— AUS（アルテミス・ユーザ・サポート）便り 2017/08/21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。

●ファイルスキャンでは検出されない「ファイルレス」なマルウェア…トレンドマイクロが警告

http://blog.trendmicro.co.jp/archives/15653
https://japan.zdnet.com/article/35105733/

このニュースをザックリ言うと・・・

- 8月14日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、ファイルスキャンでは検知されない「ファイルレス」活動を行うマルウェアが確認されたとして警告が出されています。

- 「JS_POWMET(ジェイエスパウメット)」と名付けられたこのマルウェアは、感染したPCのレジストリを書き換えてPC起動時に不正なコマンドを実行するよう登録し、外部のサーバからトロイの木馬「TROJ_PSINJECT.A」を、さらにTROJ_PSINJECT.Aが外部からバックドア「BKDR_ANDROM」を、ダウンロードすることによりPCの情報や管理者権限等を奪取するとされています。

- これらの過程で「ファイルを一時的にディスク上に保存する」という行為を一切行わないのが特徴とのことです。

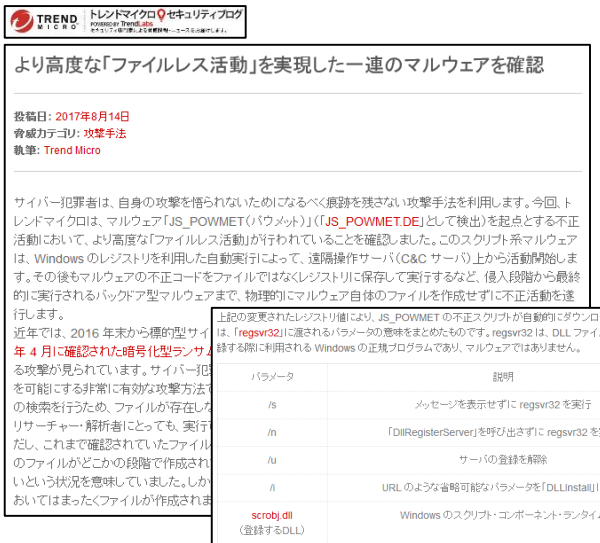
- 同社では、このマルウェアの感染による影響は比較的低いものとしている一方、マルウェア本体や作業用のファイルをディスク上に保存しないことにより、現行のアンチウイルスでの検出・解析を回避しようとする取り組みを示すものとして、ユーザや管理者に対し、さらに注意を払うよう呼び掛けています。

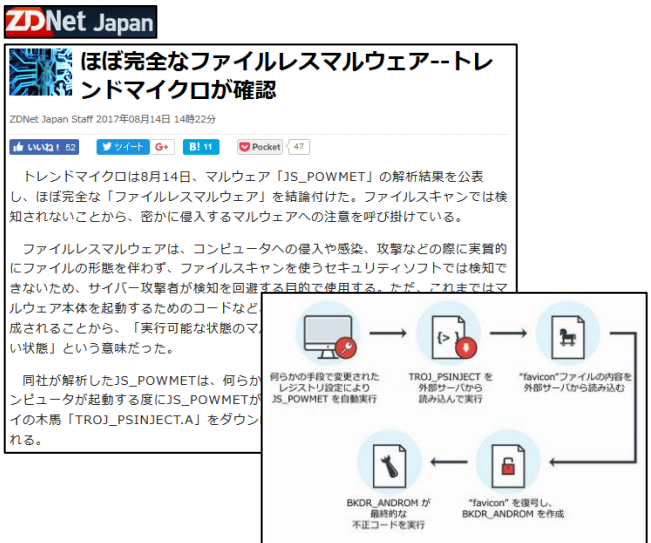
AUS便りからの所感等

- JS_POWMETの特徴は全く新しいものというわけではなく、ファイルレスな形をとるマルウェアとしては「SQL Slammer」が、レジストリの書き換えで不正なプログラムの実行を登録するものとしては「MSBlast」が、いずれも2003年に猛威をふるっています。

- トレンドマイクロ社では、こういったファイルレス型マルウェアへの対策として、レジストリの改ざんなどを検知する挙動監視や、外部からの不正コードの侵入などを検知するWebレピュテーション（ドメイン名やIPアドレスなどの情報からアクセス先の怪しさを判定する技術）型の対策を推奨しています。

- マルウェアが外部サーバとの不正な通信を行うことを食い止められよう、UTMの設置を行い適切な設定を行うと良いでしょう。





●Chromeウェブストアに相次ぎ不正な拡張機能、企業をだます手口に悪用

http://www.itmedia.co.jp/enterprise/articles/1708/17/news044.html

このニュースをザックリ言うと・・・

- 8月15日（現地時間）、米セキュリティ機関SANS Internet Storm Centerより、Google Chromeブラウザ向けの不正な拡張機能がGoogle公式のアプリストアで相次いで見つかっており、これを悪用した攻撃も確認されているとして警告が出されています。

- SANSによれば、その攻撃はブラジルで確認されたもので、銀行の担当者を装った攻撃者が企業の会計担当者に「銀行のセキュリティモジュールの新しいバージョンが公開された」と電話をかけ、アプリストア上にある不正な拡張をインストールするよう誘導するという手口だったとのことで、分析により、この拡張にはユーザが閲覧したWebサイトの全データを読み取り改ざんする機能が含まれ、口座番号やパスワードが詐取されていたとみられます。

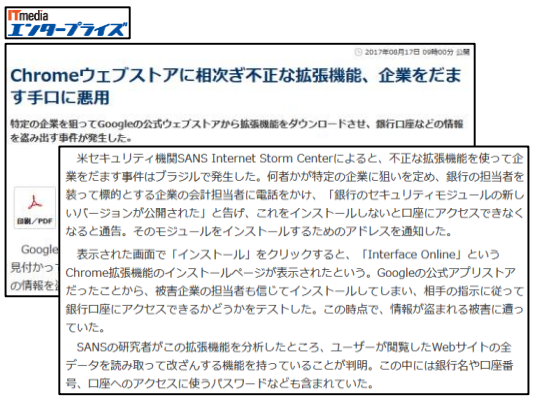
- この他、セキュリティニュースサイトのthreatpostより、過去2週間の間にChromeの人気拡張の少なくとも8本がハイジャックされ、トラフィックの不正操作や広告の挿入に利用されているのが見つかったと報告されています。

AUS便りからの所感等

- ブラウザの拡張はその仕様上ブラウザのほぼ全ての機能を操作し、あるいはデータを読み取ることが可能となっており、このためブラウザ拡張のインストール時には、どの範囲の操作やデータの読み取りを要求するかの警告が表示されます。

- 拡張のアップデート時にも、拡張が要求する範囲が広まった場合には警告が出るため、有名な拡張等でそのような事象が発生した場合は、アプリストアの掲示板あるいはSNS等といったネット上の情報を確認するようにしましょう。

- SANSが報告したようなケースでも同様で、かかってきた電話にそのまま従うのではなく、やはり銀行の公式サイトの情報を確認する等により防衛を図ることが重要です。


ITmedia エンタープライズ

2017年08月17日 09時00分 公開

Chromeウェブストアに相次ぎ不正な拡張機能、企業をだます手口に悪用

特定の企業を狙ってGoogleの公式ウェブストアから拡張機能をダウンロードさせ、銀行口座などの情報を盗み出す事件が発生した。

米セキュリティ機関SANS Internet Storm Centerによると、不正な拡張機能を使って企業をだます事件はブラジルで発生した。何者かが特定の企業に狙いを定め、銀行の担当者を装って標的とする企業の会計担当者に電話をかけ、「銀行のセキュリティモジュールの新しいバージョンが公開された」と告げ、これをインストールしないと口座にアクセスできなくなると通告。そのモジュールをインストールするためのアドレスを通知した。

表示された画面で「インストール」をクリックすると、「Interface Online」というChrome拡張機能のインストールページが表示されたという。Googleの公式アプリストアだったことから、被害企業の担当者も信じてインストールしてしまい、相手の指示に従って銀行口座にアクセスできるかどうかをテストした。この時点で、情報が盗まれる被害に遭っていた。

SANSの研究者がこの拡張機能を分析したところ、ユーザーが閲覧したWebサイトの全データを読み取って改ざんする機能を持っていることが判明。この中には銀行名や口座番号、口座へのアクセスに使うパスワードなども含まれていた。

●データベースのダンプファイルがWebサイト上に…JPCERTが警告

https://www.jpcert.or.jp/magazine/irreport-Unsecured_Databases.html

このニュースをザックリ言うと・・・

- 8月8日（日本時間）、セキュリティ専門機関JPCERT/CCより、日本国内の多数のWebサイトで、データベースのダンプファイル（メモリや(CPU内部の)レジスタ、ファイル、ディスクなどのある瞬間の中身を丸ごと記録したファイル）が外部から閲覧できる状態にあるとして警告が出されています。

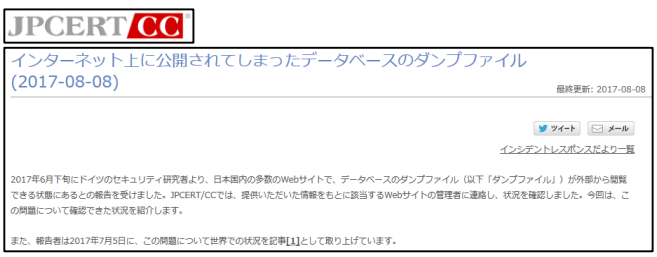
- 6月下旬にドイツのセキュリティ研究者から情報提供を受けて調査を行っており、複数のサイトでドキュメントルート（DocumentRoot）直下にdump.sqlという名前のダンプファイルが置かれていたことを確認したとのことです。

- 当初何らかの攻撃の結果ダンプファイルが生成されたものと推測していましたが、ファイルの更新日時がまちまちであることや、サイト管理者への聞き取りの結果「削除し忘れていた」または「バックアップとしてファイルを置いていた」という回答を得たことから、「管理・運用のバッドプラクティス」が原因であると結論付けています。

- JPCERTでは、本来アクセスされるべきではない機密情報を含むデータファイルはドキュメントルート配下ではなく、その外部に保存すること、もしくはWeb経由でアクセスできないようアクセス制限を適切に設定することを推奨しています。

AUS便りからの所感等

- JPCERTが推奨する管理ルールの他にも、必要のなくなった古いファイルは可能な限り残しておかないこと、不必要な情報を表示しないようあらゆる設定を確認すること、などWebサイトの運用においては重要なことです。


JPCERT CC

インターネット上に公開されてしまったデータベースのダンプファイル
(2017-08-08)

最終更新: 2017-08-08

ツイート メール

インシデントレスポンスだより一覧

2017年6月下旬にドイツのセキュリティ研究者より、日本国内の多数のWebサイトで、データベースのダンプファイル（以下「ダンプファイル」）が外部から閲覧できる状態にあるとの報告を受けました。JPCERT/CCでは、提供いただいた情報をもとに該当するWebサイトの管理者に連絡し、状況を確認しました。今回は、この問題について確認できた状況を紹介します。

また、報告者は2017年7月5日に、この問題について世界での状況を記事[1]として取り上げています。

- Webアプリケーションの脆弱性次第では、最悪の場合サーバ上の任意の場所にあるファイルにアクセスされる恐れ（ディレクトリトラバーサル）があることにも注意が必要で、Webサイト・アプリケーションの脆弱性を洗い出すセキュリティ診断を行うことや、脆弱性を突くような不正なリクエストをWebアプリケーションファイアウォール（WAF）、それを提供するUTMの設置によって遮断するような構成にすることも将来的には検討に値するでしょう。