— AUS（アルテミス・ユーザ・サポート）便り 2022/03/01号 —
https://www.artemis-jp.com

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。

●決済代行業者への不正アクセス、カード情報最大46万件流出か

https://www.itmedia.co.jp/news/articles/2202/28/news099.html
https://www.itmedia.co.jp/news/articles/2201/25/news129.html
https://www.metaps-payment.com/company/20220228.html

このニュースをザックリ言うと･･･

- 2月28日(日本時間)、クレジットカード決済代行などを手掛けるメタップスペイメント社より、同社の決済情報等が格納されているデータベースが不正アクセスを受け、クレジットカード情報が流出したと発表されました。

- 複数のデータベースが不正アクセスを受けており、クレジット決済サービス「トークン方式」の決済情報データベースに保存されていた2021年10月14日～2022年1月25日に利用された最大460,395件のカード情報(クレジットカード番号、有効期限、セキュリティコード(CVV))が被害を受けたとのことです。

- 2021年12月14日にカード会社から不正利用懸念の連絡を受けて以降調査が行われ、今年1月25日にトークン方式の決済を停止するとともに、不正アクセスに関する初報がメタップスペイメント社から公表されていました。

AUS便りからの所感等

- 今回の発表においては、前述した「トークン方式」の決済情報データベースからの流出、そして別の決済情報データベースからもクレジットカード等各種決済で利用された情報計593件、および加盟店情報データベースから加盟店等の情報38件について流出が判明したとしています。

- また、社内管理システムへの不正ログイン、一部アプリケーションにおけるSQLインジェクションの脆弱性、およびバックドアの存在が明らかになっています(初報公表の時点では全て対策されていた模様です)が、PCI DSSで基本的に保存が禁止されているCVVが他のカード情報と併せてデータベースに保存されていた可能性があります。

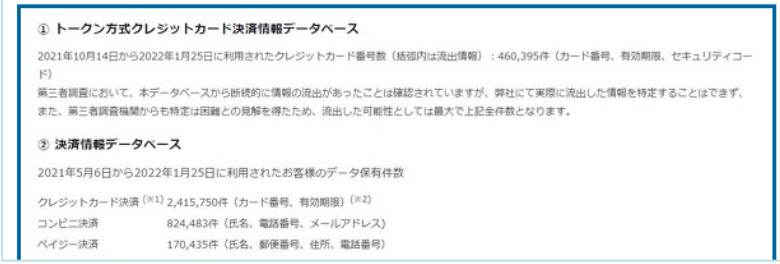
- 一方で、CVVを保存しない仕様としていた場合でも、カード情報の入力フォームの改ざんにより、攻撃者がCVVを含むカード情報を奪取するための仕掛けが作られるケースが多く発生しており、これもSQLインジェクションの脆弱性等が侵入経路となり得ますので、Webアプリケーションにおいてこれらの脆弱性を根本的に対策し(アプリケーションで使用するフレームワーク等を最新のバージョンに保つことも重要です)、加えてWAF(Webアプリケーションファイアウォール)による脆弱性への攻撃を意図したアクセスの遮断、内部からの情報流出を封じ込める出口対策等の多層防御をとるべきでしょう。

ITmedia NEWS

メタップス、不正アクセスやられ放題　最大46万件のカード番号やセキュリティコード流出か　バックドアやSQLインジェクションの痕跡見つかる

2022年02月28日 11時30分 公開　[ITmedia]

クレジットカード決済基盤を提供するメタップスペイメント（東京都港区）は2月28日、同社のデータベースから最大で46万件のクレジットカード番号、有効期限、セキュリティコードなどが流出したと発表した。サーバへの不正ログイン、SQLインジェクション、バックドアの設置などさまざまな攻撃を受けていたことが調査で分かった。



① トークン方式クレジットカード決済情報データベース

2021年10月14日から2022年1月25日に利用されたクレジットカード番号数（括弧内は流出情報）：460,395件（カード番号、有効期限、セキュリティコード）
第三者調査において、本データベースから断続的に情報の流出があったことは確認されていますが、弊社にて実際に流出した情報を特定することはできず、また、第三者調査機関からも特定は困難との見解を得たため、流出した可能性としては最大で上記全件数となります。

② 決済情報データベース

2021年5月6日から2022年1月25日に利用されたお客様のデータ保有件数

クレジットカード決済 (※1)	2,415,750件（カード番号、有効期限）(※2)
コンビニ決済	824,483件（氏名、電話番号、メールアドレス）
ペイジー決済	170,435件（氏名、郵便番号、住所、電話番号）

●「その警告画面・警告音は偽物です！！」国民生活センターが「サポート詐欺」の注意喚起

https://www.itmedia.co.jp/news/articles/2202/24/news183.html
https://www.kokusen.go.jp/news/data/n-20220224_2.html

このニュースをザックリ言うと･･･

- 2月24日(日本時間)、国民生活センターより、PC・スマートフォンでのネット利用中に突然「偽の警告画面」が現れる、いわゆる「サポート詐欺」に関する注意喚起が出されています。

- 同センターのPIO-NET(全国消費生活情報ネットワークシステム)への相談状況は、2018年度の7,211件から、2019年度は5,532件、2020年度は5,495件となり、2021年度は4月～12月期において3,700件(2020年の同期件数3,755件)となっている一方、被害額(契約購入金額)の平均額が年々上昇し、2020年度の81,103円から、2021年度は141,665円に急上昇しています。

- この他、相手から指示される支払方法として、クレジットカードによるものが年々減少し、代わってプリペイド型電子マネーによるものが増加しているとのことです。

- 同センターでは、警告画面に実在するソフトウェア会社が表示されていたとしても偽物であるとして、警告画面や警告音を鵜呑みにしたり、また慌てて表示されている窓口への電話や、契約をしたりせず、不安に思った場合には同センター等に相談するよう呼びかけています。

AUS便りからの所感

- 偽の警告画面の表示にはWebブラウザーの通知機能等が利用されますが、やはりこの機能を悪用して不審なサイトに誘導する手口については、2021年にIPA「安心相談窓口だより」で取り上げられています(https://www.ipa.go.jp/security/anshin/mgdayori20210309.html)。

- 同センターの注意喚起では参考となる動画・啓発資料等が挙げられており、どういった手口が存在するかを熟知した上で慎重に行動すること、例えば前述のような通知機能の悪用に対しても、不審な通知許可の要求に対し安易に許可しない、誤って許可したサイトについてはブラウザーの設定画面から削除するといった回避策・対策をとることが重要です。

ITmedia NEWS

「その警告画面は偽物です」　国民生活センターが「サポート詐欺」に注意喚起

2022年02月24日 21時42分 公開　[ITmedia]

国民生活センターは2月24日、PCなどの画面に偽のセキュリティ警告を表示し、サポート窓口をうたう番号に電話をかけさせる「サポート詐欺」について注意喚起を行った。困ったときは消費者ホットライン「188」に電話するように求めている。

サポート詐欺はPCやスマートフォンでインターネットを使用中に突然「ウイルスに感染している」など偽の警告画面や警告音を出し、電話をかけさせて有償のサポートやセキュリティソフトなどの契約を迫る手口。全国の消費生活センターなどには年間5000件以上の相談が寄せられており、とくに高齢者の被害が目立つという。

●国内約19万台のルーターに外部からアクセス可能、14万台近くはサポートが終了…NHK報じる

https://www3.nhk.or.jp/news/html/20220226/k10013503071000.html

このニュースをザックリ言うと･･･

- 2月26日(日本時間)、NHKのニュースにおいて、「国内にあるおよそ19万の機器(ルーター)がインターネットを通じて外部からアクセスできる状態」「うち14万台近くがすでにサポートが終了していたり最新のソフトウエアに更新されていない」と報じられています。

- 都内のセキュリティ会社が2月中旬に調査した結果によるもので、メーカーがサポートを終了、または最新のファームウェア提供が1年以上行われていないルーターが66,757台、最新のファームウェアにアップデートされていないルーターが94,070台確認されたとのことです。

- ニュースでは、ルーターにWi-Fiで接続した場合に不審なサイトに接続され、マルウェアをダウンロードされた事案が紹介され、外部から管理画面にアクセス可能かつ管理画面のID・パスワードが初期設定のままのルーターが接続先設定を書き換えられることにより、この事案を再現するデモンストレーションが行われています。

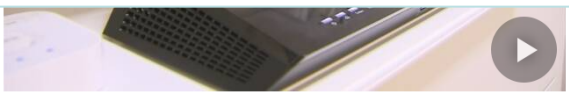
AUS便りからの所感

- 国内外のルーターに脆弱性が報告されることが度々起こっており、機種によってはファームウェアのアップデートが行われず、より新たな機種などへの移行が呼び掛けられるケースも珍しくありません。

- この他、内部ネットワークに設置したNASや複合機等が、これらの機器やルーターで有効になっていたUPnPによって外部から接続可能となるよう自動的に設定されるケースもあり、そういった状態になっている機器を探し出すサーチエンジン(SHODAN・Censys等)も存在します。

- 家庭・企業に拘わらず利用している機器の存在・機種を把握・管理し、古い機器を適宜交換する体制を整えるとともに、管理画面のID・パスワードの変更は機器設定の初期段階で忘れずに実施すること、外部への公開を意図しない機器についてはデフォルトで不要な設定がないか確認して確実に無効にすること、前述のサーチエンジン、あるいはニュースで取材に協力した横浜国立大学の研究室による「am I infected?(https://amii.ynu.codes/ ※利用にはメールアドレスが必要です)」等を活用して、機器が脆弱な状態にないかチェックすることが肝要です。

NHK



自宅の「ルーター」大丈夫？サイバー攻撃のリスク高く注意を

2022年2月26日 21時12分　IT・ネット

パソコンの無線接続などに使う機器「ルーター」についてセキュリティー会社が調査したところ、国内にあるおよそ19万の機器がインターネットを通じて外部からアクセスできる状態になっていて、このうち14万台近くがすでにサポートが終了していたり最新のソフトウエアに更新されていないことが分かりました。セキュリティー会社はサイバー攻撃を受けるリスクが高い状態にあるとして注意を呼びかけています。