— AUS（アルテミス・ユーザ・サポート）便り 2024/9/5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。

●「@」と偽の「/」を用いた偽装URLによるフィッシングの手口が話題に

https://forest.watch.impress.co.jp/docs/serial/yajiuma/1620057.html

このニュースをザックリ言うと･･･

- 8月30日(日本時間)、インプレス社「やじうまの杜」において、同29日にX(旧・Twitter)で取り上げられ話題となったフィッシングの手口が言及されています。
- メール記載のリンクにマウスカーソルを合わせて表示されるURLでは「https:// 」の直後に一見本物のドメイン名が書かれているように見えますが、実際には「@(アットマーク)」の後ろに記載されているフィッシングサイトにアクセスするというものです。
- 昔から利用されていたURL形式で、ホスト名の前に「@」と認証情報を記載する仕様を悪用し、その箇所でドメイン名とパスとを区切る「/(スラッシュ記号)」に偽装して「スラッシュっぽく見える別の文字」を使う等、より誤認しやすい手口を用いています。
- 記事では、メールは基本的に「信用できないものとして扱うべき」とし、銀行やカード会社からの連絡は公式Webサイトや専用アプリで確認すべきとしています。

AUS便りからの所感等

- 古くはFTPで、現在でもHTTPのBASIC認証等において、ユーザー名・パスワードを「https://username@example.co.jp/path」もしくは「https://username:password@example.co.jp/path」といった形式で記載するのが本来の用法で、今回の手口では「username」「username:password」の部分で偽装を行っており、また「スラッシュっぽく見える別の文字」としては、UnicodeのU+2044(FRACTION SLASH)・U+2215(DIVISION SLASH)・U+29F8(BIG SOLIDUS)等、多くの種類が考えられます。
- 従来のフィッシングにおける、リンク先URLのホスト名(FQDN)に本物のドメイン名やそれと似た文字を含む、さらには国際化ドメイン名(IDN)の仕様を突いてアルファベット以外の似た文字を用いるケースと異なり、偽のドメイン名の登録やDNSの用意は必要でなく、「@」より前の部分でIDNで許可されていない記号(「スラッシュっぽく見える別の文字」も含まれます)を利用可能であるという「利点」があると考えられます。
- ブラウザー・メーラー側やメールサーバー上・UTM等でのメールチェックにおいて、リンクURL中に不審なUnicode文字を含む認証情報部分がある場合に警告を出す、または認証情報部分の誤認されやすい記号等をURLエンコード状態で表示する、といった対策が取られるものと考えられる一方、DNSによる不審サイトのブロックサービスではFQDN部分のみをチェックするため回避される可能性があることに注意が必要でしょう。

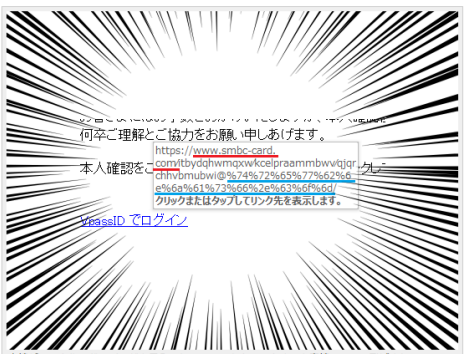
Impress Watch

やじうまの杜

こんなの絶対騙される……古いURL形式を使った巧妙な詐欺リンクの偽装方法が話題に

なるほど、頭いいなぁ

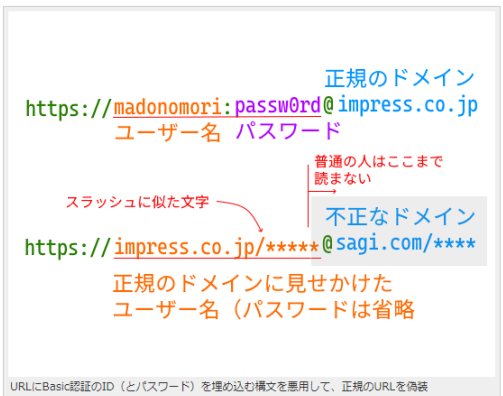
樽井 秀人　2024年8月30日 15:35



赤線がリンク先のドメインだと思うでしょ？　でもクリックすると青線のURLに飛ばされる

メールで送られてきたリンクは、アクセス先のドメインがホンモノかどうか注意深く確認してからクリックしましょう――というのはセキュリティの初歩としてよく言われますが、「目視でチェックしても絶対にわからないだろ！」という巧妙な手法が発見されて、「X」（旧称：Twitter）で少し話題になっています。

この方法は、URLにBasic認証のIDとパスワードを埋め込む構文を悪用したもの。「@」より前の部分をもつURLを見かけることは最近なくなりましたが――かつてFTP接続などでよく見かけましたよね――、れっきとした正しい記法です。



URLにBasic認証のID（とパスワード）を埋め込む構文を悪用して、正規のURLを偽装

本来ユーザー名に「スラッシュ」（/）を含めることはできませんが、そこは「スラッシュっぽく見える別の文字」で代用されているようです。これでパッと見、パスワード部分が正規のドメインのように見えてしまうわけ。

また、「@」以下の部分は不正なドメインだと悟られないよう、URLエンコードで隠蔽されています。実に巧妙ですね。

●XSS攻撃による不正アクセスで改ざん…個人情報21,728件・クレカ情報11,844件流出か

https://xtech.nikkei.com/atcl/nxt/news/24/01373/
https://www.zengyoren.or.jp/news/press_20240819/

このニュースをザックリ言うと・・・

－5月17日(日本時間)、全国漁業協同組合連合会(JF全漁連)より、ECサイト「JFおさかなマルシェ ギョギョいち」が不正アクセスを受け、個人情報およびクレジットカード情報が流出した可能性があると発表されました。

－8月19日に発表された続報によれば、被害を受けたのは、サイトに会員登録した21,728件の氏名・性別・生年月日・メールアドレス・住所・電話番号と、2021年4月22日～2024年5月14日にサイトでの決済に使用されたクレジットカード情報11,844件のカード番号・有効期限・セキュリティコード(CVV)とされています。

－5月14日にサイトの一部が改ざんされているとの警視庁からの連絡を受けサイトを停止しており、「サイト構築サービスにおけるクロスサイトスクリプティング(XSS)の脆弱性を突いての不正アクセスにより、不正ファイルの設置およびペイメントアプリケーションの改ざんが行われた」としています。

AUS便りからの所感

－当該サイトは現在も閉鎖中ですが、取り扱っていた商品は全国農業協同組合連合会(JA全農)「JAタウン」で販売しているとのことです。

－XSSから不正アクセスに至った経緯は、あくまで推測ながら、管理画面内で脆弱性が発現するよう仕掛ける不正な注文等を行う、いわゆる「Stored XSS(格納型・持続型XSS)」の攻撃を受けた可能性が考えられます。

－ECサイトを構築するメジャーなソフトウェアにおいても度々そのような脆弱性が発見・修正されており、随時最新のバージョンにアップデートすること、また特に独自でサイトを構築した場合は、可能な限り管理画面側も含めXSS他の脆弱性がないか第三者による診断を受けることを推奨致します。

日経XTECH

JF全漁連の通販サイトから個人情報2万件漏洩の可能性、XSS攻撃受け改ざん

渥美 友里　日経クロステック／日経コンピュータ

2024.08.19

全国漁業協同組合連合会（JF全漁連）は2024年8月19日、同会が運営する通販サイト「JFおさかなマルシェ ギョギョいち」への不正アクセス被害により、氏名や住所などの個人情報2万1728件、クレジットカード情報1万1844件が漏洩した可能性があると発表した。個人情報が漏洩した可能性のある顧客には、同日から電子メールで個別に連絡している。

●Windowsを脆弱なバージョンにダウングレードする攻撃「Windows Downdate」

https://www.itmedia.co.jp/news/articles/2408/21/news058.html
https://www.safebreach.com/blog/downgrade-attacks-using-windows-updates/
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21302
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38202

このニュースをザックリ言うと・・・

－8月7日(現地時間)、セキュリティカンファレンス「Black Hat USA」において、セキュリティ企業SafeBreach社の研究者により、Windowsを最新ではない脆弱なバージョンにダウングレードさせる攻撃「Windows Downdate」が発表されました。

－Windows Update機能を含むOSの脆弱性を悪用してこれを乗っ取り、OSを過去の脆弱なバージョンに戻したうえで、「完全にパッチ適用済み」であると偽装させるものとなっています。

－マイクロソフト(以下・MS)では2月にSafeBreach社から連絡を受けていたとし、8月7日に脆弱性「CVE-2024-21302」「CVE-2024-38202」として情報を発表、同14日の月例セキュリティアップデートでは一部(CVE-2024-21302)について対策しています。

AUS便りからの所感

－Windowsが最新のバージョンかは、通常であればwinverコマンド等で表示される「OS ビルド」の番号とMSの情報(https://learn.microsoft.com/ja-jp/windows/release-health/release-information 等)を照合させることにより確認可能ですが、ダウングレード攻撃の際に一部コンポーネントのみを差し替えられたり、ビルド番号を改ざんされたりすることも考えられます。

－今回の攻撃に関連する脆弱性はリモートから直接悪用可能ではない模様ですが、とにかくこのような攻撃を目論むマルウェアへの感染等を防止するため、OSを最新に保ち、アンチウイルスやUTMによる防御を固めること、またサーバーへのリモートデスクトップからの不正アクセス等にも注意を払うことが肝要です。

－8月時点で対策されていない残りの脆弱性(CVE-2024-38202)についてMSよりリスク軽減策が提案されているものの、将来的にはこれもアップデートによって解消されること、また攻撃が成立してダウングレードされた状態となっていないか検知あるいは修復できるような機構やツールが提供されることを期待したいものです。

ITmedia NEWS

Innovative Tech

Windowsを“古いバージョン”に戻す「ダウングレード攻撃」　修正済みの脆弱性をゼロデイ化、“最新の状態”を偽り検出も困難

2024年08月21日 08時00分 公開　［山下裕毅，ITmedia］

イスラエルのサイバーセキュリティ企業の米SafeBreachの研究者であるアロン・レヴィーさんは、セキュリティカンファレンス「Black Hat USA 2024」でWindowsアップデートプロセスを悪用してシステムを古い脆弱なバージョンに戻すダウングレード攻撃「Windows Downdate」を発表した。

この攻撃はWindowsアップデートを乗っ取り、カスタムダウングレードを作成して、過去の数千もの脆弱性を露呈させ、修正済みの脆弱性をゼロデイ化する。これにより、世界中のWindowsマシンにおいて「完全にパッチ適用済み」が無意味になる可能性がある。