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。

●フィッシング詐欺で奪取した情報か…PCから1億件のメールアドレス、290万件のパスワード、1.7万件のクレカ情報

https://www.sankei.com/article/20230501-EIDZXQCGDFNA7KUHQ6WAJUN26Y/
https://www.yomiuri.co.jp/national/20230501-OYT1T50151/
https://www.asahi.com/articles/ASR5B6JFWR5BUTIL034.html

このニュースをザックリ言うと･･･

- 5月1日(日本時間)、神奈川県警等による合同捜査本部より、2月にフリマアプリ「メルカリ」の電子決済サービス「メルペイ」の不正利用容疑で逮捕された中国籍の男のPC等に約1億件のメールアドレス、約290万件のID・パスワード情報および約1万7千件のクレジットカード情報が保存されていたことを確認し、容疑者を不正アクセス禁止法違反の疑いで再逮捕したと発表されました。

- 発表によれば、男は2021年12月から2022年1月にかけてメルカリ利用者12人のアカウントを悪用して不正アクセスを行った容疑が持たれています。

- 合同捜査本部において2022年6月以降に相次いで摘発している、中国・ベトナム籍等の人物のグループによる決済サービスの不正利用事件の中心人物である疑いがあるとして、捜査が進められています。

AUS便りからの所感等

- 発表や報道においては、各種情報を詐取するためのフィッシングサイトを作成するプログラム等もPCに保存されていたとされ、決済サービスのQRコードを不正に生成し、コンビニでたばこ等の不正購入を行う実行役のメンバーに渡す役割をしていたとみられています。

- 保存されていた情報のうち、例えばクレジットカード情報については海外ブランドのものも含まれており、日本国内のユーザーが中心とは推察されるものの、世界中でフィッシング詐欺を実行していたものとみられます。

- フィッシングに対する啓発を行っているフィッシング対策協議会に報告されているフィッシングの報告件数は月毎に急増の傾向を見せており、実際に騙されて各種情報を入力してしまった事例もまた多くあるとみられ、決して「フィッシングはあからさまに偽物だとわかる」などと慢心することなく、不審なメール・SMSやそこから誘導された先のサイトが本物か、ネット上での報告等で十分確認すること、また普段利用するサービスへはブックマークや公式のアプリからアクセスすること等を改めて心掛けることが肝要です。

THE SANKEI NEWS 産経新聞

メアド１億件、クレカ情報１万７千件も…決済アプリ不正使用

2023/5/1 21:07 橋本 愛
社会 | 事件・疑惑

フリーマーケットサービス「メルカリ」系のスマートフォン決済アプリ「メルペイ」を他人のアカウントで不正使用した疑いで、神奈川県警などに逮捕された中国人の男のパソコンなどから、決済サービスなどに使われるＩＤとパスワードの組み合わせ約２９０万件など大量の個人情報が見つかった。個人情報を入力させる「フィッシングサイト」の作成用プログラムも保存。県警などは押収品を精査し、中国を拠点に膨大な個人情報をかき集めて悪用する犯罪グループの実態解明を進める。

●自治体の委託先で個人情報1,695人分流出…偽のセキュリティ警告・偽のMSサポートによる不正アクセスか

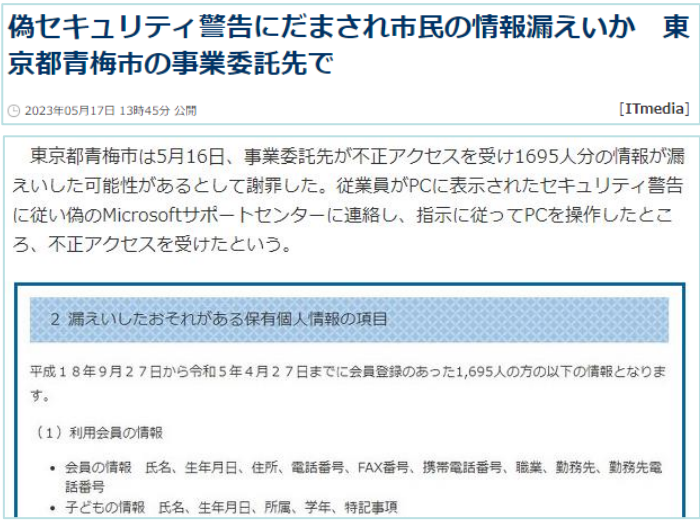
https://www.itmedia.co.jp/news/articles/2305/17/news136.html
https://www.city.ome.tokyo.jp/soshiki/34/68110.html
https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20230228.html

このニュースをザックリ言うと･･･

- 5月16日(日本時間)、東京都青梅市より、同市の事業委託先が不正アクセスを受け、個人情報が流出したと発表されました。
- 被害を受けたのは、ボランティア事業「青梅市ファミリー・サポート・センター事業」に2006年9月27日～2023年4月27日に会員登録等がされた1,695人分の氏名・住所・電話番号・勤務先・資格・活動時間および子供の学年等とされています。
- 委託先従業員のPCに表示されたセキュリティ警告に従って偽のマイクロソフトサポートセンターに連絡し、不正なソフトウェアのインストール等を指示された結果、不正アクセスを受けたとされています。

AUS便りからの所感

- 偽のセキュリティ警告からサポート電話を騙って詐欺を行う行為は2000年代から報告されていますが、度々啓発を行っていた情報処理推進機構(IPA)では2023年1月の相談件数が401件と過去最高になったとしています。
- 偽のセキュリティ警告等を表示する手段として、近年はWebブラウザーの通知機能等の悪用が目立っていますが、普段利用していないWebサイトから通知機能を有効にするよう求められても安易に有効にせず、ブロックするよう心掛けましょう。
- アンチウイルスやUTMによる防御を固めるとともに、マイクロソフトやその他の実在するソフトウェア会社が警告に表示されたとしても、決して鵜呑みにせず、表示された連絡先ではなく、IPAの安心相談窓口等に連絡を行い、相談を受けることが重要です。



偽セキュリティ警告にだまされ市民の情報漏えいか　東京都青梅市の事業委託先で

2023年05月17日 13時45分 公開　[ITmedia]

東京都青梅市は5月16日、事業委託先が不正アクセスを受け1695人分の情報が漏えいした可能性があるとして謝罪した。従業員がPCに表示されたセキュリティ警告に従い偽のMicrosoftサポートセンターに連絡し、指示に従ってPCを操作したところ、不正アクセスを受けたという。

2 漏えいしたおそれがある保有個人情報の項目

平成１８年９月２７日から令和５年４月２７日までに会員登録のあった1,695人の方の以下の情報となります。

（１）利用会員の情報

- 会員の情報　氏名、生年月日、住所、電話番号、FAX番号、携帯電話番号、職業、勤務先、勤務先電話番号
- 子どもの情報　氏名、生年月日、所属、学年、特記事項

●開発者向けツール「Visual Studio Code」不正な拡張機能に注意喚起

https://www.bleepingcomputer.com/news/security/malicious-microsoft-vscode-extensions-steal-passwords-open-remote-shells/
https://blog.checkpoint.com/securing-the-cloud/malicious-vscode-extensions-with-more-than-45k-downloads-steal-pii-and-enable-backdoors/

このニュースをザックリ言うと･･･

- 5月16日(現地時間)、セキュリティベンダーのCheckPoint社より、マイクロソフト(以下・MS)が開発・提供するソースコードエディター「Visual Studio Code(VSCode)」の悪意のある拡張機能が出回っているとして注意喚起が出されています。
- CheckPoint子会社によるセキュリティサービス「CloudGuard Spectral」により、MSが公式に運営する「VSCode Extensions Marketplace」において、インストールしたPCの情報やWebブラウザーの認証情報を詐取したり、攻撃者が侵入可能なバックドアを設置したりする複数の拡張機能が発見されたとしています。
- CheckPoint社は5月4日にMSに不正な拡張機能について報告し、同14日に削除されたとしていますが、それぞれの拡張機能は削除までに45,000回以上のダウンロードがあったとされています。

AUS便りからの所感

- VSCodeは2015年に登場後、多くの開発者から支持を集めており、ソースコードのハイライトや、GitHub等または内部のソースコード管理サーバーへのアクセスを容易にする等の目的で多数の拡張機能が開発・提供されています。
- 悪意のある拡張機能は、JavaやPythonといった人気のある言語向け拡張機能や、見た目をカスタマイズするテーマになりすましており、Marketplaceにおいて説明文に何も書かれていなかったにも拘らず、ダウンロードされていたものもあったとのことです。
- Chrome・Firefox等のWebブラウザーあるいはスマートフォンアプリと同様、VSCodeにインストールされる拡張機能はVSCode上で様々な機能の使用を許可されることになりますので、Marketplace上やSNS上でのレビュー等を十分に確認し、必要最低限の拡張機能のみインストール・有効化すること、身に覚えのない拡張機能が入っていれば速やかにアンインストールすることを心掛けてください。

BLEEPINGCOMPUTER

Malicious Microsoft VSCode extensions steal passwords, open remote shells

By Bill Toulas　May 17, 2023　12:37 PM

Cybercriminals are starting to target Microsoft's VSCode Marketplace, uploading three malicious Visual Studio extensions that Windows developers downloaded 46,600 times.

According to Check Point, whose analysts discovered the malicious extensions and reported them to Microsoft, the malware enabled the threat actors to steal credentials, system information, and establish a remote shell on the victim's machine.