4半期レポート（2008年1月-2008年3月）

APWG Phishing Activity Trends Report (Q1/2008)
日本語版

2008 年 9 月 20 日

目次

1. APWG Phishing Activity Trends Report 2008年第1四半期　日本語版

・レポートの調査範囲

『APWG Phishing Activity Trends Report』では、APWGがウェブサイトhttp://www.antiphishing.org上あるいはAPWGグループ宛ての次の電子メールreportphishing@antiphishing.orgにて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。またAPWG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。Crimeware（クライムウェア）についてはこのレポートの後半でまとめています。

・フィッシング（phishing）の定義

『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ウェブ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乗っ取ることにより、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用されています。さらに、インターネット接続時に経由するルートを不正に改ざんし、偽装ウェブサイトへ誘導するような手法もあります。

・レポートの要約

IRS関連のAPWGへ送られてきたフィッシング報告は、2月の急増の後、12.5%減少しています。またAPWGによる調査で、IRS攻撃関連のフィッシングサイトは2月に36,002件まで増加した後12%減少し、3月には25,630件になりました。

乗っ取られた商標の数は四半期中で131件から141件まで増加しました。アメリカがフィッシングサイトのホスティング国1位をキープする一方、中国は5位に下がりました。またキーロガーなどの有害なアプリケーションは、最大で430件の検知を記録しました。

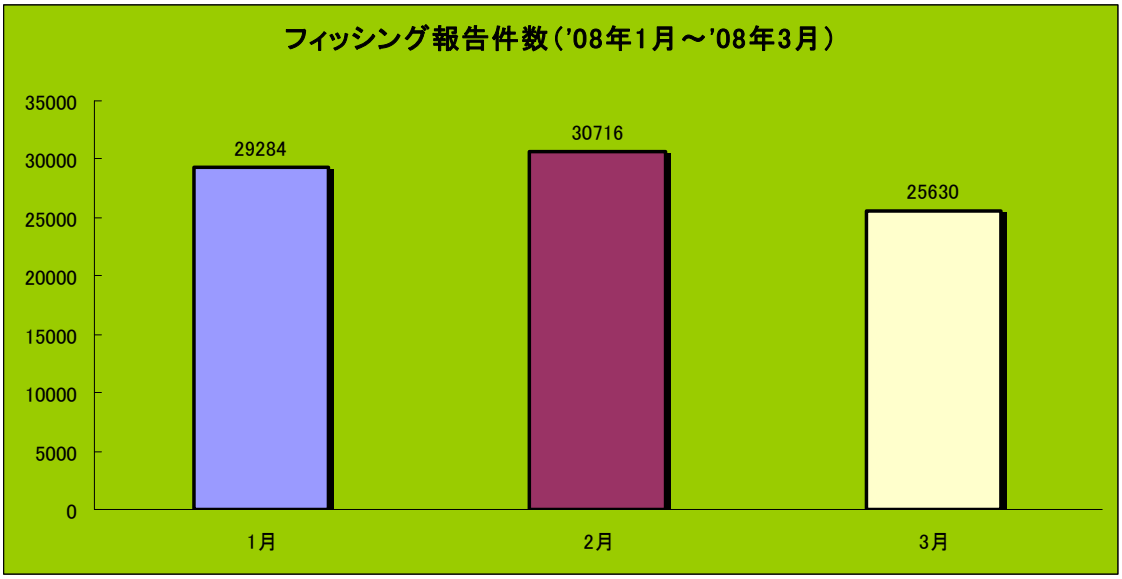
2.【Statical Highlights】統計によるハイライト

表 2.1　フィッシングに関する統計

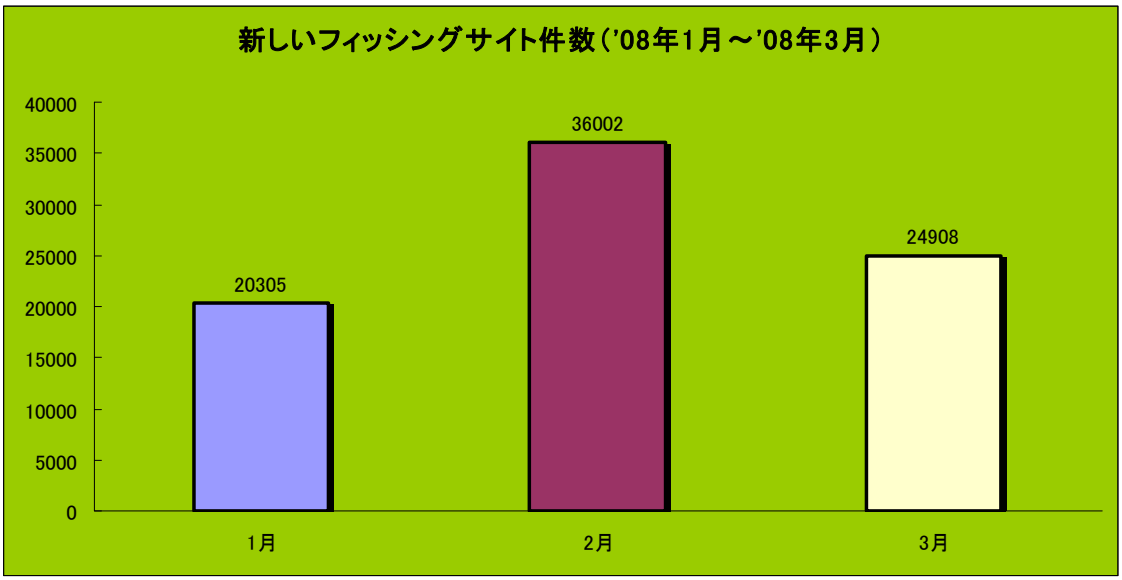
	1 月	2 月	3 月
フィッシングに関する報告件数	29,284	30,716	25,630
報告されたフィッシングサイト数	20,305	36,002	24,908
フィッシングにより乗っ取られた商標数	131	139	141
最も多くのフィッシングサイトをホストした国	アメリカ	アメリカ	アメリカ
商標の名前が URL に含まれていた割合	28.3%	23.2%	26.1%
IP アドレスのみでホストネームなしのサイト	5.5%	13.2%	4%
ポート 80 を使用しないサイトの割合	0.81%	0.45%	0.49%
サイトの最長オンライン残存期間	31 日間	29 日間	31 日間

3.【Phishing Email Reports and Phishing Trends】フィッシングメールとフィッシングサイトの傾向

2008 年第 1 四半期のフィッシングに関する報告件数は、相変わらず 5,000 件を超えています（日本語訳注：5,000 という数値は誤植の可能性があります）。期間中、報告件数は 2 月に増加し 30,716 件を記録した後 12.5%減少し、25,630 件で 3 月を終えました。3 月の報告は、2007 年 9 月に記録した最高値より 33%小さい値を記録しています。フィッシング報告メールの件数は、一般の方や、APWG メンバー、共同研究者の方々から APWG へ送られてきたものをカウントしています。



2008 年第 1 四半期、APWG によって検知されたフィッシングサイト数は、2 月中に大幅に増加を見せ、1 月に比べ 77%増加しました。しかしながら、限定的に IRS 関連の攻撃が少なくなったことを反映して、3 月中は 31%以上減少しています。

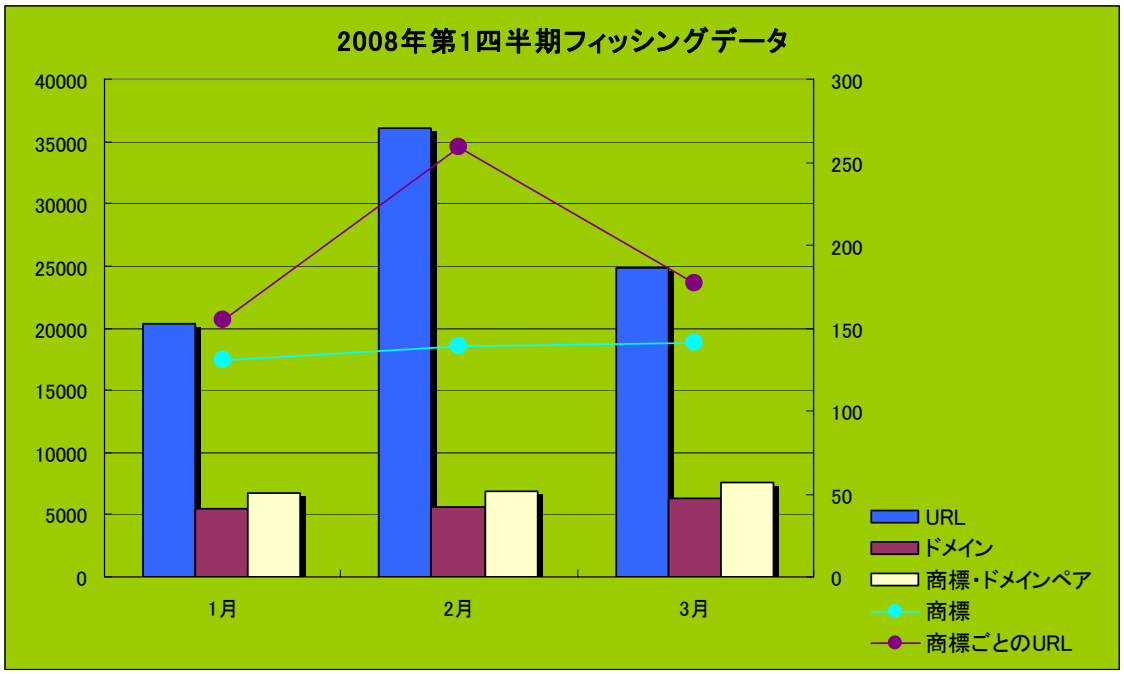


4.【Brand-Domain Pairs Measurement】商標－ドメインペアの観測

次に示す図は、フィッシングされた商標、ドメイン、商標・ドメインのペア、そして URL に基づいた統計値をまとめたものです。商標・ドメインのペアは、特定の商標を標的にするために使用された場合をカウントしています。

※いくつかの URL が同じ商標を標的にしていて、同じドメインにホスティングされている場合、この商標・ドメインのペアは、複数でなく 1 つとしてカウントします。

フォレンジックユーティリティ：フィッシングされた URL の数が、商標・ドメインのペアの数より多い場合、それは多くの URL が同じ商標を標的にするために同じドメインにホスティングされていることを表しています。それぞれのドメインにいくつの URL が対応しているのかを知ることで、攻撃される商標を持つ会社や組織が場所を特定し、無効化する必要があるような攻撃ドメインの最大数が分かります。またフィッシング対策技術（ブラウザおよびメールブロッキングなど）が、URL を要求することで、ドメインごとにある URL の数の理解に役立つと言えます。



商標・ドメインのペアは、1 月から 3 月の調査を通して 6,682 件から 7,584 件へと着実に増加しています。これを受けて、MarkMonitor のアンチフィッシングソリューションのディレクターで、本レポートのアナリストである John LaCour 氏は、「フィッシング犯はとどまることを知らないようだ。」と発言しています。また同氏は、「減少するフィッシング詐欺によって URL 数が 3 分の 1 減少する一方で、商標とフィッシングドメイン名の組み合わせで測定される実際の攻撃数は 11%増加している。これは、従来のフィッシング手法がいまだ強力で、増加し続けていることを示している」と結論付けました。

表 4.1　フィッシングデータに関する表

	1 月	2 月	3 月
URL 数	20,305	36,002	24,908
ドメイン数	5,490	5,671	6,271
商標・ドメインペア数	6,682	6,681	7,584
商標数	131	139	141
商標あたりの URL 数	155	259	177

5.【Most Used Ports Hosting Phishing Data Collection Servers】フィッシングデータをホスティングする収集サーバで最も使用されたポート

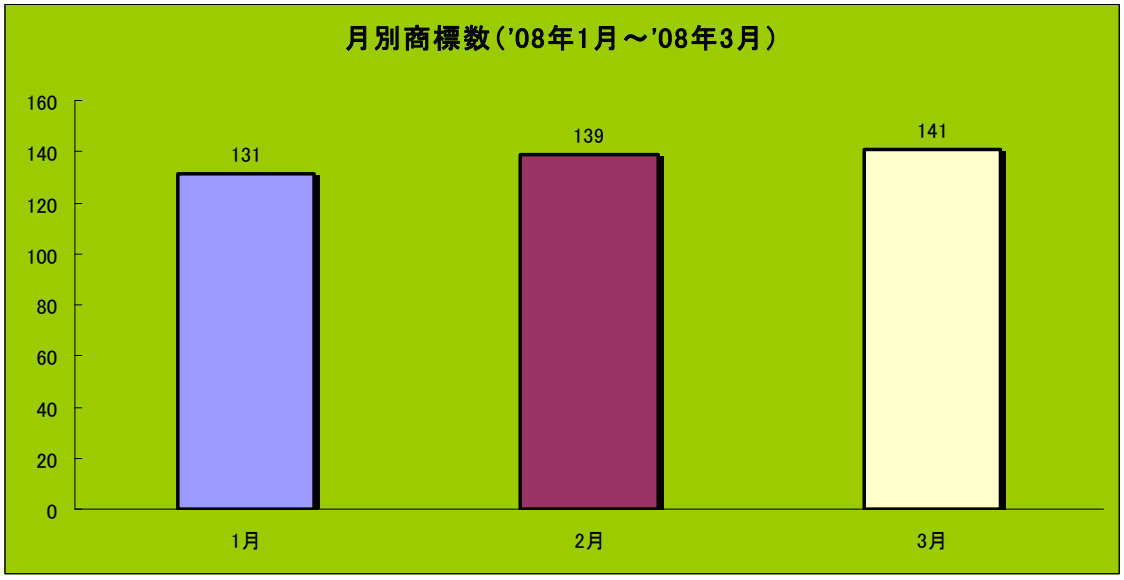
2008 年第 1 四半期は、全てのフィッシングサイトで最も HTTP ポート 80 番の使用が多いと報告され、この傾向は APWG が調査、報告を始めてから一貫して続いています。

表 5.1　月、ポート別の使用された割合

1 月		2 月		3 月	
ポート 80	99.23%	ポート 80	99.57%	ポート 80	99.48%
ポート 443	0.28%	ポート 82	0.17%	ポート 443	0.20%
ポート 84	0.20%	ポート 443	0.12%	ポート 81	0.09%
ポート 82	0.17%	ポート 8080	0.07%	ポート 82	0.07%
ポート 88	0.04%	ポート 4100	0.04%	ポート 84	0.05%
その他 3 つ	0.08%	その他 2 つ	0.03%	その他 4 つ	0.11%

6.【Brand and Legitimate Entities Hijacked by Email Phishing Attacks】メールフィッシング攻撃によって乗っ取られた商標および正規の組織等

2008 年第 1 四半期、期間中乗っ取られた商標の数は 131 件から 141 件と 7.6%の上昇を見せました。相変わらず被害に合った商標は、120－160 件の範囲にとどまっており、攻撃は類似した標的へ向けられています。3 月の商標数は、2007 年 11 月の最高値 178 件の約 20%小さい値です。



7.【Most Targeted Industry Sectors】最も標的にされた産業分野

2008年第1四半期は、引き続き金融関連サービスが最も標的にされた産業分野になりました。これはAPWGが標的にされた産業分野の調査を始めてからは変わっていません。3月に見られる標的としての“政府およびその他”の項目の上昇は、IRS関連の攻撃およびそれに似た攻撃の増加による影響だと思われます（2008年にIRSが行った景気刺激政策を利用したフィッシングによる）。

表7.1　最も標的にされた産業分野表

	1月	2月	3月
金融サービス業	92.4%	94.2%	92.9%
小売、販売業	1.5%	1.4%	1.4%
ISP	3.8%	2.2%	1.4%
政府およびその他	2.3%	2.2%	4.3%

8.【Countries Hosting Phishing Sites】フィッシングサイトをホスティングしている国

2008年第1四半期は、引き続きアメリカが最もフィッシングサイトをホスティングしており、その大部分の攻撃がアメリカの会社へ向けたものです。ロシアは期間中全ての月で4位内に入っています。3月には、中国が全てのフィッシングサイトの3%しかホスティングしていないという興味深い結果となりました。

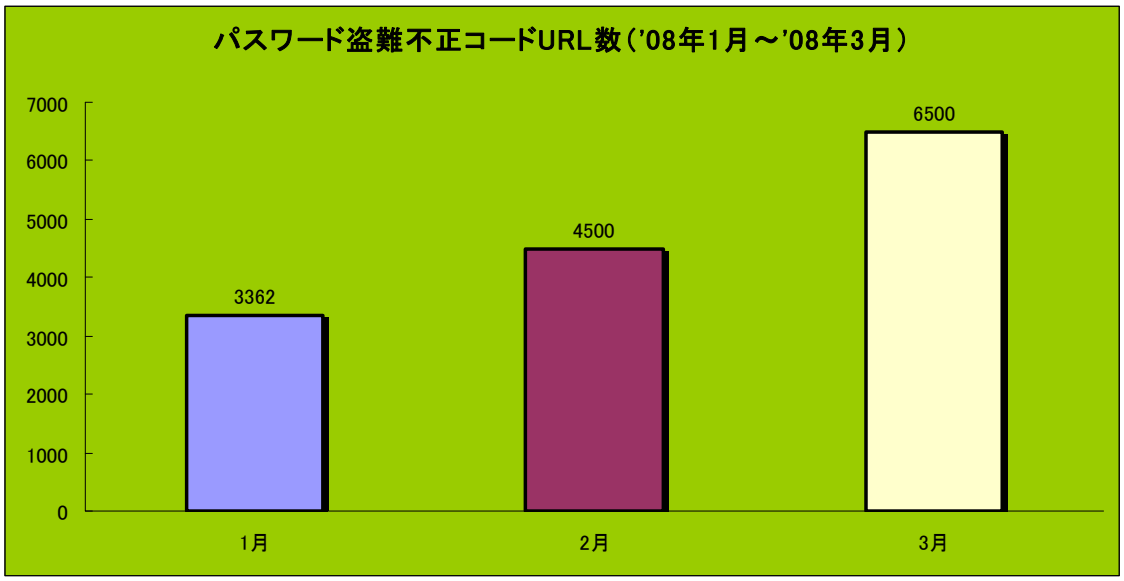
表8.1 国別フィッシングサイトホスト率

1月		2月		3月	
アメリカ	37.28%	アメリカ	27.11%	アメリカ	38.23%
ロシア	11.66%	中国	19.25%	ロシア	10.58%
中国	10.30%	カナダ	12.66%	フランス	6.38%
ドイツ	5.64%	ロシア	10.22%	ドイツ	4.71%
ルーマニア	5.09%	フランス	3.39%	イギリス	4.49%
韓国	3.76%	ドイツ	2.94%	中国	3.07%
フランス	3.28%	トルコ	2.59%	レバノン	2.48%
カナダ	1.94%	韓国	2.23%	カナダ	2.28%
イギリス	1.91%	インドネシア	2.08%	イタリア	1.96%
イタリア	1.59%	イギリス	2.04%	韓国	1.87%

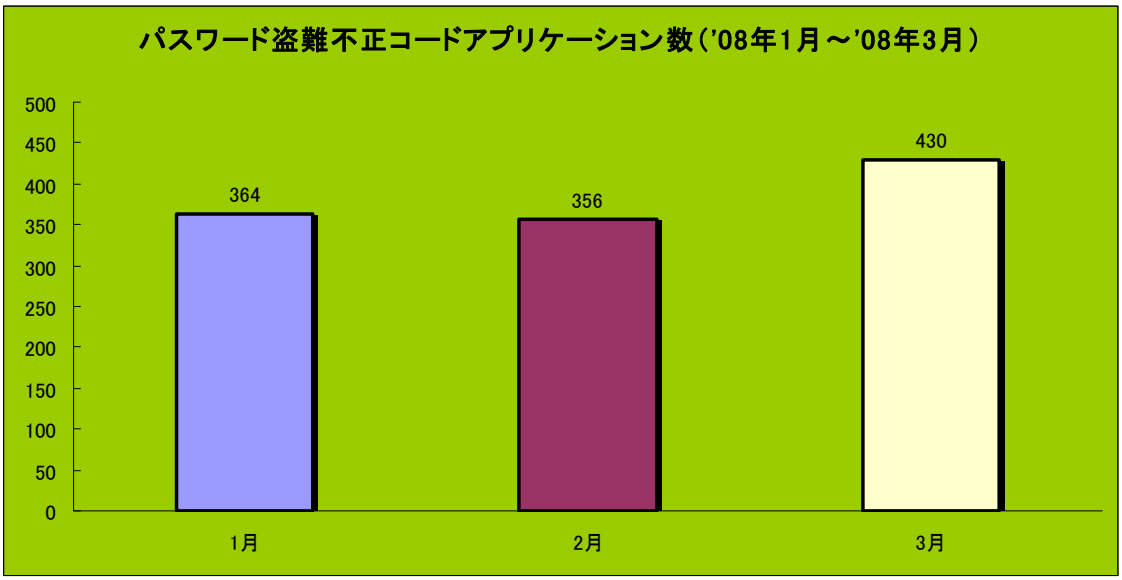
9.【Phishing-based Trojans-keyloggers】フィッシングベースのトロイの木馬およびキーロガー

クライムウェアを広める URL の数は、1 月の 3,362 件から、3 月の 6,500 件まで増加が見られました。これは 2007 年 11 月の記録よりほぼ 86%の上昇です。また 3 月に報告されたクライムウェアを広める URL の数は 2007 年の 3 月より 337%も増加しています。

Websense 主任技術員であり、本レポートのアナリストである Dan Hubbard 氏は、「この上昇は今年に入って増加した大量の SQL インジェクション攻撃に影響を受けたのではないか」と発言しています。



キーロガーおよびクライムウェア指向の有害アプリケーションの数は、四半期で着実に増加し、3 月には、364 件の有害なアプリケーションが検知された 2008 年 1 月より 18%多い最高記録、430 件で終えました。結果からハッカーたちは、明らかに企業やその消費者のセキュリティ対策をすり抜けるための新技術開発を行っていると思われます。



・フィッシングベース　トロイの木馬－リダイレクタ

定義：エンドユーザーを本来意図されていないネットワーク上の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みます。これらは全て個人情報の盗難やその他の信用情報の不正取得という犯罪目的のためにインストールされます。

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、単純にユーザーPC 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。

10.【Phishing-based Trojans and Downloader's Host Countries(by IP address)】IP アドレスによるトロイの木馬およびキーロガーのダウンローダホスト国

以下の表はこの四半期、フィッシング用キーロガーもしくはキーロガーのダウンローダのいずれかの形で有害なコードをホスティングしているとして分類されたウェブサイトの調査結果です。

表 10.1 トロイの木馬およびキーロガーのダウンローダホスト国分類

1 月		2 月		3 月	
アメリカ	43.39%	アメリカ	38.55%	アメリカ	46.21%
中国	16.95%	中国	11.59%	中国	11.41%
フランス	6.89%	韓国	10.38%	韓国	7.38%
イギリス	5.92%	ロシア	8.15%	ロシア	7.25%
韓国	5.84%	ポーランド	7.77%	ポーランド	6.32%
ロシア	4.46%	ルーマニア	6.75%	ルーマニア	4.90%
スペイン	3.81%	インド	5.77%	インド	4.77%
ポーランド	3.41%	ドイツ	4.28%	ドイツ	4.42%
ルーマニア	3.24%	フランス	3.49%	フランス	3.93%
ドイツ	3.16%	アルゼンチン	3.26%	アルゼンチン	3.42%

11.【APWG Phishing Trends Report Contributors】APWG Phishing Trends Report 協力事業者

・MarkMonitor

MarkMonitor は、オンライン決済などに対してする安全に特化した統合的オンライン個人情報プロテクションサービスを提供する国際リーダー企業です。

・PandaSecurity

PandaSecurity は、ユーザをマルウェアから守ることに特化した研究と技術サポートセンターの国際ネットワーク企業です。

・Websense

Websense Security ラボの目的は、コンピュータ環境で働く従業員を脅かす進化するインターネットの脅威に関する発見、調査、報告です。

Phishing Attack Trends Report は、APWG によって四半期毎に発行され、フィッシング、クライムウェア、メール盗聴の問題増加によって引き起こされる個人情報の盗難や詐欺の撲滅に焦点を当てた産業および司法当局などの団体から成ります。より詳しい情報についてはこちらのいずれかへ連絡して下さい、APWG Deputy Secretary General Foy Shiver 404.434.7282、Cas Purdy 858.320.9493、cpurdy@websense.com、TeSmith 831.818.1267、Te.Smith@markmonitor.com。

APWG は、このレポートでのデータ、分析について全ての上記協力メンバーに感謝します。

・APWG について

フィッシング対策ワーキンググループ（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場合があります。

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 1,800 以上の企業および政府機関が加入しており、会員数は 3,000 名以上に上ります。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。

フィッシング対策ワーキング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。

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。