

SecurITy  
made  
in  
Germany

# G Data

## White Paper 2011

— ネット攻撃の現状 —

G Dataセキュリティラボ所長

ラルフ・ベンツミュラー

(岸本真輔 + 瀧本往人 訳)



Go safe. Go safer. G Data.

# 目次

<b>1.イントロダクション</b>	3
<b>2.どのように悪意あるサイトに遭遇するか</b>	3
2.1 メール	4
2.2 インタラクティブなウェブのリスク	5
2.3 偽の検索結果	6
2.4 ハックされたサイト	7
2.5 マルバタイジング—悪意ある広告バナー	9
<b>3.ウェブサイト訪問者への攻撃</b>	10
3.1 ドライブバイ感染	10
3.2 もっともよく知られている詐欺	11
<b>4.結論</b>	11

# 1.概要

近年、インターネットのない暮らし、というものは、大部分の人にとって想像しがたいものとなりました。今やインターネットは、情報、エンターテインメント、およびコミュニケーションと、多岐にわたって私たちの暮らしを支えています。ショッピングやゲームを楽しみ、銀行口座のチェックをするだけでなく、大きな組織や政府などに直接働きかけことさえ可能となりました。しかし、忘れてはならないのは、ネット犯罪者もまた、この同じインターネットを最大限に利用しているということです。

ネット犯罪者たちは、誰もが使っているようなインターネットのサービスを悪用して、一般ユーザーのコンピュータを外部から勝手に操り、個人情報盗み出し、広告やマルウェアを拡散させているのです。

25年前に最初のウイルスが登場した頃は、フロッピー感染が主流でした。その後、マルウェアの大部分は、メールの添付ファイルを使って、ばらまかれるようになりました。そして今、彼らは明らかに、「ネット」に狙いを定めています。

犯罪者たちの目的は、はっきりしており、できるだけ多くのお金を得ること、に尽きます。すでにはっきりと地下経済が形成されており、ネット犯罪に必要なものを売買する裏市場は、活況を呈しています。

以下では、このような犯罪への対策として、ネット犯罪者たちがどこに狙いを定めているのかについて素描します。

## 2.どのようにして、悪意あるサイトに遭遇するか

ネット犯罪者は、ウェブサーバーをコントロールし、そして（または）、マルウェアをばらまくためにウェブに悪質なコードを仕掛けようとします。

攻撃者がこういったことを行う場合の最も簡単な方法は、自分自身のサイトを操作することです。

とはいえ、実際に支持されているやり方は、可能な限り規模の大きなサイトのサーバをハッキングして使用することです。そうすることによって攻撃者は、多くの人々にマルウェアをばらまくのが可能になるからです。

しかしまた、無名のサイトであっても訪問者を誘い出すという手段も、しばしば用いられています。

## 2.1 メール

メールは今なお、マルウェアをばらまくための重要な手段となっています。かつてと比べるとマルウェアを含む添付ファイルは、かなり減りましたが、まだ完全になくなったわけではありません。最近では、PDFの添付ファイルか、またはHTMLを用いる手口が、しばしば見かけられます。PDFもHTMLも、これらのファイル形式のメールは、今でも完全に安全とは言えません。

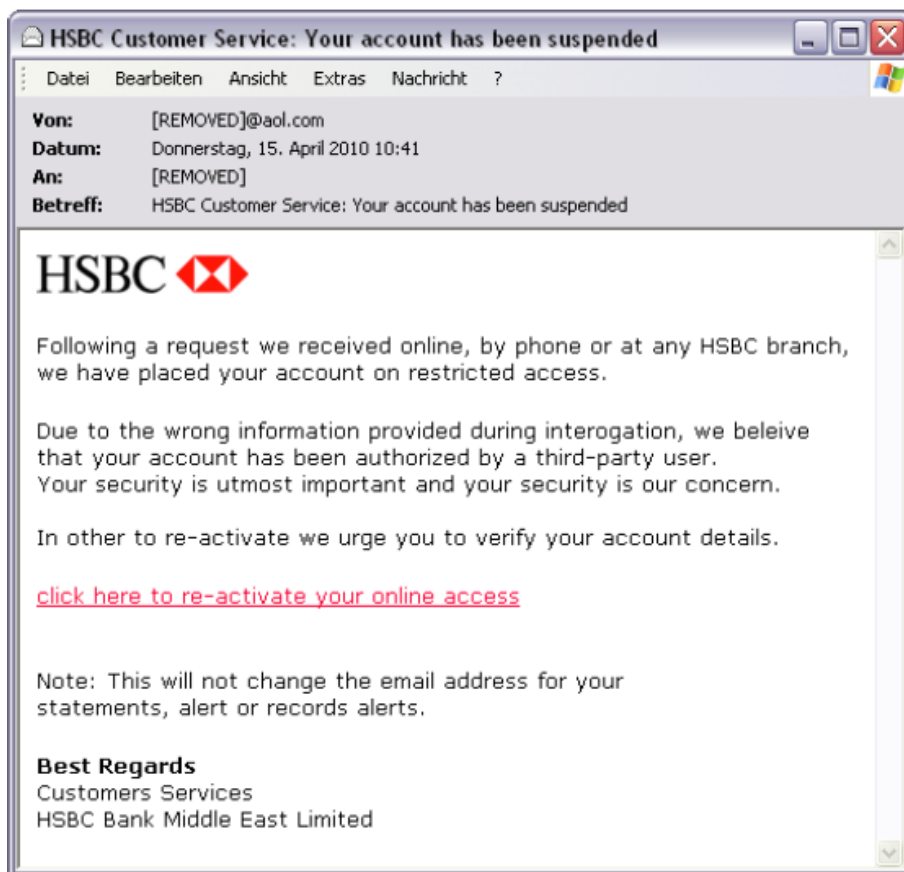
コンピュータがマルウェア感染するのは、悪質なサイトの罠にはまるのと、似た部分がないわけではありません。しかし、メールはさらに多様な危険性があります。毎日、悪質サイトへのリンクを貼った膨大な量のメールを送りつけることができるからです。内容も、センセーショナルなニュースやエラーメッセージ、または何らかの通知、請求、さらには法的な告発や、偽物の当選通知など、多種多様です。いずれもリンクが貼ってあり、悪質サイトに飛ばされるという仕組みが主に使われています。

フィッシング詐欺も、同様の方法を用います。ただし、サイトのリンクを使ってマルウェアをばらまく代わりに、ユーザーの個人情報を狙います。悪質メールもフィッシング詐欺サイトも、大部分はオリジナルと見分けがつきにくくなっています。しかも数年前には、フィッシング詐欺は、オンラインバンキングの顧客にターゲットを絞っていましたが、現在、攻撃範囲は、かなり広がっています。

そのなかで特に照準が定められているのは、以下のアクセスデータです。

- ・ SNS（ソーシャルネットワークサービス）（Facebook、MySpace、Twitterなど）
- ・ 配達サービスや支払いサービス（PayPalやDHLなど）
- ・ ネット銀行（シティバンクなど）
- ・ ポータルサイト（Yahoo!、GoogleまたはMSNなど）
- ・ オンラインショップやオークションサイト（eBayなど）
- ・ オンラインゲーム（World of Warcraft、Habboなど）

ネット犯罪者の標的は、ユーザー名とパスワードが主であり、この二つのデータがあるところであれば、どこでも積極的に罠を仕掛ける傾向があります。奪ったデータは、スパムメールの送信、盗品の支払いや配達、裏市場で販売されたものの支払いや配達など、さまざまな局面で使用されます。



スクリーンショット1 フィッシング詐欺メールの例。本物の銀行からの連絡であるようにみえる。

## 2.2 「ソーシャル」サイトのリスク

インターネットは多くの人々にとって、「コミュニケーション」や「出会い」の場となっています。しかし、人々がインターネットのどこかに集まると、そこにはリスクも生まれています。インスタントメッセージ、チャットルーム、ソーシャルネットワーク、フォーラム、ブログ、およびwikisなど、危険が全くないところは、一つもありません。

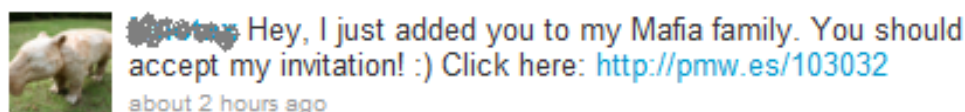
チャットルームとインスタントメッセージングサービスでよく使われているのは、悪意あるサイトへのリンクです。最近のインスタントメッセンジャーやSNSサイトで発生しているワームの罠は、紹介コメントの後にリンク先を示すだけのものです。ある場合は、ユーザーとチャットルームの間でのコミュニケーションに規制をかけることさえあります。また、ユーザーのチャットルームの一つもしくはすべてへの悪意あるリンクを付与することもあります。しかし、コンピュータが感染していなくとも、危険性があります。ログイン情報はセッションが持続しているあいだ、セッションクッキーに保存されます。また、やりようによっては、他のウェブサイトからもこれらのクッキーにアクセスできます。このような事態になったならば、攻撃者は、犠牲者の名を騙って、メッセージを送ったり、設定を変えたり、データを読んだりできるようになります。事実上、ユーザーができることなら何でも、実行可能です。ユーザーがサインアウトするとき、通常、セッションクッキーは削除されます。そうやってはじめて悪用が、できなくなります。

また、ソーシャルネットワークは、マルウェアをまき散らすことを目的として、かなり頻繁に利用されています。友人からのポスティングは通常より信頼度合いが高いため、そのなかにあるリンクは、見知らぬ他

人からメールよりも、クリック率が高まります。



スクリーンショット2 2011年1月に登場したツイッター・ワーム。「セキュリティシールド」という偽ウイルス対策ソフトを広めるためのもの。「goo.gl」サービスが用いられている。



スクリーンショット3 2009年から登場し、最近もお頻発するツイッター・ワーム。クリックすると、自分のフォロワーにツイートされてしまう。

ネット犯罪者たちは、ソーシャルネットワークのこの「ソーシャル」性に、かなり目をつけはじめています。クープフェイス (Koobface) のワームは、ソーシャルネットワークを介したまきちらしに特化するようになっています。このワームは、Facebook、MySpace、Hi5、Friendster、Twitter Bebo、Twitterなどのコンタクトリストにある「友だち」全員に対して、偽物の動画へのリンクがあるメッセージを送ります。そして、動画のあるページには、Flashプレーヤーかコーデックをダウンロードするよう要求してきます。ダウンロードしてしまえば誰であっても、コンピュータはクープフェイスのボットネットの管理下に入っています。

誰でもフォーラム、ブログ、およびwikisに登録することができる、ということは、つまり、犯罪者も同様に、そこに侵入している、ということです。裏市場では、ほぼ自動的にフォーラムかブログにログインできるツールが取り引きされています。メッセージは、広告の場合もあれば、悪意のあるサイトへのリンクの場合もあります。人気の高いウィキペディアでさえ、ある場合には、マルウェアであると判明した、ワームを取り除くツールへのリンクを含んだブラスター・ワームについての文献があり、この点については妥協し、「ソーシャル」サービスを使うときに、警告が発せられるようになっています。

## 2.3 偽の検索結果

ネット犯罪者には、悪意あるサイトに追いこむための別の方法もあります。サイトを特定の検索ワードに最適化しておけば、検索エンジンのクエリーによって検索結果において上位に表示されるようになります。ネット犯罪者もまた、これを利用して、特定の検索キーワードのときに悪意あるサイトを上位に表示させようとします。選択されたキーワードは、特定のターゲット・グループを狙い、その分野における特殊用語を含みこませます。特によく用いられるのは、オンラインゲームとアダルト・コンテンツです。

しかしまた、彼らは時事ネタに飛びつくこともあります。これは、Google、Twitter Facebookなどに関する検索キーワードのヒットリストを評価することによって生じます。したがって、例えば、Google Trendsに関する検索キーワードのときに、悪意あるサイトを上位表示できます。そのページは、また、検索エンジンプロバイダーのURLリストに入れ、人気のあるフォーラムでのポスティングでさらに人気のポジション

を挙げることができます。当然Google社は、検索結果からそのような悪意あるサイトをフィルターにかけようとしています。しかし、これはいつもうまくいっているわけではありません。2010年10月に、Googleのウイルス対策チームの一員であるファブリシュ・ジャベール (Fabrice Jaubert) は、Googleにおけるすべての検索クエリーのうち、1.5%が悪意あるウェブサイトにつながったとSecTor (セキュリティ国際会議) のカンファレンスで述べていました。初心者ユーザーに大打撃を与えるサイトに誘導されてしまう問題は、無視されるべきではないでしょう。

## 2.4 ハックされたサイト

マルウェアの拡散に関する前節の説明は、悪意あるサイトのオペレータ自身で見知らぬウェブサーバーを操作している、と仮定します。しかし、これは絶対に必要なものではありません。また、攻撃者にはマルウェアは、有名サイトのウェブサーバーをハイジャックするのに利用可能です。これには多くの方法があります。Webアプリケーションセキュリティに関する世界最大のNPOであるOWASP (Open Web Application Security Project) は、ウェブサーバーに対する攻撃の成功の原因について、定期的な統計データを公表しています。以下では、そのトップ10に関するOWASPからの抜粋で、6つの最も一般的な攻撃についてまとめました。

### ■OWASP Top10のランク1～10とセキュリティリスク

#### 1 インジェクション

インジェクションの脆弱性は、オペレーティングシステム (OS)、データベース (SQL)、ログインデータ (LDAP) に関係があります。それらが生じるのは、ユーザーデータのフィルターが不十分で、検索クエリーで生成されたコードが実行されてしまうときです。これは、攻撃者が認可なしにデータにアクセスできるようにします。さらには、サーバで攻撃を行うことさえ可能にします。

#### 2 XSS(クロスサイト・スクリプティング)

ブラウザ上に文字列を出力する際に、適切に処理されない場合、スクリプトが動作してしまいます。このスクリプトを悪用して、ユーザーに罠を仕掛けることが可能です。たとえば、攻撃者は、ウェブサイト(例えば、偽のメッセージ)の中身を改ざんしたり、ユーザーのセッションデータを盗み出したり、悪意あるサイトを表示させたりします。

#### 3 不完全な認証と不完全なセッション管理

認証とセッション管理に関連した機能が不完全な場合、他のユーザーの名のもとに動作を実行するために攻撃者がパスワードを盗み出すか、または暗号化かセッションデータを利用するのを可能にします。

#### 4 オブジェクトへの直接参照の欠陥

ファイルやデータベースのキーディレクトリなど、本来は見えないはずのオブジェクトへのアクセス権がウェブ・アプリケーションで十分チェックされない場合があります。その場合、攻撃者はオブジェクトを操作できてしまいます。

## 5 クロスサイト要求の偽造 (CSRF)

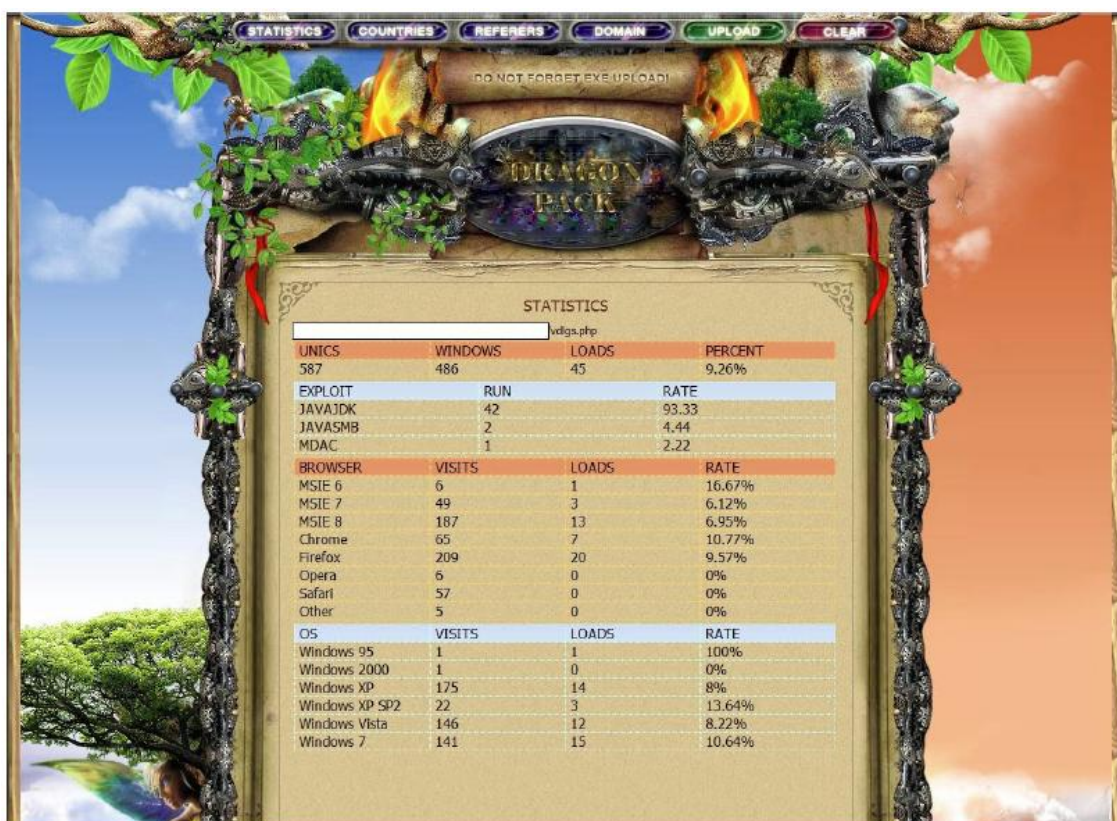
CSRF攻撃においては、ログインしたユーザーの名を騙って攻撃者がHTTP要求を行うものです。脆弱性のあるウェブ・アプリケーションは、正当な要求と虚偽の要求とを区別できません。すると、攻撃者は、例えば、メッセージを送ったり、ルータを構成したり、物を買ったり金融取引を行うなど、認証ユーザーができることをすべてできるようになります。

## 6 誤ったセキュリティ設定

セキュリティを高めるには、しばしば、設定次第のところがあります。特にウェブサーバー、データベース、ウェブ・アプリケーション、およびプラットフォームはデフォルトの設定のままではセキュリティが不十分であり、そのまま使用していると、大規模な攻撃の餌食となってしまいます。

コンテンツ管理システム、ウェブショップ、wikisまたは掲示板など、最近ウェブサーバーの大部分で使用されており、よく知られているウェブ・アプリケーションへの攻撃は、かなり一般化しています。これらのアプリケーションの1つがセキュリティホールを含んでいるなら、手広く利用されてしまいます。検索エンジンに標的にされているクエリーを使用することで、そのようなソフトウェアを動かしているドメインを見つけることができます。攻撃者は検索結果のリストとツールを使って標的となったサーバーへの攻撃にのりだします。攻撃がうまくいくなら、どんなマルウェアもそこにインストールできます。時折、これは技術的に非常に複雑ですが、初心者であってもこの複雑さをマスターすることができます。

ウェブ攻撃キットが提供するのは完全パッケージで、これさえあればサーバーをハッキングしたあとにマルウェアを実行させる一連の流れに必要なものがすべて揃います。さまざまな攻撃を実行し、あれこれとセキュリティホールを利用するのも、このような攻撃ツールが自動的に行います、にもかかわらずコンピュータ知識はただ基本的な事柄さえわかれば十分なのです。Fragus、Elenore、Neosploitといったウェブ攻撃キットが提供するの、簡単な使い方や感染コンピュータの比率が分かる統計データを表示させるツールなど、至れり尽くせりであり、それで価格は米ドルで500ドルか、それよりやや上くらいなのです。セキュリティホールはしばしばすぐに古くなっていきますが、攻撃ツールの大多数は、このほんのわずかな可能性のために新たなセキュリティホール情報を定期的に追加します。攻撃者は、成功の際のハックされたコンピュータにどの攻撃を試みるか、どのファイルをロードしたらよいかを定義することができます。こういったツールは、技術的に不慣れな人間であっても容易に裏市場にかかわり、ハイジャックしたコンピュータをロボットのように操ることを可能にします。



スクリーンショット3 ウェブ攻撃キット「ドラゴンパック」のAdmin-GUIは、統計を示しています。

## 2.5 マルバタイジング——悪意あるバナー広告

オンラインで活動する犯罪者は、できるだけ多くの犠牲者に届くように、新聞、ニュース雑誌またはインターネットポータルなどのような、もっとも人気があるウェブサーバーのコントロールを目論みます。しかし当然ながら、これらが使用しているのは、安全性のきわめて高いサーバです。といっても、落とし穴があります。多くの人気があるウェブサイトは、広告収入によって維持されています。広告のコンテンツは、一般に、特別なウェブサーバー(アドサーバーと呼ばれる)に保存されて、そこからポータルのオペレータとニュースサイトのページに統合されます。通常、そのようなポータルのオペレーターは、広告サービスプロバイダーの規制措置が十分であると仮定します。しかしながら、広告会社のウェブサーバーをハックしているなら、そこでウェブバナーを操作できます。これはイギリスのニュースサイトである「レジスター」(The Register)のようなサイトへ悪意あるバナー広告を提供するサーバのあるFalk eSolutionsと共に2004年11月20日に起こりました。

しかし攻撃者は、アドサーバーがしっかりと保護されているときでさえも、広告主を出し抜き、簡単に悪意あるバナーを滑り込ませることができます。残念ながら、毎日洪水のように現れる新しいアドバナーからマルウェアを検出するのは、簡単ではありません。アドバナーのJavaScriptまたはFlashのコンポーネントは、激しくコードを混乱させます。それゆえ、アクティブなコンテンツに悪意ある機能が含まれているかどうかを決定するためには、多大な努力を要します。その上、ある状況(例えば、日付、インプレッションなどの数)においてのみアクティブになるような方法で、それらをプログラムすることも可能です。これは、よ

り大きなウェブポータルが影響を受けるのを可能にします。昨年こういった被害は、MySpace、ニューヨーク・タイムズ、MSNノルウェー、zeit.de、およびhandelsblatt.deなどを含んでいました。訪問者にとって、インターネットポータルにおける広告は、退屈であるだけでなく、危険でもある場合もあります。

## 3 ウェブサイト訪問者への攻撃

ここまでは、インターネットユーザーが悪意あるサイトへ誘導される方法を考察してきました。では、次のステップでは実際に何が起こるのでしょうか？出発点は、前のセクションに記載されている情報源の一つです。最も単純なケースでは、リンクが悪意のあるファイルに直接繋がっています。ブラウザの種類や設定に応じて、特定のファイルをダウンロード、そして（もしくは）実行するようにユーザーに求めます。ここで、誤った選択を行うと、自身のコンピュータがマルウェアに感染してしまうのです。この手法より更に高い頻度で使われる手口が、悪意あるサイト、つまり『ランディングページ』へのリンクです。この手口では、ユーザーはバックグラウンド（ユーザーの知らないうちに）それ以降の操作を実行するか、コンピュータを乗っ取るため、存在するセキュリティホールを悪用する試みが行われます。これらの実行方法（直接実行、ユーザーとの対話形式、もしくはサイレント）については、次の項で詳しく説明します。

典型的なケースにおいて、コンピュータに送りこまれる最初のマルウェアコンポーネントがダウンローダーです。ダウンローダーは、侵入したシステムを隈なくチェックし、コンピュータの構成、OS、インストールされたウイルス対策ソフトなどの情報を外部に送信します。その後、ダウンローダーは追加のコンポーネントをダウンロードするように命令を受け取ります。通常、ダウンロードされる最初のコンポーネントはバックドアです。一旦、コンピュータがバックドアに感染してしまうと、コンピュータが完全にオンライン犯罪者側の手に渡ったといっても過言ではありません。特殊なコマンドを使って追加のファイルをダウンロードさせたり、コンピュータ上で起動させるための操作（再起動やスパムメール送信）を実行させます。また、バックドアは自身が送り込んだスパイウェアにコンピュータに保存された様々なデータをトラッキングします。トラッキングされる対象の情報には、メールアドレス、コンピュータ内に保存されたパスワード、またはソフトウェアのレジストレーションキーなどが含まれます。また、コンピュータに入力されるパスワードを記録するためキーロガーというマルウェアコンポーネントも存在します。

盗み出されデータは、『ドロップゾーン』と呼ばれる専用のコンピュータに転送されます。一度データが盗まれたコンピュータは、更に犯罪行為に悪用できるかどうかのチェックが行われます。インターネット接続が良くなければ、単にスパム配信またはプロキシとして使用されます。インターネット接続が良好であれば、ウェブサイトや海賊版のホスティングに使用できます。ワンクリック詐欺に悪用されるケースも珍しくはありません。これらは、ユーザーが全く気づかないところで実行されているのです。

### 3.1 ドライブバイ感染

多くの悪意あるサイト、とりわけexploit kitが運用されているサイトは、ブラウザのセキュリティホールやコンポーネントを悪用してWeb訪問者のコンピュータに侵入します。この感染手法においては、訪問者は感染に気付かないように実行されます。これが『ドライブバイ感染』といわれる所以です。最も頻繁に悪用されるセキュリティホールは、PDFやFlashファイル、Javaアプレット、QuickTimeやRealmediaなどのメ

ディープレーヤーが挙げられます。この感染から身を守る効果的な方法は、自分のコンピュータとインストール済みのプログラムを常に最新の常体に保つことです。

## 3.2 もっともよく知られている詐欺

コンピュータの乗っ取りに技術的に高度な手法を用いることができない、もしくはそれを回避したいときは、オンライン犯罪者側はWebサイトの訪問者をソフトウェアが実行されているWebサイトへと誘導します。これを『ソーシャルエンジニアリング』と言います。以下は最も成功した詐欺のリストです。

- ・映画やマルチメディアコンテンツが閲覧できるなどと、メールで巧みに誘います。しかし、訪問先ではエラーメッセージが表示され、インストールされているプレーヤーやコーデックのインストールを求めます。もしそのようなメッセージが表示されても、メッセージ内容には絶対に従わないようにしてください。必要なコンポーネントは必ず製造元のWebサイトから直接インストールしてください。

- ・Web上には無数のゲーム関連サイトが存在しています。欧米では World of WarcraftのようなMMORPGは非常に高い人気を誇っています。ゲーム関連フォーラムには、ゲームのパフォーマンスアップや最適化ツールを提供していることがあります。このようなツールは不注意にダウンロードせず、マルウェアであると疑ってかかりましょう。

- ・「コンピュータがウイルスに感染している」と虚偽の情報を表示させてユーザーを騙す詐欺サイトもあります。そのようなサイトを訪れると、ポップアップ画面が開き、コンピュータのスキャンが始まります。その後、スキャン終了のあと、「コンピュータが感染している」という閲覧者に警告を表示し、ウイルス感染からの保護を約束するプログラムの購入を促します。価格は、50 USドル以上が相場です。このような悪質なプログラムを「スケアウェア」または「rogueware」と言います。このようなプログラムは絶対にインストールしないでください。

- ・スケアウェアによる攻撃は、マルウェアのインストールだけでは終わらず、金銭的損害にまで及ぶケースがあります。十分に注意していないと、Web上のフォームに登録しただけで、勝手に複数年の契約や何万円もの金額を請求されるケースも多々報告されています。これとよく似た事例が、Web上での無料プログラムを探しているときに起こる可能性があります。ソフトウェアの試用版をダウンロードするために、登録フォームに必要な事項を記入を求めるポータルが多く存在しています。無料の試用版をダウンロードしただけのつもりでも、後日登録先に請求書が送付されてきます。費用に関する説明は登録時にユーザーの目に付かないところに小さな文字で記載されています。登録の際に少しでも疑わしいと感じた場合には、ダウンロードしないようにしましょう。

## 4 結論

今日のインターネットには数多くの脅威が潜んでいます。悪意は、いかにも怪しげなサイトや一部のサイトだけに仕掛けられているわけではありません。毎日利用しているニュースサイト、チャットサイト、製品検索など、あらゆるサイトも同様に危険で、悪意のあるサイトに導かれる可能性があります。最悪の場合、ユーザーは自身のコンピュータの感染に全く気付かずに乗っ取られることとなってしまいます。しかし、これらの脅威から自分自身を護ることもできます。特にブラウザとウイルス対策ソフトは必ず最新の状態に保つように心がけてください。また、ブラウザはマルウェアにとって最も重要なゲートウェイですので、ブラ



ウザへの追加の保護対策を施すことも重要でしょう。

Attacs from the Web  
by Ralf Benzmüller,  
Translated by Shinsuke Kishimoto  
& Yukito Takimoto

日本語版： 2011年4月8日発行

Copyright ©2011 G Data Software AG