— AUS（アルテミス・ユーザ・サポート）便り 2016/03/07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。

●『貴様』のアカウントの利用中止を避けるために･･･りそな銀行グループをかたるフィッシングメールに注意

http://internet.watch.impress.co.jp/docs/news/20160226_745607.html
http://news.mynavi.jp/news/2016/02/26/400/

このニュースをザックリ言うと･･･

- 2月26日（日本時間）、フィッシング詐欺に関する調査・啓発を行っているフィッシング対策協議会より、りそな銀行グループをかたるフィッシングメールが出回っているとして注意が呼びかけられています。

- 発表によると、件名は「りそな銀行重要なお知らせ」「りそな銀行本人認証サービス」「りそな銀行メールアドレスの確認」「お知らせ内容」などが挙げられており、「2016年「りそな銀行」のシステムセキュリティのアップグレードのため、貴様のアカウントの利用中止を避けるために、検証する必要があります。」といった文面とともに偽のログインページへのリンクが記載されているとのことです。

- 同協議会は1月25日にも同様にりそな銀行について、2月22日には同グループの埼玉りそな銀行についてのフィッシングメールを警告しています。

AUS便りからの所感等

- 近年、より巧妙な文言や本物と見分けが付きにくいWebサイトのデザインを用いるフィッシングも多い中、「貴様」という不自然な呼びかけをするフィッシングは、2014年1月に三菱東京UFJ銀行をかたるものが確認されて以降、いくつかの銀行のフィッシングで同様の文面の使い回しが見られています。

- りそな銀行の該当するログインページでは、より厳密に組織の証明を行うEV-SSL証明書が利用されていますが、ブラウザ（Google Chrome等）によってはこの証明書を安全なものとみなさず、EV-SSL証明書特有の表示をしない模様です。

- 当便りで常々呼びかけていることですが、まずは自己防衛のために、メールに記載されたリンクを安易にクリックせず、ブラウザのブックマークから正規のサイトへアクセスするよう心がけること、そしてより確実にフィッシングからの防御を行うため、ブラウザ・アンチウイルスソフトあるいはUTM等のアンチフィッシング機能を活用することが重要です。

INTERNET Watch

貴様のアカウントの利用中止を避けるために――りそな銀行かたるフィッシングメールに注意

(2016/2/26 12:34)

りそな銀行をかたるフィッシングメールが出回っているとして、フィッシング対策協議会が26日、緊急情報を出した。リンク先の偽サイトは同日11時30分現在も稼働中だとしており、アカウント情報[illegible]ドなど）を入力してしまわないよう注意を呼び掛けている。

フィッシングメ[illegible]「りそな銀行メ[illegible]行」のシステム[illegible]ために、検証す[illegible]そな銀行マイク[illegible]

マイナビ ニュース

JPCERT/CC、1月に続きりそな銀行のフィッシングメールについて注意喚起

[2016/02/26]

2月26日、りそな銀行をかたるフィッシングの報告を複数受けたとして、JPCERTコーディネーションセンターが運営するフィッシング対策協議会が再び注意喚起を行った。

同協議会は1月25日にもりそな銀行のフィッシングサイトとフィッシングメールを確認したとして、注意を呼びかけていた。

2月26日11時30分時点で、りそな銀行をかたるフィッシングサイトは稼働中であり、JPCERT/CCがサイト閉鎖のための調査を依頼中とのこと。類似のフィッシングサイトが公開される恐れがあるため、注意が必要だ。

フィッシングメールはログインIDやパスワード等の情報を盗みとろうとしており、タイトルとして以下が確認されている

りそな銀行をかたるフィッシングメール①

2016年「りそな銀行」のシステムセキュリティのアップグレードのため、貴様のアカウントの利用中止を避けるために、検証する必要があります。

本人認証サービス

りそな銀行をかたるフィッシングメール②

こんにちは！
最近、利用者の個人情報が一部のネットショップサーバーに不正取得され、利用者の個人情報漏洩事件が起こりました。
お客様のアカウントの安全性を保つために、「埼玉りそな銀行システム」がアップグレードされましたが、お客様はアカウントが凍結されないように直ちにご登録のうえご確認ください。

以下のページより登録を続けてください。

https://mp.resona-gr.co.jp/mypage/MPMB010X010M
<http://www.●●●●●.com/images/>

Copyright (c) Resona Holdings, Inc. All Rights

りそな銀行をかたるフィッシングサイト →

●Androidの90%、iOSの80%が古いバージョンを使用

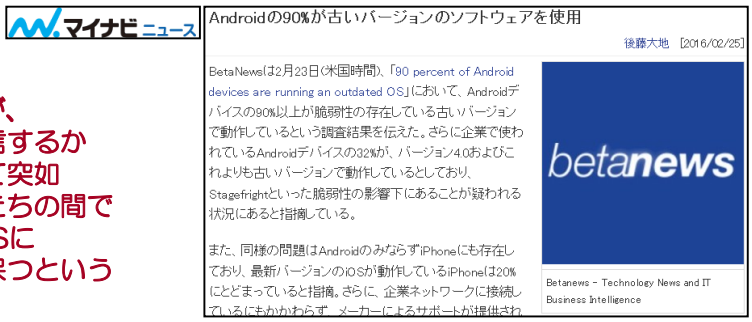
http://news.mynavi.jp/news/2016/02/25/281/

このニュースをザックリ言うと・・・

- 2月23日（米国時間）、IT系ニュースサイト「BetaNews」より、スマホ・タブレット等のデバイスで使用されているAndroidおよびiOSのバージョンに関する調査結果が報じられました。

- 記事によると、Androidデバイスの90%以上が脆弱性の存在する古いバージョンで動作しており、さらに企業で使われているもののうち32%はAndroid 4.0以前が動作し、Stagefright（メディア再生エンジン）に存在する脆弱性を悪用されてリモートからデバイスを乗っ取られる可能性があるとされています。

- また、iOSについても最新でないバージョンが動作しているのは80%とされていること、企業ネットワークに接続しているにもかかわらず、メーカーによるサポートが提供されなくなっているデバイスが2,000万台以上存在すること、さらにはサポートが提供されていてもアップデートが適用されていないデバイスもあるとされています。


マイナビニュース
Androidの90%が古いバージョンのソフトウェアを使用
後藤大地 [2016/02/25]
BetaNewsは2月23日(米国時間)、「90 percent of Android devices are running an outdated OS」において、Androidデバイスの90%以上が脆弱性の存在している古いバージョンで動作しているという調査結果を伝えた。さらに企業で使われているAndroidデバイスの32%が、バージョン4.0およびこれよりも古いバージョンで動作しているとしており、Stagefrightといった脆弱性の影響下にあることが疑われる状況にあると指摘している。
また、同様の問題はAndroidのみならずiPhoneにも存在しており、最新バージョンのiOSが動作しているiPhoneは20%にとどまっていると指摘。さらに、企業ネットワークに接続しているにもかかわらず、メーカーによるサポートが提供され
betanews
Betanews - Technology News and IT Business Intelligence

AUS便りからの所感等

- 特にAndroidデバイスについて言えることですが、機種毎にメーカー・キャリアがアップデートを配信するかどうかの判断はまちまちであり、ある機種について突如アップデートを行わないことが発表され、ユーザたちの間で話題になることも多々見られ、PCのように日々OSにセキュリティパッチを当て続け、常にセキュアに保つということができないケースも珍しくないようです。

- せめてデバイスにインストールされるその他の各種アプリについては常時アップデートを行い、またPCと同様にアンチウイルス等のセキュリティソフトを導入、および可能な限りUTM等へのVPN接続を経由しての外部へ接続するよう心がけるべきでしょう。

●古いSSL暗号化通信プロトコルを悪用する脆弱性「DROWN」、HTTPSサイトの33%に影響か

http://japan.zdnet.com/article/35078777/

このニュースをザックリ言うと・・・

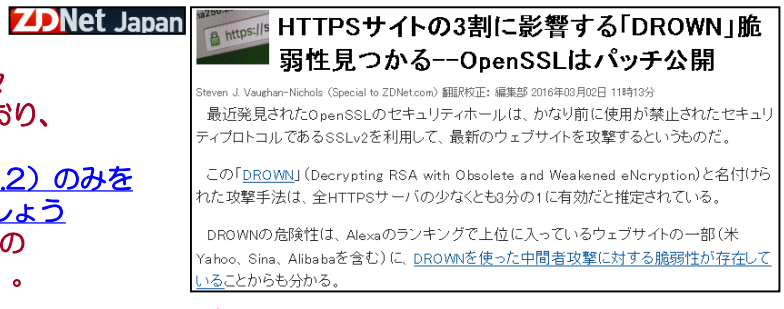
- 3月1日（米国時間）、古い暗号化通信プロトコル「SSLv2」を悪用し、暗号化通信を解読される可能性のある脆弱性「DROWN」の存在が発表されました。

- 脆弱性の発見者によると、ひと度あるサーバで解読が可能になると、秘密鍵を共有しているサーバ（同じホスト上でメールサーバも動かしている等）についても同様に暗号化通信が解読可能になるとされています。

- 脆弱性はHTTPSサーバ等においてSSLv2での通信が有効になっている場合に影響を受けるとされており、OpenSSLは1.0.1s/1.0.2gがリリースされています。

AUS便りからの所感等

- SSLv2（およびSSLv3）はここ数年でも度々プロトコル自体に起因する脆弱性が発表されており、古い携帯電話等に対応する必要がない限りは、より新しいTLS（TLSv1.0, TLSv1.1, TLSv1.2）のみを受け入れるようサーバ側で設定を変更すべきでしょう（暗号化ソフトウェアによっては、SSLv3以前のサポートを完全に削除しているものもあります）。


ZDNet Japan
HTTPSサイトの3割に影響する「DROWN」脆弱性見つかる--OpenSSLはパッチ公開
Steven J. Vaughan-Nichols (Special to ZDNet.com) 翻訳校正: 編集部 2016年03月02日 11時13分
最近発見されたOpenSSLのセキュリティホールは、かなり前に使用が禁止されたセキュリティプロトコルであるSSLv2を利用して、最新のウェブサイトを攻撃するというものだ。
この「DROWN」(Decrypting RSA with Obsolete and Weakened eNcryption)と名付けられた攻撃手法は、全HTTPSサーバの少なくとも3分の1に有効だと推定されている。
DROWNの危険性は、Alexaのランキングで上位に入っているウェブサイトの一部(米Yahoo、Sina、Alibabaを含む)に、DROWNを使った中間者攻撃に対する脆弱性が存在していることからも分かる。

- また、クライアント側でも、いわゆる「中間者攻撃」等で古いプロトコルを使わされるよう誘導されるのを防ぐため、可能な限り設定を推奨致します。

- 将来的には、UTMにおいて古いプロトコルでのネゴシエーションを行おうとする通信を遮断するような機能が実装されることも考えられます。