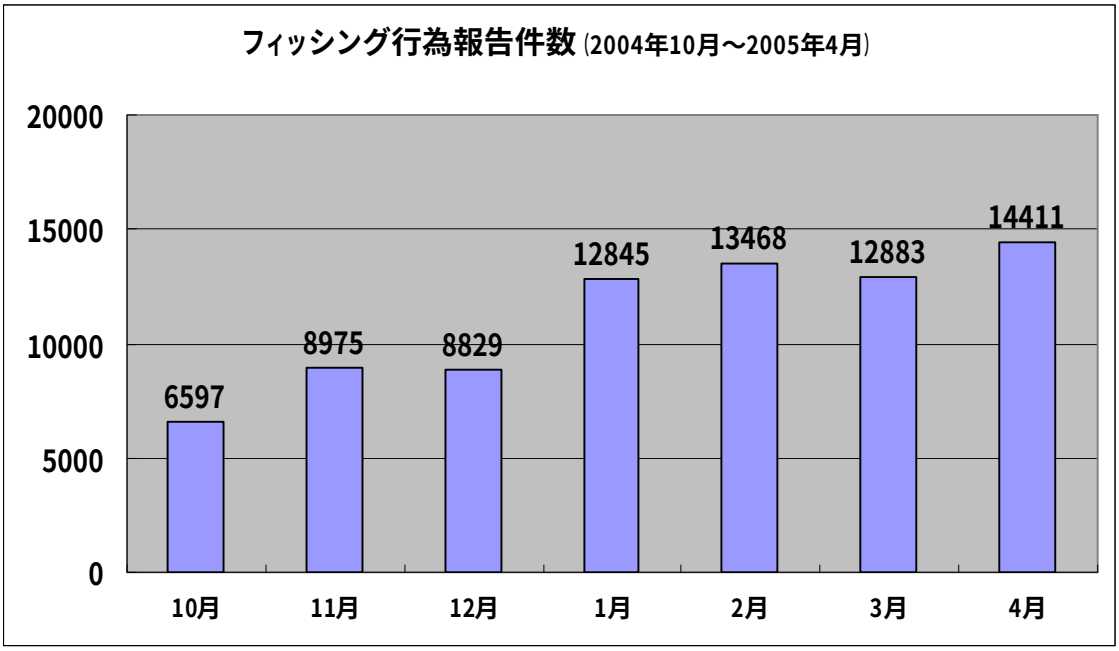
4 月中に報告を受けたフィッシング・ドメイン数の合計は 3 月に比べ若干減少しましたが、4 月第一週のみの報告件数はそれまでの記録で第 3 位となる大変顕著なものでした。

もう一つの注目すべき傾向としては、IP アドレスのみのドメインの割合が減少したことです。過去 3 ヵ月に渡り減少傾向にありましたが、4 月は最も顕著で 11%減でした。これはフィッシャーによるハッキングや詐欺用ソフトのインストール等の詐欺行為における偽装技術の向上を示すもので、実際最近のフィッシング・サイトの多くはハイジャックしたサーバを使用しています。つまり、詐欺行為は合法な事業体が運営するドメイン上で行われ、フィッシャーはそこにリモート・アクセスすることができるわけです。この手法により、好都合にも詐欺犯達はブラックリス

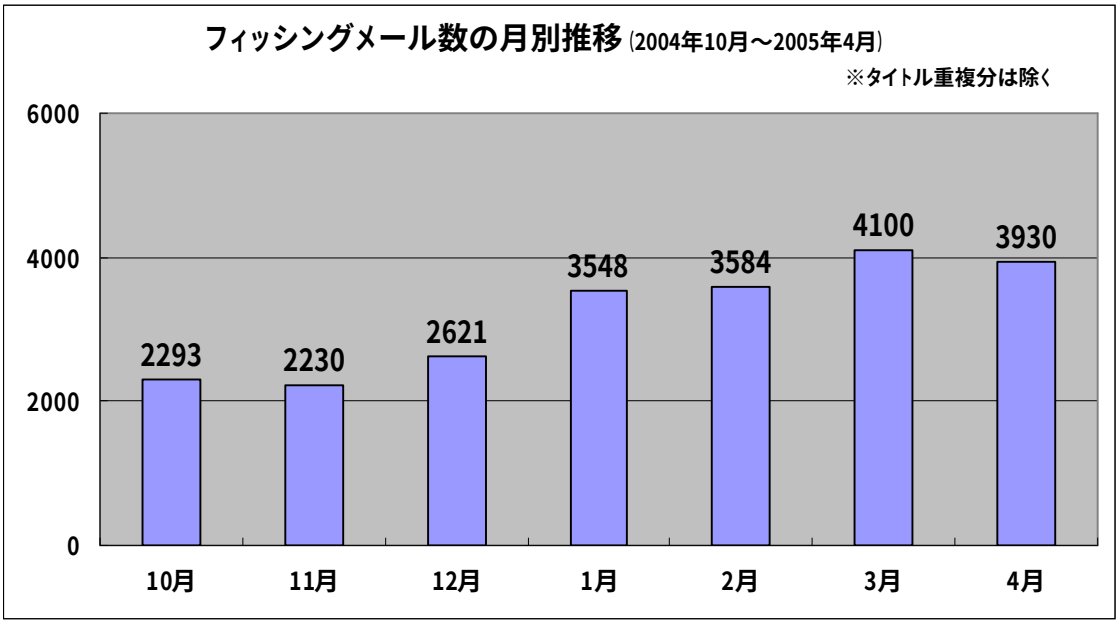
トに載ることがない合法的に運営されているドメインにリンクできるのです。事実、そのようなフィッシング・メッセージは「ホワイトリスティング(Whitelisting)」を使用するスパム・フィルターを通過してしまいます。

1.3. 【Email Phishing Attack Trends】e メールによるフィッシング攻撃最新事情

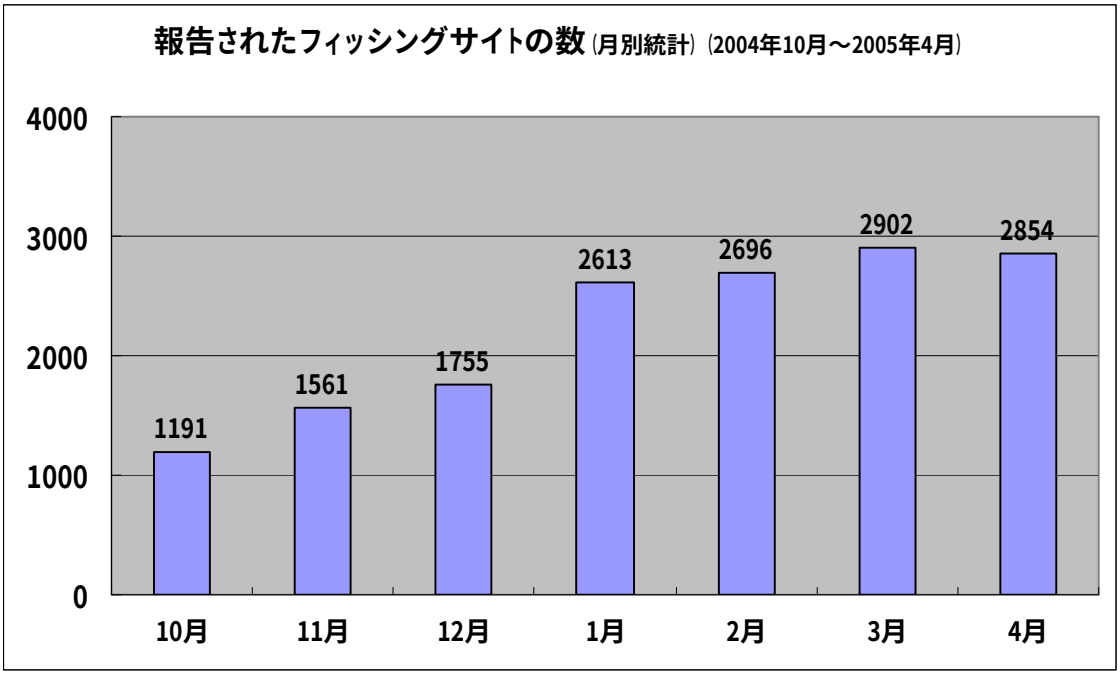
4 月期に報告を受けた件数は 14,411 件に増加し、2005 年に入ってからの微増傾向が続いています。（注）4 月期の報告件数には前月分のフィッシング・メッセージと関連のあるメッセージを含む場合があります。これまでに報告がない初めての内容による e メールを用いたフィッシング攻撃の 4 月期の件数は若干減少しました。これに連動して 4 月期に報告を受けた稼動中のサイト数も同様に減少しましたが、これは e メールを用いるフィッシング行為が同月期において若干減少したことを示しています。



フィッシング行為報告件数（2004 年 10 月～2005 年 4 月）



初めて報告される内容での e メール・フィッシング数（2004 年 10 月～2005 年 4 月）

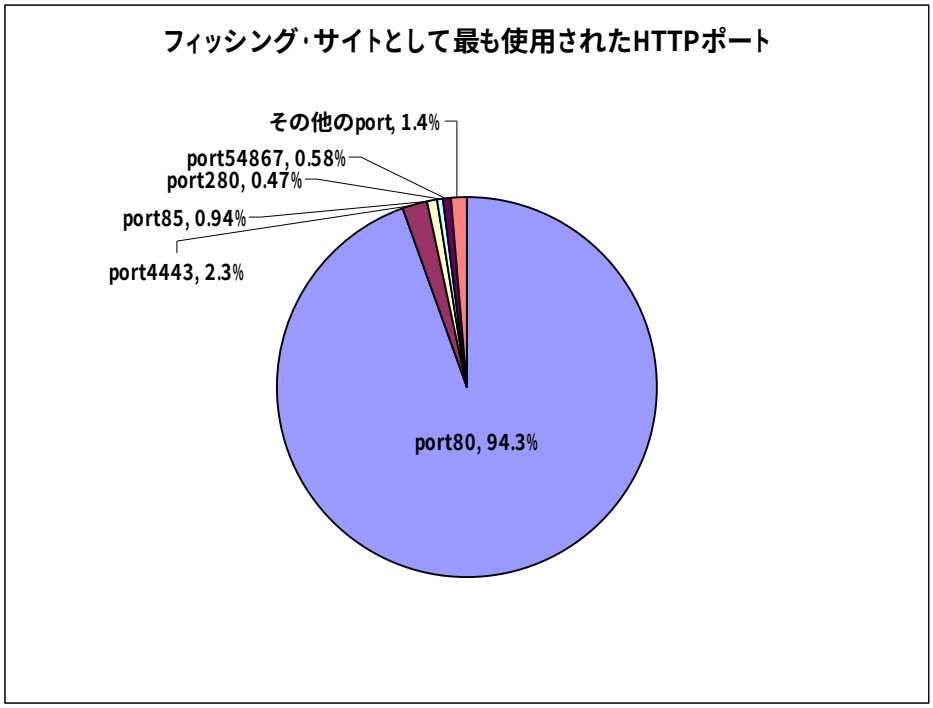


稼動中のフィッシング・サイト数（2004 年 10 月～2005 年 4 月）

1.4. 【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 月期においてもフィッシング用サイトにカズン（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 94.3%に上りました。



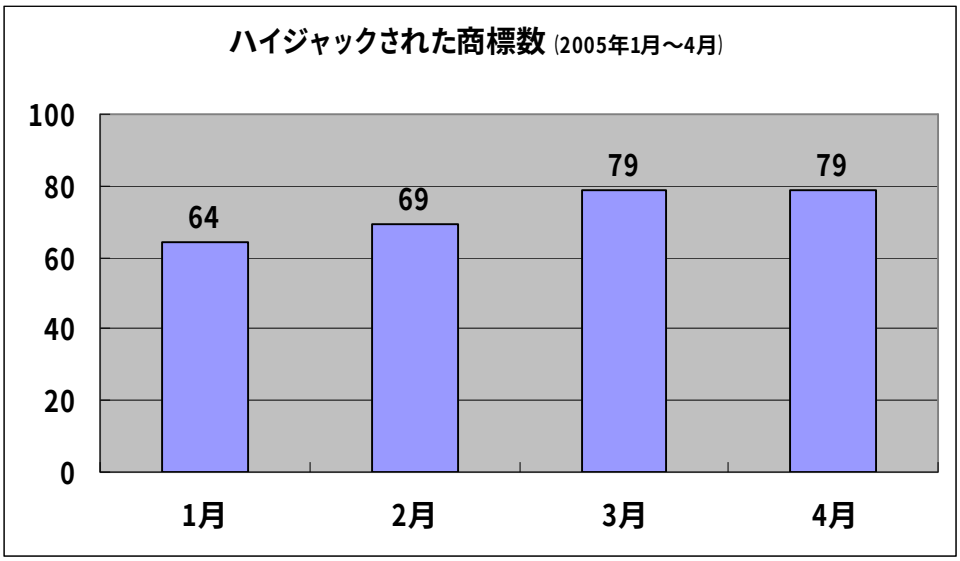
フィッシング・サイトとして最も使用された HTTP ポート

1.5. 【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

4 月期にフィッシング被害を被った商標の報告件数は 3 月期と同数に留まりましたが、これは 11 件の新規に攻撃を受けた商標が、同数のリストから消えた商標と入れ替わったことによる偶然の結果でした。目に見える傾向としては、フィッシャーの「お気に入り」の攻撃対象として不変の商標が常に存在するのと同時に、より広範囲の市場における常時変化する攻撃対象としての商標の「しっぽ」の存在があるということです。「お気に入り」商標のリストは長期に渡り変化が少なく、ほとんどのビッグ・ネームもこれに含まれますが、「しっぽ」に属す商標は頻繁に入れ替わります。この分割傾向には論理があり、商標の知名度に頼ってフィッシング・サイトへの

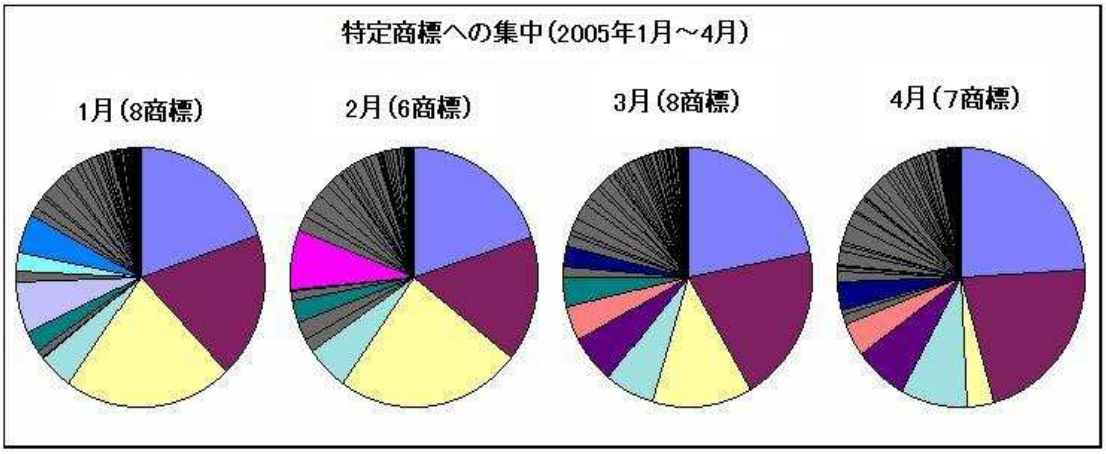
より多くのヒット数を狙う信用詐欺犯がいる一方（「お気に入り」リストの商標）、こういった詐欺行為にまだ一度も出合ったことがなかったり、フィッシング攻撃にもそれほどさらされていないと思われる組織体の顧客（「しっぽ」のリストの商標）を狙う信用詐欺犯もいるということです。



ハイジャック商標数（2005 年 1 月～4 月）

1.6. 【Brand Concentration】特定商標への集中

4 月期は上位 7 件の商標で攻撃サイトの 80%以上を占めました。これらの商標はすべて 3 月期の上位 80%の 8 件のリストに登場したものでした。攻撃目標として人気のある商標に変化がない一方で、新たにターゲットとなる商標数は毎月増加しています。4 月期は 11 件（金融機関 10 件、ISP 1 件）の新たな商標について報告がありました。



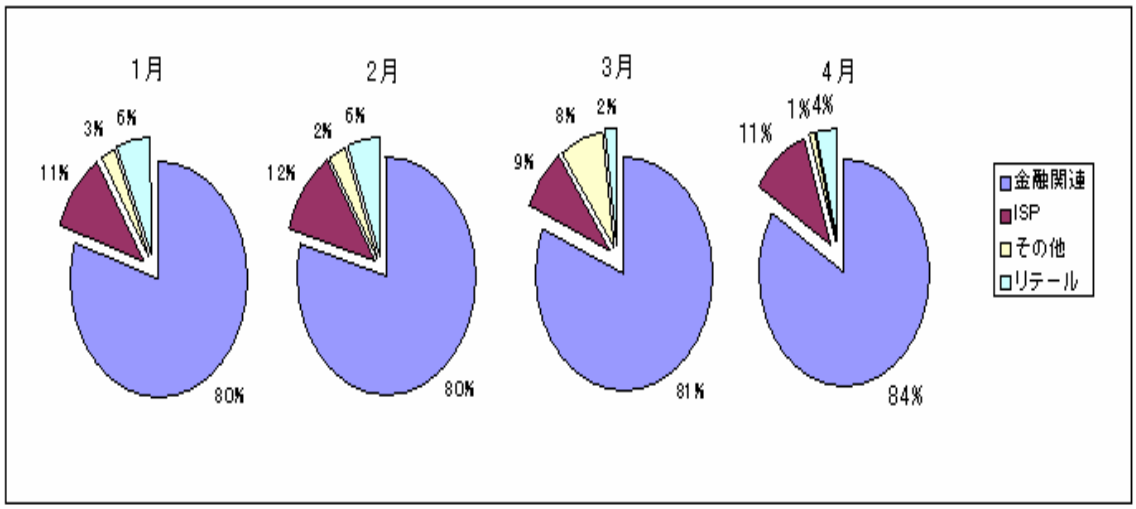
特定商標への集中（2005 年 1 月～4 月）

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

「お気に入り」標的リストに登場する商標のほとんどが金融機関のものだという事実は、当然、最も頻繁にフィッシングの標的になる産業分野も金融分野だということです。

標的となる産業分野は、標的となる商標が何かによるため、金融の分野が大きく安定したシェアを占め、その他の分野が小さく流動的なシェアを持つことになります。

3 月期と比較した場合、ISP 分野の占める割合が増加しましたが、これは 4 月中期に於いて ISP への集中攻撃と思われるものが相当数あったことによります。

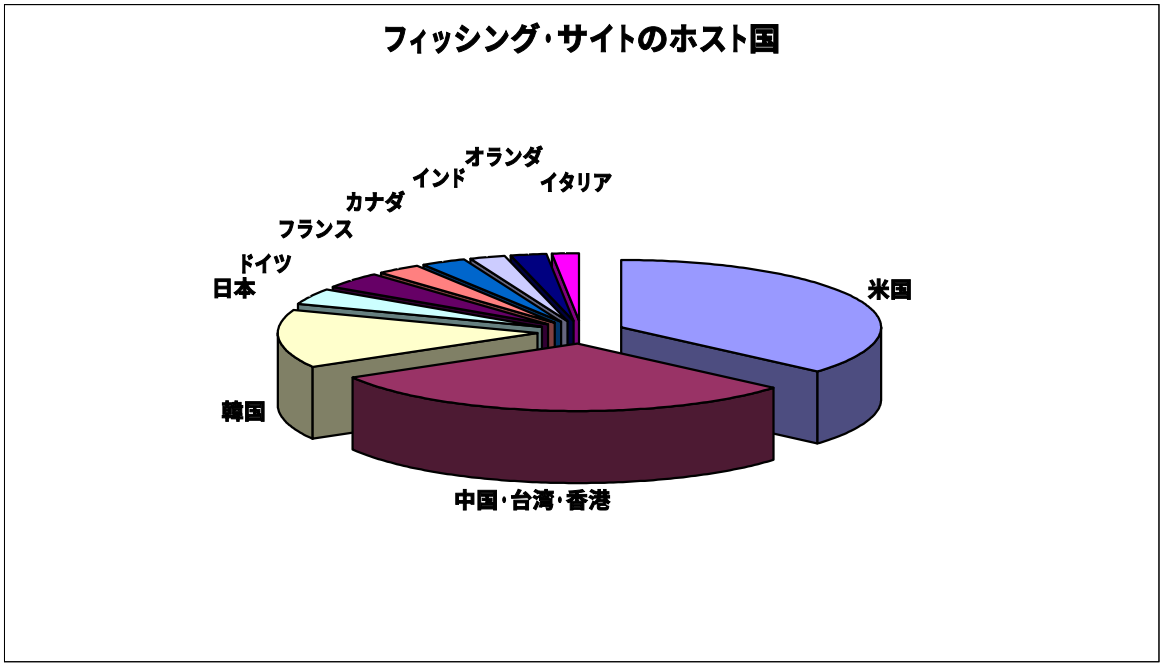


産業分野別ハイジャック商標（2005 年 1 月～4 月）

1.8. 【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

中国でのブロードバンドのユーザー数の増加に伴い、中国がホスト国のフィッシング・サイト数も増加しているようです。フィッシング・サイトのホスト国としてアメリカを追い越し第一位となる勢いでした。アメリカ 26.3%、中国 22%、韓国 10%、日本 2.87%、ドイツ 2.71%、フランス 2.1%、カナダ 1.94%、インド 1.70%、オランダ 1.50%、イタリア 1.30%でした。

今月はフィッシング・サイトのこれまでのホスト国の合計が 68 ヵ国になりました。



フィッシング・サイトのホスト国

1.9. 【標的の変化】信用組合への攻撃が増える

Websense(R) Security Labs(TM) は、4 月期においてフィッシング詐欺の標的となる信用組合（クレジット・ユニオン）の件数が激増したことを確認しました。これらは一定の地域全体を対象とした信用組合から特定の従業員グループの個人のみを対象とした「すきま」信用組合まで幅がありました。ハッカーは、これまでの知名度があったり大規模な組織を狙うというものからその手法を変えつつあります。

1.10. 【攻撃方法最新事情】

4 月期においてもフィッシング攻撃の進化は続きます。トロイの木馬やキーロガーあるいは Proxy サーバの形態をとった窃盗用コードの使用が増加しています。窃盗用コードをどのようにダウンロードさせ動かすかを決めるベクトルも変化しています。Websense Security Labs では数種の新しいペイロードとベクトルの形態の出現を確認しています。

新形態ペイロード

・フィッシング用トロイの木馬　―　キーロガー

エンドユーザーの信用情報を盗むための情報収集を目的として設計された窃盗用コードです。他のほとんどの一般的なキーロガーと異なり、フィッシング目的のものは特定の情報（最も一般的には金融関連のウェブサイト、e コマースのサイトおよびウェブを利用した e メールサイトへのアクセスです）を標的とするために特定の入力操作を監視しようとする入力操作記録の追跡機能を備えています。

・フィッシング用トロイの木馬　―　リディレクター

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犯罪用コードです。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不正コード、詐欺サイトへ情報を誘導するようなブラウザー・ヘルパーへの不正コード、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不正コードを含みます。これらの不正コードはすべて個人情報の盗み取りやその他の信用情報を犯罪目的で取り出すという情報についての窃盗を行う目的でインストールされるものです。

・ファーミング攻撃

これは、二者間のコミュニケーションにおける情報の流れを妨害することにより、ユーザーを詐欺地点に誘導しようとするものです。現在最も流通しているファーミングの形は DNS キャッシュ汚染です。

今後出現するベクトル

・タイポ攻撃

これは、ユーザーがあるドメインに接続するための URL を打ち込んだ際、文字の入力エラー（タイポ）が起こるように仕組まれた不正コードを持つウェブサイトへ誘導して行う攻撃です。例えば、ある URL に含まれる「L」の文字が入力されると、アタッカーがキーボード上では隣にある「K」の文字と入れ替えてしまうというようなことです。そして、打ち込んだ文字が他の文字と入れ替わった URL は詐欺用ウェブサイトにつながっていくのです。

・サーチ・エンジンの汚染

これは、サーチ・エンジンでの検索結果に目的のウェブサイトを割り込み表示し、そのウェブサイトに誘導するものです。誰もが使用する用語の場合や、検索用語のタイポ攻撃や社会工学用語を組み合わせたものがあります。

1.11. 【Dominating and Emerging Attack Techniques】現在支配的な攻撃手法と今後出現してくるもの

・合法サイトを利用した新型リディレクターの使用の普及

フィッシャーは、合法サイトを利用するリディレクターをより広範囲に使用できるものにし、合法的であると見せかけたリンクの形成に引き続き使用していくでしょう。

・メイン・プロセスの最中で行われるフィッシング攻撃

この種の攻撃についての報告数は増加しています。標的となった合法サイトでログイン・プロセスが行われる際の情報が得られると、詐欺犯はたとえばその合法的にログインされたサイトの最表層に不正なマスクページ構築することができ、そこを間違ったログイン・データが通過した場合にエラーメッセージを返すというようなことをします。

このような攻撃は他のものよりも発見が難しいため、大変危険な状況になろうとしています。

・新しい e メール・フィッシングの流布傾向

今後予想される新しい形態のフィッシング詐欺が発見されました。それは、同一の標的に対して同時に複数の異なった仕組みを用いた攻撃を加えるというものでした。これにより、フィッシング犯同士の共通の結びつきや、少なくとも相互連絡性や組織性を与えることになるでしょう。

1.12. 【Phishing Research Contributors】フィッシング研究・提供

TUMBLEWEED COMMUNICATIONS
Tumbleweed Message Protection Lab
Tumbleweed Message Protection Lab の使命は、現在あるいは今後起こりうる企業を標的とした e メールによる窃盗行為の分析と新しい e メール保護技術の開発です。

主任研究員： Jhon Thielens, johnt@tumbleweed.com

WEBSENSE
Websense Security Lab(TM)
Websense Security Lab 使命は、インターネットに対する高度化した脅威の発見、調査と報告により、従業員のコンピューター使用環境を保護していくことです。
主任研究員： Dan Hubbard, dhubbard@websense.com

メディアからのお問い合わせは、Ronnie Manning, manning@websense.com または 858-320-9274
または、APWG 事務局長 Peter Cassidy, 617-669-1123

Anti-Phishing Working Group について

Anti-Phishing Working Group（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。

Anti-Phishing Working Group 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 Tumbleweed Communications の Tumbleweed Message Protection Lab により提供されています。

APWG は Tumbleweed Communications 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。

Anti-Phishing Working Group
http://www.antiphishing.org info@antiphishing.org