German
Data
Security

G Data

White Paper 2009

―社内PCへのマルウェア侵入手口―

G Dataセキュリティラボ

ラルフ・ベンツミュラー＆ヴェルナー・クリアー

(岸本眞輔 訳)

Go safe. Go safer. G Data.

目次

1 マルウェアの用途

マルウェアを作成し拡散する人びとの動機は、ここ数年で大きく転換しました。コンピュータウイルスが登場して間もない頃には、自己の能力をひけらかすための野心がマルウェア作者の動機の根底にありましたが、今日の攻撃者は、確実に、金銭目的型に移行しています。

デジタル世界の地下部には、マルウェアの生成・拡散などを行う闇の業界が存在しており、すでにしっかりした基盤を持っています。

サイバー犯罪においては、あらゆるツールとそれにまつわるサービスの取引が盛んに行われています。特定の取引場所では、新たに発見されたセキュリティホールに関する情報や、マルウェア作者によって機能保証されカスタマイズされたマルウェアなどが、容易に入手可能です。

PC が感染すると、ボットネットに取り込まれ、ゾンビ PC と化してしまいます。ボットネットの運営者は、これらのゾンビ PC を自身で使用することもあれば、スパムメール送信やウェブサイトやメールサーバーへの攻撃用のサービスとして、レンタルで提供することもあります。

感染 PC から盗みだした情報の現金化なども、サイバー犯罪者の業務となっています。架空の会社を用意しそこで無知な PC ユーザーをファイナンスエージェントとして雇い入れ、彼らの個人銀行口座を使って資金洗浄を行います。

犯罪者たちの攻撃目標は、単に悪性ソフトウェアを作成することにあるのではなく、作成したマルウェアの拡散にあります。明らかに企業ネットワークに関しては、金銭に直結するさまざまな種類の情報が蓄積されており、企業インフラを他の犯罪活動に利用することができるため、攻撃者たちにとって、格好の攻撃目標として考えられています。

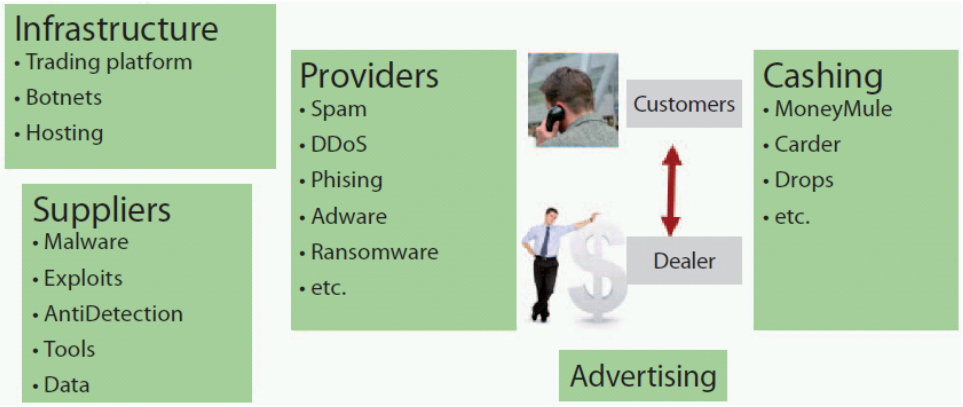

図 1 ：サイバー犯罪業界の各セクター

図 1 にあるとおり、サイバー犯罪は多くの業者から構成され、各々分業しています。裏舞台では、全体を仕切る犯罪者が支配し、マルウェア、セキュリティホールの存在に関する情報を流し、盗み出した情報を売りさばきます。これらの販売対象物は、特殊な販売プラットフォームやリセラー経由で売買されたり、レンタルされます。最終的には、犯罪に加担させられているとは知らずに雇われた人々によって資金洗浄が行われます。

2 サイバー犯罪者のツールとそれらを利用した商売方法

犯罪者は、さまざまな手法やツールを用いて商売を行ないます。犯罪者が利用するツールの中で最も重要なものは、ボットネットです。ボットネットは、ウイルスに感染した PC を攻撃者の支配下におき、思い通りに操作します。ボットネットを使えば、さまざまなサイバー犯罪関連の違法行為を行うことが可能となります。

2.1 ボットネット

ボットネットはサイバー犯罪を構成するツールの中で主要な要素として機能しています。ボットネットの利用領域には、スパムメールの送信や DDoS（＝分散型サービス不能化）攻撃などが代表として挙げられます。また、マルウェアに感染して犯罪者が運用するボットネットに組み込まれたゾンビ PC は、フィッシングやマルウェアサイトのホスティング、さらにはメールサーバーのアドレスを探るためにも利用されます。そのため、感染 PC を取り込んだ数が多ければ多いほど、ボットネットのパフォーマンスはより強力なものとなります。こう考えると、犯罪者が PC のゾンビ化、およびボットネットの規模拡大に傾注し、それに伴い、現在のボットネットに取り込まれた PC の数が非常に増加している現在の傾向は、至極当然のものといえます。ボットネットはゾンビ PC を細かく分けて支配下に置くので（約数千単位）、ボットネット自身の数も増加しています。

元来のボットネットは、IRC （インターネットリレーチャット）のプロトコルを利用して操作されていましたが、その後、ボットネット技術も高度化し、IRC 以外のプロトコルを使って操作を行うボットネット技術が確認されるようになります。更に記憶に新しいところでは、ストーム・ボットネットなどの昨今のボットネットが、コマンドの受けとりに、P2P 技術を利用しています。同様に、大規模なボットネットのズンカー（Zunker）は HTTP で通信しています。また、不法行為を行っていた ISP のモッコロ（McColo）が閉鎖された後は、数個のボットネットがコマンドとコントロールサーバを失った関係、で操作不能に陥りました。その結果、シュリズビ（Srizbi）や ストーム（Storm）といったボットネットは、存在を消しました。しかし、ワレダック（Waledac）やコンフィッカー（Conficker）などによる比較的新しいボットネットは、無数の接続を生成するため、常にボットネット経由でゾンビ PC を利用できるようになっています。

潜伏方法は巧妙になっています。頻繁な更新やルートキット、バックドアによって、効果的にユーザーに気付かれないように隠れることができます。実行タスク用プログラムやファイルは、実行直前にゾンビ PC に配布され、実行後に削除されてしまいます。

2.2 スパムメール

スパムメールによる広告メール送信は大規模に行われています。しかしご存知のように、広告提供者側がスパムメールで利益を得るのは、商品の売上によるものだけではありません。通常スパムメールは、ボットネット経由で送付されますが、たとえば、14 日間にわたって 200 万通ものメールを送信したい場合、スパム送信業者ソロモン（Solomon）では約 2 万円（195 ドル）でサービスが提供されています。また同様にメールアドレスも取引されており、2000 万件ものメールアドレスが約 5 万円（495 ドル）で販売されています。効果のない偽の錠剤、不正ソフト、偽者ブランド品など、違法性のある製品の購入になびくインターネットユーザー層は少なくはないのです。また、取引においては購入者に対し詐欺を働くだけにとどまりません。ジェレミー・ジェインズ（Jeremy Jaynes）は、当時、世界で 8 番目の規模のスパム配信を行うスパマーでしたが、彼の 1 ヶ月の収入は約 7500 万円（75 万ドル）にものぼりました。効能のない偽の錠剤、不法コピーソフト、低品質の模造品の取引では、返品率が非常に低く、犯罪者にとって格好のビジネスモデルとなっているのです。

2.3 脅迫

繁盛しているオンラインショップ、もしくは業務上メールを遅延なく送信する必要のある企業は、犯罪者の脅迫標的として狙われる可能性が高くなります。攻撃者は、ボットネットに組み込まれたゾンビ PC に指示を送るだけで、オンラインショップのサイトやメールサーバーを攻撃します。大量の情報を送信された、攻撃を受けた側のシステムは、大量の情報を処理するためにリソースを占有され、利用不可能な状態に陥ります。

この DDoS 攻撃を利用した脅迫犯罪の被害者は、オンラインカジノやその他のギャンブル運営者だけにおさまりません。1 時間に数百万～数千万円単位の金額が動くサービス運営者、サービスを提供するオンラインゲーム運営者も攻撃対象となります。攻撃された側は、攻撃者から攻撃を止めることを引き換えに、高額な支払いを求められます。犯罪者からの請求額は、通常、数十万円単位というのが一般的です。また、被害にあっていても報告されていないケースが非常に多いとの見方が支配的です。

DDoS 攻撃はまた、政治目的でも利用されています。2007 年 4 月下旬と 5 月上旬には、DDoS 攻撃により、エストニアの政府、関連省庁、銀行、新聞社、その他企業の機能が麻痺しました。ロシア人兵士の像を撤去したことを不満とするロシア人犯罪者が背景に隠れていると考えられています。また、デモが武力鎮圧する際に、ボットネットが政治的手段にも用いられたこともあります。

すでに述べた DDoS 攻撃を用いた脅迫手口の他にも、金をゆする手はあります。ランサムウェアがそうです。ランサムウェアは、PC 内に保存されている特定のファイルを暗号化するソフトで、例えばジーピーコーダー（GPCoder）がその 1 つです。一旦、ランサムウェアによってファイルが暗号化されると、そのファイルにアクセスするには、ケースにもよりますが、通常はファイルの復号化に 1,000～20,000 円程度（12～200 ドル）を要求されます。

また、上述の 2 種類のモデル以外にも、会社の社員が、児童ポルノ画像、不正ソフト、コピー保護された動画、オーディオファイルなどを会社の PC でダウンロードし、ファイルに紛れていたトロイの木馬を介して、会社内のコンピュータが入り込む事例もあります。この事例において

は、攻撃者は業務中に不正ファイルをダウンロードした会社員に対し、上司に不正ファイルのダウンロードについて漏らすなどと脅したり、警察に通報するなどと会社を脅したりすることにより、金銭を要求する場合もあります。

2.4 データ窃盗

盗みだしたデータの取引は、盗難クレジットカード情報や銀行口座情報などに限りません。フィッシング攻撃は、ネットオークション、SNS、オンラインショップ、メールアカウントなどのアクセスデータを盗みだすために利用される常套手段となっています。キーボードで入力された情報を記録する不正ソフト、キーロガーが PC にインストールされると、犯罪者はさらに多くのデータを容易に盗みだすことが可能です。会社のサーバーや VPN 接続のアクセスデータ、オンラインゲームのアカウント、機密性の高い内容を含むメールや文書の内容などが盗む対象となります。ウェブサーバーがキーロガーに感染し、駆除した数日後、再びキーロガーの感染が確認された場合は、システムアドミニストレーターのパスワードが盗まれている可能性が高いといえます。キーロガーを使って盗み出されたログファイルは、今日ブラックマーケットでは、数 10GB あたり数万円で取引されています。購入者は入手したログファイルを利用した後、再び別の人物に転売するのが一般的です。

盗み出されたデータの利用は広範囲：

- クレジットカード情報は偽造クレジットカードの作成やオンラインショップでのショッピングで利用される
- 銀行の口座情報は振込みで被害者の口座から金を詐取する。特に狙われている対象は、振込額のリミットが設定されていない法人の銀行口座。（個人銀行口座には振込額リミットが設定されているため）
- 盗まれたネットオークションのアカウントは、オークションに出品されている商品を購入することによって、マネーロンダリングが行われる。
- オンラインゲームのアクセスは、ゲーム内で流通する仮想貨幣や、レアなグッズ（武器、防具など）を盗みだすために利用される。
- メールアカウントや SNS のアクセスデータを利用すると、被害者の名義でスパムメールの送信が行われる。
- 盗まれた個人情報は、インターネットの特定のフォーラムで、アカウントを開設するために利用される。このアカウントは違法活動や詐欺活動にために悪用される。

2.5 アドウェア

アドウェアとはユーザーのインターネット閲覧履歴を記録し、特定のサイトで広告を表示したり、検索情報を操作するものです。アドウェアの支払いは、クリック数（その後、ブラウザのスタートページが不正に操作される）もしくはインストールされたバージョンの数に応じて支払

われますが、それら詳細は、それぞれのアドウェアのパートナープログラムで規定されており、このパートナープログラムは関連オンラインフォーラムで見つけることができます。近年にアドウェア業界の大企業が敗訴したにもかかわらず、広告型マルウェアや潜在性の不正プログラムは増加傾向にあり、その数は 5 倍以上にもなりました。

結論：

ここに挙げた手法は、現在のサイバー犯罪の手法すべてを包含しているわけではありません。しかし、サイバー犯罪の手口が多岐にわたり、インターネットインフラの普及に伴い、その被害の裾野も広がっていることがわかります。実際に年間被害総額は、１兆円規模と考えられています。ボットネットは、スパムメール送信、フィッシング攻撃に欠かせない基盤ツールとなっています。脅迫、データ窃盗、および広告表示も、その次に重要視されています。

3 マルウェアの侵入経路

前章でマルウェア拡散の動機を明らかにしました。本章ではいよいよ本研究の本題に進みます。まず、どのようにマルウェアが社内 PC へ侵入してゆくか、について説明しましょう。あるケースでは、PC をインターネットやローカルネットワークと接続するだけで十分です。また一方で、メール、ファイル共有サービス、インスタントメッセンジャー、リムーバブルメディア経由で、マルウェアが忍びこむこともあります。とりわけ、現在最も危険なのは、マルウェアが仕掛けられたウェブサイトです。このようなウェブサイトはユーザーが訪れるだけで、ユーザーに気付かれずに自動的にマルウェアがインストールされ、感染します（いわゆるドライブバイ・ダウンロードです）。

3.1 ネット接続だけで感染

無数のワームやボットが恒常的かつ自動的にインターネットを循環しているため、常時接続している PC は、常に脅威にさらされています。たとえば、あるマルウェアは、ランダムに IP アドレスを生成し、その IP アドレスに従属する PC に悪用できるセキュリティホールの有無を調べています。IP アドレスの選択は、例えば ISP や地域を絞った特定のネットワーク領域のみ選択できるように制限されていることが少なくありません。利用されるセキュリティホールは、時と場合によって異なります。すでにパッチが提供済みのセキュリティホールもまだ利用されており、ブラスター（Blaster, 2003）やサッサー（Sasser, 2007）など、古いタイプのウイルスだからといって安心するのは禁物です。

頻繁に攻撃目標となる対象：

- プラグ アンド プレイ(MS05-039)、TCP/445, TCP/139 経由
- RPC/DCOM (MS03-026/MS03-039)、TCP/135, TCP/445, TCP/1025 経由
- LSASS （ローカル セキュリティ オーソリティ サブシステム サービス）(MS04-011)、TCP/445 経由
- マイエスキューエル（MySQL）、TCP/3306 経由
- アルケイア（Arkeia）、TCP/617 経由
- ヴェリタス（Veritas）、TCP/6101 経由
- ヴェリタス、TCP/10000 経由
- ウィンズ（WINS）、TCP/42 経由
- アークサーブ（Arcserve）、TCP/41523 経由
- ネットバックアップ（NetBackup）、TCP/13701 経由
- ワークステーションサービス（Workstation Service） (MS03-049)、TCP/135, TCP/445 経由
- ウェブダヴ（WebDaV）、TCP/80 経由
- デイムウェア（DameWare）、TCP/6129 経由

- マイドゥーム（MyDoom-Backdoor）、 TCP/3127 経由
- バグル（Bagle-Backdoor）、 TCP/2745 経由
- IIS 5.x SSL PCT (MS04-011)、 TCP/443 経由
- 安易なパスワード設定のアカウント、TCP/139 または TCP/445 経由の接続
- エムエス エスキューエルサーバー（MSSQL-Server、パスワードが空白のシステムアドミニストレーターのアカウントなど、安易なパスワード設定）、TCP/1433 経由

3 ヶ月の期間を設けてさまざまな PC アーキテクチャへの攻撃を調査した研究結果によると、ウィンドウズマシンは平均して 38 秒に 1 回の攻撃が行われていました。新規購入マシンであっても、パッチをダウンロードしている数分の間に PC に攻撃を加えられ、乗っ取られるケースも珍しくはありません。多くのエンドユーザーを抱えるネットワーク（たとえばドイツテレコムのネットワーク）などでは、攻撃間隔が 38 秒より遅くなっています。それには、脆弱性を利用し不正を行うためのエクスプロイト（Exploit）コードの生成技術が高度化したことがあります。通常、エクスプロイトコードはセキュリティホールが公表された数日後には登場します。ゼロデイのエクスプロイトなどのマルウェアに悪用されるエクスプロイトの数も序々に増加してきています。最近の報告では、コンフィッカーワームがそれです。コンフィッカーワームは簡単なパスワードで保護されているローカル共有で自動的に広がるだけでなく、USB メモリなどのオート機能を悪用して、拡散します。

この種の攻撃は PC ユーザーに気付かずに実行されているのが、ほとんどのケースです。これらの攻撃に対しては、適切な設定が行われたファイアウォールやルーターを設置することにより、対策が可能です。

3.2 メール経由

メールを利用したマルウェア拡散は今もなお行われています。ラブレター（Loveletter）、メリッサ（Melissa）、ソイグ（Soig）やネットスカイ（Netsky）などのメール経由でのマルウェア大流行は、稀に見るケースとなってきてはいますが、ワームの配布者もこれを企図しているわけではありません。ソバー（Sober）、ニクセム（Nyzem, Nyxem）やワレゾフ（Warezoy）は、メディアでの注目度が非常に高かった最後のメールワームの流行です。それに代わり、期間や地域を絞った、ピンポイント型が各所で確認されています。自動的に感染するインターネットワームとは異なり、メールワームはメール受信者がメールを受信しただけでは感染しません。感染は、メール受信者がメールに添付されているファイルを開いてはじめて感染するケースがほとんどで、バブルボーイ（Bubbleboy）やクレズ（Klez）のように、メールを表示させるだけで感染するタイプは、稀です。このことから、メール送信者は、ソーシャルエンジニアリングで受信者の心理を突き、添付ファイルを開くように誘導する手口が発展してきました。たとえば 1 つの手口としては、メールヘッダーの不正変更があります。この手口で特に利用頻度が高いのが、送信者アドレスの変更です。メールワームの第 1 世代は、被害者の名前を装い、メールを転送していました。今日では、メールワームのほぼすべての送信者アドレスが偽物になっています。

今日では、ゲートウェイやクライアント側でのメールに添付された実行ファイルのフィルタリング処理、メールユーザーの危険に対する意識の向上などにより、マルウェア作者は攻撃手口を変更するようになり、最も多いのは、メールに不正ファイルを送りつけるリンクを記載してい

る場合です。マルウェアを添付しないことにより、送信されたメールは、有害なメールと検出されなくなります（スパムフィルタの種類によっては場合によって検出されます）。このリンクを押すと、ブラウザが何らかのメッセージを表示（通常はファイルの実行）します。このようなリンクはすぐさま有害リンクと認識されてしまうので、マルウェア作者は、別のサイトに誘導し受信者にダウンロードを新たにさせるか、もしくは複数のリダイレクトサイトを経由します。

ファイルの実行やサイトをクリックして読みこむように誘導するため、人間の心理や隙をつくソーシャルエンジニアリングは、送信者、件名、メール文書においてはさまざまな工夫が凝らされていますが、添付ファイル名、拡張子のトリック、有名なアイコンやドメイン名などもよく利用されます。マルウェア研究者のジョルダンとグーディは、2001 年から 2004 年までの流行したワームにおける、12 個の心理的要因をあげています（Myles Jordan & Heather Goudey, "The Signs, Signifiers and Semiotics of the Successful Semantic Attack," 2005. ） 。

流行したワームにおける心理的要因：

- 未経験
- 好奇心
- 欲目
- 遠慮
- 丁寧
- 自愛
- 軽信
- 欲
- 色恋
- 脅迫
- 協力
- 友好

また、他のマルウェア研究者、ブレイヴァーマンは、以下の点がジョルダンとグーディの指摘内容に補足されています（Matthew Braverman, "Behavioural Modelling of Social Engineering-based Malicious Software, " 2006.）。

- 何気ない日常のやりとり：短い文章（例：Cool）
- ウイルス警告およびソフトウェアパッチ
- PC におけるマルウェア検出
- メールの最後に挿入されるウイルススキャンメッセージ
- 口座に関する情報やメッセージ（例：架空の電話料超過請求）
- メール送信のエラーメッセージ
- 肉体的欲望 （Jordan & Goudey の色恋と同一）
- 告発：PC 内の違法ファイル存在の発見を指摘するトロイの木馬
- 時事問題
- 無料：多数の人々は、「無料」という言葉を聞くと、「無料」が「警戒」に打ち勝つ

マルウェアがその目的に達し実行しただけでは、詐欺の波は収まりません。攻撃成功のあとは、被害者に PC がウイルス感染した事実が見つかることを回避するような手立てをうちます。その

ためには、エラーメッセージ、イメージ、文書を開いて偽装します。サーカム（Sircam）やマジストラ（Magistr）などのワームはファイルを添付し、マルウェアが開始されたら、オリジナルファイルを開き、感染に気付かせないようする仕組みとなっています。

3.3 インスタントメッセンジャー経由

インスタントメッセンジャーのワームはウェブサイトのリンクを含んだメッセージを送りつけます。マルウェアファイルがインスタントメッセンジャーで直接送信されることは稀です。メール同様にソーシャルエンジニアリングを使って感染させようとします。チャットエンジンが組み込まれ、簡単なチャットが実行可能なインスタントメッセンジャーワームも数種確認されています。

インスタントメッセンジャーを企業内で利用するには、内部から外部へのやりとりをチェックできるクライアントを選ぶべきでしょう。ウイルススキャナをコマンドラインにて呼び出すことができるクライアントもあります。

3.4 ファイル共有ネットワーク経由

ジーデータは、ファイル共有ネットワークにてカテゴリごとに探し出し、最新オンラインゲームランキングのトップ 20 に入っているゲームを検索の対象とした調査を行いました。研究を始めて 1000 個のファイルをダウンロードした結果、約 33%のファイルがマルウェアに感染していました。そのうち、約 68%のマルウェアがアドウェア、23%がトロイの木馬、5%がバックドアでした。

6 ヶ月以上にわたって追跡した結果、調査したファイルの半数以上が P2P のファイル共有にてマルウェアが仕掛けられていました。調査の最終段階では、この数は 65%に達していました。

この数値からも、ファイル共有ネットワークはマルウェア作者にとって重要な意味を持っていることがうかがえます。会社内でファイル共有ネットワークを利用する場合は注意が必要です。

特に日本では、ウィニー（Winny）やシェア（Share）をはじめとしたファイル共有ソフトが普及し、かつ山田ウイルス、山田オルタナティブ、原田ウイルスをはじめとした猛威をふるったウイルスによって過去に何度となく企業情報が漏洩しているので、更に注意すべきでしょう。

3.5 リムーバブルメディア経由

工場出荷時にすでにハードディスク、DVD、MP3 プレーヤーなどのリムーバブルメディアがマルウェアに感染していたという事例の報告が増加しています。まるで映画のような話ですが、スパイウェアが入った USB メモリをわざとある企業の駐車場に落とし、USB メモリを拾った従業員経由で社内情報を盗みだすという手口も報告されています。

2009 年始めには、コンフィッカーワームがウィンドウズのオートスタート機能を悪用するなどして、リムーバブルメディア経由で大流行しました。オートラン系のワームは同様にオートス

タート機能を利用するワームでしたが、2008 年下半期から再流行となりました。オートラン機能を無効にする対策もありましたが、これはマイクロソフトが提供するパッチの適用後に有効となるため、当初、この対策の効果も限定的でした。

これらの事例から、特に重要な情報を保存していたり、取り扱う企業には、あらゆる手法で攻撃がなされているので、ＵＳＢメモリについては、社内への十分な注意喚起や対策を講じるべきです。

3.6 ローカルネットワーク経由

次なる拡散手口はローカルネットワーク内での共有です。すべての共有領域に自身のコピーを作成するワームがあります。多くのケースでは、ワームは一般的なパスワードのリストを利用しています。コンフィッカーもこの弱点をついたものです。そのため、社内では強力なパスワードを生成・利用し、共有領域を定期的にスキャンするなどして対策するべきです。アールボット（Rbot）やコンフィッカーの亜種は次のログインやパスワードを利用します。

ログイン：

" admin", "administrador", "administrat", "administrateur", "administrator", "admins", "computer", "database", "db2", "dba", "default", "guest", "net", "network", "oracle", "owner", "root", "staff" "student", "teacher", "user", "virus", "wwwadmin "

パスワード：

" 0", "000", "007", "1", "12", "123", "1234", "12345", "123456", "1234567", "12345678", "123456789", "1234567890", "12345678910", "2000", "2001", "2002", "2003", "2004", "access", "accounting", "accounts", "adm", "admin", "administrador", "administrat", "administrateur", "administrator", "admins", "basd", "backup", "bill", "bitch", "blank", "bob", "brian", "changeme", "chris", "cisco", "compaq", "computer", "control", "data", "database", "databasepass", "databasepassword", "db1", "db1234", "db2", "dba", "dbpass", "dbpassword", "default", "dell", "demo", "domain", "domainpass", "domainpassword", "eric", "exchange", "fred", "fuck", "george", "god", "guest", "hell", "hello", "home", "homeuser", "hp", "ian", "ibm", "internet", "intranet", "jen", "joe", "john", "kate", "katie", "lan", "lee", "linux", "login", "loginpass", "luke", "mail", "main", "mary", "mike", "neil", "net", "network", "nokia", "none", "null", "oainstall", "oem", "oeminstall", "oemuser", "office", "oracle", "orainstall", "outlook", "owner", "pass", "pass1234", "passwd", "password", "password1", "peter", "pwd", "qaz", "qwe", "qwerty", "root", "sa", "sam", "server", "sex", "siemens", "slut", "sql", "sqlpass", "staff", "student", "sue", "susan", "system", "teacher", "technical", "test", "unix", "user", "virus", "web", "win2000", "win2k", "win98", "windows", "winnt", "winpass", "winxp", "www", "wwwadmin", "xp", "zxc "

上記および類似のパスワードは、ネットワーク内での利用は控えるべきでしょう。

3.7　ウェブサイト経由

マルウェアへの感染経路において、現在最も感染頻度の高いのが、ウェブサイトを介したものです。この手法はウイルス対策ソフトに搭載されているウイルススキャナの機能の構造的弱点をついた攻撃です。ウイルススキャナは、システムコンポーネントへのアクセス時（オンアクセス）、もしくは都度の要求（オンデマンド）に従って、ファイルをスキャンします。ウイルススキャナのスキャンは、マルウェアがファイルとして存在する場合に、ウイルスを検出します。HTTP 経由でウェブサイトのデータがブラウザに送信されると、ファイルに含まれる HTML コードやスクリプトコマンドがまずブラウザのメモリ上で解読され、その後、実行されます。そうこうする内に、ブラウザはハードディスクにコンテンツを保存するかどうかを決定します。このコンテンツにウイルスが含まれ、かつウイルススキャナがこのウイルスを検出すれば、ウイルススキャナが警告を発します。しかし、この際にマルウェアはすでに実行済みなのです。ウイルススキャナで感染サイトから適切に保護するには、ブラウザに届く前に、HTTP 通信の内容をスキャンする必要があります。

メール経由での感染手口で記述したように、ウェブサイトから不正ファイルをダウンロードさせる手口が横行しています。この手口では、メール内のリンク、閲覧ウェブサイトからの転送先、その他の巧みな手口によって、ボタンを１度クリックしたり、リンクをクリックするだけで、PC に不正ファイルを密かにダウンロードし、実行させることができます。

ここで、マルウェアのダウンロードやインストールに利用される典型的な 2 つの手口を簡単に紹介しましょう。

まず、1 つめは、スケアウェアです。スケアウェアはニセのウイルス感染が検出されたという偽の警告を発し、ユーザーにウイルスを除去するに偽ウイルス対策ソフトの購入を促すタイプのものです。ここでは入力すると、偽ウイルス対策ソフトの購入だけではなく、クレジットカード情報なども悪用される可能性があります。

図２：スケアウェアのサイト。被害者のクレジットカード情報の入力が求められている

もう 1 つの手口は、ある動画を再生するために特殊なコーデックのインストールを求められるサイトです。ここではアダルトコンテンツやメディアで普通に報道されている自然災害、航空機事故、大統領選、スポーツの試合などの日常の最新ニュースなどの動画が置いてあり、それを再生するために特殊なコーデックとフラッシュプレイヤーの最新版のインストールを求められます。もちろんこのコーデックにはマルウェアが隠されています。

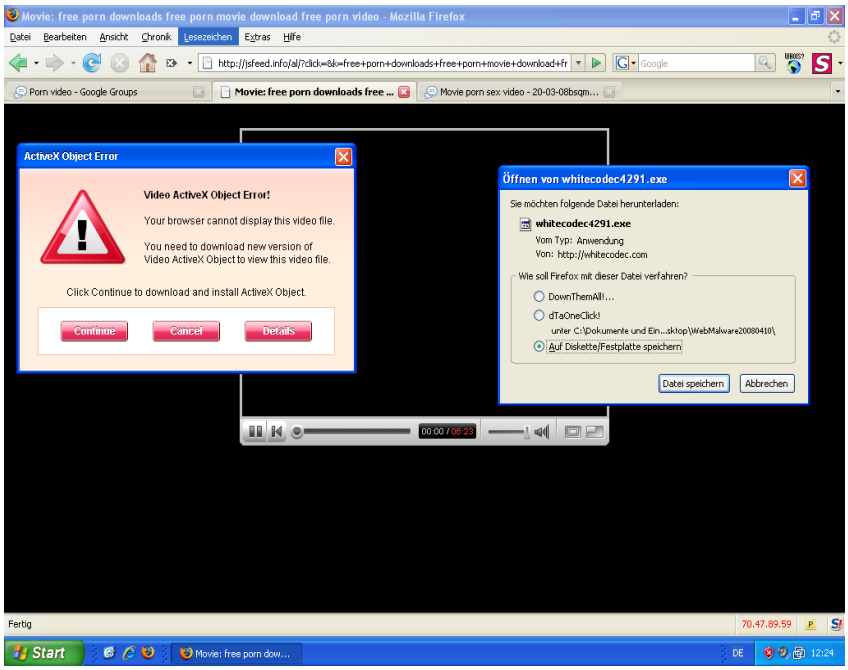

図 3：コーデックのダウンロードを求めるビデオ閲覧サイト。実際は不正ファイルをダウンロードし、インストールされる

その他には、被害者が何もしていないのにユーザーの PC を感染させるドライブバイ・ダウンロードという手口があります。訪問先のウェブサイトのデータをダウンロードされる間、ドライブバイ・ダウンロードはユーザーの気付かないところで動作します。攻撃者は、まず自身で制御するサーバーマシンに、訪問者のブラウザと OS の種類を調べるスクリプトを仕掛けます。そしてユーザーがこのサイトを訪れると、ユーザーの環境にマッチしたマルウェアがロードされ、このコードはブラウザやブラウザのコンポーネントのセキュリティホールを調べます。ここで、セキュリティコードが見つかれば、マシンを乗っ取るためのマルウェアを送りつけます。このようなマルウェアはエクスプロイトと呼ばれています。エクスプロイトの標的となる対象はインターネットエクスプローラーですが、ファイアフォックス、オペラ、サファリなどのセキュリティホールが悪用されることももちろんあります。ウェブサイト攻撃スクリプトのツールとしては、エムパック（Mpack）、アイスパック（IcePack）、ファイアパック（FirePack）などがあります。現在、マルウェア作者が頻繁に利用するセキュリティホールは、次のとおりです。

- CVE 2007-0071 ：フラッシュ（Adobe Flash）
- CVE 2008-1309 ：リアルプレイヤー（RealPlayer）
- ourgame_GLIEDown2 ：インターネット エクスプローラー（Internet Explorer）
- CVE 2006-0003 MS06-01：マイクロソフト データ アクセス コンポーネント(MDAC)

- CVE 2007-5601 ：リアルプレイヤー

サーバーへの仕掛けが準備できたら、次はできるだけ多くのインターネットユーザーを誘導しようとします。常套手段として使われるのは、興味をそそる内容（安売り、宝くじ当選）を記載したスパムメールです。また、増加中の手口として、グーグルやヤフーでの検索において、マルウェアを仕掛けたサイトを上位にランクインさせるように操作することです。また、リンクの入力ミスを狙って、"mircosoft.com"、 "goggle.com"、"mcaffe.de"などのように、有名サイトの URL に似せた紛らわしいアドレスをつけているサイトもあり、注意が必要です。

さらに効果的な手法と考えられているのは、有名なドメインのページにマルウェアを仕掛ける手口です。攻撃者がウェブサーバーの制御を掌握すると、上で述べたウェブでのエクスプロイトのためのツールキットを利用して、ドメイン内の各サイトに、他のサーバーからマルウェアをロードするコードをアイフレーム（IFRAME）やスクリプトで埋め込みます。また、アドミニストレーターのアクセス用パスワードを破る辞書攻撃ツールなどもあります。同様に、コンテンツマネジメントシステム（CMS）、ブログやフォーラム関連のソフトウェア、そしてアドミニストレーションツールなど、ウェブにかかわるソフトウェアのセキュリティホールも、ウェブサーバーの乗っ取りに悪用されています。事例の大多数において、この攻撃は個々のウェブサーバーに限定されているのではなく、自動的に大量のウェブサーバーを目的として実行されています。現在、マルウェアは、怪しそうにみえるサイトだけでなく、どのようなドメインにも仕掛けられている可能性があることを理解する必要があります。

他の手口としては任意のウェブサイト上への広告表示があります。人気のあるドメインのほとんどは、ウェブサイト上にバナー広告を表示させることにより収入を得ています。ウェブバナーは通常、アイフレームでサイト上に表示されるため、運営者側でバナーの表示内容を操作することはできません。広告運営者には広告内容をチェックする責任がありますが、これは非常に困難です。エムパックなどのツールで生成されるマルウェアは、巧妙かつ高度な技術を使っているため、わかりにくいのが実情です。このように一般のウェブサイトであってもマルウェアを仕掛けることに成功し、ドライブバイ ダウンロードのすべての感染のうち、約 80%が一般のウェブサイトからとなっています。

しかし、ウェブサーバーのクラックなどをせずに、手間なくマルウェアを送信することも可能です。掲示板やブログ上に貼り付けられたリンク先に、マルウェアが含まれ、訪問すると自動的に実行されることも十分に考えられます。現在、インターネット上ではウィキペディアや巨大掲示板で誰でも簡単にコメントを書きこんだり、閲覧することができます。ウィキペディアにおいては、以前大流行したブラスターの記事において、ブラスターの駆除ツールのリンク先をトロイの木馬をダウンロードさせるリンクに書き換えたケースもあります。このようなフォーラムは、よからぬ思いを抱くユーザーの活動拠点となっています。盗難された ID が容易に入手できるような取引が行われています。

とはいえ、マルウェアをサーバーに仕掛けることは、必ずしも必要ではありません。任意のウェブサイトのリンクにマルウェアが含まれ、目的のサイトでコードが実行される、という危険な手口もあります。こういた攻撃は、クロスサイトスクリプティング（XSS）と呼ばれています。ユーザーの入力した内容が HTML ページに表示される際に入力内容を適切にチェックしない場合、XSS の攻撃が可能となります。

たとえば、フォームに名前を再表示させるスクリプトがある場合に XSS は使用されます。攻撃者が名前の代わりにジャバスクリプトのコードを入力すると、ブラウザはこのスクリプトを実

行します。例として、フォームに名前の入力を求められる場合をみてみましょう。名前の代わりに入力欄に次のコードを入力します。

```
<SCRIPT>alert("注意")</SCRIPT>
```

フォームを送信すると、この入力したコードは表示されないまま、実行されます。上の例では「注意」が表示されますが、実際の攻撃においては、入力欄に危険なコードが入力されることになります。

また、次のように入力すると、フォームの記入内容がフィルタされている場合でも、マルウェアは呼び出されたページのリンクに書きこむことが可能です。

```
http://www.myserver.dom/site.php?name=<SCRIPT>alert("注意")</SCRIPT>
```

このようなリンクは、掲示板やブログにあるテキストに仕掛けられている可能性があります。さらに姑息な手口は、グーグルの検索結果に XSS のリンクを表示させることです。グーグル側も XSS のリンクを探し出し、検索結果から削除などの対応を講じていますが、マルウェア作者はグーグルの検索結果用の汚染されたブログのエントリーを最適化して、その対策をすり抜けているのです。

同様のことがウェブ 2.0 においても見られます。この脅威の状況から、ブラウザでアクティブコンテンツやスクリプト言語をブロックする対策を考えるユーザーもいるでしょう。しかし、そうなるとウェブ 2.0 のメリットを失うことになります。この新機能の多くは、悪用される可能性を孕み、潜在的なセキュリティホールの数を増加させます。サミー（Samy）の XSS ワームは、2005 年終わり頃、マイスペース（Myspace）で 18 時間の間に XSS によって 100 万ものフレンドの関係を作り出しました。XSS の危険性については、依然として過小評価されている傾向にあります。

マルウェアを配布するドメインは、怪しげなサイト、ダウンロードポータルサイト、クラックされたインターネットページだけでなく、正規のウェブサイトやグーグルの検索結果にも潜んでいます。どのウェブサイトもマルウェアに狙われているといわれても過言ではないでしょう。

4 典型的な感染の流れ

サイバー犯罪による攻撃の実行は、一定のパターンをもって行われています。典型的な感染はここ数年において大きく変わってきています。ネットスカイやマイドゥームのようなワームは、さまざまな機能を一つにまとめたようなマルウェアもしくはソフトウェアが添付されていました。それが今は、必要に応じてファイルのロードが自由にできる、多くの細かな特化モジュールとなりました。

感染も、複数のフェーズに分かれます。まずマルウェアが作成され、ターゲットユーザーを選定し、そして攻撃がはじまります。そして、マルウェアに感染したシステムが攻撃者の制御下に落ちると、さまざまな種類の犯罪行為に加担させられるようになります。

4.1 感染の準備

まず、拡散させるマルウェアを開発する必要があります。これは感染のパターンの流行ごとにマルウェアを新たに開発するということではありません。マルウェア作者がマルウェアを書くと、ランタイムパッカー、別のコンパイラーやツールなどを使って、一般的なウイルス対策ソフトでは検出できない新たな亜種を作成します。マルウェアがウイルス対策ソフトに検出されるころには、検出不可能な新たな亜種がもうすでに生成されています。このような準備作業を自分で行いたくない場合は、インターネット上の闇フォーラムで必要なサービスを保証付きで購入するのが一般的です。

マルウェアが用意できると、攻撃者は拡散方法や経路を決めます。たとえば、攻撃者はセキュリティホールへの自動攻撃が可能です。このケースでは、被害者は自身に降りかかっている攻撃や感染に気づきません。他には、ユーザー自身にマルウェアを実行させるような詐欺もあります。最初の手口においては、マシンを乗っとるエクスプロイトが必要です。二つめの手口においては、ユーザーを誘導しマルウェアをダウンロードさせるためのメール、インスタントメッセンジャー、ウェブサイトなどを用意する必要があります。ウェブサイトにマルウェアを仕掛ける場合、ドメインは登録済みで、適切なファイルが仕掛けられていなければなりません。

この一連のアクションのほとんどにおいては、取扱いが非常に容易なツールが存在します。

4.2 実行

マシンを乗っとった後は、トロイの木馬系のダウンローダーが起動します。このダウンローダーは不正ファイルをマシンに呼び込み、起動させる役割を担います。まず最初の攻撃者が、感染と乗っとりに成功したシステムに関する情報を広めます。その後、感染したマシンのセキュリティの設定が下げられます。これでマシンはマルウェアの活動に対し保護できない状態となりま

す。次のステップで、マルウェアがマシンにロードされます。この実行には、複数のマルウェアが必要となります。

多くのケースでは、追加ロードが行われる最初の不正ファイルは、バックドアです。バックドアはルートキットによって隠れながら活動を行います。これにより感染マシンは、外部から自由に操作できるようになります。他の可能性としては、バックドアは IRC、P2P、HTTP 経由で世界中の PC と調整を行うのに使用されます。いまやコンピュータは、巨大なゾンビ PC 群の一部へと組み込まれてしまったのです。

バックドアのインストール後は、感染システムは細かい監視下に置かれ、攻撃者は自由にマシンを操作できるようになります。クラックされたマシンはスパイウェアで活用できるデータ単位で検索され、アドウェアが備えられます。マシンが常時インターネット接続されている場合、もしくは、高速インターネットを利用している場合は、スパム送信、不正ファイルのダウンロード提供、フィッシングやマルウェアサイトのホストにも悪用されます。

4.3 感染マシンを利用

ボットネットのゾンビ PC がスパム送信に利用される場合は、ボットネット運営者はバックドアによって、メール文書、メールアドレス、メール送信用ソフトウェアなどが含まれた、マルウェアパックを感染マシンにインストールします。このファイルが準備されると、スパム送信の用意が完了となり、送信が開始されます。全部のメールが送信完了すると、インストール済みのスパム送信用ソフトウェアはマシン内のスパム送信関連ファイルをすべて削除します。ただし、バックドアはそのまま感染マシン内で、次の攻撃指令を受ける機会を待ちながら、潜伏を続けます。

5 保護対策

社内 PC をマルウェアから保護することは、会社の全 IT セキュリティに関わる問題です。IT セキュリティは一度行えばそれで済むというものではなく、継続してはじめて意味を持ちます。企業においては特定のユーザーグループや領域が特に危険に晒され、それに対し、特殊な保護対策を講じる必要があります。会社はこのプロセスにおいて、あらゆる観点について考慮し、各会社にあった適切な意思決定を下す必要があります。

マルウェアからの保護を定義された脅威から守る技術方法の導入と結びつける必要があります。最も重要な技術対策は次のとおりです。

- ウイルス対策

  ウイルス対策ソフトは、サーバーとクライアント両方にインストールしてください。HTTP データトラフィックと ICQ や IRC 経由のマルウェアもチェックする機能をもったものをお薦めします。

- スパム対策

  添付ファイルのみならず有害なウェブサイトへのリンクもスパムメールには含まれているので、スパム保護はマルウェア対策にもなります。

- 不正アクセス対策

  ファイアウォールによる不正侵入を検出し防止するソリューションが必要です。ネットワークトラフィックからのデータは、インターネットワームの攻撃発見や防御に役立ちます。

しかし、他の技術的な改善もウイルス対策には有効でしょう。パッチマネージメント、ソフトの仮想化、会社マシンのユーザー権、ファイルやネットワーク領域へのアクセスコントロールなどの備えなどは、透明性の高いセキュリティ対策を補完することができます。これらの内容については、情報処理機構が提供しているドキュメントを参照ください。

ただ、技術面での対策を実行しただけでは、会社のネットワークを効果的に保護するうえでは完璧とはいえません。社員レベルでのセキュリティ対策の実行がどうしても必要となります。またそのためにも、コンピュータ、リムーバブルメディア、機密情報の取扱いに関するガイドラインや倫理的規則、セキュリティポリシーなどを社内の管理セクションが制定するとともに、その内容が日常に生かされる必要があります。保護対策は、組織構造に反映されねばなりません。たとえば、規則に反した場合の罰則等についても決める必要があるのです。

最後になりますが、インターネットはもちろん就業中に直面する脅威全般について、社員は何でも明るみにする必要があるでしょう。社員が積極的にこのような脅威への対策に貢献している企業は、社内の PC へのウイルス感染率を下げ続けることにつながるでしょう。