

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●Google、WebサイトおよびChromeによる「望ましくないソフト」に対する取り組みを強化

http://www.forest.impress.co.jp/docs/news/20150224_689820.html
<https://www.google.com/about/company/unwanted-software-policy.html>



このニュースをザックリ言うと…

- 2月23日（現地時間）、米Google社は、同社サイトの検索結果・広告表示およびChromeブラウザにおいて行っている、安全でないサイトからユーザを保護する「セーフブラウジング」機能の新たな取組みについて発表しました。
- 同社では、「別のプログラムのインストールに便乗する」「ユーザが気付かないうちに個人情報を送信する」「簡単に削除できない」等のユーザの利便性に悪影響を及ぼす問題点を持つソフトウェアを「望ましくないソフトウェア」と定義しています。
- Chromeでは「望ましくないソフトウェア」を配布するサイトへアクセス時に警告を表示してダウンロードを防止する機能が搭載されるようになり、一方でGoogleのサイトにおいても、そういったWebサイトへ誘導する検索結果や広告を無効化する取組みを進めているとのこと。

AUS便りからの所感等

- 無料でインストールできるフリーウェア、特に海外製のものには、密かに不正な挙動を行うマルウェアまがいのソフトウェアがバンドルされ、本来の目的であるソフトウェアのインストール時にそれらのインストールを行うかを尋ね、明確に拒否する選択をせずに「次へ」をクリックすると、それらのソフトウェアもインストールされてしまうことがしばしばあります。
- また、ソフトウェアをダウンロードしようとする際、本家のサイトや実績のあるダウンロードサイト以外に、不審なサイトが検索上位や広告に表示されることも珍しくなく、そこからダウンロードしたインストールにやはり不正なソフトウェアが含まれるというケースも散見されます。
- ソフトウェアのダウンロードとインストール時には十分な情報収集を行い、またインストール実行時に余計なソフトウェアをインストールしないような選択方法の情報も参照することが重要です。
- Chromeだけでなく、多くのブラウザに搭載されている安全なブラウジングを行う機能、あるいはアンチウイルス・UTMによる同様の機能も活用するのが良いでしょう。

The screenshot shows a news article on the '窓の杜' (Windows Forest) website. The article title is 'Google、「Google Chrome」での望ましくないソフトに対する取り組みを強化' (Google strengthens measures against unwanted software in Google Chrome). The text discusses Google's policy on unwanted software, mentioning that such software is often bundled with legitimate software and can be installed without the user's knowledge. It also notes that Google is blocking search results and ads for these sites. A small image shows a warning dialog box from Chrome: 'This site contains harmful programs'.

Googleは、同社が「望ましくないソフトウェア」と判定するソフトのほぼ全てに、以下に引用した項目の中から最低1つは当てはまるものがあるとしている。

- ◆表示に虚偽がある。すなわちできていないことをできると約束している。
- ◆ユーザーをインストールに強制的に誘導しようとする、または別のプログラムのインストールに便乗する。
- ◆ユーザーにメインとなる重要な機能をすべて説明しない。
- ◆ユーザーのシステムに予期しない方法で影響を与える。
- ◆簡単に削除できない。
- ◆ユーザーが気付かないうちに個人情報を収集または送信する。
- ◆他のソフトウェアとバンドル（同梱）され、その存在が開示されていない。

(以上、同社の日本語版Webページ内の「望ましくないソフトウェアのポリシー」より引用)

● 楽天市場の偽サイト2500件以上確認、楽天が注意呼び掛け

<http://www.itmedia.co.jp/news/articles/1502/17/news061.html>

<http://www.yomiuri.co.jp/it/security/goshiniyutsu/20150227-OYT8T50119.html>



このニュースをザックリ言うと…

- 2月17日(日本時間)、大手ショッピングモール「楽天市場」を運営する楽天株式会社(以下、楽天)が楽天市場になりました偽サイトが多数確認されたことを発表し、偽サイトのURLリストを公開しています。

- リストに掲載されているサイトは、閉鎖されたものも含め2月27日の段階で2619件に上っており、検索サイトで「〇〇(商品名) 激安 楽天」等と検索すると上位に表示されるケースもあるとされています。

- 楽天では、これらのサイトのURLを確認し、またそこから「日本の楽天市場へアクセス」等と書かれた偽のリンクをクリックしたり、表示されたフォームへの個人情報・クレジットカード番号・アカウント情報等の入力を行ったりしないよう呼びかけています。



AUS便りからの所感等

- 素性の知れない、見慣れないショッピングサイトで安易に物を購入しようとしないうこと、普段利用しているサイトへのアクセスのほすが偽サイトに誘導されていないか確認し、またはそういったサイトへはブックマークからアクセスすることが重要です。

- ブラウザやセキュリティソフトあるいはUTMのアンチフィッシング機能を有効活用することも、偽サイトへのアクセスを食い止める一助になることでしょう。

● 「my_sexy_photo.exe」「my_new_photo.exe」を開くと感染、5年前のウイルスが日本で検出増

http://internet.watch.impress.co.jp/docs/news/20150227_690447.html

http://canon-its.jp/eset/malware_info/news/150227/



このニュースをザックリ言うと…

- 2月27日(日本時間)、スロバキアのアンチウイルスベンダーであるESET社は「Win32/Agent.QKJ」と呼ばれるウイルスの検出が2月16日以降急増していることを発表しました。

- Win32/Agent.QKJは、メールに添付される「my_sexy_photo.exe」「my_new_photo.exe」といった名前の添付ファイルを実行することで感染するという古典的な感染方法をとるトロイの木馬型ウイルスです。

- Win32/Agent.QKJは2009年11月に初めて確認され、2014年以降大量の亜種が発生しており、日本とクロアチアで特に感染が拡大しているとのこと。

AUS便りからの所感等

- 興味を引くような名前でファイルを開かせウイルスに感染させようとする手口は、先にも書いたとおり非常に古典的であり、それこそ20世紀から存在するものですが、依然として少なからぬ被害がもたらされているようです。

- ユーザのうっかりした行動からPCとネットワークを防御するためにも、アンチウイルス・UTMの利用は決して欠かせないものです。

INTERNET Watch

最新ニュース

クラウド会計ソフト利用開始は会計ソフト利用増全体の73%、発生が調査結果公開 2015/02/26

経路省、光回線を利用した光回線サービスの電話勧誘でU-NEXTとHi-Bitを指導 2015/02/27

Twitterが悪意ユーザー対策を強化、なりすましなどの報告が簡単に 2015/02/27

ウェブユーザーが「花粉フォック」開発、くしゃみ回数をカウントするウェアラブルデバイス 2015/02/27

ダークル、「日本の総選挙天候」のストリートビュー公開、入浴中の浴(サリ以外)も 2015/02/27

ニュース

「my_sexy_photo.exe」「my_new_photo.exe」を開くと感染、5年前のウイルスが日本で検出増 (2015/2/27 15:21)

スロバキアのセキュリティベンダーであるESETは、ウイルス「Win32/Agent.QKJ」の検出数が2月16日から急増していることを発表した。主に日本とクロアチアが顕著だとしている。2009年11月に初めて検出されたウイルスだが、2014年以降に亜種が多数登場しているという。

「Win32/Agent.QKJ」の検出状況。日本とクロアチアで急増しているという(画像はESET Virus Radarより引用)