— AUS（アルテミス・ユーザ・サポート）便り 2016/06/20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。

●JTBから約793万人分の個人情報流出か？標的型攻撃受ける

http://www3.nhk.or.jp/news/html/20160614/k10010556201000.html
http://www3.nhk.or.jp/news/html/20160614/k10010556651000.html
http://itpro.nikkeibp.co.jp/atcl/column/14/346926/061500549/

このニュースをザックリ言うと・・・

- 6月14日（日本時間）、大手旅行会社のJTB社は、旅行商品のインターネット販売を行う子会社i.JTB（アイドットジェイティービー）社のサーバが不正アクセスを受け、個人情報約793万人分が流出した可能性があると発表しました。

- 発表によれば、3月15日にi.JTBの問合せメールアドレス宛に対し取引先を装った標的型攻撃メールが送信されており、オペレーター端末上でメールの添付ファイルを開いたことにより二種類のマルウェアに感染、その後19日から24日にかけて内部からの不審な通信が検知され、内部サーバの調査の結果、個人情報データを攻撃者が送信しようとしていた痕跡が確認された模様です。

- 流出した可能性のある個人情報は、JTBやその提携サービスから一部商品の予約を申し込んだ利用者の氏名・住所・生年月日・メールアドレス・電話番号等、および一部利用者のパスポート番号・取得日とされています（なお、クレジットカード番号、銀行口座情報、旅行の予約内容は含まれていないとのことです）。

AUS便りからの所感等

- JTBは、標的型攻撃のメールは取引先を装ったもので一見しただけでは本物と見間違うものだったと主張しており、メールが本物かどうかの確認は、送信者欄（From: ヘッダ）を人間が見るだけでは不十分であり、サーバやメーラー等によるメールヘッダ全体の機械的なチェックが欠かせません。

- 感染の発生から公式発表まで3ヶ月のタイムラグがあった点等は批判があるものの、社内ネットワークとサーバにおける不正アクセスの内容について（実際にどれだけ流出したかまでは確認されていませんが）、可能な限り正確に調査するための体制は整っていたという印象があります。

- こと標的型攻撃に対しては、マルウェアに感染しないこと以上に、感染してしまった後の不正行為や外部への不審な通信の早期検知・遮断が重要であり、いわゆる「出口対策」を的確に行えるよう、UTMの導入と設定をはじめとするシステム・ネットワーク構成の確認と見直しは必要不可欠です。

NHK NEWS WEB

ＪＴＢ 個人情報 最大７９０万人分流出か 不正アクセスで

6月14日 18時48分

大手旅行会社、ＪＴＢは顧客の個人情報を管理するサーバーがいわゆる「標的型メール」による不正なアクセスを受けて、最大でおよ

大手旅行会社、「ＪＴＢ」部から不正にアクセスされした。このサーバーには保管されていていわゆるて、最大でおよそ７９３万ＪＴＢによりますとこれまいう報告はないとしていま

ＪＴＢ不正アクセスは「標的型メール」攻撃

6月14日 19時39分

最大でおよそ７９０万人分の個人情報が外部に流出したおそれがある、ＪＴＢに対する不正アクセスでは「標的型」と呼ばれるサイバー攻撃が行われていました。

ＪＴＢによりますと、ことし３月１５日、取引先を装った偽の電子メールがＪＴＢのグループ会社の担当者宛てに届きました。メールの差出人は担当者が日常的に取り引きをしている会社の従業員となっていて「お客様の旅行内容を確認したい」という内容が書かれていました。
添付されたファイルを開いたところ、パソコンがコンピューターウイルスに感染し、その４日後からグループ会社のサーバーが外部と不審な通信をしていることが確認されました。

News & Trend 日経コンピュータ

［詳報］JTBを襲った標的型攻撃

2016/06/15
井上 英明＝日経コンピュータ （筆者執筆記事一覧） 、広田 望＝日経コンピュータ （筆者執筆記事一覧） 、

ジェイティービー（JTB）が2016年6月14日に公表した、最大で約793万人分の個人情報が流出した可能性がある事案の発端は巧妙に取引先を装った標的型メールだった（関連記事：「流出事実ないがお客様にお詫びする」、793万人の情報流出可能性でJTBの高橋社長が謝罪）。

約4300人分の有効期限中の
した可能性のある事案は国内
の取材で分かった経緯を追っ

発端は3カ月前の2016年3
売する子会社であるi.JTB（
イトで公開する、問い合わせ
何者かが標的型メールを送り

問い合わせを装い、PDFを表示するマルウエアで攻撃

届いた標的型メールは「極めて巧妙だった。開封はやむを得なかった」とJTBの今井敏行グループ本社取締約国内事業本部長（CS推進、Web戦略担当）は話す。メールソフトに表示されるメールアドレスのドメインは、これまで取引のある航空会社系列の販売会社のドメイン。ただしユーザー名は知らない人だった。

件名は「航空券控え　添付のご連絡」で、本文については会見当日は「無かった」との説明だったが、6月15日にJTB広報室は「本文はあった。サプライヤーからの送信と見誤る内容のものだった」と訂正した。「問い合わせ内容も特段おかしいものではなかった。一目しただけでは（攻撃メールかどうか）分からない」（今井氏）。

添付ファイルは「圧縮ファイルで、その中にPDFファイルが入っていた」（JTB広報室）。PDFファイルは航空券のeチケットだったという。誤って圧縮ファイルを開封したオペレーターはeチケットに表示された人物の申し込みが見当たらなかったため「該当なし」の旨を返信した。

●ランサムウェア、エクスプロイトキットから生成されるマルウェアで最大勢力へ

http://news.mynavi.jp/news/2016/06/10/086/

このニュースをザックリ言うと・・・

- 6月7日（米国時間）、セキュリティベンダーの米Malwarebytes社より、エクスプロイトキット（さまざまな脆弱性を攻撃するためのパッケージ化されたプログラム）から生成されるマルウェアの種類で最も多いのがランサムウェアであるとする調査結果がブログにて発表されました。

- 調査では、2015年12月時点でのランサムウェアの割合は17%であり、ダウンローダーの25%の後塵を拝していましたが、今年5月の調査ではランサムウェアの割合が61%にまで上昇（ダウンローダーは13%）したとのことです。

マイナビニュース

ランサムウェア、エクスプロイトキットから生成されるマルウェアで最大勢力へ

後藤大地　[2016/06/10]

Malwarebytesは6月7日(米国時間)、「Ransomware dominates the threat landscape | Malwarebytes Labs」において、エクスプロイトキットから生成されたマルウェアに占めるランサムウェアの割合がこの半年で大きく増加して60%に到達したと伝えた。これはエクスプロイトキットから生成されたと推定される割合のみを示したものだが、サイバー攻撃においてランサムウェアが高い注目を浴びていることを示すものとして注目される。

掲載されたデータによると、2015年12月にエクスプロイトキットから生成されたマルウェアのうち、ランサムウェアの割合は17%、ダウンローダの割合は25%となっている。これが半年後の2016年5月にはランサムウェアの割合が61%、ダウンローダの割合が13%になっている。ランサムウェアはこの2年間で増加しているが、この半年で強い存在感を示すようになったことがわかる。

近年、サイバー攻撃は愉快犯的な取り組みから確実に金銭的利益を期待できる方法へ推移する傾向を見せている。ランサムウェアは特に金銭的利益を得やすい方法として、サイバー攻撃で頻繁に使われるようになっており、今後さらに被害の拡大が推定される。

Malwarebytes

Malwarebytes was founded on the belief that you and everyone have a fundamental right to a malware-free existence.

AUS便りからの所感等

- ランサムウェアによる被害の報告は衰えることを知らず、当分はこの状態が続くと思われ、最近では、一旦身代金を払ったにも拘らず、より高額な身代金を要求されるケースも報告されています。

- アンチウイルスやUTMによる可能な限りの感染防止策の他、重要なデータのバックアップ、かつバックアップデータを感染したPCから直接アクセスできない場所に保存する等、ランサムウェアへの対応策を確実に行うようにしましょう。

●SNS約1億件、Twitter3千万件、ロシアでアカウント情報流出相次ぐ

http://gigazine.net/news/20160607-100-million-passwords-stolen/
http://gigazine.net/news/20160610-32-million-twitter-password-sale/

このニュースをザックリ言うと・・・

- アカウント流出情報およびその検索サービスを提供するサイトであるLeakedSourceにて、6月に複数のサービスのアカウント流出を相次いで伝えられています。

- 6月5日（現地時間）、同サイトは、ロシアの大手SNS「VK」から、全ユーザの1/3以上となる約1億54万件のアカウント情報が流出したと発表しており、アカウント情報はユーザの氏名・住所・電話番号および暗号化されていない状態のパスワードを含む形でインターネット上に存在していたとされています。

- 次いで同8日には、Twitterのアカウント情報3200万件分がアンダーグラウンドで売買されていることを発表していますが、Twitter社ではこれらのデータはTwitterのサーバ自体への不正アクセスによるものではないとしており、LeakedSourceもブラウザに保存されたパスワードがマルウェアに奪取されたものと推測しています。

GIGAZINE

2016年06月07日 14時28分00秒
ロシア最大のSNSがハッキングされて1億ものパスワードが暗号化されずに平文で流出

ロシア最大のソーシャルネットワーキングサービスである「VK」がハッキングされ、1億件分のアカウントのパスワードが「暗号化されていない クリアテキスト の状態で流出していることが発覚しました。

2016年06月10日 11時11分00秒
3200万件分のTwitterアカウント情報(ユーザー名・パスワード・メールアドレス)が売買されていることが明らかに

月間アクティブユーザー数が世界全体で3億2000万人、日本ではFacebookなどを凌ぐ3500万人のユーザーを抱えるSNSがTwitterです。そのTwitterのアカウント情報約3200万件分が、インターネット上でハッカーたちの間で売買されていることが明らかになりました。

AUS便りからの所感等

- この2件の共通点としては、最も多かったパスワードが「123456」「123456789」「qwerty」だったことが挙げられ、こういったパスワードは攻撃者が不正ログインを試すにあたり真っ先に使うものです。

- Twitter社は今回流出したとみられるアカウントに対しパスワードのリセットを行い、メールでその旨を通知しており、それ以外のユーザについても、他のサービスと同じパスワードを使い回していないか確認の上、もしそうであればある程度複雑でかつ他と共通でないパスワードに変更することを推奨しています。

- もちろん、マルウェアの感染により、PC上のパスワードあるいはその入力を奪取される可能性に対しても、アンチウイルスやUTMによる十分な防御をとってください。