

「ファージングを中心とした悪意ある行為」

渡辺弘美@JETRO/IPA NY

1. はじめに

インターネット上での悪意ある行為は、個人によるハッキングやスパムメールの送信といった迷惑行為から、組織的な詐欺行為に発展しつつある。インターネット上での決済行為が増加するにつれ、新たな資金調達のルートとして組織的な犯罪がインターネット上で増加しつつある。また、詐欺行為に使用される技術レベルやインターネット・ユーザを騙す手口もより高度になっている。

フィッシング(Phishing)という聞きなれない言葉が登場してまだそれほど時間がたっていないが、米国では新手の悪意ある行為がまた新たな言葉を伴って現れている。セキュリティ企業がビジネス上の戦略から新たな言葉を作り出している感は拭えないものの、現実には悪意ある攻撃者はユーザが気づかない手口で忍び寄っている。

ここでは、フィッシング詐欺の派生である「ファージング(Pharming)」を中心に、それ以外の悪意ある行為である、「悪魔の双子(Evil Twin)」、「ランサムウェア(Ransomware)」、「IM(インスタント・メッセージング)利用のフィッシング」、「パーソナライズド・フィッシング」、「キーロガー(Key Logger)利用によるフィッシング」、「偽ショッピングサイト」、「特殊文字利用のフィッシング」の現況について解説する。

いずれの行為も悪意ある者が将来の本格的な攻撃の前兆として試行的に実行しているとの指摘もあるので、今後これらの行為は大きく変化することが予想されるが、いずれの事例もインターネット・ユーザを保護するための方策を考える重要なケースと言えるものである。

2. ファージング(Pharming)

(1) ファージングとは

ファージングとは 2005年初頭より徐々に広まってきたインターネット・ユーザを対象とする詐欺行為である。フィッシング(Phishing)詐欺は既に社会問題化しており多くの被害が報告されているが、このファージングもフィッシングの一種であると言ってよい。

ファージングの被害実態を統計的にまとめたものはまだ存在しない。フィッシングについては、調査会社 Gartner 社の調査によると、2004年には5,700万人の米

国人がフィッシング詐欺のメールを受け取り、銀行やクレジットカード会社は合計で102億ドルの被害を被ったとされているが、今後はより巧妙な手段を取るファームング詐欺の被害が増えていくものと予想されている。また、フィッシング対策団体 APWG(Anti-Phishing Working Group)に2005年3月までに報告されたフィッシングの偽サイトは2870サイト。フィッシング・サイトのうち34%以上が米国内にあるという。日本は中国・台湾・香港、韓国、ドイツ、カナダに次いで6番目に多いとされている。

サイバー犯罪対策に取り組む団体 National Cyber-Forensics and Training Alliance (NCFTA) は、2005年4月に、インターネット詐欺のワースト5を発表しており、ファームングを最も悪質としている。

インターネット詐欺のワースト5

(ワースト1) Pharming

(ワースト2) Google ハッキング

検索エンジンの Google を利用して個人情報盗む。個人が Web 上にアップロードした履歴書などから、社会保障番号、家族の履歴、住所、電話番号、学歴などが含まれるドキュメントから情報を収集する。

(ワースト3) FBI の名を騙るウイルス/スパムメール

FBI は、同局の名をかたって送信されているウイルス感染メールに対する警告を発表している。この種のスパムは、「調査により、違法な Web サイトを訪問していたことが明らかになった」として、受信者に添付ファイルの質問に答えるように促す。添付ファイルには、「W32.Sober.K@mm」が潜んでいる。送信元として police@fbi.gov、fbi@fbi.gov、officer@fbi.gov、web@fbi.gov といったアドレスから送信されたように見せかけている。

(ワースト4) Phishing

(ワースト5) ナイジェリア詐欺

架空の融資話や違法なマネー・ロンダリングなどをもちかける詐欺メールで、受信者に手数料を求めたり、取引を行うために個人の経済情報などを要求したりするもの。この種の詐欺行為は、津波関連の詐欺と一緒に復活した。

ファームングの基本的な構成要因としては、「インターネット上での詐欺行為」であり、「サーバーへのハッキング行為と、なりすましによる個人情報の不正入手と悪用」である。

ファームングの基本的な仕組みは、フィッシングのように餌（偽サイトに導くためのメール）を必要とせず、インターネット・ユーザが自身の手でブラウザ上に URL を打ち込んで希望のサイトを閲覧しても、気づかないままに詐欺行為を働くための別の偽サイトへ導かれ、そのサイト上で個人情報を入力すれば、結果的に詐欺行為の被害者になってしまうというものである。

これは専門家の中で「DNS Poisoning 攻撃」と呼ばれるウイルスやワームによるサーバーへのハッキング攻撃であり、既にサーバーがこの種の攻撃を受け、DNS ファイルの書き換えなどが行われていた場合には、これを知らぬユーザーはこのような被害にあう可能性が高い。

ファームングは、メールによる詐欺行為が主体のフィッシングに対して、何らかの警戒をしているユーザーにも詐欺行為を働くことができ、しかも個別にメールを発信する必要があるフィッシングと異なりサーバーに対する攻撃であるため、一カ所への攻撃の後には多くのユーザーを詐欺行為の対象とできることから、攻撃側にとっての魅力であると言える。

ただ、このようなサイトに対する攻撃は以前からも確認されており、スパイウェア等を利用しキーロガー(Key Logger：入力記録ソフトウェア)を秘密裏にユーザーの PC にインストールし、ユーザーの個人情報盗み見する行為や今回目立ってきている「ホストファイル」を利用している物などはこれまで「ステルス型フィッシング詐欺」と呼ばれていた。

しかし 2005 年に入ってからはこの種のフィッシングが増えてきたことからこれらを特別にファームングと呼ぶようになってきていた。

特に、米国のコンピューターセキュリティ専門の教育機関 SANS Institute が 2005 年 3 月に具体的な詐欺事例を報告したことでファームングが広く知られるようになった。SANS Institute の発表によれば、このレポートの時点で、Google、eBay 等の大手商用サイトにアクセスしようとしたユーザーが偽のサイトにアクセスしてしまったことが報告されている。

誘導されたサイトは大手商用サイトによく似たデザインを採用し、個人情報や各種のパスワードを入力させようとするものや、スパイウェア(ABX toolbar など)や他のウイルスなどをインストールさせようとするものなどがあつたという。SANS Institute では過去のいずれかの時点ですでに多くの DNS サーバーが攻撃されており、結果として多くのユーザーに被害が出たものとしている。

しかしこの時期の DNS Poisoning には、「なりすまし」行為は無く、その意味ではファームングの定義からは、ややはずれていると見られている。しかし専門家の間ではこの攻撃は後日の大規模なファームング詐欺の実験であつたのではないかと見る向きも多く、今後のより一層の警戒が必要とされると警告している。

(2) ファームングの命名由来

ファームングは「Pharming」と表記するが、これは、フィッシング(Phishing)が餌(偽サイトへ誘導するためのメール)を必要とする魚釣り(fishing)に相当するのに対して、ファームングは、餌を必要とせず、サーバーへの攻撃から実際の詐欺

行為までに何らかのタイムラグがあることから、あたかも農業の種蒔きから収穫までのようだというので、農業 (farming) をもじってこのような呼び方をされている、

しかしこの呼び方を始めたのが幾つかの商業ニュースサイトや有力な大手インターネット・セキュリティ会社とすることで、この命名には非難の声もある。

なお、スペルを「f」ではなく「ph」とするのは leetspeak と呼ばれる一種のハッカー用語である。leetspeak とは、elite (エリート) を自負するハッカー達が使う暗号のようなスラングであり、チャット上の会話、著作権問題の回避策などの手段として用いられている。leetspeak のルールは、多少の例外はあるが、発音どおりに綴る (for は 4)、形の似たものに置き換える (A は 4、S は 5 や \$、F は | や ph) などがあり、例えば、「leetspeak」は「1337\$ph34k」となる。leetspeak は「おれよ (おはよの意味)」のようなギャル文字に通じるものがある。ウェブ上には leetspeak 変換サイトや、leetspeak で記載された検索サイト Google H4x0r (Google Hacker の意味) も存在する。

(3) 技術概要

ファーミングには、「hosts file hacking」と「DNS Poisoning」の2つの手口がある。

1 つ目の hosts file hacking は、ユーザーのコンピュータを舞台にする方法である。

まず、急速に普及する P2P (ピア・ツー・ピア) アプリケーションを利用してコンピュータの防御網をかいくぐり、スパイウェアあるいはウイルスをユーザーの PC の内部に仕掛ける。その後、ウイルスは PC 上の OS 内の hosts ファイルを探し出し、そこに正規サイトを模して作られた偽装サイトの IP アドレスを設定する。

スパイウェアは、ユーザーが銀行やクレジットカード会社の URL を Web ブラウザに入力すると、そのアドレスを DNS で検索させず代わりに偽の URL へ誘導する。

この hosts file hacking は、ウイルスやスパイウェアによっても感染するほか、Microsoft Outlook などのメールソフトでも感染する場合もある。もし感染した場合はユーザーに見えないように作業が行われる特殊なスクリプトが起動し、そこにある hosts ファイルが書き換えられる。

もう 1 つの手口である DNS Poisoning は、DNS (Domain Name System) システム自体を攻撃する方法である。攻撃者は、対象となる DNS サーバの hosts ファイルのキャッシュに偽りの情報を記載し、そのサーバを利用するインターネット・ユ

ーザが特定のサイトにアクセスしようとした際に、別のサーバーにアクセスするよう誘導する。

DNS Poisoning の手法

1. 攻撃対象のユーザが利用する DNS サーバーに、ユーザが利用しようとしているサイトの URL について IP アドレスの問い合わせを行う。
2. 当該 DNS サーバーは対象となるサイトの IP アドレス情報が自身のドメインの管理下には無いケースが大半なため、情報の入手のため当該ドメインの DNS サーバーに情報のリクエストをする。
3. 攻撃者は 2. の要求転送先である DNS サーバーになりすまし、誘導したい IP アドレスを回答として送信する。

DNS は通常 UDP (User Datagram Protocol) を使用して通信を行うため、IP パケットの送信元を書き換えるだけで容易に詐称することができる。

サーバー側の対策としては返答の送信元の詐称を困難にする為、情報入手のリクエストを発信する際に、無作為なシーケンス番号を指定するが、攻撃者が総当りの異なるシーケンス番号を持つパケットを大量に送信することで DNS サーバーを詐称することができてしまう。また、古い DNS サーバーでは、一つの問い合わせについて複数の要求パケットを送信する事もあり、シーケンス番号が偶然一致する確率が高くなる。

(4) DNS Poisoning への対策

このような DNS Poisoning の対策としては、目的とするサイトの SSL(Secure Sockets Layer)のサーバ認証を利用し、ユーザーに安全性を確認する為に発行される証明書を毎回確認する事がせいぜいである。

SSL を使用していることをユーザーには毎回きちんと認識してもらい、もし SSL を経由せずに目的のサイトに接続された場合は偽物のサイトであることを理解してもらう。

また、仮に SSL で接続された場合でも攻撃者のドメイン名に対する証明書の場合もあり、当該サイトに対する正しいドメインの証明書であることを毎回きちんと確認する必要性がある。

自らが管理、運営する DNS サーバーに対して DNS Poisoning が行われなくするための対策としては、外部からの自ドメインに関する問い合わせについて回答する DNS サーバーと、ユーザーからの問い合わせを処理するサーバーをそれ

それぞれ異なる IP アドレスを持つよう分離し、外部から内部ユーザが利用する DNS サーバを攻撃対象とされないようにすることが考えられる。

また内部用の DNS サーバには外部から直接問い合わせができないようアクセス制限を行う。またファイアウォールや IDS(Intrusion Detection System)を用いて不正なパケットを制限・監視する方法などが考えられる。

結論として DNS というサービスのプロトコル上の制約から、今回紹介したような DNS Poisoning について完全な対策を行うのは容易ではない。

DNSSEC (DNS Security Extension) などセキュアなプロトコルとサービスに関する研究が進められているが、その種の新たな技術が開発され一般に広く普及する時期までは、DNS Poisoning の危険性は今後も長く存在し続けるものと考えられる。

(5) DNS サーバのセキュリティホールを利用する DNS Poisoning

前述の SANS Institute は、DNS Poisoning 攻撃を許す原因の一つとして、DNS サーバのセキュリティ・ホールを挙げる。例えば、セキュリティ企業 Symantec 社の Gateway Security や Enterprise Firewall などの DNS サーバ機能には、DNS Poisoning 攻撃を許すセキュリティ・ホールが 2004 年 6 月に見つかっている。

Symantec 社は、自社の製品 Gateway Security に悪影響を及ぼすと報告されていた DNS Poisoning の脆弱性を認め、その後対象となる脆弱性を封鎖したことを発表した。

これはある特定の条件下において、不正もしくは詐称された偽の DNS データが挿入される可能性があり、結果として正規のサイトの情報ではない不正なデータの返答を行う恐れがあるものであった。

米 Symantec 社のサイトより抜粋

Symantec Security Gateway 製品には、DNS サーバとして機能するよう設定することが可能な DNS プロキシ、DNSd が含まれています。特定の状況下では、DNSd は DNS キャッシュ・Poisoning の影響を受ける可能性があります。DNS キャッシュ・Poisoning は、不正あるいは偽の DNS レコードが DNS サーバのキャッシュ・テーブルに挿入された場合に発生します。偶然あるいは意図的に DNS キャッシュ・Poisoning が起こされた場合、サービスが意図に反して失われたり、悪意ある活動が実行されてしまう可能性があります。

同社によれば現時点ではこの問題点を突いた攻撃やその試みに関する情報や報告は無いということである。

しかし、同社の問題点の発覚は、今回の DNS Poisoning の大量発生に関係している可能性があるという指摘もある。このような脆弱性が発覚したことで新手の詐欺行為のアイデアが生まれ、現在ではその為に各種のテストを繰り返し替えているのではないかという指摘である。

一方、前述の SANS Institute によって組織化されたインシデントレスポンス専門家グループである Internet Storm Center(ISC)は、Symantec 社製品を使用していないサイトも被害にあっていると指摘している。ISCによると、この問題で 30~40 のネットワークに影響が出たという。ISCによれば、「今回の問題の原因は、まだ完全には特定できていない。報告が十分に集まっていないので、結論を急ぐことはできない」とされている。また、複数のメディアが米 Symantec にこの件に対するコメントを求めたが、回答は得られていないという。

DNS サーバーの脆弱性については、同サーバーの管理にも問題があると言われている。DNS サーバーを管理する多くの企業がセキュリティ・ソフトウェアが古いままであり、そうしたサーバーは攻撃に無防備である。現実には古いソフトウェアのコードの中にはそうしたセキュリティ・ホールがあり、そこへのファームウェア攻撃はある意味当然であるという見方が主流である。

(6) 技術的な対応

このような DNS Poisoning などによるファームウェアへの対抗策も幾つか出始めている。

セキュリティソフトウェア企業 Anonymizer 社が発表した Anonymizer2005 (Windows XP/2000 対応。\$29.99(年)) では、ブラウザに URL を入力したときに hosts ファイルを無視し、必ず DNS を参照するようにすることで hosts ファイルハッキングを防ぐ事が出来るようになっている。また、同社ではユーザーが一旦同社のネットワークを通るようにし、情報の流れを調べて、ユーザーのコンピュータと Web サイトの間で暗号化されたパスを作成するサービスも提供している。このサービスでは、ブラウザのリクエストがすべて捕捉され、個人情報を送る前に正当なサイトに接続していることが確認できる。これによってファームウェア攻撃を阻止する。

ブラウザを強化してファームウェアに対抗する方法もある。インターネット監視会社の英 Netcraft 社は、ユーザーが開いたサイトの所在地情報を表示するブラウザ・プラグインを提供している。これを使えば、米国の金融機関関連のローン会社のサイトのサーバーがアジアや東欧やアフリカ諸国にあることがわかれば、偽装の可能性があると判断できるだろう (Firefox 用の同社のツールバーが 5 月 24 日に発表されたので、実際に使用してみたところ、ユーザーに分かりやすい情報を表示する機能を持っていると評価できる)。なお、eBay や PayPal は、Netcraft 社

のプラグインに似た、オンラインでの取引を検証する独自のツールバーを開発している。

また、Windows の hosts ファイルを常に監視し、書き換えがあると警告したり、書き換え前の状態に簡単に戻したりすることができる常駐アプリケーション・ソフトウェアも公開されている。

さらに、Web サイトの素性をパブリック DNS システムで確認する方法もある。電子メールによる取引を検証する際の材料を提供するのが目的である。

こうした技術的な対策に加え、手続き面での対策も強化されつつある。たとえば、金融機関は多段階の認証を稼働し始めている。ユーザーが電話をかけ直しして送金を確認しなければ、取引が終了しないようにするものである。

3. ファーミングに対する関係者の見方

(1) APWG の見方

フィッシング対策団体 APWG は、毎月フィッシングに関するレポート(Phishing Activity Trends Report)を発表しているが、同レポートの 2005 年 2 月版において、ファーミングや IM (インスタント・メッセージング) 利用のフィッシングなどを例に挙げて、従来のフィッシングとは異なる手法が増加傾向にあるとして注意を呼びかけている。

しかしながら、このような被害に対する警告を発しながらも、APWG 自身はファーミングという呼称には不快感を抱いているようである。

前述のように「ファーミング (Pharming)」と言うのは「フィッシング (Phishing)」のもじりである。この表現は 2005 年に入ってから幾つかの IT 系メディアサイトで使用されるようになってきたが、米国でフィッシングとファーミングという用語が一般に広く浸透しているかという点、そうでもない。特にファーミングという用語は IT 関連のメディア以外では目にする事は少ない。

このようなことから、ファーミングという用語はメディアや、セキュリティを専門にしている関係業者がことさら状況をはやし立てるために作られた物であり、このような使用はいたずらに消費者を不安にさせ、ベンダーの営業トークに利用されるだけであるというのが APWG の考えであるように見受けられる。APWG の事務局長を務める Peter Cassidy 氏は、従来の手口と区別する上で「ステルス型の Phishing」と呼べば良いとしている。また、APWG によれば、政府関係者もこれらの意見に同調する形でこの問題は一括して考えるべきであり、対策や処置、そして呼称なども大局的な見方を持って行うべきという見解が広がりつつあるとしている。

(2) DNS Poisoning に対する専門家の見方

ウイルス対策ソフトメーカーの英 Sophos 社の上級セキュリティー・アナリストを務める Gregg Mastoras 氏は、「DNS Poisoning はすでに 10 年以上前から存在する」と言う。「われわれがこれほどまでに依存している DNS システムには、もともと設計に脆弱性がある。これまでさまざまな攻撃が成功を収められたのは、最初から存在するこの設計上の弱点をついたためだという意見も多い。」、「そういう意味で DNS Poisoning は目新しいものではないが、詐欺が急増している現状、そしてさらに深刻なことに、新しく出てきたファーミング詐欺が巧妙をきわめている事実は懸念すべきだ。」とも同氏は述べる。

前述の SANS Institute が組織化した Internet Storm Center(ISC)や英 Netcraft 社も、インターネット上の悪意ある行為について日々新しい情報を発表しているが、しかし DNS Poisoning が目新しいもので無いことも伝えている。

オープンソースの BIND(UNIX およびリナックス搭載機で最も広く使用されている DNS サーバーソフトウェア)やその他の DNS ソリューションに代わる商業ベースの製品を販売している Nominum 社の主任研究員であり、1983 年に The Internet Engineering Task Force(IETF)でインターネットのドメイン・ネーム・システムの開発に携わった Paul Mockapetris 氏も、DNS のもつ問題点は抜本的な解決が必要と考えている。また、同社 CEO の Chris Risley 氏は、Mockapetris 氏は DNS を刷新すべき時期が来たことを確信しているという。両氏とも、DNS と BIND を、現在の巨大な公共システムで使用できるとは全く考えていない。

一方で、DNS Poisoning 手法がそれほど広く用いられることはないとしている専門家もいる。フィンランドのセキュリティー・サービス会社 F-secure 社は、DNS Poisoning は深刻な問題にはならないだろうと考えている。これはハイレベルの DNS サーバーに侵入するには高いスキルが必要なため、それが大きな歯止めになるという判断である。

しかしながら一方で、インターネット世界に潜むコンピュータ犯罪者たちの多くは、高度の技術レベルを有し、大規模な犯罪を実行するだけの能力を備えているという見方もある。スペインのセキュリティー技術会社 Pandasoftware 社は、「大きな金額を詐取できる可能性があるため、DNS Poisoning 手法を用いたファーミング詐欺は、今年さらに大きな脅威となるだろう。」と述べている。また、英 SurfControl 社は、「正規のドメインを乗っ取るか、あるいは正規の DNS レコードを汚染することができれば、そこから大規模な金融詐欺の実行に使えるデータを盗み出すことが可能になる。問題は、コンピュータの前のユーザーが、正しい URL をブラウザに入力したのだから正しいサイトにつながっていると思い込んで

しまうことだ」、「今のところ、フィッシング詐欺が狙うのはインターネット・バンキングなどのユーザーがほとんどだ。だが、今後は企業内ユーザーも狙われる可能性がある。例えば、その企業の IT 部門になりすまして、従業員の ID やパスワードを盗むのである」としている。同社によると、フィッシングなどのオンライン詐欺による被害を恐れインターネットを使った取引を躊躇するユーザーが多く、業界の発展を妨げているという。

(3) ファーミングの今後に対する専門家の見方

DNS の書き換えはフィッシングよりかなり高度であるが、犯罪者側から見れば一回でも成功すればかなり莫大にデータが盗めてしまうことから労力を投資する魅力があるとされる。このようにその手口からして、ファーミングはフィッシングとはアプローチが異なる点に注目している見方もある。

企業がさまざまなオンライン詐欺から消費者を保護するための方法を探っているベンダー・コンソーシアム TECF (Trusted Electronic Communications Forum) の会長 Shawn Eldridge 氏は、「ファーミングはフィッシングよりも組織的だ」と言う。同氏は、「ファーミングでは仕掛けをした後ユーザーがそのリンク先を辿り偽装サイトを開くのを待つことになるが、フィッシングはもっと手っ取り早い方法だ」として、同氏は、フィッシングとファーミングは別のグループの犯行だろうと推測している。

また、専門家の中にはこの攻撃を単なるテストと見ている者もいる。これは対象範囲が限定されており、被害を受けたユーザーもほとんどいない様子だからである。また、DNS プロトコルの脆弱性を利用する巧妙な攻撃は他にもあり、やはり現在は本格的な攻撃の前の各種のテストが行なわれているとみられている。前述の Anonymizer 社は、「ファーミングは 6 か月前に登場した。当初は、有効性の検証という色彩が強かったが、使えることがわかると、ファーミング関連の活動が活発になった。」と述べている。

今後、ファーミング対策が進むにつれ、新たな攻撃法が探られている。「攻撃はインターネット接続のネットワーク層に移りつつあるようだ。ファーミングの成功率が落ちてくれば、ルーティングを攻撃し始めるだろう。どのような攻撃が編み出されるかはわからないが、新手が登場するだろう」と見る専門家もいる。

(4) 法的な対応

ファーミングだけを対象としたものではないが、上院では既にフィッシング詐欺対策法案が提出されている。

民主党、バーモント州選出の Patrick Leahy 上院議員は、上院提出法案としては初のハイテク関連法案の 1 つとして、フィッシング詐欺対策法案『Anti-Phishing Act of 2005』を提出した。Leahy 議員は、同法案を提出する際の演説で、「フィッシングやファーミングを行う犯罪者は、詐欺行為または ID セフトに関する法令に基づき法的に訴追し起訴できるが、多くの場合、被害が起きてからの立件となる。このことは、大半の詐欺師には証拠隠ぺいの時間がたっぷりとある事を意味するものである」と、述べている。

同法案は、フィッシングメールの頒布とアクセスサイトのユーザーの意志に反する無断且つ強制的な変更を犯罪として認定するものである。同法案は、通常的一般企業を詐称し、実際には犯罪目的で送信するメールの作成や準備を禁止している。またさらに、合法を装いながら、犯罪目的で、個人の秘匿情報を入手しようとする web サイトの作成や調達も禁止している。また、同法案はファーミング詐欺も対象としている。同法案は、フィッシング詐欺およびファーミング詐欺に対する罰則として、最高 25 万ドルの罰金と最長 5 年間の懲役刑を求めている。

また、私企業による法的措置もとられ始めている。ファーミングではなく、フィッシングを対象としたものであるが、Microsoft 社は、2005 年 3 月 31 日、MSN インターネットや Hotmail のサービスを利用するユーザをターゲットとしたフィッシング・サイトの運営者に対して 117 件の訴訟を起こした。サイトの運営者の身元については、プライバシーの観点からインターネット・サービス・プロバイダ (ISP) が明らかにしていないため、連邦商標法 (Lanham Act) の下、相手を身元不明のまま訴えた(このような相手不明のまま起こされる裁判を「John Doe 訴訟」という)。ISP である America Online (AOL) 社のスポークスパーソン Nicholas Graham 氏は、「プライバシー方針およびサービス約款で、召還令状、裁判所命令や捜査令状なしで契約者の情報を公開することを禁止している」とワシントンポスト紙に語っている。

犯人は正規の企業の商標を許可なく使用して詐欺を行うことから、Microsoft 社は商標権の侵害で起訴している。違反者は連邦商標法では違反 1 件につき、最高 100 万ドルの罰金が課せられる。

ウェブサイトやメールは、サービスを追跡することのできるインターネットアドレスを含んでいる。連邦裁判所が起訴状の内容を認めて捜査が可能になると、Microsoft はフィッシングメールを送付していたと見られる容疑者が使用していた ISP に必要な情報を請求でき、当該 web サイトの運営者を特定することができる。

この手法では過去にフィッシング詐欺の告発に用いて、起訴から 6 カ月、そして召還令状 2 件で犯人の断定に成功した事例がある。

前述の英 Netcraft 社によれば、ISP の中には記録の保管方法があまり効率的ではないところがあり、名前と住所を偽るユーザーが登録されることがよくあるという。しかし ISP が新サイトの登録に際して、登録者の名前や住所などの綿密な情報を収集したとしても、問題は解決しない。先の Microsoft の訴訟に見られるよう

に、そうした情報の開示は米国憲法修正第 1 条（言論の自由）に抵触する恐れがあるため、ISP は逆に個人情報を開示したことに対する訴訟を恐れ、個人や企業の情報を開示しようとしなない。

そしてこのような状況がフィッシングやファーミングによる詐欺を行った犯罪者の隠匿に手を貸していることになる。

4. ファーミング以外の最近のケース

(1) 悪魔の双子(Evil Twin)

2005 年 5 月 17 日付け Wall Street Journal 誌は、2005 年の新たな脅威としてファーミングと併せて「悪魔の双子 (Evil Twin)」について解説している。

現在、ホットスポット(WiFi ネットワーク)と呼ばれる無線ネットワークがコーヒーショップ、ホテル、カンファレンス会場などに普及してきたが、悪魔の双子とは、ユーザーが日頃ログインする正規のホットスポットと全く同じに見える偽のネットワークである。詐欺犯は、ホットスポットを利用するユーザーが入力するパスワードやクレジットカード番号を手に入れようとする。悪魔の双子は、AP（アクセスポイント）フィッシング攻撃とも呼ばれる。

セキュリティ企業 VeriSign 社の最高セキュリティ責任者（CSO）である Ken Silva 氏は、悪魔の双子は個人情報窃盗の新たなフロンティアであるとしている。これまで、ハッカー達は、ユーザーが公共の場所で正規のホットスポットを使っているときに傍受していたが、最近は通信の暗号化によりデータを守れるようになったため、新たな手段をとるようになったと見られている。

今回、詐欺犯は、ホテルや空港のラウンジなどにあるホットスポットを利用するのは一定の所得のあるビジネスマンである点に目をつけたようである。カンファレンス会場では実際に被害例が報告されている。

無線セキュリティ企業 AirDefense 社の報告によれば、2005 年 4 月にロンドンで IT カンファレンスが開催された際には、詐欺犯は来場者用の無料ホットスポットや BT Group 及び Deutsche Telekom の T-Mobile 部門が用意したネットワークを装ったホットスポットを設置した。この偽のネットワークに接続した無防備なユーザーは、ユーザーの個人情報を収集するウィルスなど 45 種類ものウィルスで感染させられたという。

また、2005 年 5 月にラスベガスで開催された別のカンファレンスでは、1 日に 7 つの悪魔の双子が現れたという。その中には、T-Mobile や Hilton Hotel のネットワークを装ったものがあったという。ログイン情報の入力ボックスなどあらゆる点で正規のホットスポットと同じに見えるページが表示されたので、詐欺犯は正規の Web ページファイルをコピーして、自分のコンピュータ上で利用したと見られている。

AirDefense 社の会長兼共同創業者である Jay Chaudhry 氏は、「この手の攻撃はビジネスとして行われており、インターネットを介して行われてる膨大なビジネスや取引を食い物にしようとしている。こうした攻撃は多数行われており、ビジネスユーザーは注意が必要だ。平均的なビジネスユーザーは餌食になっても全く気づかない。クラッカー(cracker)が単にデバイスにアクセスしようと挑戦していたのはもう過去の話だ。今では彼らの目的は金だ。クラッカーにとって一番楽に設けられる場所は、空港のラウンジやホテル、カンファレンス会場などにあるビジネスユーザーが使うホットスポットだ」と述べている。

悪魔の双子によって、詐欺犯が何らかの機密情報の盗み出しに成功したかどうかはまだ明らかではないが、AirDefense 社は悪魔の双子の犠牲にならないようユーザーがいくつかの安全対策を取るよう勧めている。例えば、「ホットスポットで自分のアカウントにアクセスする場合には、ブラウザに SSL(Secure Sockets Layer)の鍵のマークが表示されることを確認する」、「ホテルや空港のラウンジなど誰が接続しているか分からないようなホットスポットは避ける」、「ホットスポットではパスワードなどが必要となるようなオンラインショッピングのような利用は避け、サイトの閲覧だけに利用する」などである。他のセキュリティ専門家は、「偶然悪魔の双子につながらないように、PC の WiFi 機能を使用しない場合にはオフにする」、「ワイヤレス環境でクレジットカード番号を送信しなくても済むように、固定回線インターネットにつながった PC から、T-Mobile ネットワーク（米国では Starbucks コーヒーショップには T-Mobile がホットスポットサービスを提供）のような WiFi サービスに登録しておく（T-Mobile は WiFi ネットワークのデジタル証明書を自動的にチェックし、正規のものかどうか確認する無料接続ソフトを PC 向けに提供）」というアドバイスをしている。

米国では、フィラデルフィアなど地方政府自身が街全体を「ホットゾーン」化する計画を立てるなど、ワイヤレス環境の拡大が急速に進みつつある。悪魔の双子は今後大きな脅威になる可能性をはらんでいる。

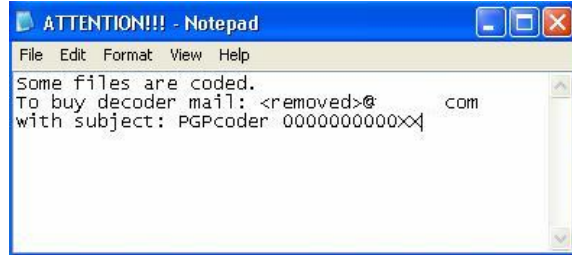
(2) ランサムウェア(Ransomware)

「詐欺」とは別の犯罪であるが、悪意をもった人間がユーザーが所有する PC 上のファイルを勝手に暗号化し、そのファイルの復号に必要な鍵の代償として「身代金(ransom)」を要求する新たなハッキングが登場した。

セキュリティ会社 Websense 社が 2005 年 5 月 23 日に行った報告によれば、Internet Explorer(IE)の既知の欠陥を利用したもので、あるウェブサイトアクセスしたところ、勝手に PC 上のファイルを暗号化するプログラムをダウンロードし、PC 上の 15 種類以上のファイルが暗号化されたという。その際、復号化のための鍵を購入するために指定のアドレスまで電子メールを送るよう指示したメモが残されていた。「Trojan.Pgpcoder」と呼ばれるこの悪質なプログラムは、ユーザーの

PC のハードディスク内から、画像ファイルや Microsoft Office ファイルなど一般的な 15 種類のフォーマットのファイルを探すと、それを暗号化し、元のファイルを消去するという。

暗号化されたファイルの鍵を買うよう指示したメール



ユーザーが指定されたアドレスにメールを送ると、悪意をもったハッカーは、「電子メールにてプログラムを送る」として「身代金」200 ドルをネット銀行の口座に振り込むよう要求してきたと報告している。

「身代金」を要求してきたメール



セキュリティ会社 Semantec 社の Security Response のシニアマネージャーである Oliver Friedrichs 氏は、「これは明らかに懸念すべき問題であり、この種の攻撃でユーザーの情報を人質にするために暗号化技術が利用されたのは今回が初めてだ。」と述べている。

セキュリティ各社はこの事件を受けて、「ランサムウェア(Ransomware)」と名づけられたハッキング行為に対処するため、企業及び消費者向けのセキュリティ・ソフトをアップデートしている。

セキュリティサービス企業 Lurhq Corp 社のリサーチャーである Joe Stewart 氏は、今回は身代金を払うことなく感染ファイルを復号することができたが、手口が高度になれば困難になると危惧している。

(3) IM (インスタント・メッセージング) 利用のフィッシング

IM (インスタント・メッセージング) 関連ソフトウェア企業 IMlogic 社は、2005 年 5 月 24 日に Yahoo! Messenger のユーザーに対してフィッシング詐欺に関する注

意を呼びかけている（America Online のユーザーに対しても同様の注意が出されている）。同社最高技術責任者(CTO)の Jon Sakoda 氏によれば、いずれの場合も新作映画「スター・ウォーズ エピソード 3：シスの復讐」に関する話題であるように偽装し、IM の本文に映画と関係あるかのような「StarGames」という用語を用いたというメッセージを流し、ハイパーリンクとなっている StarGames の部分をクリックすると本物の Yahoo のサイトに似せて作られたフィッシングサイト(http://yahoopremium.bravehost.com/STAR_GAMES、現在は接続できない)に飛ぶようになっているという。このメッセージは、感染したマシンから Yahoo! Messenger の友達リストに載っているユーザーに送付されたと言われている。このサイトに飛ばされたユーザーは、Yahoo アカウント情報の入力を促されるが、ここで入力された情報は Hotmail のあるアドレス宛に送信されるようになっているという。IM フィッシングは、信頼できる送信元（友人）から送信されたかのように見せかけたメッセージを元にするという巧妙な手口を使っている。Imlogic 社の Sakoda は、「IM もメールの添付ファイルやリンクと全く同じように、たとえそれが知人からのメッセージであってもリンクをクリックする際には注意が必要である」と述べている。

このような IM 利用のフィッシングは、フィッシング対策団体 APWG の 2005 年 2 月の報告においても、「これまでのフィッシング詐欺は、電子メールやウェブサイトを使うものだったが、最近は、IM を使って情報を盗み出す手口が頻繁に使われるようになっている」と指摘されている。

また、2005 年 4 月 12 日に、セキュリティ会社 Websense 社は、IM をユーザーに送り悪質なブログにおびき寄せ、ユーザーがブログにアクセスするとパスワードなどの個人情報を盗み出すトロイの木馬などの不正プログラムに PC が感染してしまうという事例が多数あることを報告している。米国ではフィッシングなどに利用されているブログは既に 200 件以上あるとも報道されている。同社でセキュリティ技術研究を担当するシニアディレクターの Dan Hubbard 氏は、「これらの攻撃が成功している理由は、リンクをクリックするように個人ユーザーに働きかける巧みなソーシャルエンジニアリングにある。」と述べている。

(4) パーソナライズド・フィッシング

オンラインセキュリティ企業 Cyota 社は、2005 年 5 月 16 日に、予め盗んだ個人情報を利用して、個々のユーザー毎に「個人化（パーソナライズ）」したメールを送り、より重要な個人情報を盗もうとするパーソナライズド・フィッシングについて報告している。Cyota 社によれば、詐欺犯らは盗まれた個人情報を購入し、その個人情報をもとにユーザー宛に、氏名、メールアドレス、口座番号などの正確な情報が書かれたメールを送る。ユーザーは大手金融サービス企業の顧客だと

いう。メールを受け取ったユーザーは、メールの文面に自分の正確な個人情報が記載されているために、金融機関から本当に送られてきたメールと勘違いしてしまう。メールには、個人識別番号（PIN、暗証番号）やクレジットカードの CVD コード（クレジットカードの裏面にある 3 桁の識別番号）といったより重要度の高い個人情報を確認するために送られてきたかのような内容が記載されている。

Cyota 社の共同創業者である Amid Orad 氏は、「本格的な研究開発リソースを備える、組織化されたグループの仕業であることは明らかである。これまでの成功率は驚異的な高さである。」と述べている。

フィッシング対策団体 APWG 会長の Dave Jevans 氏は、「攻撃者は攻撃対象の狙いを絞るようになってきた。個人に送りつけられるメールもパーソナライズされたものになっている」と述べている。

また、2005 年 5 月、セキュリティ企業 Blue Security 社は、パーソナライズド・フィッシングや効果的なスパムメールを送るために、スパム業者やフィッシング業者がターゲットとなるメールアドレスを絞り込む手口をレポートにまとめている。同レポートによれば、この手口には「登録攻撃(Registration Attacks)」と「パスワードリマインダー攻撃 (Password Reminder Attacks)」の 2 種類があり、大手ウェブサイトのうち 8 割には脆弱性があるという。

「登録攻撃」とは、メールアドレスをアカウントとして利用しているウェブサイトの場合、例えば、スパム業者やフィッシング業者が john@bluesecurity.com というメールアドレスを試し、以下のようなエラーメッセージが出た場合には、そのメールアドレスが実在のものであるという情報を得るものである。

「パスワードリマインダー攻撃」とは、スパム業者やフィッシング業者がパスワードを忘れたユーザーを装って、ウェブサイト上のパスワードリマインダー（パスワードをお忘れですか？）に何種類かのメールアドレスを送って見た場合、エラーメッセージが返ってくればそのアドレスは存在しないことが分かり、「ペットの名前」などの更なる質問が返ってくればそのアドレスが実在のものであるという情報を得るものである。

パスワードリマインダー

アドレスが実在しない場合

アドレスが実在する場合

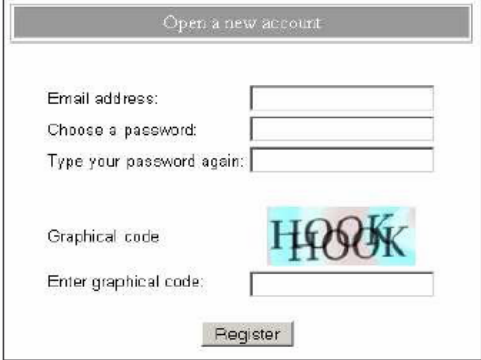
また、同レポートでは、大手電子メール提供者や ISP（インターネット・サービス・プロバイダ）の 9 割がユーザーのメールアドレスをスパム業者やフィッシング業者に漏らしているという。それはフィッシング業者らが、メールアドレスの登録手続きの際にその利用可能性を繰り返して確認できるからであるという。

メールアドレスの利用可能性確認画面

さらに、同レポートによれば、スパム業者やフィッシング業者が、メールアドレスを突き止めた後、このユーザーのプロフィールを絞り込むことは容易だとも述べている。例えば、いくつかの住居地域のケータリング用サイト、スポーツファンサイト、政治団体サイト、出会いサイト、健康・医療サイトに bowman@bluesecurity.com というユーザーの登録状況を単純な自動プログラムで調べれば、「ロサンゼルス在住、野球好き、中絶賛成派、55 歳以上、心臓病を患っている」という情報が得られると解説している。

このようなスパム業者やフィッシング業者による悪意あるプロファイリングから逃れる方法についても同レポートはいくつか解説している。

- メールアドレスをユーザーIDとして使用しない（Blue Security 社の調査によれば金融機関は全てこの措置をとっている）。
- 自動プログラムは認識できないグラフィカルな文字をユーザーに判読させ、人間がアクセスしていることを確認する（以下画面）。



The image shows a registration form titled "Open a new account". It contains the following fields and elements:

- Email address: [input field]
- Choose a password: [input field]
- Type your password again: [input field]
- Graphical code: [visual code "H00K"]
- Enter graphical code: [input field]
- Register [button]

- 非登録ユーザーからのパスワードリマインダーにはエラーメッセージを返さない（オークションサイトに多い）。
- 登録手続きをする前に有効なクレジットカード番号を要求する（いくつかのポルノサイトが採用）。

大手オークション企業 eBay 社のサイトでは、フィッシング問題が表面化する以前からメールアドレスをユーザーIDとして利用することを禁止しており、登録やパスワードの確認には独自の保護策を取り入れているという。同社の上級顧問 Scott Shipman 氏は、「任意のメールアドレスやユーザーIDが、実際に登録されている有効なものかどうかといった単純な情報でも、権限なしには決して参照できないように設計されている」と述べている。

(5) キーロガー(Key Logger : 入力記録ソフトウェア)利用によるフィッシング

フィッシング対策団体 APWG の 2005 年 3 月の報告によれば、セキュリティソフトウェア企業 Websense 社の Security Labs.は、キーロガーを利用するフィッシングが急増していると報告している。これは、ユーザーがあるウェブサイトアクセスした場合などに、キーロガーと呼ばれる悪質なプログラムをユーザーの PC に忍ばせ、ユーザーがオンラインバンクのログイン名やパスワードなどを入力 (Keystroke)するのを記録(Log)し、その情報を詐欺犯に送信するものである。同社の報告によればポルトガル語圏のユーザーを対象にしたものが多い。2005 年 2 月

から 3 月までの間に、週に 8~10 の新たなキーロガーとそれらを植え付ける 100 以上のウェブサイトが発見されたという。

ブラジルの有名なポータルを装ったもの（クリックするとキーロガーがインストールされる）



メールが感染したと知らせワクチンのダウンロードを促す偽メール（クリックするとキーロガーがインストールされる）



(6) 偽ショッピングサイト

2004 年 12 月 1 日、セキュリティ企業 CyberGuard 社は、クリスマス商戦を前にして偽のオンラインショッピングサイトに関する警告を発表した。これはフィッシングと異なり、偽のメールでユーザーを誘導することなく、もっともらしく作ったショッピングサイトにユーザーがアクセスしてくるのを待つ手法である。同社のシニアバイスプレジデントである Paul Henry 氏によれば、ユーザーが Google などで商品検索を行った結果、検索結果に悪質なサイトが生じられ、サイトには

「製品の画像をダウンロードするにはここをクリック」と書かれたリンクが表示されているという。ユーザーがクリックすると代わりにトロイの木馬が PC に仕掛けられ、その後、ユーザーの個人情報を盗み出すという。

セキュリティ企業 Websense の Security Labs が発表した「セキュリティ・トレンド・レポート 2004（下半期）」においても、2004 年下半期にこのような偽ウェブサイトが急増したと報告されている。同レポートによれば、2005 年も増加するだろうとしており、家庭用医薬品、オンラインゲーム、宝くじ、住宅ローンなどのサイトを装ったものが新分野として現れるとしている。

(7) 特殊文字利用のフィッシング

現在、インターネットのドメインには、英数字などの ASCII 文字以外の特殊文字（日本語では、ひらがな、カタカナ、漢字など）を URL などに使えるようにするための国際化ドメイン名（IDN：Internationalized Domain Name）が使用できるようになっている。さらに 2005 年 1 月には、ファイルのパスやメールアドレスなどにも非 ASCII 文字を利用できる国際化 URI (IRI：Internationalized Resource Identifier) も制定されている。

これにより ASCII 文字によく似た文字を他の言語で表記させることにより、非常に判別が難しい偽装を行うことが出来るようになってきている。2005 年 2 月複数のセキュリティ・ベンダー等が IDN 使用によりこれまでとは違う手法での URL の偽装が可能になることを示し、IDN 対応ブラウザ側のセキュリティ問題だと指摘した。しかし、現時点では主要なブラウザのほとんど画この欠陥についての対応は施されていない。

またブラウザの配布元や開発者などは、このような紛らわしく事実上詐欺行為に利用されることが容易に推測される URL の登録を許したレジストレーション企業に問題があると反論している。

急成長しているブラウザ Firefox の作成元である Mozilla Foundation ではこの問題に対しての処置を既に行っているが、彼らの多くは自らの問題とは考えていないと見られ、もし他のブラウザ配布元が同意すればすぐに従来の設定に戻すべく、この対策を「Mozilla Foundation's short-term response」としている。

一方この Mozilla Foundation の対応に対し、TLD レジストリで構成される協会 The Council of European National TLD Registries (CENTR) は、2005 年 2 月にこの件についての声明を出しこれを批判した。CENTR は、「ブラウザが IDN をデフォルトで無効にしても多くのユーザーは自分で有効とするので、インターネットの国際化を妨げる。」「この問題は以前から知られていることであり、今急に慌てる必要はない。」などとしている。

なお、フィッシング対策団体 APWG は、2005 年 2 月に発表したフィッシングに関するレポートで、IDN 問題についても詐欺行為に悪用されうるとして注意を呼

びかけている。ただし、APWGはこの問題を悪用した事例についてはそれほど多くは確認していないという。

(参考資料)

<http://www.antiphishing.org>
<http://www.the-dma.org/cgi/disppressrelease?article=643>
<http://isc.sans.org/diary.php?date=2005-03-04>
<http://securityresponse.symantec.com/avcenter/security/Content/2004.06.21.html>
<http://www.isc.sans.org>
<http://www.anonymizer.com/anonymizer2005/1.5/>
<http://www.centri.org/docs/2005/02/homographs.html>
<http://www.sophos.com/>
<http://www.wired.com/news/infostructure/0,1377,66853,00.html>
<http://www.computerworld.com/printthis/2003/0,4814,82528,00.html>
<http://news.netcraft.com/>
<http://www.f-secure.com/>
<http://www.pandasoftware.com/home/default.asp>
<http://www.surfcontrol.com/>
<http://www.washingtonpost.com/wp-dyn/articles/A16257-2005Mar31.html>
http://online.wsj.com/public/article/0,、SB111628737022135214-vzmiOwINUZp8jh0 CDu6q0 KMiY 20060517, 00.html?mod=tff_main_tff_top
<http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=194>
http://imlogic.com/im_threat_center/threatdetail.asp?iThreatID=597&mr=top3&hr=top3
<http://www.cyota.com/news.asp?id=179>
http://antiphishing.org/APWG_Phishing_Activity_Report_Feb05.pdf
<http://www.websensesecuritylabs.com/resource/PDF/APWGPhishingActivityReportMarch2005.pdf>
<http://ww2.websense.com/global/en/PressRoom/PressReleases/PressReleaseDetail/?Release=050412889>
http://www.cyberguard.com/news_room/advisories/holiday_phishing_scam.html?lang=de_EN
<http://download.bluesecurity.com/research/HostileProfiling.pdf>

このレポートに対するご質問、ご意見、ご要望がありましたら、
hiroyoshi_watanabe@jetro.go.jpまでお願いします。