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。

●「こんにちは！」 三菱東京UFJ銀行をかたるフィッシングメールに注意

http://www.itmedia.co.jp/news/articles/1507/28/news150.html
https://www.antiphishing.jp/news/alert/mufj_20150728.html

このニュースをザックリ言うと･･･

- 7月28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が三菱東京UFJ銀行をかたる新たなフィッシングメールを確認したとして警告しています。

- このフィッシングメールは件名が「三菱東京UFJ銀行より大切なお知らせです」等で、また本文は「こんにちは！」で始まり、オンラインバンキングのアカウント凍結・休眠を防ぐためにログインを促し、下図に挙げるようなURLの偽ログインページへ誘導するものとなっています。

- 同評議会では、28日午後0時30分の段階でまだサイトが稼働しているとしてJPCERTコーディネーションセンターに閉鎖のための調査を依頼しており、またフィッシングサイトに情報を入力してしまったユーザに対し同行の緊急連絡先に問合せるよう呼びかけています。

AUS便りからの所感等

- 7月31日時点での同行オンラインバンキングのログイン画面は「https://entry11.bk.mufg.jp/...」となっており、前述した偽サイトについてはURL例を見る限り、httpになっていないか、またホスト名がjp以外のドメインで終わっていないかが確認のポイントとなります。

- 一方で、偽サイトは現時点でも本物のサイトの見栄えを完全にコピーしているものと見られ、将来的には本物の警告メールをもコピーあるいは的確に模倣した文面を用いたりすることにより、フィッシングの精度をさらに向上させていくことでしょう。

- 人間の判断だけでフィッシングサイトを回避するのではなく、ブラウザ・アンチウイルスソフトあるいはUTMによるアンチフィッシング機能を有効活用することが肝要です。

ITmedia ニュース

ITmedia ニュース ＞ セキュリティ ＞「こんにちは！」 三菱東京UFJ銀行かたるフィッシ...

2015年07月28日 20時22分 更新

「こんにちは！」 三菱東京UFJ銀行かたるフィッシングメールに注意

三菱東京UFJ銀行をかたるフィッシングメールに注意喚起。メール本文は「こんにちは！」で始まるという。

[ITmedia]

フィッシング対策協議会は7月28日、三菱東京UFJ銀行をかたるフィッシングメールの報告を複数受けているとして注意を呼び掛けた。件名は「三菱東京UFJ銀行より大切なお知らせです」で、本文は「こんにちは！」で始まるという。

こんにちは！

（平成27年7月28日更新）「三菱東京UFJ銀行」のシステムが安全性の更新がされたため、お客様はアカウントが凍結?休眠されないように、直ちにアカウントをご認証ください。

以下のページより登録を続けてください。

ログイン - 三菱東京UFJ銀行<http://bk.mufg.jp.●●●●.work/ibg/dfw/APLIN/loginib/login?_TRANID=AA000_001>

――Copyright(C)2015 The Bank of Tokyo-Mitsubishi UFJ,Ltd.All rights reserved――

フィッシングメール本文

フィッシング対策協議会 Council of Anti-Phishing Japan

三菱東京UFJ銀行をかたるフィッシング（2015/07/28）

概要

三菱東京UFJ銀行をかたるフィッシングメールが出回っています。

メールの件名

重要なお知らせ
三菱東京UFJ銀行より大切なお知らせです

詳細内容

三菱東京UFJ銀行をかたるフィッシングの報告を複数受けています。

1. 2015/07/28 12:30 現在フィッシングサイトは稼働中であり、JPCERT/CC にサイト閉鎖のための調査を依頼中です。類似のフィッシングサイトが公開される可能性がありますので引き続きご注意ください。

2. このようなフィッシングサイトにてアカウント情報（ご契約番号、IBログインパスワード、乱数表の番号など）を絶対に入力しないようにご注意してください。

サイトのURL

http://bk.mufg.jp.●●●●.uno/ibg/dfw/APLIN/loginib/login.htm?_TRANID=AA000_001
http://bk.mufg.jp.●●●●.work/ibg/dfw/APLIN/loginib/login.htm?_TRANID=AA000_001
http://bk.mufg.jp.●●●●.work/ibg/dfw/APLIN/loginib/login?_TRANID=AA000_001
http://bk.mufg.jp.●●●●.space/ibg/dfw/APLIN/loginib/login.htm?_TRANID=AA000_001
http://bk.mufg.jp.●●●●.party/ibg/dfw/APLIN/loginib/login.htm?_TRANID=AA000_001

●Androidスマートフォンの95%に脆弱性

http://news.mynavi.jp/news/2015/07/28/611/
http://www.itmedia.co.jp/enterprise/articles/1507/30/news113.html

このニュースをザックリ言うと･･･

- 7月27日（現地時間）、米Zimperium社より、OSにAndroidを使用するスマートフォンに脆弱性が存在することが発表されました。

- この脆弱性はAndroidのメディア再生エンジン「Stagefright」に存在するもので、攻撃者が細工した動画等を含むMMS（マルチメディアメッセージングサービス）メッセージを受信することにより、スマートフォンがマルウェアに感染する等、リモートからほぼ完全に乗っ取ることができるというものです。

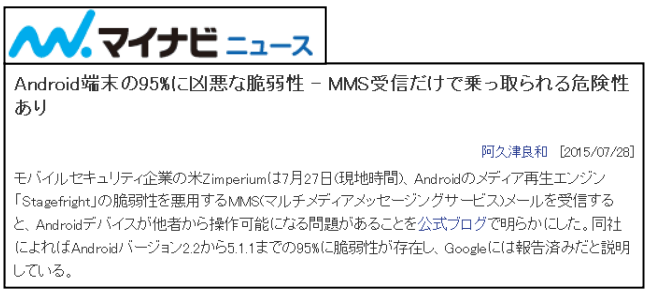
- 脆弱性はAndroid 2.2から5.1.1 r5より前のバージョンに存在し、Androidスマートフォンの実に95%に影響が及ぶとされています。

- 既に修正パッチがGoogleからリリースされていますが、各スマートフォンベンダーを通してアップデートが行われるには時間がかかる模様で、「見知らぬ送信者からのすべてのテキストメッセージをブロックする」「MMSの自動取込みを無効にする」といった回避策をとることが推奨されています。

AUS便りからの所感等

- かつての携帯電話と異なり、スマートフォンはPCと同等の機能が実行可能であり、またPC以上の普及率を誇る今では格好のマルウェアのターゲットとなっています。

- 修正パッチが適用されるまでは前述した回避策をとること、スマートフォン向けの何らかのアンチウイルスソフトを導入すること、そして、可能な限りUTMを経由して通信を行うことがマルウェアへの感染を効果的に抑制することでしょう。


マイナビ ニュース

Android端末の95%に凶悪な脆弱性 － MMS受信だけで乗っ取られる危険性あり

阿久津良和 [2015/07/28]

モバイルセキュリティ企業の米Zimperium(は7月27日(現地時間)、Androidのメディア再生エンジン「Stagefright」の脆弱性を悪用するMMS(マルチメディアメッセージングサービス)メールを受信すると、Androidデバイスが他者から操作可能になる問題があることを公式ブログで明らかにした。同社によればAndroidバージョン2.2から5.1.1までの95%に脆弱性が存在し、Googleには報告済みだと説明している。

●WebサイトへのSQLインジェクション攻撃、約21万人分の個人情報流出か

http://itpro.nikkeibp.co.jp/atcl/news/15/073002537/

このニュースをザックリ言うと･･･

- 7月30日（日本時間）、洋菓子等の製造・販売業であるシャトレーゼ社のWebサイトが不正アクセスを受け、同社Web会員約21万人のID・暗号化されたパスワード・メールアドレス・電話番号等が流出した可能性があると発表されました。

- 発表によれば、同28日に不審な入力内容の問合せが多くみられたことによって調査した結果、同27日夜から不正アクセスが行われており、Webサイトの問合せフォームに存在していた「SQLインジェクション」の脆弱性を突くことによって個人情報の流出が発生していたとされています。

AUS便りからの所感等

- 「SQLインジェクション」はWebサイト・Webアプリケーションに対する直接的な攻撃によってデータベースに不正アクセスを行う古典的な脆弱性であり、根本的な対策は本来Webアプリケーションの適切なプログラミングにより可能ですが、同社が「SQLインジェクション対策は講じていたつもりだったが、結果的にはセキュリティホールが残っていた」と述べているように、その適切なプログラミングを行うことが困難と考える向きもあるようです。

- SQLインジェクションやクロスサイトスクリプティング（XSS）等のアプリケーションレベルでの対策を確実に行う自信がないのであれば、Webアプリケーションファイアウォール（WAF）ないしそれを提供するUTMをWebサーバの前面に設置することにより、脆弱性を突くような不正なリクエストをある程度は遮断することができるでしょう。


ニュース　日経コンピュータ

シャトレーゼにSQLインジェクション攻撃、Web会員情報約21万人分流出の可能性

2015/07/30
清嶋 直樹＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

49 おすすめ　29 共有　14 ブックマーク　31 Pocket　54 ツイート　シェア

洋菓子などの製造・販売を手掛けるシャトレーゼ（甲府市）は2015年7月30日、Webサイトが外部から不正アクセス攻撃を受け、個人情報が流出した可能性があると発表した（画面）。

Châteraisé