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。

●「ウイルス検出の偽警告」「ワンクリック請求」増加…IPA相談窓口 10月～12月の相談状況発表

https://www.ipa.go.jp/security/txt/2021/q4outline.html

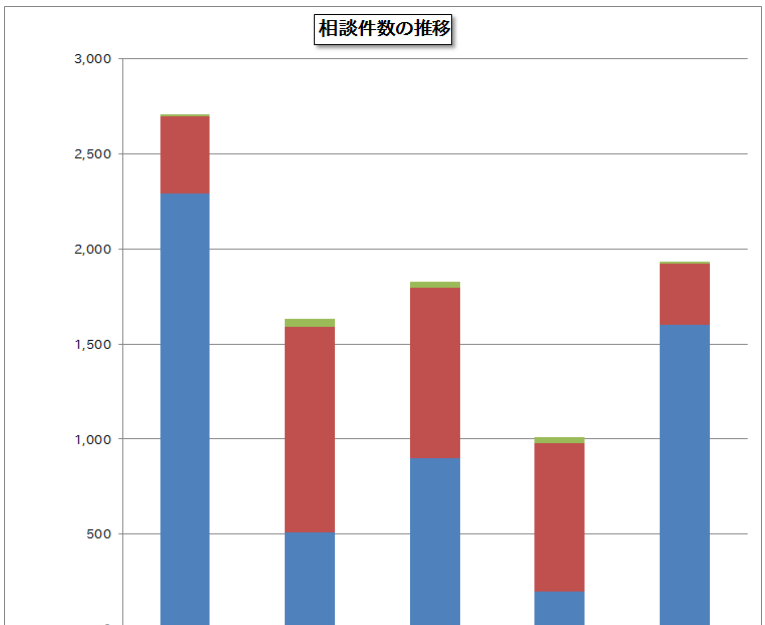
このニュースをザックリ言うと・・・

- 1月18日(日本時間)、情報処理推進機構(IPA)より、同機構の情報セキュリティ安心相談窓口で2021年第4四半期(10月～12月)に受け付けられた相談状況について発表されました。
- 同時期における相談員対応件数は1,933件で、前四半期(7～9月)の1,012件より約91.0%増加となっています。
- 相談件数の多いとされる手口7種類のうち、前四半期から増加したものとしては「ウイルス検出の偽警告(前四半期192件→今四半期420件、以下同様)」「宅配便業者をかたる偽SMS(67件→161件)」「ワンクリック請求(21件→58件)」「不正ログイン(16件→53件)」「Emotet関連(0件→12件)」が挙げられています。

AUS便りからの所感等

- 同窓口の相談件数は、過去最少水準となった前四半期から増加に転じており、特にEmotetに関しては半年間相談0件だったものが活動再開により再び相談が来ていた模様です。
- 前四半期から相談件数が減少していた手口は「仮想通貨で金銭を要求する迷惑メール(98件→57件)」「Facebookのメッセンジャーに届く動画(1件→0件)」ですが、前者は2021年第1四半期(204件)をピークに減少しているとはいえ、様々な文言での大量送信が現在も確認されており、明らかな迷惑メールとして相談されることが少なくなったものとも考えられます。
- 2022年第1四半期(1～3月)においては、これまで以上の感染者数増加をみせる新型コロナ感染症や、現在開催中の北京冬季オリンピック等に乗じた詐欺行為等が発生すると考えられ、アンチウイルスやUTM等による防御も含め、油断なく各種防衛策をとるに越したことはありません。

IPA 情報セキュリティ安心相談窓口の相談状況［2021年第4四半期（10月～12月）］



	2020/10～12	2021/1～3	2021/4～6	2021/7～9	2021/10～12
FAX・その他	12	41	29	33	10
電子メール	407	1,082	901	783	322
電話	2,290	508	897	196	1,601
合計	2,709	1,631	1,827	1,012	1,933

● 1月度フィッシング報告数は50,615件、引き続き5万件越え

https://www.antiphishing.jp/report/monthly/202201.html

このニュースをザックリ言うと・・・

- 2月3日(日本時間)、フィッシング対策協議会より、1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。

- 1月度の報告件数は50,615件で、昨年12月度(https://www.antiphishing.jp/report/monthly/202112.html)の63,159件からは12,544件減少となっています。

- 一方、フィッシングサイトのURL件数は8,025件(12月度 7,471件)、悪用されたブランド件数は86件(12月度 77件)とそれぞれ増加しています。

- 報告全体に対するブランドの割合については、最も多いAmazonは約33.8%と12月度(27.4%)より増加、これにメルカリ・JCB・三井住友カードを合わせた4ブランドで約67.6%、また1,000件以上の報告があったブランドが10あり、これらで全体の約82.9%を占めたとしています。

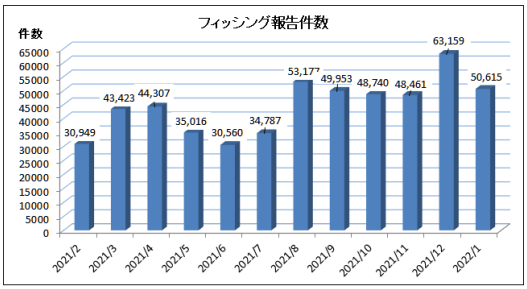
AUS便りからの所感

- これまでに比べ突出した報告件数となった12月度から一転、今月度は8月度以降の水準に立ち戻っているものの、依然として5万件前後という高い水準は維持しています。

- 同協議会で1月に出された4件の注意喚起のうち、例えば1月28日分のUber Eatsを騙るフィッシングについて(https://www.antiphishing.jp/news/alert/uber_eats_20220128.html)では、誘導先の偽サイトでメールアドレス・電話番号および4桁の認証コードの入力が求められるとしており、詐取された情報を悪用して他のサービスへの不正なログインやアカウントの登録等が行われるの恐れもあるため、決して各種情報を入力しないよう注意しましょう(同協議会では、身に覚えのないタイミングで認証コードの通知があった場合、サービスの使用履歴の確認あるいはパスワードの変更を行うよう推奨しています)。

- メールサーバーの管理者としては、何らかのサービスの運営者でなくとも、メールをやり取りする取引先等の相手がなりすましメールを排除できるよう、これまでにも挙げられているDMARC・SPFあるいは先月紹介されたBIMIのような機構の導入を検討すること、またメール・SMSを受信するユーザー側としても、「不審な文面について検索で裏をとる」「利用しているサービスへはブラウザーのブックマークからアクセスする」等フィッシングに引っかからないよう慎重な行動をとるよう心掛けることが肝要です。

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



●Sambaに脆弱性、ファイルサーバー・NAS乗っ取りの恐れも

https://news.mynavi.jp/techplus/article/20220202-2262365/
https://jvn.jp/vu/JVNVU92602689/

このニュースをザックリ言うと・・・

- 2月1日(日本時間)、Linux等からWindows Serverと互換性のあるファイル共有機能等を提供するソフトウェア「Samba」の開発元より、Sambaの脆弱性(CVE-2021-44142)について注意喚起が出されています。

- 発表によれば、脆弱性はSambaのvfs_fruitモジュールに存在し、当該モジュールが有効の場合に、サーバー上の管理者権限で任意のコードを実行される恐れがあるとのことです。

- この他にも複数の脆弱性(CVE-2021-44141, CVE-2022-0336)を修正した最新バージョンとして4.13.17、4.14.12および4.15.5がリリースされ、一部Linuxディストリビューションでも修正バージョンがリリースされている模様で、アップデートもしくは回避策としてvfs_fruitの無効化が推奨されています。

AUS便りからの所感

- SambaはLinuxによるファイルサーバーのみならず、NAS製品等でもWindowsクライアント等にファイル共有機能を提供する目的で使用されており、今回の脆弱性についてはSambaが管理する共有フォルダーに攻撃者がアクセス可能な場合に悪用されることが考えられます。

- vfs_fruitモジュールはmacOSと互換性をとるための拡張機能を提供するものであり、社内でmacOSを利用していない場合などは前述した回避策をとるようファイルサーバーの設定を行うことも検討に値します。

- Sambaを利用しているNAS製品においては、macOSへの対応を謳い当該モジュールが利用されているケースがあり、ファームウェアのアップデートが行われることが考えられる一方、回避策をとるような設定項目があるかは製品によるとみられるため、いずれにしろメーカー情報を注視し、アップデートがあれば速やかに適用できる体制を整えておくべきでしょう。

TECH Powered by マイナビニュース

Sambaにリモートからroot権限で任意のコード実行できる脆弱性

2022/02/02 14:02　　著者：後藤大地

CERT Coordination Center (CERT/CC, Carnegie Mellon University)は1月31日(米国時間)、「VU#119678 - Samba vfs_fruit module insecurely handles extended file attributes」において、SMBネットワークプロトコル対応のファイルシステム・ソフトウェア「Samba」のvfs_fruitモジュールに脆弱性が報告されていると伝えた。この脆弱性を悪用されると、リモートの攻撃者によって影響を受けたシステム上でroot権限で任意のコードを実行される恐れがある。

この脆弱性はCVE-2021-44142として追跡されており、詳細はSambaチームによる次のセキュリティアナウンスにまとめられている。

- Samba - Security Announcement Archive