— AUS（アルテミス・ユーザ・サポート）便り 2016/08/22号 —
http://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。

●ポケモンGOのWindows版アプリに偽装してファイルを暗号化し人質に取るランサムウェアが確認される

http://gigazine.net/news/20160816-pokemon-go-ransomware-windows/

このニュースをザックリ言うと・・・

- 8月14日（現地時間）、セキュリティ研究者のMichael Gillespie氏より、スマートフォン（iOS・Android）向けゲーム「ポケモンGO(Pokemon GO)」のWindows版になりすましたランサムウェアを確認したことが発表されました。

- 当該ランサムウェアは、Windowsを使用するPCやスマートフォン等のデバイスに感染することにより、文書・画像ファイル等の暗号化を行った上で脅迫文を表示する他、攻撃者が後から侵入できるようバックドアを作成する等の行動をとるとされています。

- また、デバイスに接続したUSBメモリ等のリムーバブルドライブに不正な自動再生プログラムを設定し、そのドライブを別のWindowsデバイスに接続することにより、感染を拡大することも確認されています。

AUS便りからの所感等

- ポケモンGOに関連したマルウェアとしては、7月6日の公開直後に正規のアプリにマルウェアが仕込まれたものが出回り、警告されていました（AUS便り2016/07/19号参照）。

- 現時点でポケモンGOのWindows版はリリースされておらず、今回も自分の所有するモバイル等でポケモンGOを早く遊びたいと期待するユーザの心理を悪用した攻撃であると思われます。

- PC・モバイル、あるいはWindowsでもiOS・Androidでも言えることですが、アプリケーションやリリース情報の入手にあたっては必ず公式情報をあたるようにし、そのうえで、モバイルデバイスでのネットワークへのアクセスにおいても、アンチウイルスの導入および可能な限りUTMへのVPN接続を経由してアクセスすることを強く推奨致します。

GIGAZINE

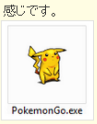
2016年08月16日 12時00分00秒

ポケモンGOのWindows版アプリに偽装してファイルを暗号化し人質に取るランサムウェアが確認される

「Windows版Pokémon GO(ポケモンGO)」という存在しない偽アプリが開発され、本物のポケモンGOアプリだと勘違いしてインストールした人がランサムウェアに感染、被害者が端末のデータにアクセスできないようにして身代金を脅迫するという事態が報告されています。ポケモンGOランサムウェアは、これまでに報告されてきた一般的なランサムウェアとは異なる挙動をしているとのこと。

PokemonGo Ransomware installs Backdoor Account and Spreads to other Drives
http://www.bleepingcomputer.com/news/security/pokemongo-ransomware-installs-backdoor-accounts-and-spreads-to-other-drives/

このランサムウェアは、セキュリティ研究者の**Michael Gillespie**氏によって発見されたもの。アプリのアイコンはこんな感じです。



被害者のデバイスに感染したランサムウェアは、まず端末をスキャンして以下のような拡張子のファイルが含まれていないかを調べます。

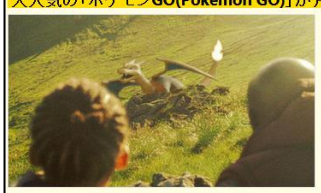
.txt, .rtf, .doc, .pdf, .mht, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .png, .csv, .sql, .mdb, .sln, .php, .asp, .aspx, .html, .xml, .psd, .htm, .gif, .png

被害者のデバイスに感染したランサムウェアは、まず端末をスキャンして以下のような拡張子のファイルが含まれていないかを調べます。
.txt, .rtf, .doc, .pdf, .mht, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .png, .csv, .sql, .mdb, .sln, .php, .asp, .aspx, .html, .xml, .psd, .htm, .gif, .png
そして、これらのファイルをAESで暗号化し、さらに暗号化されたファイルに「.locked」という拡張子を追加。ユーザーが端末のファイルにアクセスできないようにします。そして作業が完了したら「この端末のデータにアクセスしたければ身代金を払う方法を示すので『me.blackhat20152015@mt2015』まで連絡するように」という内容を表示します。

そのほか、ポケモンGO関連では、7月に以下のようなスパムメールが出回っているとのニュースもあり、流行ものに便乗したなりすまし事件はあとを絶ちません。
http://gigazine.net/news/20160713-pokemon-go-scam/

2016年07月13日 11時10分00秒

大人気の「ポケモンGO(Pokémon GO)」が月額有料制になるというスパムメールが出回る



アメリカ・オーストラリア・ニュージーランドでリリースされたアプリ「**Pokémon GO**」は瞬く間に**AppStore**と**Google Play**のランキングで1位となり、アメリカだけでも7500万ダウンロードを突破しています。Pokémon GOが世界中の注目を集めている中、「サーバーが重くなりすぎたため、Pokémon GOは月額制に移行します」といった内容のスパムメールが出回っていることが確認されました。

●道立総合研究機構のPCがウイルスに感染･･･Windows XP使用

http://dd.hokkaido-np.co.jp/news/society/society/1-0305381.html

このニュースをザックリ言うと･･･

- 8月16日（日本時間）、北海道立総合研究機構（道総研）より、同機構環境科学研究センターのPC1台がウイルスに感染し、外部との不正通信が発生していたと発表されました。

- 不正通信の発生は内閣サイバーセキュリティセンターからの連絡で発覚しており、同5日9:20から13日1:30まで約30回発生していたとのことです。

- 被害を受けたPCには機密情報や使用していた職員のもの以外の個人情報は入っていませんでしたが、OSにWindows XPを使用し続けていて、インターネットへの接続により、ウイルス感染の危険がある状態だったとされています。

- なお、感染したウイルスの種類および侵入経路については調査中とのことです。

どうしん（ウェブ）

道立総合研究機構のＰＣに不正アクセス　ウィンドウズＸＰ

08/17 07:00

道立総合研究機構（道総研）は１６日、同機構環境科学研究センター（札幌市北区）のパソコン１台がウイルスに感染し、不正アクセスがあったと発表した。外部との接続を全て遮断し、情報流出の有無や感染経路などを調べている。

同機構によると、内閣サイバーセキュリティセンターから連絡を受け発覚。外部との不正アクセスは５～１３日にかけて約３０回あった。サポート期間が終了した基本ソフト「ウィンドウズＸＰ」を更新しないままインターネットに接続していたといい、ウイルス感染の危険にさらされる状態だった。

パソコンを使っていた職員１人の出張計画と音響に関する研究データが保存され、機密情報やこの職員以外の個人情報は入っていなかったという。同機構は「研修などを通じて再発防止に努める」と話している。

AUS便りからの所感等

- 2014年4月に延長サポートが終了したWindows XPが依然として利用されていたことが原因で、例えば、今年1月には、オーストラリアの病院でPCがウイルスに感染し、病院の事務機能が麻痺してしまうという事態が発生しています（AUS便り2016/02/01号参照）。

- 同機構では「研修などを通じて再発防止に努める」としていますが、もしユーザ側の注意だけで攻撃を食い止めるというのであれば、遠からず破たんし、限界に突き当たることが考えられます。

- 一つには何よりもOSのアップグレードを、そしてもう一つには、感染や侵入あるいは万が一それが発生した場合の出口対策を、アンチウイルスやUTMの設置およびネットワーク構成の見直しで行うことが今後必要不可欠となるでしょう。

●上司のIDとパスワード盗み見る…ネットバンキング悪用、57万円不正送金

http://headlines.yahoo.co.jp/hl?a=20160812-00000593-san-soci

このニュースをザックリ言うと･･･

- 8月12日（日本時間）、大阪府警サイバー犯罪対策課等より、東京都の会社経営者の男性の口座から、57万円をネットバンキングにより不正送金した容疑で、勤務していた会社員および大阪府の自営業者の計2名を逮捕したと発表されました。

- 発表によれば、当該会社員は経営者のネットバンキングのIDとパスワードを盗み見て自営業者に伝え、自営業者がスマートフォンを用い、自分の口座へ送金を行っていたとのことです。

YAHOO! JAPAN ニュース

上司のＩＤとパスワード盗み見る　５７万円不正送金　容疑の男２人逮捕　大阪府警

産経新聞 8月12日(金)22時13分配信

インターネットバンキングを悪用し、他人の口座から現金を不正送金したとして、大阪府警サイバー犯罪対策課などは１２日、電子計算機使用詐欺容疑で、東京都昭島市福島町、会社員、吉田憲生（４６）と大阪府和泉市浦田町、自営業、松本和也（３８）の両容疑者を逮捕、送検したと発表した。いずれも容疑を認めている。

逮捕・送検容疑は、共謀し４月１１日、スマートフォンでネットバンキングを操作し、勤務先の上司だった都内に住む会社経営の男性（６７）の口座から、５７万円を松本容疑者の口座に不正送金したとしている。

府警によると、吉田容疑者が男性のネットバンキングのＩＤとパスワードを盗み見て知人の松本容疑者に伝えていた。預金が減っているのを不審に思った男性が銀行に相談していた。

AUS便りからの所感等

- 画面上に表示された重要な入力内容等を後ろから盗み見る「ショルダーハック」は非常に古典的な情報入手方法の一つで、パスワードについては、通常は画面上に入力内容が表示されたとは考えにくく、例えば、ディスプレイに付箋等で張り付けられていた状態だった、もしくは「ソフトウェアキーボード」を使っていたために読み取り可能だったものと推測されます。

- また今日において、ログインID・パスワードのみで振込等の送金処理を実際に行えるケースは稀であり、さらなる認証のための番号やワンタイムパスワード等の入力を求められることが一般的ですが、それらを使用する設定になっていなかった可能性もあります。

- 利用しているサービスにおいて、より安全に送金等の重要な処理を実行可能かをそのサービスのサイトで確認すること、また自分が現状で利便性のために行っている行為が安全性を損ねていないか等について、ネット上の情報等をもとに振り返ってみることは非常に大事なことと言えるでしょう。