— AUS（アルテミス・ユーザ・サポート）便り 2018/06/25号 —
https://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。

●LINEやMUFGカード等をかたるフィッシング、対策協議会が警告

http://www.antiphishing.jp/news/alert/line_20180606.html
http://www.antiphishing.jp/news/alert/mufgcard_20180621.html

このニュースをザックリ言うと・・・

- 6月6日および21日（日本時間）、フィッシング対策協議会より、LINEおよびMUFGカードをかたるフィッシングが確認されているとして注意喚起が出されています。

- 6日に注意喚起が出されたLINEのフィッシングメールは、本文に「最近LINEアカウントの盗用が多発しており、ご不便をもたらして、申し訳ありません」「あなたのアカウントが盗まれないよう、システムは2段階パスワードに更新しました」等と書かれ、メールアドレスとパスワードを詐取する下記のようなURLのページへのリンクが貼られています。
http://www.line●●.cn/

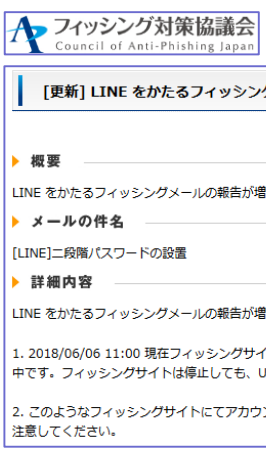
- 21日に注意喚起が出されたMUFGカードのフィッシングメールは、本文に「通知：アカウント情報の有効期限が切れました」等と書かれ、以下のようなURL短縮サービスを利用したURLによるリンクが貼られています。
http://ht.ly/●●●●
http://owl.li/●●●●
またこれをクリックすることにより、以下のようなURLの偽のログインページにリダイレクトするようになっています。
https://mitsubishi-ufj-mufg-financial.●●●●.com/

AUS便りからの所感等

- LINEをかたるフィッシングについては、今回と全く同じ文面のメールが2017年7月にも確認され、同協議会（https://www.antiphishing.jp/news/alert/line_20170707.html）でも注意喚起されています。

- 同協議会では、類似のフィッシングサイトがURLを変えて公開される可能性もあるとし、このようなサイトにてアカウント情報（ID、パスワード）、クレジットカード情報（カード番号、カード有効期限、セキュリティコード）等を絶対に入力しないよう呼び掛けています。

- Webブラウザやアンチウイルスソフト・UTMが提供する、フィッシングサイトへのアクセスを警告あるいは遮断する等のアンチフィッシング機能を必ず有効にするとともに、フィッシングに騙される可能性を減らすための自衛策として、通常使用するサービスのログインページ等にはブックマークからアクセスすることを推奨致します。


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

[更新] LINE をかたるフィッシング (2018/06/06)

概要

LINE をかたるフィッシングメールの報告が増えています。

メールの件名

[LINE]二段階パスワードの設置

詳細内容

LINE をかたるフィッシングメールの報告が増えています。

1. 2018/06/06 11:00 現在フィッシングサイトは稼働中であり、JPCERT/CC にテイクダウン（サイト閉鎖）を依頼中です。フィッシングサイトは停止しても、URL を変えて次々と立ち上がっているため、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 (メールアドレス・パスワードなど) を絶対に入力しないように注意してください。


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

MUFG カードをかたるフィッシング (2018/06/21)

概要

MUFG カード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

三菱ＵＦＪダイレクト

詳細内容

MUFG カードをかたるフィッシングの報告を受けています。

1. 2018/06/21 14:30 現在、フィッシングサイトが稼働中であり、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（ID、パスワード）、クレジットカード情報 (カード番号、カード有効期限、セキュリティコード) 等を絶対に入力しないように注意してください。

●「Mirai」「Satori」によるアクセス再び増加か…警察庁等が警告

https://www.npa.go.jp/cyberpolice/important/2018/201806131.html

このニュースをザックリ言うと・・・

- 6月13日（日本時間）、警察庁より、2007年に猛威を振るったIoTマルウェア「Mirai」によるとみられるアクセスが増加しているとして注意喚起が出されています。

- 同10日以降に定点観測システムにおいてTCPポート80番（HTTP）宛のアクセスの増加が観測され、かつそのTCPパケットの特徴からMiraiによるものとされています。

- その後、海外のセキュリティベンダー数社も、Miraiの亜種「Satori」による攻撃が激化していると相次いで警告しています。

AUS便りからの所感等

- MiraiやSatoriによるアクセスの発信元ではネットワークビデオレコーダ等の様々なIoT機器に搭載されているWebサーバソフトウェア「XiongMai uc-httpd」の稼働が確認されており、6月に公表されたばかりのものを含むいくつかの脆弱性が悪用されているとしています。

- IoT機器はそれ自身がファイアウォール等の十分なセキュリティ機能を持っていない可能性もありますので、決してインターネットに直接接続せず、ルータ・UTMのポートフィルタリング機能等による防御を行うことが重要です。

- また機器自体についても、管理画面のユーザ・パスワードを必ず推測されにくいものに変更すること、ベンダーのサイトを確認してファームウェアのアップデートを行うこと、あるいは脆弱性が修正されないままサポートが終了しているものについては使用を中止すること、等を警察庁では推奨しています。

●約57万件の個人情報が漏洩、WAF設定ミスでSQLインジェクション攻撃防げず

https://cybersecurity-jp.com/news/24926

このニュースをザックリ言うと・・・

- 5月14日（日本時間）、リサーチ業務を行うMS&Consulting社より、同社運営サイト「ミステリーショッピングリサーチ」が不正アクセスを受け、個人情報が流出していたことが発表されましたが、6月1日にも続報が発表されています。

- 流出の被害を受けたのは、同サイトに登録されたメールアドレス・パスワード・電話番号（重複登録・登録未完了およびメール配信停止中のもの含む）約57万件とされています。

- 5月の発表の時点では5月2日に不正アクセスがあったとされ、被害件数は6119件とされていましたが、その後5月以前にも不正アクセスがあったことが明らかになり、6月の続報では件数が約57万件と修正されています。

AUS便りからの所感等

- WebアプリケーションのSQLインジェクションの脆弱性を突かれたうえ、WAFが設定ミスにより機能していなかったことが流出の原因とされています。

- アンチウイルス・UTM等のセキュリティ防御策以外にも（例えばデータバックアップ等）言えることですが、何らかのソリューションの採用にあたってはそれが確実に機能しているか、いざというときに機能するかを確認することもまた重要です。

- 一方で、WAFが確実に機能していたとしても、それを回避してWebアプリケーションの脆弱性を突く攻撃が出てくる可能性は皆無ではありませんので、根本的な対策として、脆弱性の存在を確認し、修正することが最も大事であることは常に意識しておくべきでしょう。