SANS SECURING THE HUMAN
NRI SECURE TECHNOLOGIES

OUCH! | 2014 年 12 月

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...

ウイルス対策とは？

はじめに

ゲストエディター

ジェイク・ウイリアムズ氏は、Rendition Infosec (www.renditioninfosec.com)の創設者で、SANS認定講師でもあり、コースの作成も担当しています。ツイッター (@MalwareJake)やmalwarejake.blogspot.comのブログでも積極的に情報発信をしています。

アンチウイルスソフトは、パソコンやモバイル機器をマルウェア感染から守るためにインストールするセキュリティアプリケーションです。マルウェアという単語は、悪意あるソフトウェア、例えばウイルス、ワーム、トロイの木馬やスパイウェアなどの総称として使われており、MALICIOUS(悪意)とSOFTWARE(ソフトウェア)という単語を単純に掛け合わせたものです。パソコンがマルウェアに感染すると、サイバー攻撃者によって、キー入力の内容を取得されたり、ドキュメントを盗んだり、パソコンを踏み台にして別の多くのパソコンに攻撃を行われたりします。一般に考えられていることとは異なり、すべてのOS、MACOSやLINUXも含め、マルウェアに感染することがあります。

現在、サイバー攻撃者が新種のマルウェアを作成し、配布するスピードにアンチウイルスソフトがついていけてない問題があります。毎日のように新しいバージョンのマルウェアがリリースされているため、どんなアンチウイルスソフトを持ってしてもすべてのマルウェアを検知して防御することは不可能です。アンチウイルスソフトは、単品またはセキュリティパッケージの一部として購入することが可能ですが、すべてのマルウェアを検知して防御することは不可能だという理由を理解しておく必要があります。

アンチウイルスソフトの仕組み

アンチウイルスソフトがマルウェアを特定する手法は、シグニチャー検知とふるまい検知の二つがあります。シグニチャー検知は、人間の持つ免疫機構に似ています。パソコンをスキャンし、既知の悪意あるソフトウェアの特徴を探します。既知マルウェアの特徴とパソコン上のシグニチャーに収録された特徴が同じパターンを持つ場合、アンチウイルスソフトがマルウェアの無効化を試みます。人間の持つ免疫機構と同じで、このシグニチャーは新たなマルウェアを防御するために、インフルエンザの予防注射のような更新が必要です。アンチウイルスソフトは、悪意あるものと判断できるものに対してのみ防御が行われます。ここで問題となるのは、サイバー攻撃者が早いスピードで新たなマルウェアを作成し、アンチウイルスソフトの開発者がシグネチャーの更新についていけないことです。結果として、アンチウイルスアプリケーションがどんなに最近シグネチャーを更新したものであっても、新種のマルウェアによってアンチウイルスソフトの防御をすり抜けることができてしまうのです。

ウイルス対策とは?

ふるまい検知では、既知のマルウェアを特定することはせず、インストールされているソフトウェアの挙動を監視します。そのかわり、アプリケーションが保護されているファイルへのアクセスや他のアプリケーションに変更を加えるなどの不審な挙動を示すと警告を出す仕組みです。この手法は、シグニチャーに存在しない新種のマルウェアに対する防御ができることです。しかし、この手法には誤判定の可能性があるという問題があります。ユーザは、アプリケーションのふるまいのうち、許可していいものと禁止すべきものの判断ができないだけでなく、時間の経過とともに様々な警告に無関心になってしまうことが挙げられます。すべての警告に対し、承認ボタンを押すという誘惑にかられると、アンチウイルスソフトが導入されているにも関わらず、攻撃の被害を受けやすくするだけでなく感染する確率も上げてしまうことになるのです。また、ふるまいが検知された時点で、マルウェアはパソコン上で実行されている可能性が高く、アンチウイルスソフトによって検知される前までの感染経路や実行までの挙動を知ることは困難です。

アンチウイルスソフトは、セキュリティ確保のために重要ですが、すべてのマルウェア感染や攻撃を防ぐことはできません。最終的には、テクノロジーだけではなく、ユーザ自身が最大の防御策となります。

アンチウイルスソフトは、パソコンやモバイル機器をセキュアにするために重要であり、インストールおよび活用することを推奨します。覚えておかなければならないのは、どんなアンチウイルスソフトを使っていても、すべてのマルウェアからは保護されないことです。最終的には、テクノロジーだけではなく、ユーザ自身が最大の防御策となることを忘れないでください。

ウイルス対策におけるアドバイス：

1. アンチウイルスソフトは、よく知られていて、信用できるベンダから取得してください。サイバー攻撃者は、よく偽物をマルウェアとして配布しています。
2. アンチウイルスソフトの最新バージョンがインストールされていることを確認し、定期利用の契約がされている状態にした上で、アプリケーションが自動更新される設定にしてください。パソコンが長い時間オフラインの状態または電源を入れていなかった場合は、改めてオンライン状態または電源を入れた時、アンチウイルスソフトを更新する必要があります。更新が行われている間は強制的に中止または中断しないでください。
3. アンチウイルスソフトは、USBメモリのような取り外し可能なメディアを自動的にスキャンする設定をし、リアルタイム保護を有効にしてください。
4. アンチウイルスソフトが出す警告に気を配ってください。多くの警告には、追加情報や推奨事項を取得するオプションがあります。業務用の端末で警告が出た場合は、速やかにヘルプデスクや上司に報告してください。
5. パソコンのパフォーマンスが低下するから、ウェブサイトをブロックしているから、他のアプリケーションのインス

ウイルス対策とは?

トール妨げている原因だからという理由で、アンチウイルスソフトを無効にしたり、アンインストールしたりしないでください。アンチウイルス機能を無効にすることで不要なリスクに晒され、重大なセキュリティインシデントが起きる可能性があります。業務用の端末で問題が続く場合は、アンチウイルスソフトのベンダに連絡を取ってみたり、ウェブサイトから情報を取得したり、別の製品に乗り換えるなどを検討してください。

6. 同時に複数のアンチウイルスソフトを同じパソコンにインストールしないでください。これにより、アンチウイルスソフト同士が衝突を起こし、パソコンのセキュリティが低下する可能性があります。
7. アンチウイルソフトの警告を正しく見分けられるように努力してください。サイバー攻撃者は、本物に似た警告を表示する悪意あるウェブサイトを立ち上げ、パソコンを修復できるとユーザに訴えますが、これは偽物です。これらのウェブサイト上にあるリンクやボタンをクリックすることでパソコンに悪影響を与えることがあります。

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

アンチウイルスソフトの製品比較:	http://www.av-test.org/en/
ソーシャルエンジニアリングとは:	http://www.securingthehuman.org/ouch/2014#november2014
メールを使ったフィッシング攻撃:	http://www.securingthehuman.org/ouch/2013#february2013
ハッキングされました、どうすれば良いでしょうか?:	http://www.securingthehuman.org/ouch/2014#may2014

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