— AUS（アルテミス・ユーザ・サポート）便り 2022/08/16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。

●7月度フィッシング報告件数は107,948件で初の10万件突破、フィッシングサイトURL件数も49,188件と激増

https://www.antiphishing.jp/report/monthly/202207.html

このニュースをザックリ言うと･･･

- 8月3日(日本時間)、フィッシング対策協議会より、7月に寄せられたフィッシング報告状況が発表されました。
- 7月度の報告件数は107,948件で、6月度(https://www.antiphishing.jp/report/monthly/202206.html)の88,250件から19,698件増加し、初めて10万件を突破しています。
- フィッシングサイトのURL件数は49,188件と、6月度の27,217件から21,971件の急増で、こちらも初めて3万件を突破、過去最高を引き続き更新しています(ただしIPアドレスが同一のものが多いとされています)。
- またフィッシングサイトで使用されるTLD(トップレベルドメイン)の割合は.coが約41.6%でトップ、次いで.topが約27.7%、.cnが約9.1%、以下.tt、.shop、.xyz、.comが上位に挙げられています。

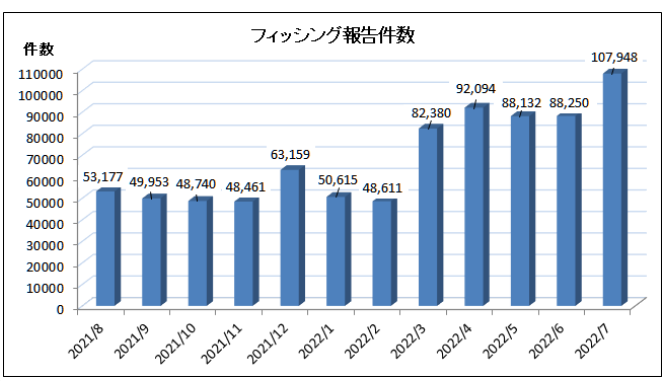
AUS便りからの所感等

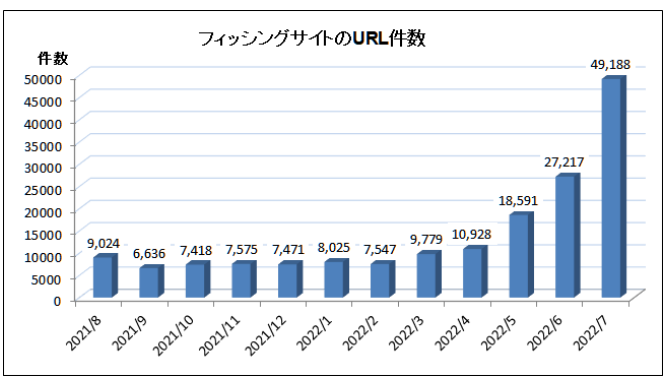
- 報告件数の水準は、2021年8月～2022年2月に5万件前後、2022年3月～6月に9万件前後と、どんどん増加を見せており、以前の水準に落ち着くことは恐らくないでしょう。
- 今回、報告全体の約47.6%がクレジットカードの利用確認を装うフィッシングとされ、またブランド別ではVISA・マスターカード・JCB・Amazon・三井住友カードで約73.2%、さらに1000件以上の報告があった15ブランドで約92.7%を占める、等の結果が出ています。
- また、8月に同協議会が注意喚起を出しているフィッシングの一例において「Google翻訳の正規URL(https://translate.google.com/translate?●●●●)からフィッシングサイトに誘導する」ものが挙げられています(https://www.antiphishing.jp/news/alert/googletranslate_20220809.html)。
- 短縮URLサービスの利用等も含め、メール記載のURLや最初のアクセス先からフィッシングサイトに誘導されるか否かを判断しづらいようにする手口は既に珍しいものではなく、ユーザー側でのフィッシングからの防御においては、決して自分たちだけで判断するのではなく、ブラウザーやアンチウイルス・UTMのアンチフィッシング機能を確実に有効化すること等を行うよう強く推奨致します。

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

2022/07 フィッシング報告状況　　月次報告書

2022年08月03日





●Twitter、540万人分のアカウント情報流出認める…パスワードは含まれず

https://www.itmedia.co.jp/news/articles/2208/08/news065.html
https://privacy.twitter.com/en/blog/2022/an-issue-affecting-some-anonymous-accounts
https://www.bleepingcomputer.com/news/security/twitter-confirms-zero-day-used-to-expose-data-of-54-million-accounts/

このニュースをザックリ言うと・・・

- 8月5日(米国時間)、Twitter運営より、同ユーザー540万人分のアカウント情報の一部が流出していたと発表されました。
- 7月21日にセキュリティ情報サイト「Restore Privacy」において、当該情報がアンダーグラウンドのハッキングフォーラムで販売されていたとされ、Twitterシステムの脆弱性を悪用し、大量に奪取された可能性が報じられていたもの(AUS便り 2022/07/26号参照)で、今回Twitter運営がこれを事実と認めた形となっています。
- PC情報サイト「Bleeping Computer」が報じたところでは、含まれる情報は電話番号あるいはメールアドレス・フォロワー数・ユーザー名・ログイン名・プロフィール画像のURL等とされ、パスワードは流出していないとのことです。
- Twitterでは、Restore Privacyの報道を受けて、影響を受けたことが確認できるユーザーに対しては直接通知を行うとともに、アカウント保護のため二段階認証の設定を行うよう呼び掛けています。

AUS便りからの所感

- 悪用された脆弱性は昨年6月のシステム修正で発生したもので、指定したメールアドレスまたは電話番号に関連付けられたTwitterのアカウント情報を取得可能なものとされていますが、運営では今年1月にバグ報奨金プラットフォームを通して報告を受けていたとのことで、現在は既に修正されています。
- アカウントへの不正ログインや連携アプリの不正操作につながるような情報の流出こそなかったものの、ハッキングフォーラムで攻撃者が購入したとされており、SPAMメール・フィッシングメールを送信する等の対象となるまとまった情報としては十分に有用な情報となり得ることが窺えます。
- 二段階認証の設定は、今回のケースにおいて流出の対象となったユーザーが流出による弊害を直接緩和できる可能性こそ低いでしょうが、他のサービスも含め可能な限り実行して頂き、また個人のみならず、企業組織で導入しているグループウェア等でも、利用可能なものについて利用を呼び掛け、外部の第三者による機密情報へのアクセスを防止するために活用されるのが望ましいでしょう。

●夏季休暇における情報セキュリティの注意喚起、IPA・NISCより発表

https://www.ipa.go.jp/security/topics/alert20220803.html
https://www.meti.go.jp/press/2022/08/20220808003/20220808003.html

このニュースをザックリ言うと・・・

- 8月3日(日本時間)にIPAより、同8日には経済産業省(METI)・総務省・警察庁および内閣官房内閣サイバーセキュリティセンター(NISC)の連名で、夏季休暇を迎えるにあたっての、情報セキュリティに関する注意喚起が出されました。
- 企業・組織によっては、この時期に多くの人が長期休暇を取得、常駐する人が少なくなる等「いつもとは違う状況」となり、通常時には生じにくい様々な問題が発生し得ることを鑑み、「組織のシステム管理者」「組織の利用者」「家庭の利用者」それぞれを対象に、「休暇前」「休暇中」「休暇明け」に行うべき基本的な対策と心得が「長期休暇における情報セキュリティ対策」においてまとめられています。
- IPAは毎年の夏季・冬季休暇およびゴールデンウィークの時期に注意喚起を行っており(https://www.ipa.go.jp/security/measures/vacation.html)、一方METI・NISC等の連名による注意喚起は今年2月から開始しています。

AUS便りからの所感

- 注意喚起の内容は、システム管理者が長期間不在になる等により、ウイルス感染や不正アクセス等のインシデント発生に気付きにくく対処が遅れてしまう可能性から、従業員が旅行先等でSNSへの書き込みを行った場合に、最悪関係者にも思わぬ被害が及んでしまう可能性まで、多様なものとなっています。
- 一方で、挙げられているセキュリティ対策の内容は毎回大きく異なるようなものではなく、この他にも長期休暇に関係なく常時から注意すべき普遍的なものも「日常的に実施すべき情報セキュリティ対策(https://www.ipa.go.jp/security/measures/everyday.html)」として別途まとまっています。
- 以後も冬期休暇、あるいはそれ以前に9月後半のいわゆる「シルバーウィーク」において3連休が続いたり、長期休暇をとる人が出てくるといった状況が狙われる恐れがあり、準備・点検を行うよう意識していくことが肝要です。