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。

●古い「Internet Explorer」が呼び出される脆弱性…7月のWindowsアップデートで修正

https://news.mynavi.jp/techplus/article/20240711-2983211/
https://blog.checkpoint.com/research/cpr-warns-threat-actors-are-leveraging-internet-explorer-in-new-zero-day-spoofing-attack-cve-2024-38112/

このニュースをザックリ言うと･･･

- 7月9日(現地時間)、セキュリティベンダーのCheckPoint社より、Windowsにおいて長らく未修正だった脆弱性「CVE-2024-38112」について注意喚起が出されています。

- 脆弱性はWindowsのMSHTMLプラットフォームに存在し、不正な「.url」拡張子のファイルにより、既に廃止されたWebブラウザーである「Internet Explorer(IE)」を呼び出され、IEの脆弱性を悪用する攻撃に繋がる可能性があるとしています。

- 脆弱性は同日にマイクロソフト(以下・MS)よりリリースされた月例のアップデートで修正されましたが、CheckPoint社ではこれを悪用した攻撃が2023年1月から確認されていたとしています。

- CheckPoint社ではIPS等同社製品で脆弱性を悪用するファイルを遮断するよう対応したとしており、一方でWindowsユーザーに対しアップデートの適用を強く推奨しています。

AUS便りからの所感等

- IEは2023年までにセキュリティアップデート等のサポートが終了し、MSでは既に後継のブラウザーとしてEdgeを提供していますが、IEでのみ動くようなWebサイト・Webアプリケーションに対応する「IEモード」も2029年まで提供されていることから、最新のWindowsである11においても引き続きIEが残存しており、VBScript等で呼び出す「裏技」がネットで紹介されたりしています。

- CVE-2024-38112の悪用には攻撃対象のユーザー側にいくつかの手順をとらせる必要がある模様ですが、IEが想定外の経路で起動し、それに含まれる未知・未修正の脆弱性等が悪用される恐れがあることには注意が必要です。

- 今月リリースされたWindowsのセキュリティアップデートを必ず適用することはもちろん、以後も信用できない相手からの誘導等で安易にIEの起動や常用を行うことがないよう注意を払うことが重要です。

TECHF Powered by マイナビニュース

Internet Explorerを悪用する攻撃を確認、アップデート適用を

掲載日 2024/07/11 08:46　　著者：後藤大地

Check Point Software Technologiesは7月9日(米国時間)、「CPR Warns Threat Actors are Leveraging Internet Explorer in New Zero-Day Spoofing Attack (CVE-2024-38112) - Check Point Blog」において、HTMLレンダリングエンジンの「MSHTML」に存在する脆弱性を通じて、サイバー攻撃にMicrosoft Internet Explorerが悪用されていると報じた。この脆弱性はゼロデイの脆弱性として1年以上前から悪用されていたとみられている。

今回発見された攻撃は特別なURLファイルを用いる。攻撃者は悪意のあるURLファイルをユーザーに送付し、ユーザーをだましてそれを実行させ、さらにWindowsの警告を無視させてInternet Explorerを実行する。攻撃を完遂するには複数のユーザー操作を必要とすることから、脆弱性の深刻度は重要(Important)にとどまるが、悪用が確認されており注意が必要。

●東京ガス子会社へ不正アクセス、取引先約416万人分等の個人情報流出か

https://www.itmedia.co.jp/news/articles/2407/17/news172.html
https://xtech.nikkei.com/atcl/nxt/news/24/01202/
https://www.tokyogas-es.co.jp/notice/pdf/20240717-01.pdf

このニュースをザックリ言うと・・・

- 7月17日(日本時間)、東京ガスとグループ会社の東京ガスエンジニアリングソリューションズ株式会社(以下・TGES社)より、TGES社が保持していた個人情報が同社への不正アクセスにより流出した可能性があると発表されました。

- 被害を受けたとされるのは大きく三種類に分類され、(1)TGES社が「業務上必要な情報として業務委託元から提供を受けている一般消費者」約416万人分の氏名・住所・連絡先等(東京ガスとの「家庭用の都市ガス、電気などの契約情報」は含まれないとのことです)、(2)「法人用の都市ガス、電気、サービス」で取引のあった法人等の所属者(人数は調査中とのこと)の氏名・メールアドレス等業務上連絡先・金融機関口座番号・マイナンバー情報等(クレジットカード情報は含まないとのこと)、および(3)TGES社従業員(退職者含む)約3,000人分の氏名・住所・金融機関口座番号情報(約1,000件)・クレジットカード情報(8件)、とのことです。

- TGES社のネットワークが不正アクセスを受け、同社および東京ガス社のサーバーに保管されている情報について流出した可能性があることが7月9日に判明したとしています。

AUS便りからの所感

- 一部報道によれば、不正アクセスはVPN装置を経由して行われ、ファイルサーバーのアカウント情報が窃取されていたとしていますが、個人情報の不正利用は確認されていないとのことです。

- 国内での不正アクセスによる個人情報流出の事例は今回のようなVPN装置からの侵入(脆弱性の悪用もしくは推測されやすいパスワードの利用が主な原因)と、ランサムウェアの感染によるものが目立っている印象があります。

- 社内ネットワークないし個人情報等を保存するサーバーへ第三者から安易にアクセスされることのないよう、PC・サーバーのみならず各ネットワーク機器についてOS等を最新のバージョンに保ち、VPNやサーバーにログインするためのアカウントとして推測されやすいパスワードが設定されているもの、さらにはその状態で使用されないまま残されているようなものは削除する、アンチウイルス・UTM等による防御を固める等様々な防衛策をとることが重要です。

日経 XTECH

東京ガス子会社への不正アクセスは「VPN装置経由」、個人情報約416万人分漏洩か

鈴木慶太　日経クロステック／日経コンピュータ

2024.07.18

東京ガスの子会社が不正アクセスを受けて個人情報約416万人分が漏洩した可能性がある問題を巡り、侵入経路はVPN（仮想私設網）装置経由であったことが日経クロステックの取材で2024年7月18日までに分かった。現在は外部との接続を遮断するなど対策を講じた上で、被害範囲や原因などについて調査を進めている。2024年7月18日午前10時時点で情報の不正利用は確認されていないという。

●パリ五輪チケットに関する詐欺サイト、各国当局やセキュリティ企業が注意喚起

https://forbesjapan.com/articles/detail/72401
https://www.proofpoint.com/jp/blog/threat-insight/security-brief-scammers-create-fraudulent-olympics-ticketing-websites

このニュースをザックリ言うと・・・

- 7月16日(日本時間)、「Forbes JAPAN」誌のWebサイトにおいて、同27日に開催予定のパリオリンピックのチケットに関連する詐欺行為への注意喚起が各国当局や複数のセキュリティ企業等から出されていると報じられています。

- 記事では、「チケットを特別価格で提供する」あるいは「完売したはずの競技のチケットを販売する」と謳う詐欺サイトへの警戒や、同五輪に出場予定の選手の家族が詐欺の被害を受けたケースが挙げられています。

- またセキュリティ企業のProofpoint社によれば、Googleでチケットサイトを検索した結果において、公式サイトの次に「paris24tickets[.]com」というドメイン名の詐欺サイトが広告枠で表示されていたとしています。

- フランス当局では、現在までに338件の詐欺サイトを特定し、51件がすでに閉鎖、ほか140件に対し法執行機関から通告を行っているとしています。

AUS便りからの所感

- オリンピックやワールドカップ等スポーツイベントから地震・台風といった事故・災害や大規模な感染症に至るまで、世界が注目する大きな出来事には必ず便乗したサイバー犯罪が起こり得ます(やはり今年実施されるアメリカ大統領選挙でも、例えば2016年にロシア等が関与したとみられるサイバー攻撃が発生しています)。

- 2021年に開催された東京オリンピックでも、公式サイトに類似したドメイン名による詐欺行為・マルウェア感染を行う不審なサイトが多く確認されています。

- 非公式で安価に何らかのサービスが受けられるようなものを安易に検索して素性の知れないサイトに軽率に個人情報・クレジットカード番号等を入力することは決して行わないようにし、また不審な宣伝や通知を騙ったSMSやメールを受け取った際にも、セキュリティ関連団体・組織からの注意喚起、本物の業者からのメールやSMSの運用に関するポリシーを確認し、無闇にリンクをクリックしない等に注意してください。

Forbes JAPAN

スポーツ　2024.07.16 12:00

パリ五輪「チケット詐欺」が急増、英アスリートの家族も被害に

Emma Woollacott | Contributor　著者フォロー　記事を保存　SHARE

パリの夏季五輪の開催が迫る中、各国の当局は、現金や個人情報を狙うチケット詐欺に十分注意するようスポーツファンに呼びかけている。

セキュリティ企業カスペルスキーの研究者は、五輪のチケットを特別価格で提供したり、完売したはずの競技のチケットを販売すると謳う詐欺サイトへの警戒を呼びかけている。

「この種の詐欺は、以前から繰り返されているが、2024年のパリ大会でも同様のウェブサイトが急増することが予想できる」と同社は述べている。詐欺サイトの中には、ユーザーの個人データをダークウェブで転売する業者のものもあるという。