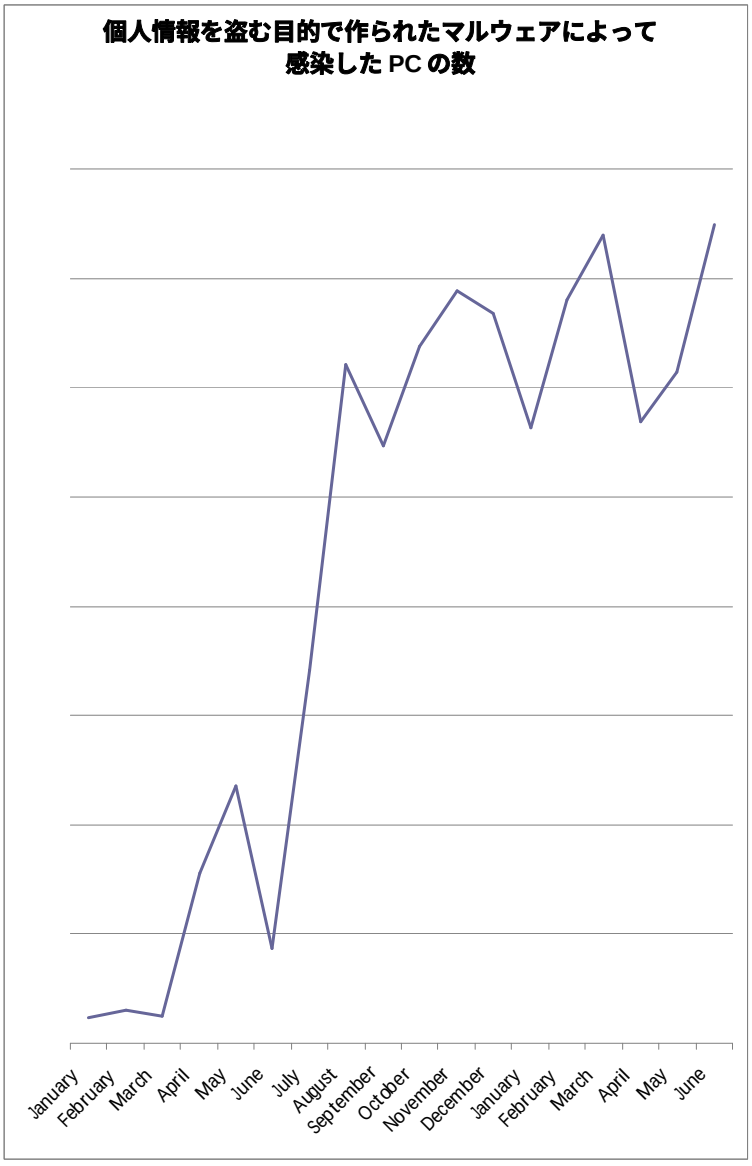
Press Release

www.pandasecurity.com

経済危機の中、多くのユーザーが
個人情報を盗むマルウェアによる影響を受けた

- **今年のこれまでのところ、個人情報や銀行の詳細情報などの機密情報を盗むために作られたマルウェアに感染させられたコンピュータの数は、昨年の同じ期間と比較して 600%増加しました。**

- **毎日平均 37,000 のウイルス、ワーム、トロイの木馬、その他のセキュリティ上脅威が出現しており、その 71%がおもに個人情報を盗むために設計されたトロイの木馬です。**



PandaLabs の調査データによると、個人情報を盗むために作られたマルウェアの影響を受けた今年これまでのユーザー数は、2008 年の同じ期間と比較して、600%増加しました。最も多いのはトロイの木馬ですが、フィッシング、ワーム、スパイウェアなども多くの例がありました。

PandaLabs のテクニカルディレクターである Luis Corrons 氏によると、「おそらくこの急増の原因のひとつは、この経済危機においてクレジットカード番号や、Paypal や Ebay のアカウント情報などを闇のマーケットで売ることが大きなビジネスになったことです。我々はさらに、ソーシャルネットワーク経由で流通および感染するタイプのマルウェアの増加も目にしました。」

例をあげますと、PandaLabs は、毎日約 37,000 の新種のウイルスやワーム、トロイの木馬、インターネット上のその他の種類の脅威のサンプルを受け取ります。これらの内 71%はトロイの木馬で、ほとんどが銀行の詳細情報やクレジットカード番号、その他商業サービスのパスワードを盗むことが目的でした。2009 年 1 月から 7 月の間、我々は 1100 万の新種の脅威を受け取り、それらの内 800 万がトロイの木馬でした。これは 2007 年に PandaLabs が受け取った新種のトロイの木馬は平均 51%であったことと比べて明白な差異を示しています。

ハッカー達は、新しい収入資源や脅威を繁殖させるための新しいチャネルを模索することにも忙しいのです。マルウェアサンプルを使って、偽の銀行サイトに彼らのユーザー名やパスワードを入力させ、それらを取得することによって、あらかじめ（ほとんどは一人の）ユーザーの

オンラインバンキング情報を標的にし、犠牲者となるべき人々は、銀行情報が格納されるもしくは彼らが入力しなければならないような、何らかのプラットフォームやオンラインサイトへ誘導されます。

支払いプラットフォーム（例:Paypal）や、ユーザーが自分の支払い明細をよく保存するようなサービスにおけるターゲット攻撃が増加しているのはそのようなケースで、一般的なオンラインストア（例:Amazon）や、オンラインオークション（例:eBay）、さらには慈善の寄付を行うNGO ポータルも含まれています。

同様に、過去においては email が犠牲者に接触するための現実的な唯一のチャネルに使われましたが、現在は他のたくさんの方法が使われています。

- 嘘の URL によるソーシャルネットワーク（Twittter や Facebook など）を使ったメッセージの配布
- クローニングした Web ページを、ポピュラーな検索エンジンにおけるキーワード検索の初めの結果の中に表示させる
- 携帯電話販売の SMS メッセージ
- スパイウェアでコンピュータを感染させ、警告メッセージの表示によってユーザーを偽の Web サイト（偽のアンチウイルスプログラムなど）へ誘導する

ソーシャルエンジニアリングを使ったメッセージは、しばしばユーザーを餌で釣って騙すための最後の決め手になります。

彼らはクレジットカードや銀行の詳細を入手すると、2 種類のオプションが選択できます
一つはそれらを使って購買をすること（犠牲者は銀行の明細を受け取るまで気付かない）、もう一つは闇のマーケットにその情報を売る（1 回あたり約 3 ユーロでよく売れる）ことです。

犠牲者になるのを避けるためには？

我々は、全ユーザーの約 3%がこのテクニックの被害にあっていると見積もっています。こういったタイプの脅威による問題は、過去の伝統的なウイルスと異なり、検出されにくいように作られているので、ユーザーは自分が犠牲者になっていることに手遅れになるまで気付きません。

けれども、一連の基本的な防止策があります。

1. まず第一に、オンラインバンクや支払いプラットフォーム、ソーシャルネットワークなどが自社のログイン証明を確認する為に、ましてやクレジットカードの詳細情報を聞く為に、ユーザーへメッセージ（email やテキストなど）を送るということは、まずあり得ないということを良く覚えておくこと。
2. オンラインバンクやストアなどへアクセスするときは、受け取ったり検索したりしたリンクをクリックするのではなく常にアドレスを直接ブラウザに入力すること。
3. ブラウザでアドレスを直接入力した場合であっても、さらにその表示される URL が本当にあなたが入力したものかどうか、また Enter をクリックした際にアドレスが普通ではない別の何かに変わらなかったかどうかをチェックすること。
4. そのページが、相応のセキュリティ証明を含んでいるかどうかをチェックすること（一般的にはブラウザ上で'鍵のかかった錠前'のアイコンで表示される）
5. 言うまでもなく、あなたは常にコンピュータに優れたセキュリティ製品をインストールしているでしょう。これはもし偽の Web サイトに入ってしまった場合、脅威の検出を助けるでしょう。また、常にセカンドオピニオンを持つことも、あなたがトロイの木馬やその類によって感染させられることを、確実に防ぐためには良いことです。Panda ActiveScan (www.pandasecurity.com)のような無料のオンラインスキャンのアプリケーションを利用することで実行できます。
6. 何より、もし何か疑いを感じたら個人情報の入力をせずに、あなたがアクセスしようとしている銀行やストア、サービスプロバイダにコンタクトしてみましょう。実際にこれらの企業は全てカスタマーサービスを電話で提供しているはずです。
7. もしあなたがオンラインショッピングや銀行などのサービスを頻繁に使うなら、オンラインアクティビティのための保険に加入することも出来ます。これは詐欺に遭った場合の補償になるでしょう。

■PandaLabs について

1990 年以来、我々はクライアントに最大限のセキュリティを可能な限り迅速に提供するため、新たな脅威を検知/除去するミッションを追求し続けて参りました。そのために、PandaLabs は一日で何千もの新たなサンプルを分析/分類し、(マルウェアか善良なウェアかどうかの)自動判定を下すことの出来る革新的な自動システムを持っています。このシステムは Collective Intelligence のベースであり、他のセキュリティソリューションでは手に負えなかったマルウェアをも検知出来る Panda Security の新しいセキュリティモデルなのです。

現在、PandaLabs に検知されるマルウェアの 99.4%は、この Collective Intelligence システムを通して分析されています。これは、特定タイプ別のマルウェア(ウイルス、ワーム、トロイの木馬、スパイウェア、フィッシング、スパム等)をそれぞれ専門で研究する各チームが、世界規模で対応するために 24 時間 365 日体制で絶えず研究を続ける事によって実現しています。このようにして、お客様により安全で、解り易く、リソースにもやさしいソリューションを提供し続けます。

より詳細な情報は PandaLabs のブログにてご覧いただけます。: http://www.pandalabs.com

■Panda Securityについて

Panda Security は、約195カ国に100 万以上のクライアントを持ち、その製品は23 種類の言語に対応している、IT セキュリティソリューションの世界的なリーディングプロバイダです。
Panda Securityは、「コレクティブインテリジェンス」テクノロジーによるクラウドコンピューティングのパワーを備えた最初のITセキュリティ企業です。この革新的なセキュリティモデルは、一日に数千の新しいマルウェアサンプルを自動的に分析および分類することが可能で、企業や個人のお客様に対して、PCパフォーマンスへの負荷を最小限に抑えながらインターネット上の脅威に立ち向かう最適なプロテクションを提供することを保証しています。
Panda Securityは、カリフォルニアの米国本社やスペインのヨーロッパ本社を始め、世界56カ国にオフィスを展開しています。
Panda Securityは、企業の社会的責任を担うポリシーの一環として、スペシャルオリンピック、WWF、Invest for Childrenをサポートしています。詳細情報はこちら
http://www.pandasecurity.com/

※Panda Japanホームページ　http://ps-japan.co.jp/

※Panda Japanブログ　http://pandajapanblogs.blogspot.com/

※Twitter　http://twitter.com/Panda_Japan

プレスリリースに関するお問い合わせ先

Panda Security 日本法人
PS Japan 株式会社
担当／島内
TEL：03－5219－1285　FAX：03－6862－8618