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。

●ホビーショップのECサイト、決済プログラム改ざんによりクレカ情報等流出

https://www.itmedia.co.jp/news/articles/2508/09/news034.html
https://www.suruga-ya.jp/feature/osirase/2025_08_08.html

このニュースをザックリ言うと･･･

- 8月8日(日本時間)、ホビーショップ駿河屋より、運営するECサイト「駿河屋.JP」が不正アクセスを受け、クレジットカード情報等個人情報が漏洩したと発表されました。

- 被害を受けたのは、7月24日から8月4日にかけて同サイトで決済を行ったユーザーの個人情報(氏名・住所・電話番号・メールアドレス他)およびクレジットカード情報(カード番号・セキュリティコード・有効期限他)とされています(駿河屋.JPのアカウント情報は、現時点では対象外の模様です)。

- 7月24日午前1時頃に不正なプログラムが設置されたとみられ、8月4日に事象確認・プログラムの削除を行ったとしており、カード決済は現在も停止中です。

AUS便りからの所感等

- 不正アクセスから対策までの情報漏洩の期間は長期間に及ばなかったものの、具体的な被害件数も含め詳細は調査中とのことで、今後の続報が待たれますが、少なくとも前述した期間においてカード情報の入力を行った利用者においては今後の不正利用の可能性に注意が必要でしょう。

- 近年のクレジットカード情報流出事案においては、既に「セキュリティコードも含んだ情報を自前のサーバー上に保持していた」というケースは皆無と言ってよく、不正アクセスによる改ざんで決済時において偽のフォームの表示等を行い、個人情報等の詐取を行う手口が一般的とされています。

- ECサイト構築で利用される有名なフレームワークであっても、SQLインジェクションの脆弱性が発見・修正された後、アップデートしていないECサイトが攻撃を受けるケースも度々報告されており、Webアプリケーション・フレームワークからサーバーに至るまで最新のバージョンに保ち脆弱性の修正・対策を確実に行うことにより、攻撃者による侵入や改ざんの余地をなくすことは必須で、併せて攻撃の形跡・兆候を検知・遮断するためのIDS・IPSおよびWAFの設置もまた肝要です。

- Webサイト上で許可していないアクセス先へのリクエスト送信やファイル読み込みを遮断するセキュリティ機構であるContent Security Policy(CSP)は多くのWebブラウザーで対応が済んでおり、近年のカード情報流出事案等の多くで効果があるとされ、決済機能を提供する外部業者からもその利用を推奨する流れとなることに期待したいものです。

ITmedia NEWS

駿河屋、ECサイトに不正アクセス　クレカ情報を含む個人情報が漏えいか　8日よりカード決済停止

2025年08月09日 00時20分 公開　[ITmedia]

駿河屋は8月8日、同社が運営するECサイト「駿河屋.JP」が第三者による不正アクセスを受け、クレジットカード情報を含む個人情報が漏洩したと発表した。被害件数は調査中としており、影響拡大防止のため同日よりクレジットカード決済を一時停止している。

漏洩した可能性がある個人情報は、氏名、住所、郵便番号、電話番号、メールアドレス、領収書の宛名・但し書きなど。クレジットカード情報では、カード番号、セキュリティコード、有効期限、カード名義、カードブランドが含まれる。対象となる具体的な件数は調査中としており、新たな事実が判明次第、公式サイトにて報告するという。

駿河屋によると、7月23日に不正アクセスを検知し、調査とモニタリングを開始。8月4日にECサイトのシステムの一部が第三者によって不正に改ざんされていることを確認した。これにより、ユーザーが入力した決済情報が外部に流出する状態になっていたという。同社は4日中にシステムの修正を完了させている。

● PuTTYの偽のインストーラーからマルウェア「Oyster」に感染させる攻撃に注意喚起

https://www.cyberproof.com/blog/oyster-backdoor-the-malvertising-menace-masquerading-as-popular-tools/

このニュースをザックリ言うと・・・

- 7月25日(現地時間)、米CyberProof社より、「Oyster」と呼ばれるマルウェアへの感染を行う攻撃キャンペーンが確認されたとして注意喚起が出されています。

- OysterはPC等にバックドアを設置するマルウェアで、過去にRhysida等のランサムウェアの導入にも用いられたとしています。

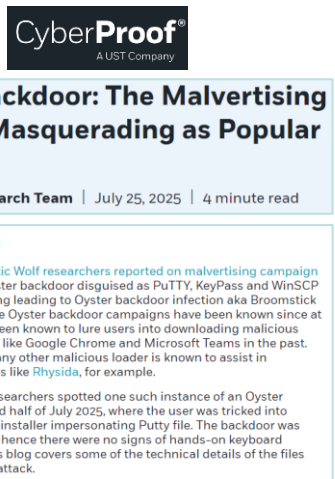
- 同社によれば、SSHに対応するターミナルソフト「PuTTY」等の偽のインストーラーにOysterを混入させ、サーチエンジンに表示させる不正な広告からダウンロードするよう誘導する、いわゆる「マルバタイジング」攻撃を確認したとしています。

AUS便りからの所感

- 同社の注意喚起では、6月上旬にPuTTYの他、PuTTYと同じくSSHプロトコルによってファイル転送を行う「WinSCP」や、パスワード管理ツール「KeePass」でOysterを混入させたインストーラーによる攻撃を確認しているとのことです。

- マルバタイジングによる偽のインストーラーへの誘導攻撃の事例は過去にも画像ソフトウェア「GIMP」等でみられており、時にはURLに国際化ドメイン名(IDN)等を用いるケースもあります。

- PuTTYはサーバー等へのリモートアクセス用途で人気のあるソフトウェアの一つですが、現在Googleで「PuTTY」を検索した際、危険ではないとみられるものの、公式ではないサイトがトップに表示されるようになっていることもあり、入手・インストールの際は安易に検索結果の上位に手を出さないこと、万全を期すならば公式サイトのURL(https://www.chiark.greenend.org.uk/~sgtatham/putty/)を確認すること、または日本人開発者によって長年開発され信頼されている日本語対応版(PuTTYrv・iceiv+putty等)のサイトをブックマークするのも一考でしょう。



●Microsoft等月例のセキュリティアップデート…Chromeも週例、Zoomは緊急のパッチ

https://forest.watch.impress.co.jp/docs/news/2038690.html
https://msrc.microsoft.com/blog/2025/08/202508-security-update/
https://forest.watch.impress.co.jp/docs/news/2038711.html
https://forest.watch.impress.co.jp/docs/news/2038707.html
https://forest.watch.impress.co.jp/docs/news/2039094.html

このニュースをザックリ言うと・・・

- 8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 KB5063709(ビルド 19045.6216)、11 23H2 KB5063875(ビルド 22631.5768)および11 24H2 KB5063878(ビルド 26100.4946)等となります。

- この他同日にはGoogle社よりChromeブラウザーの週例アップデートとなるv139.0.7258.127/.128(Windows版)、Adobe社よりPhotoshop・Illustrator・Animate等13製品についてセキュリティアップデートがリリース、またZoom社からは同12日にWindows版Zoom Workplaceにおいて緊急性の高い2点の脆弱点を修正したv6.5.9がリリースされています。

AUS便りからの所感

- MSの月例アップデートではWindows Kerberos認証に関する脆弱性(CVE-2025-53779)が既に攻撃手法が公知となっており、Windows・Office・Hyper-V等の脆弱性12件特に危険度が高い(4段階中最高の「Critical」)と評価されています。

- Chromeでは「Chromeについて」、Zoom Workplaceでは「更新を確認」でアップデートがインストールできますが、「窓の杜」では、Zoom WorkplaceをMSIファイルからインストールしていた場合に「更新を確認」が表示されないため、アンインストールおよびEXEファイルをダウンロードして再インストールすることを推奨しています(必要に応じ適宜システム管理者に確認すべきでしょう)。

- MSを中心としてベンダー各社がセキュリティパッチをリリースする第2火曜日(米国時間)「パッチチューズデー」について、今月は多くの企業・組織で夏季休暇中のリリースとなったと思われ、連休明けである程度のタイムラグが発生していますが、速やかにアップデートを実施すること、以後も各種ソフトウェアの定期的なパッチリリースに対し計画的なアップデートと、アンチウイルス・UTM等による多重防御を適切に行うことを常に心掛けましょう。