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。

●福岡銀行やジャパンネット銀行の偽メールに注意、フィッシングは地方銀行にも

http://www.itmedia.co.jp/enterprise/articles/1608/19/news113.html
https://www.antiphishing.jp/news/alert/

このニュースをザックリ言うと･･･

- 8月19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により、福岡銀行とジャパンネット銀行を名乗るフィッシングメールおよびサイトを確認したとして警告が出されています。

- フィッシングメールの件名は、銀行名に続いて「重要なお知らせ(2016年8月18日更新)」「メールアドレスの確認」「本人認証サービス」等となっており、本文は「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」等、両方の銀行とも共通した文面とともに、以下のURLのような偽のログイン画面を表示するサイトへ誘導するものとなっています。

http://direct.fukuokabank.co.jp.●●●●.cc/0177/B/B/B/C100/KBC11BN000B000.htm
http://login.japannetbank.co.jp.●●●●.cc/wctx/f5dcfej6b826409601.htm

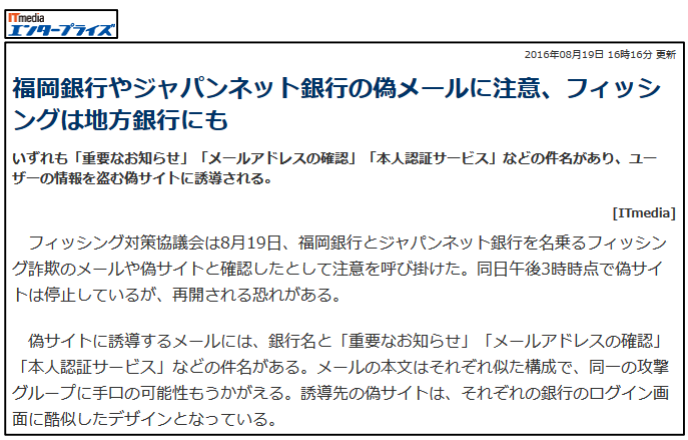
- 同協議会によれば、いずれも発表の時点でフィッシングサイトは閉鎖されているものの、今後再開あるいは類似したサイトが公開される恐れがあるとしており、こういったサイトでアカウント情報を絶対に入力しないよう、また同様のサイトやメールを見かけた場合は協議会へ連絡するよう呼び掛けられています。

AUS便りからの所感等

- 本文にて「貴様」と呼びかける不自然な文面のフィッシングは2014年から報告されており、協議会が発表した情報を確認する限りでは、当時と全く同じ文面を用い続けている模様です（AUS便り2016/03/07号参照）。

- 偽サイトのURLは「http://」である一方、福岡銀行、ジャパンネット銀行をはじめ多くの銀行では本物のログイン画面において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るため、これに注意している限り確認は可能です。

- この他、メールに記載されたリンクを安易にクリックしないことはもちろんですが、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を自己防衛の方法として強く推奨致します。


ITmedia エンタープライズ

2016年08月19日 16時16分 更新

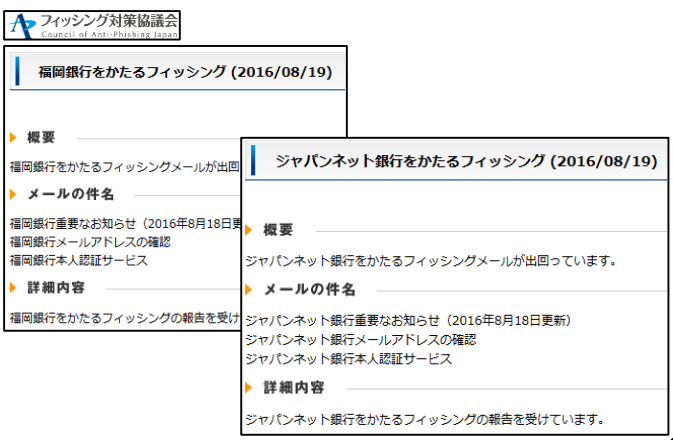
福岡銀行やジャパンネット銀行の偽メールに注意、フィッシングは地方銀行にも

いずれも「重要なお知らせ」「メールアドレスの確認」「本人認証サービス」などの件名があり、ユーザーの情報を盗む偽サイトに誘導される。

[ITmedia]

フィッシング対策協議会は8月19日、福岡銀行とジャパンネット銀行を名乗るフィッシング詐欺のメールや偽サイトと確認したとして注意を呼び掛けた。同日午後3時時点で偽サイトは停止しているが、再開される恐れがある。

偽サイトに誘導するメールには、銀行名と「重要なお知らせ」「メールアドレスの確認」「本人認証サービス」などの件名がある。メールの本文はそれぞれ似た構成で、同一の攻撃グループに手口の可能性もうかがえる。誘導先の偽サイトは、それぞれの銀行のログイン画面に酷似したデザインとなっている。


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

福岡銀行をかたるフィッシング (2016/08/19)

概要
福岡銀行をかたるフィッシングメールが出回

メールの件名
福岡銀行重要なお知らせ（2016年8月18日更
福岡銀行メールアドレスの確認
福岡銀行本人認証サービス

詳細内容
福岡銀行をかたるフィッシングの報告を受け

ジャパンネット銀行をかたるフィッシング (2016/08/19)

概要
ジャパンネット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
ジャパンネット銀行重要なお知らせ（2016年8月18日更新）
ジャパンネット銀行メールアドレスの確認
ジャパンネット銀行本人認証サービス

詳細内容
ジャパンネット銀行をかたるフィッシングの報告を受けています。

●LinuxとAndroidに通信乗っ取りの脆弱性

http://internet.watch.impress.co.jp/docs/news/1015198.html

このニュースをザックリ言うと･･･

- 8月9日（米国時間）、米カリフォルニア大学リバーサイド校(UCR)により、Linuxカーネル バージョン3.6（2012年リリース）以降において、TCP/IP実装に脆弱性が存在することが報告されました。

- 続いて8月15日には、モバイルセキュリティベンダーの米Lookout社により、Android バージョン4.4（2013年リリース）以降も同様の脆弱性の影響を受ける恐れがあるとの警告が出されおり、現在出回っているAndroidデバイスの79.9%がこれに該当するとの報告もあります。

- 脆弱性を悪用した中間者攻撃を行うことにより、TCP通信に第三者が割り込み、不正なTCPパケットを送信することが可能とされており、Linuxについてはカーネルに対するパッチが7月にリリースされ、ディストリビューションでの対応が進んでいますが、Androidについてはまだパッチがリリースされていない模様です。

AUS便りからの所感等

- この脆弱性による攻撃にあたっては、攻撃者は送信元・送信先のIPアドレスと、送信元TCPポートを把握している必要があるとされていますが、一方で、Lookoutによれば、SSL/TLSあるいはVPNによる暗号化通信等により、回避可能とのことです。

- Androidが影響を受けるとされるのは、カスタマイズされたLinuxカーネルが使用されているためで、同様にLinuxを用いているアプライアンス（NAS・ルータ・UTM等）についても影響を受ける可能性は高く、可能な限りベンダーに問合せることが肝要です。

INTERNET Watch

Linux TCPスタック実装の脆弱性、Android 4.4以降の14億台の端末に影響

岩崎 宰守　2016年8月16日 15:40

Red Hat Enterprise Linuxから7月12日に公表されていたLinuxカーネルにおけるTCPスタック実装の脆弱性「CVE-2016-5696」が、Android 4.4以降の14億台の端末に影響するとして、米Lookoutが8月15日付けの同社公式ブログで注意を喚起している。

CVE-2016-5696は、米国テキサス州オースティンで開催された「USENIX Security 2016 conference」で、米カリフォルニア大学リバーサイド校（UCR）により報告されたもの。リモートの攻撃者が暗号化されていないトラフィックを傍受し、通信を停止したり偽の通信に変更できる。このため、標的型攻撃に利用することもできるという。ただし、攻撃する場合には送信元・送信先のIPアドレスと、送信元ポートを把握している必要があるとのこと。共通脆弱性評価システムCVSS v3による脆弱性評価は4.8。

- 今後の状況によっては、この脆弱性を狙っているとみられる攻撃パケットをアンチウイルスやUTM等で検出・遮断可能になることも考えられますが、前述のとおりUTM自体が脆弱性の影響を受ける可能性もまた存在することに注意してください。

●「ln.is」で始まるリンクに注意･･･投稿を書き換えるTwitterアプリ

http://nlab.itmedia.co.jp/nl/articles/1608/19/news097.html

このニュースをザックリ言うと･･･

- URLを含むツイートを書き換える挙動をし、2013年にTwitter上で問題となったアプリ「Linkis.com」（以下Linkis）によるツイートが8月18日以降多く確認されています。

- Linkisによるツイートは、URLが「ln.is」を含んでいることが特徴で、このURLをクリックすると、本来のリンク先のコンテンツと共に、Linkisと連携するよう誘導するメッセージが表示されます。

- これを利用しているとみられるツイートは2013年に問題となった以後も散見されていましたが、8月18日に登場したWebサイト「日本語ボキャブラリーテスト」（Linkisとは無関係）での診断結果の投稿において、URLに「ln.is」を含むものが頻繁に確認されるようになったことから、Twitterユーザにより、心当たりのある者はLinkisとの連携を解除するよう呼びかけられています。

AUS便りからの所感等

- Linkisと連携すると、以後ユーザが投稿したツイートが監視され、URLを含んでいる場合は一旦そのツイートを削除し、「ln.is」を含むURLに書き換えて再投稿され、その際のURLのアクセス先は本来のサイトではなく、Linkisのサイトとなります。

ねとらぼ

2016年08月19日 13時10分 更新

「ln.is」で始まるリンクにご用心　2013年のスパムが「語彙力テスト」きっかけで再び拡散中

8月18日に流行した語彙力テストの結果を、多数の人がスパムアプリに感染したままシェアしてしまったもよう。

[岩澤真二，ねとらぼ]

8月18日から「日本語ボキャブラリーテスト」という語彙力テストがTwitterで流行中。50の四択問題に答えると診断結果が表示されるもので、大勢が結果をシェアしていました。しかしそのなかには、「ln.is」なるスパムに感染している人がたくさんいると、指摘する声があがっています。

- Twitterでは、このような不正なアプリとの連携により、身に覚えのない投稿やDM送信を行ってしまう等のケースが以前から度々報告されており、アプリとの連携は、そういった行動をユーザ自身の権限で行うこと、また自分が投稿したツイートや送信したDMを見ることをアプリの提供者に対し許可することを意味します。

- また、その際のTwitterへのアクセスは、必ずしもユーザ自身のPCやスマホ等から発生するものとは限らないため、UTM等での通信の遮断による防御も困難です。

- アプリとの連携の際は、必ずユーザに対し連携を行うか否か尋ねられますので、Twitterやその他の情報源を検索した上で、信用できるアプリか判断し、そして、連携するアプリを必要最小限に留めることが肝要です。