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

マルウェアの侵入を阻止する

はじめに

コンピュータウイルスやトロイの木馬、ランサムウェア、ルートキットといった言葉を聞いたことがあるでしょうか。これらは全て、種類は異なりますが、サイバー犯罪者がコンピュータや機器を感染させるために用いる、マルウェアと呼ばれる悪意のあるプログラムです。ひとたびインストールされると、犯罪者が思い通りの操作をできるようになります。マルウェアとは何か、どのような危険をはらんでいるのか、そして最も大事なことである、自分の身を守るために何ができるのかを学びましょう。

マルウェアとは何か

簡単に言うと、マルウェアとは悪意のある操作を実行するソフトウェア/コンピュータプログラムです。悪意のあるという意味のMALICIOUSと、SOFTWAREの2つの単語から成っています。サイバー犯罪者は、あなたのコンピュータや機器にマルウェアをインストールすることで、コントロールを奪います。ひとたびインストールされると、犯罪者はマルウェアを介して、あなたのインターネット上での活動を監視したり、パスワードやファイルを窃取したり、システムを利用して他人を攻撃したりできるようになります。マルウェアはさらに、あなたのファイルの管理権限を奪い、ファイルの返却と引き換えに身代金を要求することまでできてしまいます。多くの人は、マルウェアがWINDOWSコンピュータのみで発生する問題だと考えています。しかし残念ながら、マルウェアはMACコンピュータやスマートフォンからDVRや防犯カメラまで、どのような機器でも感染させることが可能です。より多くのコンピュータや機器を感染させることで、犯罪者はより多く稼ぎ出すことができるのです。つまり、あなたを含む誰もが標的なのです。

自分の身を守る – マルウェアの侵入を阻止する

アンチウイルスソフトウェアのようなセキュリティソフトウェアをインストールすれば、感染は防げると考えているかもしれません。残念ながら、アンチウイルスソフトウェアはマルウェアの侵入を防ぐことができません。サイバー犯罪者は、常に新型でより洗練された、ウイルス検知を回避できるマルウェアを開発しています。同様に、アンチウイルス製品のベンダーはマルウェアを検知するため、新しい機能を追加し、製品を常にアップデートしています。いろいろな意味で現在の状況は、軍備拡張競争のようなものであり、たいていは悪意をもった人たちが一歩前を進んでいます。アンチウイルス製品のみに頼ることはできません。自分の身を守るためにとるべき対策を次に挙げます。

サイバー犯罪者は多くの場合、あなたが使用しているソフトウェアの脆弱性を悪用し、コンピュータや機器を感染させます。使用しているソフトウェアが新しければ新しいほど、あなたのシステムに存在する脆弱性の数は少なくなり、サイバー犯罪者にとって感染させることが困難になります。オペレーティングシステムやアプリケーション、ブラウザ、ブラウザのプラグイン、そして機器が常にアップデートされていて最新であることを確認しましょう。これを達成する一番簡単な方法は、可能な限りいつでも自動アップデート機能を有効にしておくことです。

サイバー犯罪者がコンピュータやモバイル機器を感染させる一般的な方法は、偽物のコンピュータプログラムやモバイルアプリを作成した後、それらをインターネット上に公開し、ダウンロードやインストールをするようあなたを誘導するというものです。プログラムやアプリをダウンロードやインストールする際は、信頼されているオンラインストアのみを利用するようにしましょう。また、新作、肯定的な意見が少ない、滅多にアップデートされない、ダウンロードした人数が少ないといったモバイルアプリは避けるようにしましょう。使用していないコンピュータプログラムやアプリがありますか？あれば削除しましょう。

サイバー犯罪者はよく、自身の代わりにあなたがマルウェアをインストールするように仕向けます。例えば、犯罪者は正当に見えて、添付ファイルかリンクが添えられているメールを送信するかもしれません。おそらくそのメールは、銀行や友人から送付されたものに見えるでしょう。しかし添付ファイルを開いたり、リンクをクリックしたりすると、あなたのシステムにマルウェアをインストールする悪意のあるコードが実行されるかもしれません。もしメールの内容が緊急性を煽るものであったり、出来過ぎた話であったりした場合、それはあなたへの攻撃かもしれません。疑う心を持ちましょう。多くの場合は、常識が最大の防御となります。

定期的にシステムやファイルのバックアップを、クラウドベースのサービスに保存しましょう。もしくは、バックアップを接続されていない外付けドライブのような、オフラインの場所に保存しましょう。こうすることで、マルウェアがバックアップファイルの暗号化や削除を試みた際に、ファイルを守ることができます。バックアップは重要であり、多くの場合、マルウェアによる感染から復旧できる唯一の手段となります。

結局のところマルウェアから身を守る最善の手段は、使用しているソフトウェアや機器を最新の状態に保ち、可能であれば信頼のあるアンチウイルスソフトウェアをインストールし、あなたのシステムを感染させる目的で、あなたをだまそうと試みる悪意ある人物に気をつけることです。全てが失敗した場合、たいていは通常のバックアップが唯一の復旧手段となります。

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、国内でも有数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などの提供を通じて、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

ゲストエディタ

レニー・ゼルツァー氏は、Minerva Labs社においてエンドポイントセキュリティ製品を開発しており、SANS Instituteでは教育に携わっています。Twitter（@lennyzeltser）やセキュリティブログ（zeltser.com）でも情報を発信しています。

リソース

ランサムウェア:	https://www.sans.org/u/EdI
バックアップ:	https://www.sans.org/u/EdN
フィッシングを阻止する:	https://www.sans.org/u/EdS

 Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | **Translated By:** 内山　貴之, 時田　剛