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。

●12月度のフィッシング報告件数は63,159件…初の6万件突破

https://www.antiphishing.jp/report/monthly/202112.html

このニュースをザックリ言うと・・・

- 1月6日(日本時間)、フィッシング対策協議会より、12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。

- 12月度の報告件数は63,159件で、11月度(https://www.antiphishing.jp/report/monthly/202111.html)の48,461件からは14,698件増加となっています。

- 一方、フィッシングサイトのURL件数は7,471件(11月度 7,575件)、悪用されたブランド件数は77件(11月度 82件)とそれぞれ減少しています。

- 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27.4%と11月度(28.5%)より微減、これにメルカリ・三井住友カード・ETC利用照会サービス・JCBを合わせた5ブランドで約74.0%(11月度 67.7%)、また1,000件以上の報告があったブランドが12あり、これらで全体の約88.4%を占めたとしています。

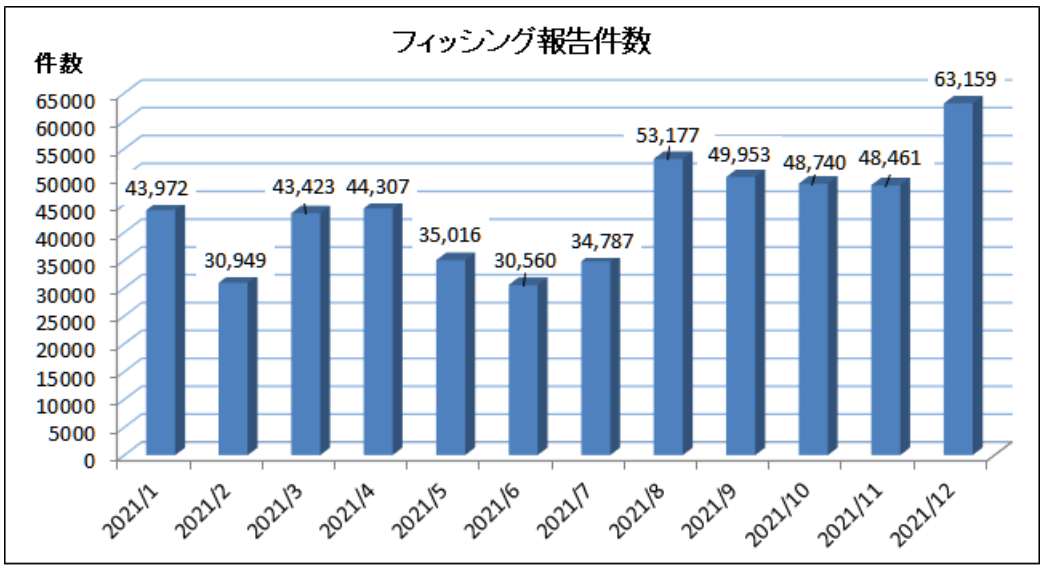
AUS便りからの所感等

- 今回、過去最高だった8月度の53,177件を一気に超え、初の6万件台となっていますが、8月度以降は48,000件以上を維持し続けており、今後も高い水準は続くとみてよいでしょう。

- なりすましメールを排除するための機構として、これまで挙げられていたDMARC・SPFに加え、DMARCで検証できた本物のメールにブランドアイコンを表示する「BIMI」が新たに紹介されており、現状ではメールクライアント側の対応がGMail程度しかないとはいえ、送信側・受信側共に採用・普及が進むか、それがフィッシングメールによる被害の効果的な抑制に繋がるか、等が今後注目されるところです。

- とにかく、メール・SMSを受信するユーザー側としては「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、また送信する側の立場でも前述したDMARC・SPFを採用し、相手をフィッシングから守ることができるよう可能な限り検討することが大切です。

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



● Microsoftより1月月例のセキュリティパッチがリリース…Windows Serverは適宜定例外パッチも適用を

https://forest.watch.impress.co.jp/docs/news/1379695.html
https://msrc-blog.microsoft.com/2022/01/11/202201-security-updates/
https://forest.watch.impress.co.jp/docs/news/1378984.html

このニュースをザックリ言うと・・・

- 1月12日(日本時間)、マイクロソフト(以下・MS)より、月例のセキュリティパッチ(Windows 10向けパッチKB5009543他)がリリースされ、96件の脆弱性が修正されています。

- 今回も脆弱性はWindowsと各種コンポーネント、.NET FrameworkおよびOffice等多岐にわたっており、オープンソースのマルチプロトコルクライアントおよびライブラリである「cURL」の脆弱性等についても対応しています。

- なお、Windows Server 2012 R2・2016・2019・2022において、12月のパッチ適用により、パフォーマンスの低下などの問題が発生することが報告されており、同6日までに定例外のパッチが別途リリースされています。

AUS便りからの所感

- cURLは例えばLinuxコマンドライン上でのHTTPによるアクセス・ファイル取得等で良く使われますが、Windows 10においても標準で含まれており、本家のcURLにも存在していた、FTP/SMTP/POP3/IMAPの暗号化通信における脆弱性が今回修正されています。

- WindowsとNET Framework(4.8まで)のセキュリティパッチは同時にインストールされない可能性があり、それぞれのインストール毎にOSの再起動を行わなければならない場合もありますので、「更新の履歴」において両方がインストールされたかを確認するようにしてください。

- 1月19日にはJavaについてもセキュリティアップデートがリリースされる予定です(https://www.java.com/releases/)が、例えばJava 16はOracleによるサポートが昨年9月で終了しており、この日にアップデートがリリースされるのはJava 17(および11, 8, 7のみ)となることに注意しましょう。

Impress Watch

2022年最初のMicrosoft製品アップデート ～「緊急」9件を含む96件の脆弱性に対処

日本語IMEでカーソルの動きがおかしくなる不具合も修正

樽井 秀人　2022年1月12日 09:12

米Microsoftは1月11日（現地時間）、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした（パッチチューズデー、Bリリース）。現在、「Windows Update」や「Microsoft Update Catalog」から入手可能。以下のMicrosoft製品に対しても、セキュリティアップデートが提供されている。

● JavaScriptライブラリ「colors.js」「faker.js」が作者により改ざん、多くのプロジェクトに影響

https://www.itmedia.co.jp/news/articles/2201/11/news160.html
https://gigazine.net/news/20220111-open-source-developer-corrupts-libraries/

このニュースをザックリ言うと・・・

- 1月9日(現地時間)頃、IT系ネットメディアにおいて、JavaScriptライブラリ「colors.js」「faker.js」が作者のMarak氏によって不正な内容への改ざんを受けたことが取り上げられています。

- これらのライブラリは主に「node.js」というサーバーサイドで動作するJavaScript処理系で使われているものですが、colors.js(コンソールで色付きのテキストを出力できるようにする)のバージョン1.4.1, 1.4.2および1.4.44-liberty-2については、インストールによりアメリカ国旗が無限に出力される等ループが引き起こされるような不正なコードが入れ込まれ、faker.js(偽データを出力する)はバージョン6.6.6で中身が削除されてしまった模様です。

- node.jsで実装されている多くのプロダクトがこれらのライブラリを使っており、不正なバージョンをインストールした場合に正常に動作しなくなる事例が多発し、各ライブラリをホスティングするパッケージ管理システム「npm」では、colors.jsの不正なバージョンを削除する等の対応を行っています。

AUS便りからの所感

- colors.jsは毎週2000万回以上、faker.jsは毎週280万回以上のダウンロードがされる程の人気でしたが、無償で開発を続けていたMarak氏が開発に対する寄付・報酬等を得られていなかったことと、生活に困窮したことが原因で開発をボイコットしたものとみられています。

- 現在npmではcolors.jsについて安全なバージョンである1.4.0を最新としていますが、一方のfaker.jsについては現時点でもバージョン6.6.6が最新となっており、インストール時に改変前のバージョン5.5.3を指定するよう呼び掛けられている模様です。

- このような問題はブラウザーがWebページ上で読み込む(クライアントサイドの)JavaScriptにおいても発生し得るもので、CDNやGithub等の外部サイトから自動的に最新のバージョンのスクリプトが読み込まれる形にしていた場合、悪意を持った開発者がスクリプトを改ざんしてアップデートすることにより、不正なコードが読み込まれてしまう恐れがあることは以前から指摘されています。

- 特定のバージョンのスクリプトを指定して読み込むよう設定すること、併せてスクリプトが改ざんされていないか検出するSubresource Integrity機構を活用することが推奨されており、新しいバージョンのスクリプトを利用しようとする場合も、ネット上でトラブルが発生していないか十分に確認した上で実行することが重要です。

ITmedia NEWS

OSS「faker.js」と「colors.js」の開発者、自身でライブラリを意図的に改ざん　「ただ働きはもうしない」

2022年01月11日 20時11分 公開　[松浦立樹, ITmedia]

オープンソースのライブラリ「colors.js」と「faker.js」の開発者であるマラック・スクワイアーズ氏が、それらの最新バージョンに無限ループ処理を仕込むなど、意図的な改ざんを加えたバージョンをリリースしていたことが分かった。

colors.jsは毎週2000万回以上、faker.jsは毎週280万回以上ダウンロードされている人気のライブラリ。それらを使用したプロジェクトに影響を与えることから、ITエンジニアを中心に物議を醸している。