— AUS（アルテミス・ユーザ・サポート）便り 2019/09/24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。

●8月度のフィッシング報告件数急増…メールの件名や文面、URLを少しずつ変える手口に注意

https://securityblog.jp/news/20190911.html
https://www.antiphishing.jp/report/monthly/201908.html

このニュースをザックリ言うと・・・

- 9月3日(日本時間)、フィッシング対策協議会より、8月に同協議会に寄せられたフィッシング報告状況が発表されました。

- 8月度のフィッシング報告件数は5,577件(6月度3,788件、7月度4,322件)、フィッシングサイトのURL件数は2,111件(6月度1,460件、7月度2,189件)、等となっています。

- フィッシングの手口の傾向として、「配達の不在通知を装ってApple IDなどを詐取する」「SMSを悪用して不正アプリのダウンロードサイトへ誘導する」ケースの報告が続いているとのことです。

AUS便りからの所感等

- フィッシング報告件数が7月度より1,255件と急増しており、フィッシングサイトの件数も7月度に急増して以降の高い水準を保っています。

- また、フィッシングメールの件名や文面、URLを少しずつ変えて小規模に送信するケースが増えており、インターネット上で検索しても情報が一致しないことがあるとして、注意を呼び掛けています。

- 当AUS便りや同協議会からもたびたび回避策として挙げられていますが、利用しているサービスのサイトへのアクセスは、不審なメール・SMS上のリンクからではなく、正規のアプリや事前に登録したブックマークからアクセスするよう是非とも心がけてください。

日立ソリューションズ Information security blog
情報セキュリティブログ

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

セキュリティニュース

件名や文面、URLを少しずつ変えるフィッシングメールの手口に注意を呼びかけ

2019年9月11日 0

9月3日、フィッシング対策協議会は、2019年8月の月次報告書を公開した。

これによると、フィッシング報告件数は5,577件となり、前月(4,322件)より1,255件増加した。また、フィッシングサイトのURL件数は2,111件で、こちらは前月より78件の減少。そして、フィッシングに悪用されたブランド件数は48件で、前月から13件減少している。

また、配達の不在通知を装ってApple IDなどを詐取するフィッシングサイトや、不正アプリのダウンロードサイトへ誘導するSMS(ショートメッセージサービス)を悪用した手口の報告も続いている。

そして、件名や文面、URLを少しずつ変えて小規模に送信するフィッシングメールも増えており、インターネット上で検索しても情報が一致しないことがあるため、注意が必要だ。

そのほかにも、事業者からの本物のお知らせメールに、フィッシングサイトへ誘導するリンクを追加した手口や、ブランド名に類似した表示名を使ったり、受信者の氏名や住所などをメールに記載して、不審なサイトへ誘導しようとしたりする手口もある。

同協議会では、フィッシングかどうかの判断に迷うメールや、不審なメールを受け取った場合は、各サービス事業者の問合せ窓口や同協議会まで連絡するよう、呼びかけている。

:: 報告書類

2019/08 フィッシング報告状況　月次報告書

2019年09月03日

フィッシング報告件数

2019 年 8 月にフィッシング対策協議会に寄せられたフィッシング報告件数 (海外含む) は、前月より 1,255 件増加し、5,577 件となりました。

総評

2019 年 8 月のフィッシング報告件数は 5,577 件となり、2019 年 7 月と比較すると 1,255 件の増加となりました。先月に引き続き Amazon、Apple、LINE、ゆうちょ銀行、MyEtherWallet をかたるフィッシングメールが大量に配信され、多くの報告を受領しました。また、配達の不在通知を装って Apple ID 等を詐取するフィッシングサイトや不正アプリのダウンロードサイトへ誘導するショートメッセージ (SMS) の報告も続いています。

フィッシングメールは同じ件名、文面で一度に大量に配信されることが多いですが、件名や文面、URL を少しずつ変えて小規模に送信する手の込んだフィッシングメールも増えており、インターネット上で検索しても情報が一致せず、確認しづらいため、注意が必要です。事業者からの本物のお知らせメールに、フィッシングサイトへ誘導するリンクを追加した、違和感を感じさせないフィッシングメールもあります。ログインを促すようなメールや SMS を受信した際は、正規のアプリやブックマークした正規の URL からサービスへログインして情報を確認するよう常に心がけてください。

また、ブランド名に類似した表示名を使ったり、受信者の氏名や住所等をメールに記載して、不審なサイトへ誘導しようとする迷惑メールが増えています。このようなメールは執拗に何度も送られてきますが、メール内の URL へアクセスしたり連絡をしないようご注意ください。

フィッシングか否かの判断に迷うメールや、不審なメールを受け取った場合は、各サービス事業者の問合せ窓口やフィッシング対策協議会 (info@antiphishing.jp) までご連絡ください。

●エクアドル、2,000万人分以上の個人情報流出…ほぼ全国民分、死亡者も含むか

https://www.nikkei.com/article/DGXMZO49918550Y9A910C1000000/
https://www.cnn.co.jp/tech/35142751.html
https://japan.cnet.com/article/35142799/

このニュースをザックリ言うと・・・

- 9月16日(現地時間)、エクアドル政府より、同国民ほぼ全員を含む約2,000万人分の個人情報(氏名・性別・生年月日・メールアドレス・個人番号および銀行口座残高等)がインターネット上のデータベースサーバーにおいて公開状態にあったと発表されました。
- サーバーは同国のコンサルティング企業「Novaestrat」が所有していたもので、全人口が約1,650万人であることから、死亡者数百万人の情報も含まれているとみられています。
- ネットセキュリティーの専門家集団「vpnMentor」が上記サーバーの存在を確認したことにより発覚したもので、同16日中にNovaestrat社の経営者が家宅捜査を受け拘束されています。

AUS便りからの所感

- 個人情報には、2012年から今年4月に逮捕されるまで在英エクアドル大使館に潜伏していた内部告発サイト「ウィキリークス」の創設者、ジュリアン・アサンジ被告のものも含まれていると報じられています。
- 今月にはFacebookユーザー約4億1,9000万件以上の電話番号が流出した(AUS便り2019/9/17号参照)ことも報じられたばかりで、データベースサーバーにアクセス制限の設定がかかっていなかったことも同様です。
- データベースサーバーを配置する場所(クラウドやオンプレミス)に拘らずパスワード等による適切なアクセス制限をかけることや、必要な対策を洗い出し実行することは当然重要ですし、一方で個人情報やセンシティブな情報を収集・保存するにあたっては、流出のリスクを考慮し、必要でない情報をそもそも収集しないこと、あるいは一箇所に多岐にわたる種類の情報を保存せずデータベースを分散することも、検討に値するでしょう。

●複数のSSL VPN製品に脆弱性、攻撃の傾向も…JPCERT/CCが注意喚起

https://news.mynavi.jp/article/20190902-887399/
https://www.jpcert.or.jp/at/2019/at190033.html

このニュースをザックリ言うと・・・

- 9月2日(日本時間)、JPCERT/CCより、複数メーカーのSSL VPN製品の脆弱性に関する注意喚起が出されました。
- 対象のメーカーはPalo Alto Networks、FortinetおよびPulse Secureで、SSL VPNのユーザーでない外部の攻撃者により、VPN機器を乗っ取られたり、システムファイルを読み取られたりする可能性があるとされており、既に攻撃ツールが出回っているという情報もあります。
- また、脆弱性のある機器を検索するスキャンパケットや、特にPulse Secure社製品の脆弱性についてはこれを悪用する攻撃が確認されたとのことで、脆弱性が存在する機器・バージョンの場合はアップデートを行うよう呼びかけられています。

AUS便りからの所感等

- 脆弱性の多くは、SSL VPNにログインするためのWeb画面に対する攻撃により悪用が可能とみられますが、モバイル回線からのVPN接続を想定するケースではアクセス元IPアドレスを限定することはできないため、不特定多数のアクセス元から攻撃者がWeb画面に不正にアクセスしてくる可能性を考えなければいけないでしょう。
- 一時的な回避策として、Web画面のポート番号を443番(HTTPS)あるいは機器のデフォルトの設定から変更することが挙げられるものの、執念深い攻撃者に変更したポート番号を探り当てられるのは時間の問題と考えられます。
- クライアントPCに比べ、サーバーPCあるいはアプライアンスについてはOS・ファームウェアのアップデートに関する意識が及びにくい傾向があり、稼働している全ての機器を確実に把握・管理し、ベンダー等からのセキュリティ情報を随時収集し、可能な限り速やかにアップデートを行う体制を整えることが肝要です。