— AUS（アルテミス・ユーザ・サポート）便り 2017/04/03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。

●USBストレージのデータを盗み取るマルウェア、JPCERT等が注意喚起

http://nlab.itmedia.co.jp/nl/articles/1703/31/news053.html
https://www.jpcert.or.jp/at/2017/at170012.html
https://www.npa.go.jp/cyberpolice/detect/pdf/20170330.pdf

このニュースをザックリ言うと・・・

- 3月30日（日本時間）、セキュリティ専門機関JPCERT/CCおよび警察庁より、USBデバイス(USBメモリ等)のデータを盗み取って外部に送信するマルウェアについての注意喚起が出されました。

- マルウェアは事前に何らかの方法でPCに感染し、接続されたUSBデバイス上のファイルのリストを作成し、その中から攻撃者が指定されたファイルを圧縮・分割して外部へ送信する挙動をとるとされています。

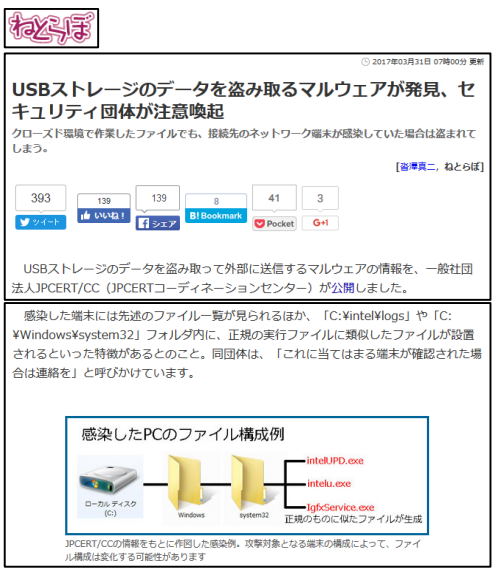
- 両組織では、インターネットと直接繋がっていないクローズドネットワーク上で機密情報を管理している場合でも、この手口によりUSBデバイスを経由して機密情報を奪取される可能性があるとしており、情報漏えい対策として「データ持ち出しの際は暗号化を行うこと」「当該データを外部にメール送信する場合は暗号化したままで行うこと」「USBデバイス内のデータは速やかに消去すること」等が呼び掛けられています。

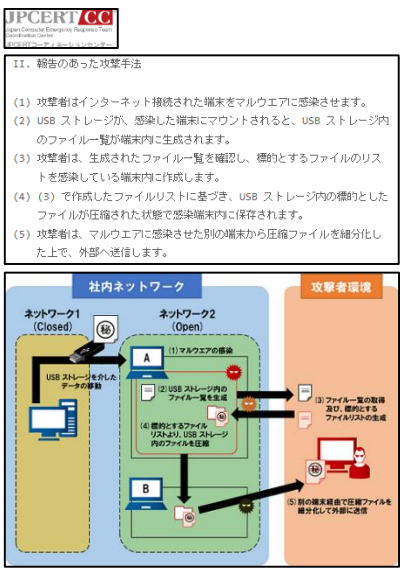
AUS便りからの所感等

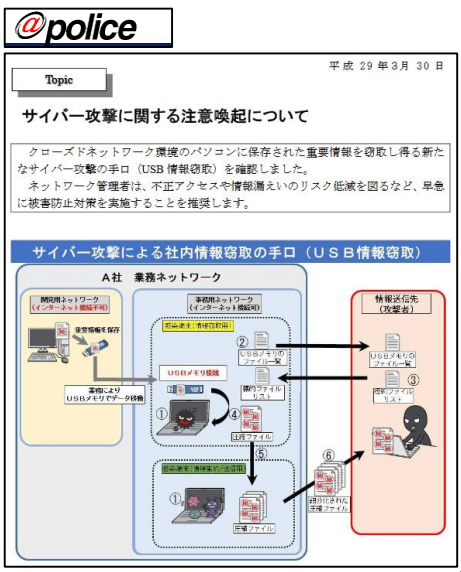
- 「USBデバイスにマルウェアが感染し、接続したPCにも拡散する」というケースはよく見られましたが、今回は「PC上でUSBデバイスが接続されるのを待ち受ける」という意味では、これまでと逆の行動をとると言うこともできるでしょう。

- マルウェアにより、「C:¥intel¥logs」あるいは「C:¥Windows¥system32」フォルダの配下に、「intelUPD.exe」「intelu.exe」「IgfxService.exe」等といった名前の不正な実行ファイルや、「interad.log」「slog.log」といったファイル名のファイルリスト、あるいは「.rar」拡張子の圧縮分割ファイルが作られるとされ、感染の調査にあたってはこういった箇所を確認することになるでしょう（ただし、今後全く違う場所・違うファイル名で保存する亜種も現れる可能性も高いです）。

- クローズドネットワーク上のPC、インターネットに接続できるネットワーク上のPCに拘らず、マルウェアが感染しないよう、またマルウェアによる外部への不正通信を遮断できるよう、アンチウイルスやUTMの導入による防御もまた不可欠です。







●危険度の高いMicrosoft以外のアプリは「iTunes」「Java JRE」「Lhaplus」

http://internet.watch.impress.co.jp/docs/news/1048871.html

このニュースをザックリ言うと・・・

- 3月10日（日本時間）、ソフトウェア資産管理製品などを手がけるFlexera Software社より、PCにインストールされたソフトウェアとその脆弱性に関する、2016年第4四半期における国別の調査結果が発表されました。

- 日本国内の調査対象PCには、平均で21ベンダーによる63のソフトウェアがインストールされており、うち28がマイクロソフト製品という結果が出ており、また、マイクロソフト製ソフトに対するセキュリティパッチを適用していないユーザは6.5%の一方、それ以外のベンダーのソフトに対しては14.4%となっています。

- 「最新版がインストールされておらず、危険度が高いアプリ」のトップ（市場シェアにパッチ未適用率を乗じた数値順）には「iTunes 12.x(最新は12.6)」が挙げられており、パッチ未適用率57%(シェア42%)となっており、次点として「Java 8(最新はUpdate 121)」がパッチ未適用率53%(シェア43%)、また「Lhaplus 1.x(最新は1.73)」はシェア26%の一方でパッチ未適用率63%となっています。

INTERNET Watch

危険度の高いMicrosoft以外のアプリは「iTunes」「Java JRE」「Lhaplus」

サポート終了ソフトでは「Flash Player」と「SQL Server」の旧バージョンがいまだ高いシェア

岩崎 宰守　2017年3月10日 13:02

フレクセラ・ソフトウェア合同会社は、インストールされたソフトウェアの脆弱性スキャンを行う「Personal Software Inspector」の2016年第4四半期のデータに基づいた国別の脆弱性調査結果を発表した。

日本国内の調査対象PCには、平均で21ベンダーによる63のソフトウェアがインストールされており、うち28のソフトウェアはMicrosoft製品だった。

AUS便りからの所感等

- Lhaplusは2015年4月にセキュリティホールが確認され、1.71で修正されていますので、もしLhaplusを使用していて最新版にアップデートしていないのであれば必ず行いましょう。

- Flexera社が今回の調査に用いたようなソフトウェア資産管理製品は、組織内の各PCにインストールされているソフトウェアとそのバージョンの情報収集を行うことにより、マルウェア等の侵入経路となり得る古いソフトウェアがインストールされたPCの存在を把握することが可能となります。

- 全てのPC上のソフトウェアが最新版へのアップデートされるまでは、必ず古いバージョンが存在し、間隙を突かれる可能性も皆無ではありませんので、そこで発生する攻撃を遮断するためにも、アンチウイルス・UTMの導入もまた必ず行われるべきです。

●ぬいぐるみから80万人のユーザ情報が流出、つながる玩具に警鐘

http://www.itmedia.co.jp/enterprise/articles/1703/02/news107.html

このニュースをザックリ言うと・・・

- 2月28日（現地時間）、セキュリティ研究者のトロイ・ハント氏により、親子間で音声メッセージをやりとりする機能を持つぬいぐるみ「CloudPets」のユーザ情報や会話が流出していた可能性があるとする調査結果が同氏のブログやセキュリティブログ「Threatpost」で発表されました。

- 発表によれば、流出の可能性のあるデータはCloudPetsのユーザ80万人あまりのメールアドレスやパスワード、およびCloudPetsによって交わされた会話200件あまりとされており、情報が保存されていたデータベースには外部からアクセス可能な状態だったとのことです。

- また、パスワードは暗号化されていたものの、非常に短い、もしくは簡単なパスワードが大多数を占めており、アカウントへの不正ログインを行うことも容易な状態だったとされています。

ITmedia エンタープライズ

ぬいぐるみから80万人のユーザー情報が流出、つながる玩具に警鐘 (1/2)

「はかにも多数のつながる玩具に深刻な脆弱性が存在しているのは間違いない。メーカーや保護者の知らないうちに不正アクセスされ、データが盗まれているかもしれない」と研究者は警鐘を鳴らしている。

[鈴木聖子, ITmedia]

インターネットに接続して、親子で音声メッセージをやりとりできる玩具から、ユーザー80万人あまりの情報が流出していたことが分かったとして、セキュリティ研究者が調査結果を公表した。この玩具を使って交わされた、親子間の会話200万件あまりも流出した可能性があるといい、同じような脆弱性は他の玩具にも存在するかもしれないと警告している。

AUS便りからの所感等

- 登場したばかりの、いわゆるIoT（モノのインターネット）のセキュリティにおける問題と捉えることもできますが、CloudPetsの製品そのものに不正に侵入できたという手合いのものではなく、個人情報・機密情報のデータベースに外部から容易にアクセス可能な設定だったという点では、IoT以前の問題だったと言わざるを得ません。

- 内部のデータベースを含め、不特定多数への公開を意図していないサービスへのアクセスをサーバ自身もしくはルータ・UTMのファイアウォール機能により遮断・制限することは、サーバを堅牢なものとするために不可欠なものです。

- また、不正アクセスの状況やアクセス元の分析を確実かつ迅速に行うためには、あらゆるアクセスについてログを取得することも重要となります。