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。

●企業Webサイト、不正アクセスで改ざん相次ぐ…「破産手続きを開始」虚偽のメッセージも

https://nlab.itmedia.co.jp/nl/articles/2309/04/news117.html

このニュースをザックリ言うと･･･

- 9月4日(日本時間)、ITMedia「ねとらぼ」において、企業・組織等の公式サイトが不正アクセスを受け改ざんされるケースが相次いでいることが取り上げられています。

- 改ざん事案は8月末～9月初めに多発しており、被害を受けた組織が「破産手続きを開始した」とする事実と異なるメッセージが追加されていることが特徴とみられています。

- 被害を受けた例として、餃子チェーン店運営の鹿児島王将、映像教材の新宿スタジオ、精肉店のミートプラザニシジマ、および湘南国際村センターが挙げられ、いずれも「2023年8月31日付で破産手続きを開始いたしました」といった虚偽のメッセージがWebページ上に記載されたり、同様の告知を行うなりすましメールが外部に送信されたりしているとのことです。

AUS便りからの所感等

- Webサイト改ざんの目的は、今回のように組織に風評被害を与えることを狙うものから、サイト閲覧者に対するマルウェア感染、フィッシングサイトの設置用、ECサイトであれば決済情報を流出させるような工作まで様々で、またWebサーバーから不審なメールを大量発信するよう仕掛けるケースも多々存在します。

- また、改ざんに至る経路も、Webサーバーに直接侵入するもの、WordPressはじめCMS(コンテンツ管理システム)の脆弱性(SQLインジェクション等)を突くもの、管理者が使用するPCに侵入・マルウェア感染するもの等多岐にわたります。

- サーバー側においてOSから各種アプリケーションに至るまで脆弱性の悪用等されないよう最新バージョンに保ち、適宜不正アクセスを抑止するような設定を行うことがまず肝要であり、同様にサーバー・Webサイト管理者のみならずサーバーを利用してメール送信等を行う一般ユーザーまで、アンチウイルスやUTM等によるPCへの侵入ないしPCからの不正行為の防止を図ることもまた重要です。

ねとらぼ

「破産手続きを開始しました」 企業サイトの改ざん被害、全国で相次ぐ 「餃子の王将」運営会社も

全国で被害相次ぐ。

[ねとらぼ]

企業の公式サイトなどが何者かによって改ざんされ、「破産手続きを開始しました」などと虚偽の内容が表示される被害が全国で相次いでいます。

全国で企業サイトの改ざん被害相次ぐ(画像は鹿児島王将公式サイトから)

● 8月度フィッシング報告件数は99,585件、4か月ぶりに10万件切る

https://www.antiphishing.jp/report/monthly/202308.html

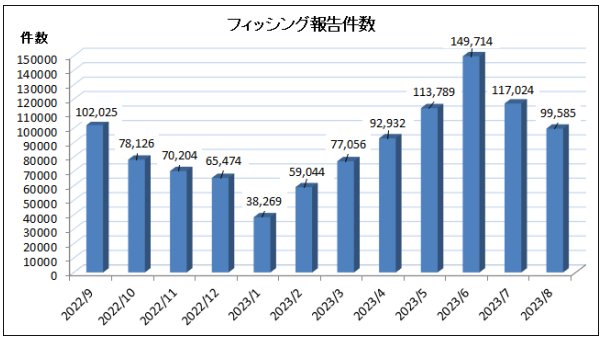
このニュースをザックリ言うと・・・

- 8月4日(日本時間)、フィッシング対策協議会より、8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99,585件で、7月度(https://www.antiphishing.jp/report/monthly/202307.html)の117,024件から17,439件減少しています。
- フィッシングサイトのURL件数は20,396件で7月度(21,585件)から1,189件減少、悪用されたブランド件数も91件で7月度(93件)から2件減少となっています。
- 最も多く悪用されたブランドは7月度に続きAmazon(全体の約36.1%)で、以下三井住友カード・クロネコヤマト・三井住友銀行・Apple・セゾンカードを合わせた6ブランドで全体の約74.2%、また1,000件以上の報告があった15ブランドで全体の約92.4%を占めたとしています。

AUS便りからの所感

- 報告件数は過去最高を記録した6月度の149,714件から4ヶ月連続で減少し、今回は4月度以来4ヶ月ぶりに10万件を切っています。
- Amazonのアカウントへ不正にログインされ、ギフトカード等を勝手に購入される被害がTwitter(現X)で報告されており、フィッシングに騙されてパスワードはもちろん、多要素認証(MFA)用のパスコードまで入力してしまうケースが国内で発生している可能性が考えられます。
- ユーザー側での自衛手段としては、これまでも度々述べている通り、利用しているサービスへのアクセスは予め登録したブックマークや公式スマホアプリから行うこと、またMFAについても、SMSでパスコードが送信される形式について指摘されている攻撃手法に万が一引っかかる可能性を鑑み、Google Authenticator等が提供するTOTP(ワンタイムパスワード)が利用可能であればそちらへ移行すること等を検討すべきでしょう。

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



● MSとAdobeの月例セキュリティアップデートリリース、必ず適用を

https://www.jpcert.or.jp/at/2023/at230019.html
https://www.ipa.go.jp/security/security-alert/2023/0913-ms.html
https://www.jpcert.or.jp/at/2023/at230018.html
https://www.ipa.go.jp/security/security-alert/2023/0913-adobereader.html

このニュースをザックリ言うと・・・

- 9月13日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対する月例のセキュリティアップデートがリリースされています。
- Windowsの最新バージョンはWindows 10 22H2 KB5030211(ビルド 19045.3448)および11 22H2 KB5030219(ビルド 22621.2283)となります。
- 同日にはAdobe社からもAcrobat・Acrobat Reader(最新バージョン 23.006.20320)等のセキュリティアップデートがリリースされています。
- 各社やJPCERT/CC・IPA等からは早急にアップデートの適用が呼び掛けられています。

AUS便りからの所感

- 既にMSではWordの脆弱性(CVE-2023-36761)、Stream Servicesの脆弱性(CVE-2023-36802)についてこれらを悪用する攻撃を確認しているとしています。
- Acrobat・Acrobat Readerの脆弱性(CVE-2023-26369)についても危険度が高いものとされ、これらの脆弱性により、不正なWordファイル・PDFファイルを開くことによる情報漏洩やPCの乗っ取り等が行われる恐れがあるため、可能な限り更新プログラムの確認を手動で行い、早い段階で最新バージョンに更新されたことを確認することを強く推奨致します。

JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

2023年9月マイクロソフトセキュリティ更新プログラムに関する注意喚起 最終更新: 2023-09-13

I. 概要

マイクロソフトから同社製品の脆弱性を修正する2023年9月のセキュリティ更新プログラムが公開されました。これらの脆弱性を悪用された場合、リモートからの攻撃によって任意のコードが実行されるなどの可能性があります。マイクロソフトが提供する情報を参照し、早急に更新プログラムを適用してください。

マイクロソフト株式会社
2023 年 9 月のセキュリティ更新プログラム
https://msrc.microsoft.com/update-guide/ja-JP/releaseNote/2023-Sep

マイクロソフト株式会社
2023 年 9 月のセキュリティ更新プログラム (月例)
https://msrc.microsoft.com/blog/2023/09/202309-security-update/