― ＡＵＳ（アルテミス・ユーザ・サポート）便り 2014/09/22号 ―

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。

●「ヤフオク！」と「Amazon」の偽フォームを表示するウイルス、カード情報入力を要求

http://www3.nhk.or.jp/news/html/20140919/k10014733101000.html
http://topic.auctions.yahoo.co.jp/notice/other/important/post_1060/

このニュースをザックリ言うと･･･

- 9月18日、国内最大手のネットオークションサイト「ヤフオク！」のクレジットカード情報を詐取するウイルスが確認されたとして、運営するヤフー株式会社が注意を呼びかけています。
- 同社の警告ページでは、ウイルスに感染した状態で「ヤフオク！」のサイトにアクセスした際、偽のフォームが表示され、クレジットカード番号・有効期限およびセキュリティコードといった情報の入力を要求するという例が挙げられています。
- ウイルスを解析したセキュリティ関係者によれば、ネット通販大手「Amazon」についても、同様のフォームを表示するウイルスが確認されている模様です。

AUS便りからの所感等

- これまでにも確認されていた、銀行のネットバンキングサイトへのアクセス時に偽のフォームを表示するウイルスの亜種と考えられ、今後さらに別のサイト等についても、クレジットカード情報等を詐取する同種のウイルスが発生することは十分に考えられます。
- 通常利用しているサイトにおいて運営からの警告情報に随時目を通し、これまでに要求されなかった場面で不審な入力を求めるフォームが表示された場合に、安易に情報を入力しないよう注意を払うこと、そして何よりも、アンチウイルスとUTMにより、PCにウイルスが感染しないようにすることが重要です。

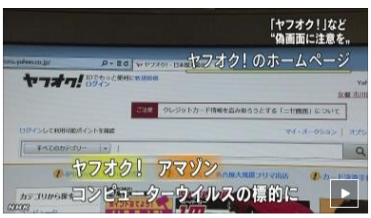
NHK NEWSWEB　2014年(平成26年)9月20日[土曜日]

トップページ ＞ 社会ニュース一覧 ＞ 「ヤフオク！」と「アマゾン」で偽画面 注意を

ニュース詳細

「ヤフオク！」と「アマゾン」で偽画面 注意を

9月19日 18時12分



ネットオークション国内最大手の「ヤフオク！」などが、偽の画面を表示することでクレジットカードの情報を盗み取るコンピューターウイルスの標的となっていることが初めて確認され、運営会社が注意を呼びかけています。

コンピューターウイルスの標的となっていたのは、ネットオークション国内最大手の「ヤフオク！」とインターネット通販大手の「アマゾン」です。

「ヤフオク！」を運営する「ヤフー」によりますと、ウイルスに感染したパソコンで本物のサイトを閲覧していると、利用者にクレジットカード番号や有効期限などを入力するよう求める偽の画面が表示されるようになっていることが分かったということです。

19日現在で、利用者からの被害の報告はないということですが、ヤフーでは、「ヤフオク！」のトップページに注意喚起するコメントを掲載し、「ふだんと違う画面が表示されたら、カード情報は入力せず、ウイルス対策ソフトを導入するなどして被害に遭わないよう注意してほしい」と呼びかけています。

また、このウィルスを解析したセキュリティ関係者によりますと、インターネット通販大手の「アマゾン」のサイトも、同じ手口で標的になっていたということです。

こうした手口は、カード会社のサイトやインターネットバンキングなどでも確認されていて、盗まれた情報をもとに高額な買い物をされたり、預金が不正に送金されたりする被害が相次いでいます。

以下のニセ画面例のような画面が表示された場合は、お客様情報の入力は絶対に行わないでください。

ニセ画面（一例）

上記はあくまでも「ニセ画面」の一例です。ヤフオクでは、身元確認などの理由で、お客様にクレジットカード情報を入力いただくことはございません。
ニセ画面例に限らず、ニセ画面と思われる画面が表示された場合は、個人情報を絶対に入力しないでください。

●Adobe ReaderとAcrobatに脆弱性 - JPCERT/CCが注意喚起

http://news.mynavi.jp/news/2014/09/18/157/
https://www.jpcert.or.jp/at/2014/at140036.html

このニュースをザックリ言うと・・・

- 9月17日(現地時間)、Adobe社が提供するPDFリーダー「Adobe Reader」の脆弱性に対し、同社から修正バージョンがリリースされ、また、JPCERT/CCから脆弱性についての警告を行っています。
- メールで送信あるいはWeb上からダウンロードした不正なPDFファイルをAdobe Readerで開くことにより、脆弱性を悪用され、最悪の場合PCを乗っ取られる可能性があります。
- 脆弱性が存在するのは「Adobe Reader XI (11.0.08)」「Adobe Reader X (10.1.11)」およびそれら以前のバージョンとなっており、「11.0.09」および「10.1.12」で修正されています。
- なお、同社のPDF作成ツール「Acrobat」にも同様に脆弱性が報告されています（問題のあるバージョンおよび修正バージョンはAdobe Readerと同様です）。

AUS便りからの所感等

- Adobe Reader（およびAcrobat）は、同じAdobe社のFlash Playerと同様に脆弱性を狙われやすいプロダクトであり、今年に入ってから1月、5月および8月に修正バージョンがリリースされています。
- 特に注意が必要なのは、Adobe Readerがブラウザのプラグインとして動作している場合で、悪意のあるサイトに誘導されることにより、自動的にPDFファイルを開き、脆弱性を突かれる可能性があり、できる限りブラウザの設定においてプラグインを無効化しておくのが安全です。
- Adobe Reader Xより前のバージョン、例えばバージョン9については2013年6月26日にサポートを終了しているため、これらを利用している場合はX以降へのアップデートが必須です。
- セキュリティを考慮する目的で、他のPDFリーダーソフトウェアや、FirefoxやChromeが備える独自のPDFリーダーに乗り換えるアプローチも考えられますが、よほど慣れたユーザでない限り、PDF表示時の再現性や操作性を考慮すると簡単に乗り換えられるものではないでしょう。
- そういった利便性を損ないたくなければ、速やかに最新バージョンにアップデートし、またそれまでの間に攻撃を受ける可能性を考慮し、アンチウイルス・UTMによる防御を十分に固めることが必要となります。

●TwitterでChromeの不正な拡張プログラムが拡散される

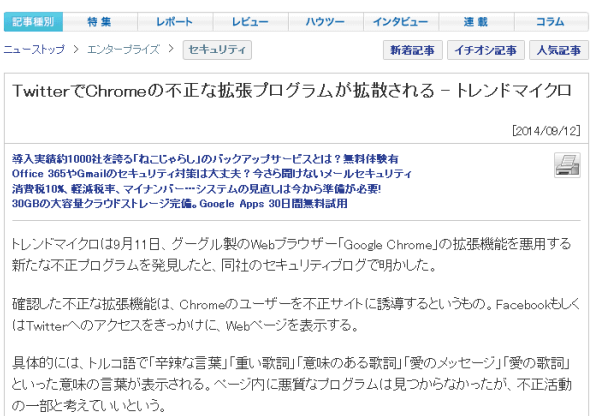
http://news.mynavi.jp/news/2014/09/12/174/
http://blog.trendmicro.co.jp/archives/9869

このニュースをザックリ言うと・・・

- 9月11日(現地時間)、大手セキュリティベンダーのトレンドマイクロ社は、Twitter上でWebブラウザ「Google Chrome」のアドオンに偽装したマルウェアをインストールさせようとする不正行為を確認したと発表しました。
- Chromeにおいては、悪意のあるアドオンのインストールを防止するため、Google社が運営する「Chrome ウェブストア」からのみダウンロード・インストール可能となるよう制限されていますが、今回確認されたマルウェアは、Windowsソフトウェアのインストーラーとして動作し、Chromeのディレクトリ上に悪意のあるファイルをインストールすることにより、制限を回避する模様です。
- マルウェアがインストールされたChromeでFacebookやTwitterにアクセスすることにより、トルコ語で書かれた不正なWebサイトが表示され、さらなる不正行為への誘導が目的と推測されています。

AUS便りからの所感等

- 記事を見る限りでは、ブラウザの拡張機能インストールにおけるセキュリティ制限の回避方法として、「ユーザーに不正なインストーラーを実行させる」という方法をとっているに過ぎませんが、非常にシンプルなだけに見落としがちであるという見方もできるでしょう。
- また、インストーラーをダウンロードさせるサイトへのリンクは短縮URLによって巧妙に隠されていたとのことです。
- ともあれ、こういったシンプルな攻撃からの防御のため、アンチウイルスやUTMの導入、そしてそういった不審なファイルを安易にダブルクリックしないという情報リテラシーの啓発は基本中の基本として押さえておくべきことです。


記事種別 特集 レポート レビュー ハウツー インタビュー 連載 コラム
ニュートップ > エンタープライズ > セキュリティ
新着記事 イチオシ記事 人気記事
TwitterでChromeの不正な拡張プログラムが拡散される - トレンドマイクロ
[2014/09/12]
導入実績約1000社を誇る「ねこじゃらし」のバックアップサービスとは？無料体験有
Office 365やGmailのセキュリティ対策は大丈夫？今さら聞けないメールセキュリティ
消費税10%、軽減税率、マイナンバー…システムの見直しは今から準備が必要!
30GBの大容量クラウドストレージ完備。Google Apps 30日間無料試用
トレンドマイクロは9月11日、グーグル製のWebブラウザー「Google Chrome」の拡張機能を悪用する新たな不正プログラムを発見したと、同社のセキュリティブログで明かした。
確認した不正な拡張機能は、Chromeのユーザーを不正サイトに誘導するというもの。Facebookもしくは Twitterへのアクセスをきっかけに、Webページを表示する。
具体的には、トルコ語で「辛辣な言葉」「重い歌詞」「意味のある歌詞」「愛のメッセージ」「愛の歌詞」といった意味の言葉が表示される。ページ内に悪質なプログラムは見つからなかったが、不正活動の一部と考えていいという。