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。

● 2月度フィッシング報告件数は55,502件、1年ぶり5万件台へ急落

https://www.antiphishing.jp/report/monthly/202402.html

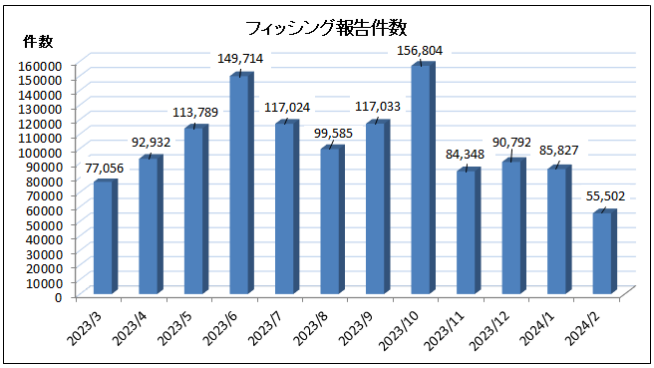
このニュースをザックリ言うと･･･

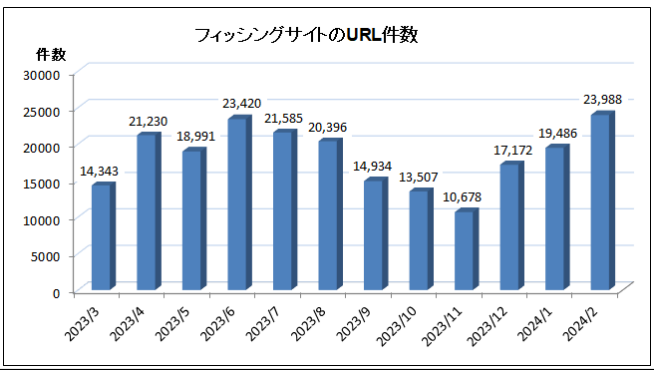
- 3月15日(日本時間)、フィッシング対策協議会より、2月に寄せられたフィッシング報告状況が発表されました。
- 2月度の報告件数は55,502件で、1月度(https://www.antiphishing.jp/report/monthly/202401.html)の85,827件から30,325件減少しています。
- フィッシングサイトのURL件数は23,988件で1月度(19,486件)から4,502件増加、悪用されたブランド件数は70件で1月度(74件)から4件減少となっています。
- 最も多く報告されたのはイオンカードを騙るフィッシングで報告数全体に対する約25.7%、次いで報告が多かったAmazon、三井住友カード、セゾンカード、マスターカードと合わせて約61.3%、さらに1,000件以上報告された13ブランドまで含めると約84.3%を占めたとのことです。

AUS便りからの所感等

- 85,000件前後～90,000件強で推移が続いていたここ3ヶ月間からさらなる急落となっており、報告件数が5万件台にとどまったのは2023年2月度の59,044件以来となります。
- 調査用メールアドレスに届いたフィッシングメールにおけるなりすましの割合も1月の約39.9%から約22.8%へと減少しているとのことです。
- 一方でフィッシングサイトURL件数は3か月連続の増加となり、うち約65.4%でサイトへのリダイレクト用に短縮URLおよびCloudflare Workersで付与できるサブドメインを悪用する傾向が続いています。
- 同協議会では、2月度の報告件数の下落を毎年の旧正月の前後にあたるためとし、3月度には再度増加する可能性があるとしており、「事業者のみなさまへ」「利用者のみなさまへ」の節を参考に、引き続き自組織のドメイン名で送受信するメールをフィッシングから保護する対策の実施を検討してください。

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





●テレビ局でサイバー攻撃、データ暗号化被害…放送に影響はなし

https://scan.netsecurity.ne.jp/article/2024/03/18/50738.html
https://www.teny.co.jp/info/20240313/20240313_001.pdf
https://www3.nhk.or.jp/shutoken-news/20240313/1000102884.html

このニュースをザックリ言うと･･･

- 3月13日(日本時間)、テレビ新潟より、同局がサイバー攻撃を受け、データ暗号化の被害を受けたと発表されました。
- 同11日に同局内で勤務する関連会社社員からファイルサーバーにアクセスできないとの問合せがあったことにより発覚、社内の情報システム系・番組制作系の複数の端末・サーバーにおいてデータ暗号化が確認されたとしています。
- 個人情報の漏えいは現時点で確認されていませんが、社内ネットワークから外部への攻撃拡大はなく、放送にも影響はなかったとしています。

AUS便りからの所感

- データ暗号化の被害が発生したことから、ランサムウェアによる攻撃を受けた可能性が考えられますが、発表においてはまだ明言はされていません。
- 昨年末から今年にかけて、地方の新聞社・スーパーおよび病院でのランサムウェア感染が立て続けに発覚、これらにおいては業務にも影響する事態となっており、サーバー・クライアントとも攻撃を受けないためおよび内部から情報流出しないためのアンチウイルスやUTMによる防御はもちろん、それによるデータの破壊等が発生した際も早々に復旧できるようバックアップの実行をはじめとした体制作りも怠りなく実施すべきです。

ScanNetSecurity by iid

テレビ新潟放送網にサイバー攻撃、データが暗号化被害

株式会社テレビ新潟放送網は3月13日、サイバー攻撃の発生について発表した。

株式会社テレビ新潟放送網は3月13日、サイバー攻撃の発生について発表した。

これは同社内のネットワークに接続されている複数の端末やサーバにサイバー攻撃があり、内部のドライブのデータを暗号化されたというもの。同社のネットワーク管理者が3月11日朝に、社内で勤務する関連会社の社員からファイルサーバのファイルにアクセスできないとの連絡を受け、ネットワーク状況を確認したところ、社内ネットワークに接続されている複数の端末やサーバの内部ドライブのデータが暗号化され、正常に動作していないことを確認した。

同社では社内のシステム担当者を中心とした調査チームを立ち上げ、調査を実施した結果、外部からのサイバー攻撃によるものと判断している。

●Apple Silicon搭載MacにmacOS Sonoma 14.4インストールでJava等が起動しなくなる不具合…アップデート保留を

https://pc.watch.impress.co.jp/docs/news/1577481.html
https://blogs.oracle.com/java/post/java-on-macos-14-4
https://faq.pfu.jp/faq/show/5305?site_domain=scansnap

このニュースをザックリ言うと･･･

- 3月8日(日本時間)にリリースされたmacOSの最新バージョン「macOS Sonoma 14.4」においてJavaをはじめとする複数のアプリケーションが起動しなくなる不具合がSNS等で報告されています。
- 同16日のOracle社からの発表によれば、不具合はApple Silicon製MacのmacOSをSonoma 14.4にアップデートした後に発生、Java 8から最新安定版のJava 21およびリリースされたばかりのJava 22にまで影響するとしています。
- 同社ではJavaに関してこの不具合を回避する策はなく、バックアップがなければアップグレード後から戻すことも困難なため、影響を受ける環境ではアップグレードを控えるよう呼び掛けています。

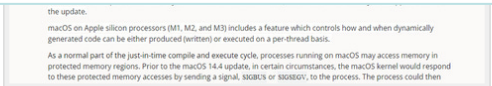
AUS便りからの所感

- 他にもMicrosoft社製「Microsoft Remote Desktop」やPFU社製スキャナー「ScanSnap」用ソフトウェア「ScanSnap Home」で不具合が発生しており、後者はPFU社から回避策が提示されています。
- Sonoma 14.4のプレビューテスト段階では含まれておらず、正式リリース時に含められた機能が影響しているとのことですが、Apple社から不具合に関する発表は21日時点でされていない模様です。
- 使用しているアプリケーション次第とは言え影響範囲は広いとみられ、可用性に大きくかかわってくるものであり、Mac PCの利用者がいる組織においては可能な限り速やかにアップグレードを保留するよう周知徹底を行い、またバックアップの実施を推奨することが重要でしょう。

Impress Watch

macOS Sonoma 14.4適用後にJavaがクラッシュする不具合。回避策なく、OS更新の延期を

宇都宮 充　2024年3月19日 12:25



the update.
macOS on Apple silicon processors (M1, M2, and M3) includes a feature which controls how and when dynamically generated code can be either produced (written) or executed on a per-thread basis.
As a normal part of the just-in-time compile and execute cycle, processes running on macOS may access memory in protected memory regions. Prior to the macOS 14.4 update, in certain circumstances, the macOS kernel would respond to these protected memory accesses by sending a signal, SIGBUS or SIGSEGV, to the process. The process could then

Oracleは15日(米国時間)、macOS Sonoma 14.4を適用した環境において、Javaプロセスが予期せず終了する不具合が発生しているとして、情報を公開した。

これによると、Appleが7日に公開したmacOS Sonoma 14.4を適用したApple Silicon搭載Macで発生する不具合で、Java 8からJDK 22のアーリーアクセスビルドまでのすべてのバージョンが影響を受けるという。macOSは以前のバージョンに簡単に戻すことができないため、現時点では回避策はなく、バックアップがない場合は安定した構成に戻せない可能性があるとしている。