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月発生の大手スーパーランサムウェア感染、個人情報最大約780万件流出の可能性…侵入はVPNから

https://www.itmedia.co.jp/news/articles/2405/10/news090.html
https://www.izumi.co.jp/corp/outline/news_release/pdf/2024/0509news_01.pdf

このニュースをザックリ言うと･･･

- 5月9日(日本時間)、西日本で展開するスーパー「ゆめタウン」「ゆめマート」を運営するいずみ社より、2月に同社システムで発生していたランサムウェア感染(AUS便り 2024/02/28号参照)に関する続報が発表されました。

- 外部専門機関による調査の結果、VPN装置を経由して同社グループのサーバーに直接侵入されたことが攻撃のきっかけであるとする一方、社外への情報流出の痕跡は見当たらず、個人情報を含む同社グループの保有情報が漏えいした可能性は極めて低いとしています。

- ただし、閲覧された可能性を完全に否定できないとする個人情報として、会員サービス「ゆめカード」会員情報最大7,782,009件(氏名・電話番号・住所・生年月日・性別・ポイント管理番号)およびグループ会社パートアルバイト応募者情報最大2,990件(氏名・電話番号・住所・生年月日・性別・メールアドレス)を挙げています。

- この他の被害として、グループ共通メールサーバーで保有していたメール履歴が毀損したとしています。

AUS便りからの所感等

- ここ数年、大手ベンダー製を含めたVPN製品において、外部からの侵入につながり得る脆弱性が度々報告され、それが原因とみられる被害もまた時々報じられています。

- PC上のソフトウェアに比べ、ネットワーク機器・IoT機器のファームウェアについてはセキュリティアップデートの適用が行き届きにくい傾向にあるとみられますが、そういった機器も確実に管理下に置き、脆弱性が報告され次第、可能な限り速やかに製品のアップデートを行えるような体制が望まれます。

- また先日には、機器の導入時に残っていたテスト用アカウントから侵入された事例も報告されており(AUS便り 2024/05/08号参照)、サーバー・VPN機器等へのログインについても、管理者・一般ユーザーに拘らず強固なパスワードの設定、想定にないアカウントが有効でないかの確認が重要ですし、加えてID・パスワードのみならず証明書や多要素認証の採用等も検討すべきでしょう。

ITmedia NEWS

ランサム攻撃でサービス停止の地方スーパー、最大778万件の情報漏えいか

2024年05月10日 06時00分 公開　[ITmedia]

総合スーパー「ゆめタウン」を展開するイズミ（広島県広島市）は5月9日、2月に受けたランサムウェア攻撃を巡り、最大で約778万件の情報が漏えいした可能性があると発表した。

クレジットカード「ゆめカード」会員の氏名や電話番号、住所、生年月日、性別など最大778万2009件が漏えいした可能性がある。クレジットカード情報は、被害を受けたシステムとは別のシステムで運用しており、影響はないという。

さらに、23年6月1日から24年2月14日にかけて、子会社であるイズミテクノの求人にパート・アルバイトとして応募した人の氏名・電話番号など最大2990件も漏えいした可能性がある。この他、公式サイトからの問い合わせ対応を除く、社内のメールサーバに保存していた業務メールの履歴データも破損した。履歴データについては、影響を受けた件数は不明という。

● 4月のフィッシング報告件数は106,757件、6か月ぶりの10万件突破

https://www.antiphishing.jp/report/monthly/202404.html

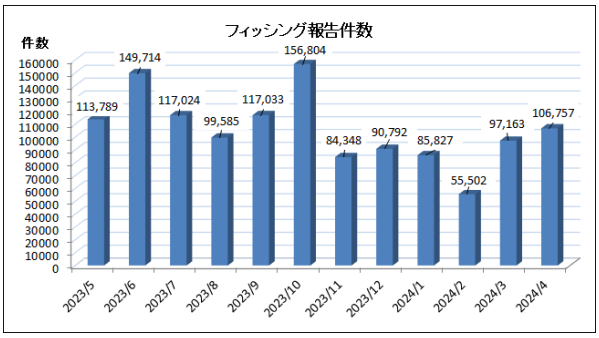
このニュースをザックリ言うと・・・

- 5月17日(日本時間)、フィッシング対策協議会より、4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。
- 4月度の報告件数は106,757件で、3月度(https://www.antiphishing.jp/report/monthly/202403.html)の97,163件から9,594件増加しています。
- フィッシングサイトのURL件数は39,863件で3月度(44,228件)から4,365件減少、悪用されたブランド件数は92件で3月度(87件)から5件増加となっています。
- 最も多く報告されたのは東京電力を騙るフィッシングで報告数全体に対する約19.5%、次いで報告が多かった三井住友カード、Mastercard、Amazon、イオンカードと合わせて約65.8%、さらに1,000件以上報告された14ブランドまで含めると約90.6%を占めたとのことです。

AUS便りからの所感

- 過去最高の報告件数(156,804件)を記録した2023年10月度を最後に急減していましたが、その時以来の10万件越えとなりました。
- フィッシングサイトURLで使用されるTLD(トップレベルドメイン名)の割合は上位から .com(約53.5%)、.ru(約13.5%)、.cn(約13.4%)等となっており、2024年に入ってから .ruの割合が増加しています。
- フィッシングメール・サイトからの自衛策として、これまでも度々言われていることですが、不審なメールが届いた場合には、同協議会や日本データ通信協会の迷惑メール相談センター(https://www.dekyo.or.jp/soudan/contents/news/alert.html)等の団体が発表する情報あるいはソーシャルネットワークでの報告がないか確認すること、利用しているサービスのサイトへは事前に登録したブラウザーのブックマーク等からアクセスするよう心掛けること等、慎重な行動が肝要です。

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



● Firefox内蔵のPDFリーダー機能に脆弱性、アップデートを…影響はFirefox以外にも

https://forest.watch.impress.co.jp/docs/news/1593338.html
https://codeanlabs.com/blog/research/cve-2024-4367-arbitrary-js-execution-in-pdf-js/

このニュースをザックリ言うと・・・

- 5月20日(現地時間)、オランダのセキュリティベンダーCodean Labsより、JavaScriptで書かれたPDFリーダー「PDF.js」に脆弱性(CVE-2024-4367)が存在するとして注意喚起が出されています。
- PDF.jsはFirefoxブラウザー内蔵のPDFリーダー機能において使用されていますが、悪意のあるPDFファイルを読み込ませることにより、不正なJavaScriptを実行される可能性があるとされています。
- 4月29日にPDF.jsの修正が行われ、5月14日リリースのFirefox 126(およびFirefox ESR 115.11・Thunderbird 115.11.0)でも修正バージョンが取り込まれたとのことです。

AUS便りからの所感

- ChromeやEdgeと同様、Firefoxも最新バージョンを自動的に確認、インストールする機能がありますが、長期間起動した状態だと更新されない場合があるため、適宜「ヘルプ>Firefoxについて」を開いて確認することを推奨致します。
- PDF.jsはWebページ内でPDF文書を表示する用途にも使用され、Slack等大手サイトでも採用されていますが、このようなWebサイト内で使用しているPDF.jsのバージョンが古く、特にサイト上に任意のPDFファイルをアップロード・表示させることができる場合、閲覧者のブラウザー上で攻撃を行われる可能性がありますので、独自に構築したWebサイト上でPDF.jsを利用している場合についても確認の上、更新を行ってください。

Impress Watch

「PDF.js」に任意コード実行の脆弱性 ～多くのWebサイト・アプリに影響

「Firefox」内蔵PDFビューワーでも用いられているPDF表示ライブラリ

樽井 秀人　2024年5月22日 06:45


Codean Labs、「PDF.js」に任意のJavaScriptコードを実行できる脆弱性（CVE-2024-4367）があることを明らかに

オランダのセキュリティベンダーCodean Labsは5月20日（現地時間）、「PDF.js」に任意のJavaScriptコードを実行できる脆弱性（CVE-2024-4367）があることを明らかにした。

「PDF.js」は、HTML5で構築されたPDFビューワー。「Firefox 19」以降に搭載されている内蔵PDFビューワーなどに用いられている。