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。

●セキュリティ意識の低いユーザや企業を狙うマルウェアスパム攻撃…日本も多数被害

https://japan.zdnet.com/article/35114476/
http://www.atmarkit.co.jp/ait/articles/1802/13/news025.html

このニュースをザックリ言うと･･･

- 2月7日（米国時間）、米Palo Alto Networks社より、不正なWord文書からのマルウェア感染を目的としたメールの拡散について警告が出されています。

- 警告によれば、「Hancitor(別名Chanitor・Tordal)」と呼ばれるオンラインバンキングを狙うマルウェアは、Windows10にデフォルトでインストールされるWindows Defenderや、セキュリティソフトなどのアンチスパム機能では検出されるため、それらが有効でない、例えばWindows7でアンチウイルスソフト等を入れていないPCがターゲットにされているものと推測されています。

- メールは平日に大量に送信され、またマルウェアを直接添付する形から、「請求書」や「配送通知」等を偽って外部サーバ上の不正なWord文書へのリンクを記載した形に移行している模様です。

- マルウェアを置くために不正アクセスを受けたサーバは米国で197件、次いで日本で23件とされ、また米国以外の（日本を含む）サーバの多くは実在する、主に中小企業のものとされています。

AUS便りからの所感等

- Hancitorがとっている攻撃手法の多くは以前から様々なマルウェアが用いているものである一方、マルウェアを分析するサービス等が使用するIPアドレスをブロックすることにより、自動システムによる分析を阻止している可能性も言及されています。

- ともあれ、組織内の全てのPCについて必要なセキュリティ対策を確実にとっているか、セキュリティ機能を無効にしているPCがあったりしないか、随時確認することは重要です。

- またWindows7の（延長）サポート終了は2020年1月となっており、それまでの間はまだセキュリティパッチが提供されますが、もし各種ベンダーが提供するアンチウイルスソフトを使用していなければ、UTMの導入のほか、最低でもMSが提供するMicrosoft Security Essentials（MSE）を導入し、Windowsファイアウォールの有効化を怠りなく実行するようにしてください。

ZDNet Japan

セキュリティ意識の低いユーザーや企業を狙うマルウェアスパム攻撃--日本も多数被害

ZDNet Japan Staff 2018年02月09日 06時00分

スパムメールからのマルウェアダウンロードは平日が多い（出典：パロアルトネットワークス）

Hancitorは、Windows Defenderなどのウイルス対策機能で検出が可能なほか、拡散に使われるスパムメールもフィルタリング機能で検出できる場合が多いという。それにもかかわらず少なくとも過去数年にわたって毎月数百件の検出が続いており、同社ではこの攻撃が古いOSを使い続けたり、ウイルス対策ソフトを導入していなかったりといった、セキュリティ意識の低いユーザーを標的にしていると分析している。

スパムメールの配信では、攻撃者に侵害されたホスティングサービスや企業のサーバが悪用されているといい、侵害されたサーバの設置国では米国が197件で最も多く、日本は23件で2番目に多い。米国ではホスティングサービスでの侵害が多い一方、日本を含む米国以外では実在企業が所有するサーバでの侵害が多く、特にアジア圏の中小企業での被害が目立つという。

@IT

最終的にはバンキング型トロイの木馬として機能：

Windows 7以前のユーザーは要警戒――偽メールから感染を拡大させる「Hancitorマルスパム攻撃」とは

Palo Alto Networksは、Windows OSに感染するマルウェア「Hancitor」について注意を促している。「Windows Defender」を搭載せず、ウイルス対策機能が無効にされているWindows 7以前のOSを狙う傾向にあるという。同社は、攻

2018年02月13日 08時00分

Palo Alto Network
「Chanitor」「Torda
は標準で有効になって
め、同社は、ウイルス
呼び掛けている。

Hancitorは、Micro
どの場合、バンキング
トールするマクロをW
た。最近は新たに「同
電子メールに埋め込む
フトによる添付ファイ

Palo Alto Networksは、攻撃用配信サーバが長期的に使われていることから、新たな攻撃手法が「今のところ成功している」とみている（画像はイメージです）

攻撃者は、平日を中心に、Hancitorを含んだ電子メールを毎月数百件送信している。新たな手法は、マルウェアに感染したWebサーバやホスティング業者の不正アカウントを利用し、攻撃用の配信サーバをさまざまな地域に設置。botネット経由で「請求書」や「宅配業者の配送通知」など、実在の企業を装った攻撃用電子メールを大量に送りつける。受信者が電子メールに埋め込まれたリンクをクリックすれば、Word文書がPCにダウンロードされ、Hancitorがインストールされる。

●4000以上の政府系サイトで閲覧者に対して仮想通貨マイニングを行わせるスクリプトが埋め込まれていたことが判明

https://gigazine.net/news/20180213-government-websites-hacked-for-mining/

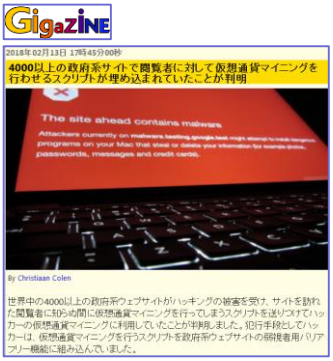
このニュースをザックリ言うと・・・

- 2月12日（現地時間）、「The Hacker News」より、アメリカ・イギリスをはじめとする世界中の4000以上の政府系ウェブサイトが改ざんされ、サイト訪問者のPC上で密かに仮想通貨の採掘を行うスクリプトが埋め込まれていたと報じられました。

- 攻撃者はWebサイトの弱視者用バリアフリー機能「BrowseAloud」を改ざんして仮想通貨「Monero」を採掘するスクリプトを埋め込み、採掘されたMoneroを自分のものにしていた模様です。

- BrowseAloudを運営するTexthelp社によれば、改ざんの発覚から4時間以内に全てのサイトからBrowseAloudを除去して対策を行っており、顧客のデータがアクセスされたり消去されたりした形跡はないとしており、また、調査完了後にBrowseAloudのアップデート版をリリースする予定としています。

AUS便りからの所感等



- ユーザのPCリソースを密かに仮想通貨の採掘に使用させる「クリプトジャッキング」については、2017年におけるマルウェアの不正行為として増加の傾向にあるとの調査結果も出ています（AUS便り 2018/02/13号参照）。

- クリプトジャッキングでよく使われるツール「Coinhive」が今回採掘スクリプトでも使用されており、本来は広告に代わりサイトを無料で運営する費用を捻出するためのツールとして期待されていたようですが、PCのCPUや電力を過剰に消費する等問題が多く指摘されています。

- 現在ではCoinhiveもマルウェアとして扱うアンチウイルスソフトも多くなっており、企業・組織のPCやネットワークリソースを浪費され、業務に支障をきたす可能性を防ぐ意味でも、アンチウイルス・UTM等による対策を行うことは一考に値するでしょう。

●FedEx、個人情報を含む119,000件の文書データをパスワード無しの状態で「Amazon S3」に放置

https://japan.zdnet.com/article/35114812/

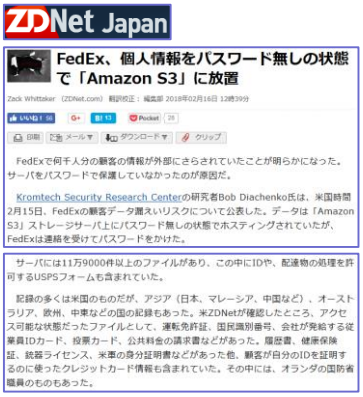
このニュースをザックリ言うと・・・

- 2月15日（米国時間）、ドイツKromtech Security Centerの研究者により、FedEx社の顧客情報を含むスキャンされた文書データ約119,000件が「Amazon S3」上で閲覧可能な状態だったと発表されました。

- 発表によれば、データはFedEx社が2014年に買収した輸送代行サービスBongo International社（のちFedEx Cross-Border International）が収集していた顧客情報で、少なくとも2008年から2015年9月までの、日本を含む様々な国のユーザの氏名・住所・電話番号および写真付き身分証明書データ等が含まれていたとのことです。

- S3上のデータは少なくとも2009年から閲覧可能な状態だったとされていますが、連絡を受け現在は非公開に設定されているとのことです。

AUS便りからの所感等



- 今や企業のシステムや機密情報の保持等においてもクラウドの利用は既に一般的なものとなっていますが、今回のような事例は適切なアクセス管理設定を行っていなかったことが原因であり、これを受けて安易に「クラウドは危険、(企業ネットワーク内でサーバを運営する)オンプレミスの方が安全」とするのは軽率でしょう。

- クラウドでの運用、オンプレミスでの運用、それぞれにおいてとるべき適切な対策を把握し、確実に実行することが肝要です。

- 2017年4月に当該サービスは終了していましたが、その際にデータを適切に破棄していなかったことも一因と言え、必要のなくなった情報の破棄は、個人情報保護のための方策としてオンプレミスであっても不可欠です。