— AUS（アルテミス・ユーザ・サポート）便り 2018/02/19号 —
https://www.artemis-jp.com

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。

●不正なChromeアドオンに含まれるマルウェア「DROIDCLUB」、ユーザ42万人に影響か

https://forest.watch.impress.co.jp/docs/news/1105504.html
http://blog.trendmicro.co.jp/archives/16971

このニュースをザックリ言うと･･･

- 2月7日（日本時間）、トレンドマイクロ社より、Google Chromeブラウザにマルウェア「DROIDCLUB」を含む不正なアドオンをインストールさせる手口が確認されたとして、同社ブログで警告が出されています。

- 警告によれば、不正な広告とソーシャルエンジニアリングによって、「Chrome ウェブストア」上にあるアドオンをインストールするようを誘導され、インストール後はDROIDCLUBが指令サーバからの指令を受け、閲覧するページに不正な広告を挿入したり、仮想通貨のマイニングを行う「Coinhive」を実行するとしています。

- また、Chromeの管理ページからアドオンをアンインストールしようとすると、偽の管理ページにリダイレクトする等して、あたかもアンインストールされたかのように偽装する機能を持つとのことです。

- DROIDCLUBを含むアドオンはChromeウェブストアにおいて89個確認され、最大423,992人のユーザが影響を受けたとしておりますが、トレンドマイクロ社はGoogle等に連絡を行い、これらは全て削除されたとしています。

AUS便りからの所感等

- Googleはトレンドマイクロ社とのやりとりにおいて、「毎月1000以上の不正なアドオンをブロックしている」と回答しています。

- 悪意を持ったアドオンがひとたびブラウザに侵入すれば、広範囲にわたって不正行為を行うことが可能になる訳であり、これまで無害だったアドオンが買収・売却によって開発・提供母体が変わり、不正行為を行うような改変が行われるケースも珍しくありません。

- トレンドマイクロ社では、「不正な広告を表示しないようスクリプトブロッカーなどのツールを使うこと」「組織内においてはシステム管理者がポリシーを設定してユーザがアドオンをインストールできなくすること」等の対策を推奨しています。

- スマホアプリやTwitterと連携するアプリ等でも言えることですが、「ネット上の評判を十分に確認すること」「インストールは必要最低限に留めること」等が重要です。

窓の杜

Chrome ウェブストアで"消せない"マルウェア「DROIDCLUB」が拡散、42万人に影響か

勝手に広告や暗号通貨のマイニングコードを挿入 ～トレンドマイクロが注意喚起

樽井 秀人　2018年2月8日 12:43

ツイート リスト　いいね！ 113　シェア　B! 32　Pocket 83

「DROIDCLUB」と呼ばれるマルウェアが広がりを見せているという。トレンドマイクロ（株）は、7日に公開した公式ブログの記事で注意を喚起している（英文記事は1日）。

トレンドマイクロの公式ブログ

「DROIDCLUB」は不正広告とソーシャルエンジニアリングを組み合わせた手法によって拡散する。ユーザーが不正な広告サーバーへアクセスすると、「Google Chrome」の拡張機能をインストールするように促すメッセージが現れる。これを受け入れてしまうと、不正な拡張機能が「Google Chrome」に侵入し、C&Cサーバーの指示でさまざまな活動を行うようになる。同社によると、閲覧ページへ勝手に広告を挿入したり、「Coinhive」を注入して暗号通貨のマイニングを行うケースが確認されているという。

TREND MICRO　トレンドマイクロ セキュリティブログ　POWERED BY TrendLabs

不正な Chrome 拡張機能「DROIDCLUB」、正規ストア利用者 42 万人に影響か

投稿日: 2018年2月7日
脅威カテゴリ: 不正プログラム
執筆: Fraud Researcher - Joseph C Chen

トレンドマイクロの「Cyber Safety Solutions チーム」が、数百万ユーザに影響を与える Chrome の不正な拡張機能（「BREX_DCBOTA」として検出）を確認しました。利用されている最も古い C&C サーバにちなんで「DROIDCLUB（ドロイドクラブ）」と名付けられたこのマルウェア（ボット）は、Chrome の拡張機能として拡散し、ユーザが訪問した Web サイトに広告や仮想通貨発掘コードを注入します。

上述した機能に加え、DROIDCLUB は正規のセッションリプレイライブラリを悪用し、ユーザのプライバシーを侵害します。このライブラリはユーザが訪問するすべての Web サイトに注入されます。セッションリプレイ機能は、本来 Web サイトの保有者がユーザが閲覧した画面や入力内容などを知ることができるように、Web サイトにおけるユーザの行動を再現するためのものです。このようなライブラリが悪用される可能性についてリサーチャも注意喚起していましたが、実際に悪用が確認されたのは今回の事例が初めてです。

攻撃者は、「malvertisement（不正広告）」とソーシャルエンジニアリングを組み合わせた手法によってユーザに DROIDCLUB をインストールさせます。この不正な拡張機能は、公式の Chrome ウェブストアで合計 89 個確認されています。これらの不正な拡張機能の詳細ページの情報によると、最大 423,992 人のユーザが影響を受けたと推定されます。Google は既に公式の Chrome ウェブストアからこれらの不正な拡張機能を削除しています。また、Cloudflare のサービスを利用していた DROIDCLUB のコマンド&コントロール（C&C）サーバも削除されています。

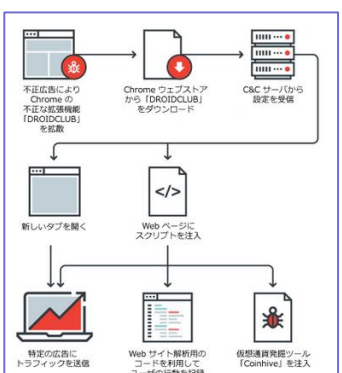


図 1：DROIDCLUB の感染の流れ

●件名「2月度発注書送付」のウイルスメール拡散、警視庁等警告

https://twitter.com/nisc_forecast/status/963939027547185153

このニュースをザックリ言うと・・・

- 2月14日（日本時間）、警視庁や内閣サイバーセキュリティセンターおよび日本サイバー犯罪対策センター（JC3）より、ウイルスが添付されたメールが同日より拡散しているとして警告が出されています。

- 拡散しているメールは、
◆件名が「Re: 2月度発注書送付」「Re: Re: 2月度発注書送付」「Fwd: Re: 2月度発注書送付」のいずれか
◆本文が「いつも大変お世話になっております。2月度の発注書を添付資料にてお送りさせていただきます。」または空のもの
◆さらに「2018.02[ユーザー名].xls」等が添付されています。

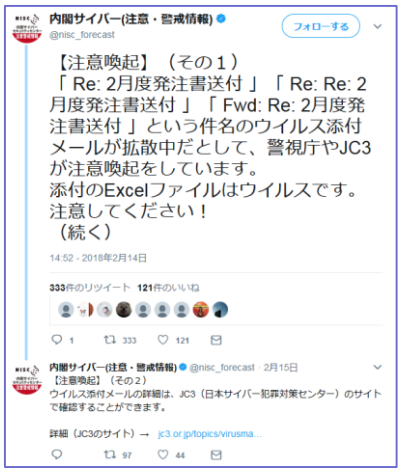
AUS便りからの所感等

- 国内のオンラインバンキングやクレジットカード利用者を狙うマルウェア「URSNIF(gozi)」への感染を意図したものであるとされています。

- 一見違和感がない文面のメールであるものの、全く同様のパターンのメールが昨年12月27日にも出回っており、JC3から警告が出ています。

- JC3のサイトではこれまでに出回っている日本語のウイルスメールの情報が随時更新されており、定点観測のための情報源として、これらのページを随時チェックし、そこで見たことがあるような不審なメールが受信された場合に慎重に行動できるよう備えましょう。

- 一方で特定の組織を狙う「標的型攻撃」では、本物の取引メールを盗み見て偽装メールを送る等が行われる可能性もあり、様々な攻撃の手口を知り、OS・各種ソフトウェア・そしてアンチウイルスのパターンファイルを最新に保ち、さらにUTMの設置による不審なメールの遮断と多層防御を行うことが肝要です。



●平昌五輪公式サイト等、開会式の最中にサイバー攻撃でダウン

http://www.itmedia.co.jp/enterprise/articles/1802/13/news048.html

このニュースをザックリ言うと・・・

- 2月11日（日本時間）、韓国・平昌冬季オリンピック組織委員会より、五輪公式サイトがサイバー攻撃を受け、一時的にダウンしていたと発表されました。

- ダウンしていたのは9日20時に開会式が始まる直前の19時15分頃から翌10日8時頃までの約12時間で、この間サイトから情報の閲覧やチケットの印刷ができなくなった他、五輪スタジアムのWi-Fiやプレスセンターのネットワーク等も障害に見舞われ、開会式においてドローンを飛ばす演出が中止になる等の影響も出たとのことです。

- 米Cisco Systemsのセキュリティ部門Talos等複数のセキュリティ企業では、攻撃がマルウェア「Olympic Destroyer」によって行われたものとし、「開会式の最中にオリンピック委員会に恥をかかせることが目的だった」と推測しています。

AUS便りからの所感等

- Olympic Destroyerのコードには五輪公式サイトの複数のアカウント情報が含まれており、事前にアカウント情報を奪取する等巧妙に攻撃が計画されていたとみられていることから、特定の国がサイバー攻撃に関与している可能性を指摘する声もあります。

- ともあれ、オリンピックのような大きなイベントにはそれに便乗して人々を騙す攻撃から今回のようなサイバー攻撃まで、様々な攻撃が行われることは常に繰り返されてきたことであり、特にシステム管理者においては、ニュースを随時チェックし、どういった攻撃が発生しているかを注視し、適宜組織内に注意喚起を行うべきでしょう。