— AUS（アルテミス・ユーザ・サポート）便り 2017/03/27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。

●「ワンタイムパスワード」要求で不正送金…ウイルス「DreamBot」の被害確認

http://itpro.nikkeibp.co.jp/atcl/news/17/031700858/
http://mainichi.jp/articles/20170317/k00/00m/040/075000c

このニュースをザックリ言うと･･･

- 3月16日（日本時間）、警視庁・日本サイバー犯罪センター（JC3）およびトレンドマイクロ社より、オンラインバンキングにおいて不正送金を行うマルウェア「DreamBot(ドリームボット)」による被害が国内で初めて確認されたとして、相次いで警告が出されています。

- DreamBotは、以前から活動しているマルウェア「Gozi(URSNIF)」の亜種とされ、感染したPCでのキー入力を記録したり、オンラインバンキングサイトを利用しようとした際に偽のワンタイムパスワード入力画面を表示したりして、盗み出したワンタイムパスワード等の情報により不正送金を行うとされています。

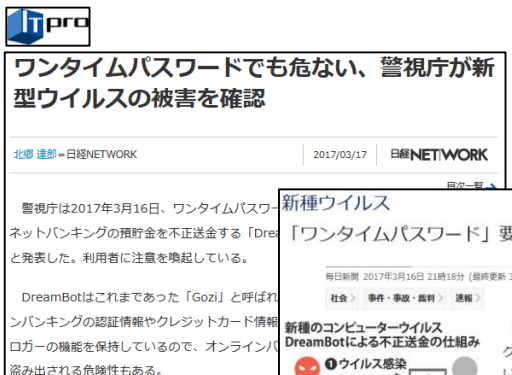
- JC3では、PCがDreamBotやGoziに感染していないかチェックするサイト（https://www.jc3.or.jp/info/dgcheck.html）を用意しており、また各組織から出されている注意喚起では、PCのOSや各ソフトウェアを最新に保つことや、日頃利用しているオンラインバンキングの利用手順を確認し、通常と異なる画面が出た場合はID・パスワードを入力しないこと等が挙げられています。

AUS便りからの所感等

- スパムメールの添付ファイル、悪意のあるWebサイトへの誘導等で感染すること、また偽の入力画面を表示すること等、基本的にはこれまでにもみられたオンラインバンキングを狙うマルウェアと同様の行動をとるものとみられます。

- JC3による感染チェックサイトも感染の検出を完全に保証するものではないため、日頃からPC上でのアンチウイルスソフトによる定期的なウイルスチェックを行う、もしくはUTMの設置等、各種防衛手段との組合せは欠かせません。

- また、ハードウェアトークンやスマホアプリとの組合せによる不正送金対策が普及している現在のオンラインバンキングですが、今後は送金処理がスマホだけで完結する仕組みが狙われる可能性も考えられるため、スマホにも忘れずにアンチウイルスソフトの導入を行い、また不審なアプリのインストールには十分に注意する等の警戒が必要です。



●JINSオンラインショップから約120万件の個人情報に不正アクセスか

http://itpro.nikkeibp.co.jp/atcl/news/17/032400930/

このニュースをザックリ言うと・・・

- 3月24日（日本時間）、メガネチェーン店「JINS」を展開するジェイアイエヌ社より、同社が運営する「JINSオンラインショップ」が攻撃を受け、約120万件のメールアドレス・個人情報に不正アクセスされた可能性があると発表されました。

- 発表によれば、被害を受けたのはメールアドレスと個人情報（氏名・住所・電話番号・生年月日・性別）749,745件、およびメールアドレスのみ438,610件の計1,188,355件となっており、クレジットカード情報は被害を受けたサーバでは保管しておらず、流出は確認されていないとのことです。

- 攻撃は当該サイトで使用していた「Apache Struts2」の脆弱性を突いたものとされており、また同社では不正アクセスを同22日に確認し、翌23日にセキュリティ対策を行った新しいサイトへの移行作業を行っています。

AUS便りからの所感等

- Struts2の脆弱性が発表されて以降、これを悪用した攻撃が各地で発生しており、3月10日に都納税サイト等から約72万件のクレカ情報流出が発表された（AUS便り 2017/03/13号）他、サイトの改ざんや個人情報の流出が相次いでいます。

- また、最初に発表された際に推奨された（アップデートができない場合の）回避策をも迂回して攻撃可能な別の脆弱性も発表され、WAFによる攻撃の遮断が通過する可能性等が指摘されており、この状況は当分続きそうです。

- 金銭面等の損害を最小限に抑えられるよう、Webサービスを稼動しながらアップデート等を行うことが理想ですが、場合によっては、実際に被害が発生し取り返しがつかない事態になる前に、不正アクセスが確認されずともサイトを一時閉鎖して対応する判断も大事でしょう。

●IPAの脆弱性被害体験ソフトにOSコマンド実行の脆弱性…使用停止呼び掛け

http://internet.watch.impress.co.jp/docs/news/1049858.html

このニュースをザックリ言うと・・・

- 3月16日（日本時間）、独立行政法人情報処理推進機構（IPA）より、同機構が提供していたセキュリティ学習ソフト「安全なウェブサイト運営入門」に脆弱性が確認されたとして、警告が出されています。

- 「安全なウェブサイト運営入門」は2008年にリリースされた、Webサイトの脆弱性によって発生する事件を体験するソフトウェアでしたが、セーブデータの読み込みに脆弱性が存在し、OS上で不正なコマンドを実行され、PCを乗っ取られる恐れがあったとされています。

- IPAによれば既に開発・サポートは終了しており、修正される予定はないとのことで、使用を停止するよう呼び掛けられています。

AUS便りからの所感等

- 今回確認された脆弱性は、基本的にローカルからのみ攻撃可能なものであり、他人から渡されたセーブデータを読み込んだりした場合に問題となり得ますが、そういったケース以外で外部から直接悪用可能な類のものではないようです。

- IPAでは同様の脆弱性体験学習ツール「AppGoat」もリリースしており、こちらにも脆弱性が確認されていましたが、修正されています。

- IPAがリリースしたセキュリティに関するツールに脆弱性があったという点でセンセーショナルに取り上げられがちですが、長年バージョンアップしていないソフトウェアにはこのように脆弱性が潜んでいる可能性があり、どんなソフトウェアでも可能な限り最新のバージョンに保つことがセキュリティの維持のためには重要な要素の一つです。