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

# OUCH!

今月のトピック...

- マルウエアとは
- マルウエアは誰が作るのか？
- 自身を守るために

## マルウエアとは

### はじめに

あなたはサイバーセキュリティに関する話を聞く時にウイルス、トロイの木馬、ランサムウエアやルートキットと言う単語を耳にしたことがあるかもしれません。これらは、犯罪者がパソコンや他の機器を感染させるために使うプログラムを表す単語で、このようなプログラムの総称をマルウエアといいます。このニュースレターでは、マルウエアとは何かを解説した上で、どのような人たちがどんな理由でこれらを作成しているのか、最後に一番大事なマルウエアから自身を守る方法を紹介します。

**ゲストエディター**

レニー・ゼルスター氏は、NCR Corp で顧客の IT オペレーションに対するセキュリティ管理を中心に活動していますが、SANS Institute でトレーニングも実施しています。レニーは、ツイッター（@lennyzeltser）や zelster.com にて情報を積極的に発信しています。

### マルウエアとは

広い定義として、マルウエアはソフトウエアまたはパソコン用プログラムの一種で、悪意ある動作を行うために使われます。また、マルウエアという単語は、MALICIOUS（悪意）とSOFTWAREを掛け合わせたものです。サイバー犯罪者は、パソコンや他の機器にマルウエアをインストールすることで乗っ取ったり、保持している情報を窃取したりします。マルウエアがインストールされてしまうと、サイバー犯罪者は、オンライン上での行為を監視したり、ファイルやパスワードを盗んだり、乗っ取ったシステムを使って他のシステムに対する攻撃を行ったりします。マルウエアには、システム内のファイルへのアクセスを拒否したり、それらのファイルへのアクセスをしたい場合は身代金を払うよう要求したりするものもあります。

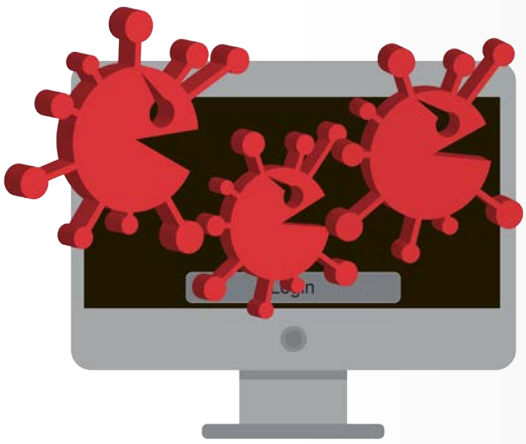
多くの人が誤解してしまいがちですが、マルウエアは WINDOWSパソコンだけの問題ではありません。WINDOWSは、広く使われているために攻撃の標的となることが多いですが、MACパソコン、スマートフォンやタブレットもマルウエアに感染します。サイバー犯罪者が感染させたパソコンや他のデバイスを増やせば増やすほど、多くの利益を得ることができます。ですから、これを読んでいる読者のあなたを含むすべての人が標的となります。

### マルウエアは誰が作るのか？

マルウエアは、今では熟練されたハッカーも作るようになりましたが、以前は趣味の範囲で作成したり、未熟なハッカーが作成したりしていました。彼らの目的は、感染させたパソコンや機器を使って金銭的な利益を得ることです。この場合の利益は、盗んだデータを売ったり、スパムメールを送ったり、サービス運用妨害攻撃を仕掛けたり、ゆすり行為をしたりして得ることになります。マルウエアを作成し、配布して、利益を得る人たちの中には、個人目的で行う人もいれば、組織化された犯罪グループや政府団体もいます。今、出回っている高度なマルウエアを作成し

## マルウエアとは

ている人たちは、日常の仕事として、マルウエアの作成を専門に行っています。さらに、マルウエアが完成したら、他人や他組織に売り、これらの「顧客」に対し、アップデートやサポートを提供しているのです。



怪しいメッセージに疑いを持ったり、デバイスを最新の状態にしたり、最新のアンチウイルソフトウエアをインストールすることで自身をマルウエア感染から守ってください。

### 自身を守るために

自身を守るために多くの人がしている事は、信頼できるベンダが提供するアンチウイルスのソフトウエアをインストールすることです。これらのツールは、アンチマルウエアソフトウエアとも呼ばれ、マルウエアを検知し、止めるために作成されています。しかしながら、アンチウイルスソフトウエアは、すべての悪意あるプログラムをブロックしたり削除したりすることができません。サイバー犯罪者は、検知をさけるために新しい、高度なマルウエアを考えだし、開発しているからです。それに対してアンチウイルスソフトウエアの開発者は、これらのマルウエアを検知できるよう製品に機能を追加したりアップデートを提供したりしています。結局、激しい競争をしていることになっており、片方が相手に被ることを常に試みている状態です。現在は、残念なことにサイバー犯罪者の方が一歩上を行っている状況であり、アンチウイルスのみに頼ることができないため、以下に自身を守るためにできることを列挙しました：

- サイバー犯罪者は、ソフトウエアに含まれる脆弱性を悪用してパソコンやデバイスを感染させることが多いです。ソフトウエアのバージョンが最新に近ければ近いほど、悪用可能な脆弱性の数が減ることになり、サイバー犯罪者によって感染させられる確率も減ります。そのため、オペレーティングシステム、アプリケーションおよび機器の設定でアップデートが自動的に適用される設定に変更してください。
- サイバー犯罪者がモバイルデバイスを感染させるために良く使う手口は、偽のモバイルアプリを作成してインターネット上で公開し、ユーザを騙すことでダウンロードさせインストールさせようとします。このため、信頼できるオンラインショップからのみアプリをダウンロードし、インストールするようにしてください。さらに、モバイルアプリの中でも長らく公開されているもの、ダウンロード数が多いもの、そして良いレビューが多くあるものを選ぶようにしてください。
- パソコン上では、権限のある「管理者」や「ROOT」アカウントを利用せず、権限に制限のある通常アカウントを利用してください。これによって、多くのマルウエアがインストールされなくなり、追加の保護とすることが期待できます。
- サイバー犯罪者は、ユーザを騙してマルウエアをインストールさせる事が多いです。例えば、正式なメールに似せたリンクまたは添付ファイル付きのメールを送りつけます。このメールは、銀行や友人を騙っていたりします。しかし、この添付ファイルを開いたり、リンクをクリックしたりした場合、マルウエアをインストールするための悪意あるコードが実行されます。メールの内容が、緊急性を要したり、分かりづらかったり、話が出来過

## マルウエアとは

ぎていたりした場合は、攻撃の可能性があります。まずは、疑ってみてください。この場合は一般常識を持つことが最大の防御です。

- システムやファイルを定期的にクラウドサービスや外付けのハードディスクなどのオフラインストレージにバックアップとして保存してください。こうすることで、バックアップデータをマルウエアによる暗号化や削除の試みから保護することができます。バックアップは重要です。マルウエア感染からのリカバリは、バックアップを活用する方法しかない場合が多いです。

最終的にマルウエアから守るための最良の方法は、ソフトウエアを最新のバージョンに保ち、広く知られているベンダが提供している信頼できるアンチウイルスソフトウエアをインストールし、システムを感染させようとしている試みには十分注意することです。

## 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

| | |
|---|---|
| フィッシングについて: | https://securingthehuman.sans.org/ouch/2015#december2015 |
| ソーシャルエンジニアリングについて: | https://securingthehuman.sans.org/ouch/2014#november2014 |
| モバイルアプリをセキュアに利用するには: | https://securingthehuman.sans.org/ouch/2015#january2015 |
| タブレットを安全に使用するには: | https://securingthehuman.sans.org/ouch/2016#january2016 |
| バックアップと復旧: | https://securingthehuman.sans.org/ouch/2015#august2015 |



**Editorial Board:** Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
**Translated By:** 内山　貴之, 時田　剛