コンピュータ利用者のためのマンスリー・セキュリティ・アウエアネス・ニュースレター

OUCH!

今月のトピック...

- マルウェアとは
- マルウェアの作成者と目的
- マルウェア対策

マルウェアとは

はじめに

サイバーセキュリティの話題になると、ウィルス、ワーム、トロイの木馬、ルートキットといった単語を耳にします。これらは、感染させることで第三者がコンピュータやモバイル機器を乗っ取ることができるプログラムを意味します。これらプログラムは、今は単にマルウェアと呼ばれています。今月号では、マルウェアとは何か、誰がどのような目的で作成するのか、マルウェアに感染しないためにできることを説明します。

ゲストエディター

レニー・ゼルツァー氏は、NCRコーポレーションで、顧客企業のITシステムのセキュリティ対策や、SANSでマルウェア対策コースのインストラクターをしています。ツイッター(@lennyzeltser)や、blog.zeltser.comのブログでも積極的に情報発信しています。

マルウェアとは

簡単に言うと、マルウェアとは、悪意のある動作をするコンピュータプログラム、つまりソフトウェアです。実際、マルウェアという言葉は、malicious（悪意のある）とsoftware（ソフトウェア）の単語を合わせてできたものです。ほとんどの場合、コンピュータやモバイル機器にマルウェアをインストールすることが、サイバー犯罪者の最終目的です。マルウェアがインストールされると、攻撃者はそのコンピュータやモバイル機器を乗っ取って操作できるようになります。マルウェアはWindowsパソコンにだけ存在すると誤解している人が多いようです。Windowsパソコンは広く利用されているため主要な攻撃対象になりますが、マルウェアはスマートフォンやタブレットなどあらゆるコンピュータ機器に感染します。実際、モバイル機器へ感染する悪意のあるソフトウェアは着実に増加しています。そして、誰もが攻撃対象になることを覚えておいてください。サイバー犯罪者はより多くのコンピュータやモバイル機器にマルウェアを感染させることで、より多くの金銭を取得します。金銭目的の犯罪者は、できる限り多く感染させることができれば、相手が誰かは気にはしません。

マルウェアの作成者と目的

マルウェアは、単に好奇心を持った素人ハッカーによってのみ作成されるものではなく、巧妙なサイバー犯罪者によって特定の目的を達成するために作成されています。犯罪者の目的には、機密データの窃取、ログイン・パスワード情報の取得、迷惑メールの送信、DoS攻撃の踏み台、恐喝、個人情報の搾取などが含まれます。例えば、Cryptolockerというマルウェアは、コンピュータに感染すると全ファイルを暗号化します。暗号化した後で、ファイルを復号するのと引き換えに金銭の支払いを要求するのです。

マルウェアとは

マルウェアを開発して利益を得る人々は、個人、組織的犯罪グループ、政府関係機関と多岐にわたります。また、現在、高度なマルウェアは、大抵の場合マルウェア開発の専業者により作成されています。これらの専業者はマルウェアを作成すると、他人や組織にそれを販売し、マルウェアの「顧客」へ定期アップデートやサポートを提供します。犯罪者は、購入後に何百万という無防備なシステムにマルウェアをインストールしたり、感染したシステムのボットネットを構築することで、荒稼ぎすることができます。ボットネットは、遠隔操作ができる武器のような役割を果たすため、サイバー犯罪者自身で利用したり、感染したコンピュータを他の犯罪者に販売したりします。

マルウェアに感染しない最善の方法は、アンチウィルスソフトウェアをインストールし、コンピュータを常に最新の状態にして、普段からのセキュリティ意識を高めることです。

マルウェア対策

コンピュータやモバイル機器をマルウェアから保護するための一般的な方法は、信頼できるベンダーのアンチウィルスソフトをインストールすることです。アンチウィルスは、アンチマルウェアとも呼ばれますが、悪意のあるソフトウェアを検出して駆除するように設計されたセキュリティソフトウェアです。しかしながら、アンチウィルスソフトは、全てのマルウェアをブロックして除去することはできません。攻撃者は、アンチウィルスプログラムを回避する方法を絶えず開発しています。これに対抗するために、ウィルス対策ベンダーは、製品を常に更新して新しいマルウェアに対応しています。いろいろな意味で、攻撃する側と対抗するベンダー側の腕比べとなっています。残念なことに、サイバー犯罪者が優勢になることが多く見受けられます。つまり、アンチウィルスソフトがマルウェアを多数検知し除去する一方で、検知されない新バージョンも常に作成されていることを覚えておいてください。アンチウィルスが万能でないため、アンチウィルスに頼るだけでなく、利用者自身を守るための手順も覚えてください。

第一に、オペレーティングシステムやアプリケーションで自動的に更新プログラムをインストールする設定が有効になっているか確かめます。ソフトウェアが最新の状態であれば、コンピュータやモバイル機器への感染は難しくなります。

第二に、マルウェアに対する最善の防御策は利用者自身であることを覚えておいてください。多くの場合、ソーシャルエンジニアリングの手法で利用者を騙してマルウェアをインストールさせます。よくある例は、一見正当に見えるメールを偽装して、コンピュータにマルウェアを感染させるフィッシング攻撃です。例えば、サイバー犯罪者が銀行を装って電子メールを送信し、メール内のリンク情報をクリックするように依頼します。ここでリンクをクリックすると、Webサイトに接続されて自動的にハッキングされ、コンピュータにマルウェアを感染させます。また、小包の未配達通知のメールを送信し、添付されたトラッキング用書類を開くとマルウェアに感染する仕組みになっている手口もあります。

マルウェアとは

ソーシャルエンジニアリング攻撃は、電話などを通じて行われることもあります。例えば、ハッカーはマイクロソフトの技術サポートのふりをして電話をかけ、あなたのコンピュータがマルウェアに感染していると伝えます。これは嘘で、コンピュータは実際問題ありません。電話の目的は、感染していると信じ込ませて、リモートからシステムへアクセスできる許可を得たり、セキュリティソフトと偽ってマルウェアを買わせたりすることです。常識で考えましょう。もし不審な電話があって、それが虫のいい話であれば、ソーシャルエンジニアリングの可能性を疑いましょう。

最終的に、マルウェアから身を守るための最善の方法は、利用しているソフトウェアを最新版にして、知名度のあるベンダーの信頼できるアンチウィルスソフトをインストールし、コンピュータがマルウェアに感染するような仕組みに騙されないように警戒することです。

詳しくは

毎月発行のセキュリティアウェアネスニュースレター「OUCH!」をご活用ください。また、OUCH!のアーカイブで過去のトピックも参照できます。詳しくは、SANSセキュリティアウェアネスソリューションのサイトをご覧ください。

http://www.securingthehuman.org

日本語版翻訳チーム

日本語版翻訳ーNRIセキュアテクノロジーズ株式会社

NRI セキュアテクノロジーズは、国内最大の情報セキュリティ専門企業です。マネージドセキュリティサービス、コンサルティング、ソフトウェアソリューションの提供を通じて、情報セキュリティのあらゆる視点からお客様をサポートします。

http://www.nri-secure.co.jp

リソース

OUCH フィッシング攻撃:
www.securingthehuman.org/resources/newsletters/ouch/2013#february2013
OUCH コンピュータを堅牢化する:
www.securingthehuman.org/resources/newsletters/ouch/2012#december2012
ポスター:
http://www.securingthehuman.org/resources/posters

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated By: 坂 恵理子, 関取 嘉浩