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。

●提供終了したアクセス解析サービスのドメイン名、第三者が取得…不正なスクリプト設置の恐れに注意喚起

https://www.itmedia.co.jp/news/articles/2205/18/news189.html
https://www.nttcoms.com/news/2022051801/

このニュースをザックリ言うと･･･

- 5月18日(日本時間)、NTTグループのNTTコム オンライン・マーケティング・ソリューション社より、同社のサービスで以前使用していたドメイン名が第三者に取得されたとして注意喚起が出されています。
- 対象となるのは、同社が2020年7月まで提供していたアクセス解析サービス「Visionalist」において、解析用スクリプトの読み込み先として使用されていた「tracer.jp」で、一旦失効後、5月5日に海外の業者とみられる第三者が登録した模様です。
- 同社ではサービス終了の時点でスクリプトを読み込むタグを削除するようユーザーに呼び掛けていましたが、今回「セキュリティ上問題があるスクリプトを設置している可能性がある」としており、セキュリティリスク回避の観点から、改めて削除を呼び掛けています。

AUS便りからの所感等

- 失効されたドメイン名が第三者に取得される「ドロップキャッチ」により、終了したイベント等のWebサイトが不審なページに変わったりする例はよく見られ、セキュリティリスクを孕む事案として注意喚起が出され、ニュースで取り上げられることは度々発生しています。
- Visionalistのサイトでは2020年3月頃にサービス終了とスクリプトタグ削除の呼び掛けがアナウンスされていましたが、同年9月にシステムを停止した際にアナウンスが消えており(https://web.archive.org/web/*/www.visionalist.com)、そこから当該ドメイン名の失効～第三者の取得まではせいぜい1年半程度だったことになります。
- 「使われなくなったドメイン名でも失効させない」ことがドロップキャッチに対する一般的な回避策となりますが、今回のケースではVisionalistのサイトで使われていたドメイン名(visionalist.com)の方がサイト閉鎖後も現在まで保持され続けていることが確認されており、tracer.jpの方も同様の措置をとる必要があったと言えるでしょう。
- ユーザー側に対する防御としては、一部Webブラウザー向け広告ブロック拡張で当該ドメイン名がブロック対象に追加されている模様で、今後もアンチウイルスやUTMによるアンチフィッシング機能において、ドロップキャッチが発生してマルウェアの拡散等の影響が発生し得るドメイン名がブロック対象となるようなコンセンサスがとられるよう期待したいものです。

ITmedia NEWS

提供終了したアクセス解析ツールのドメインが他者の手に　不審なスクリプトが設置されている可能性も

2022年05月18日 19時40分 公開　[ITmedia]

NTTグループのNTTコム オンライン・マーケティング・ソリューションは5月18日、2020年7月に提供終了した同社のアクセス解析ツール「Visionalist」で使っていたドメインが何者かに取得されたと発表した。情報セキュリティ上問題のあるスクリプトが設置されている可能性があるとしている。

●「送信」していない段階で入力中の個人情報を収集するWebサイト…パスワード収集のケースも

https://www.itmedia.co.jp/news/articles/2205/20/news044.html

このニュースをザックリ言うと・・・

- 5月20日(日本時間)、ITニュースサイト「ITMedia」において、大手Webサイトが未送信の個人情報を収集しているとするベルギー・オランダ・スイスの研究チームによる調査論文が取り上げられています。
- 論文によれば、上位10万件のWebサイトに対し、欧州と米国在住のユーザーがアクセスしてフォームへの個人情報入力を行うというシナリオで調査を行ったところ、1,844のWebサイトが欧州ユーザーの電子メールアドレスを、2,950のWebサイトが米国ユーザーの電子メールアドレスを同意なしで収集していたことが判明したとしています。
- さらに52のサイトにおいて、送信前のパスワードを収集していることも確認されたとしています。
- 研究チームでは、この問題への対策のため、個人データの漏洩を警告・保護するFirefoxアドオン「LeakInspector」を開発したとのことです。

AUS便りからの所感

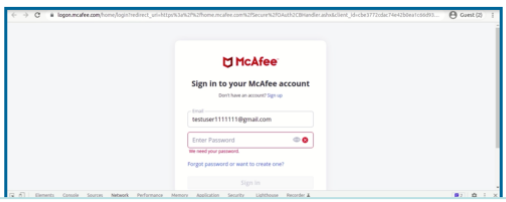
- 研究チームは調査結果を問題のあったWebサイトに開示しており、パスワードを送信前に収集していた52のサイトは全て対応されたとのことです。
- 訪問者の傾向等を解析する目的で、まだ入力が確定していない段階から各種情報をJavaScriptを用いて送信する仕組みを採用し、結果として過剰な情報収集を行っていたことが話題になっています。
- フォームへの入力完了までに、例えば郵便番号⇔住所の相互補完等のために入力内容(の一部)がWebサーバーに送信されるという形も以前からとられていましたが、今日ではブラウザー側の機能・性能も向上し、ブラウザー内で完結する形もとることができるようになっており、Webアプリケーションが可能な限り途中でのデータの送信を要求しない方向へ今後さらに進んでいくことが予想されます。

ITmedia NEWS

入力中の個人情報が"送信ボタンを押す前に"収集されている問題　約10万のWebサイトを調査

2022年05月20日 07時00分 公開　[山下裕毅，ITmedia]

ベルギーのKU Leuven、オランダのRadboud University、スイスのUniversity of Lausanneによる研究チームが発表した「Leaky Forms: A Study of Email and Password Exfiltration Before Form Submission」は、まだ送信していないのにもかかわらず、オンラインフォームで入力した個人情報（今回は電子メールアドレスとパスワード）が打ち込んだだけで収集されている問題を調査した論文だ。



●大量のTo: アドレスをBcc: に移動、メールアドレス漏洩防止機能を備えたOutlookのアドイン

https://forest.watch.impress.co.jp/docs/news/1410525.html
https://www.noraneko.co.jp/OutlookOkan/

このニュースをザックリ言うと・・・

- 5月20日(日本時間)、Windows向けソフトウェアを紹介するWebサイト「窓の杜」において、株式会社のらねこが開発しているフリーソフトウェア「おかん for Outlook」が取り上げられています。
- 「おかん for Outlook」は、Outlookによるメール送信時の様々な誤送信を防止するため、送信先メールアドレスのドメイン名や本文の内容に対し警告の表示等を行うアドインです。
- 同17日にリリースされた最新バージョン2.7.0.0では、宛先(To)およびCc: 欄で大量に入力されたメールアドレスをBcc: 欄に強制的に移動し、メール送信時のアドレス漏洩事故を防止する機能が追加されています。

AUS便りからの所感

- 昨年11月には、暗号化ZIPファイルとそのパスワードを別々のメールで送る「PPAP」防止のため、暗号化ZIPファイルの添付に対して警告を出す機能等も追加されています。
- 今日に至るまで、To: やCc: に大量のメールアドレスを貼り付けた状態でメールを送信してしまうことによるアドレス漏洩事故は枚挙にいとまがなく、人間によるチェックだけでも確実にこれを防止することは困難であると心得、メールサーバー側や、今回のようなメーラー側、あるいはUTM等で実装される誤送信防止機能を活用することが肝要です。
- 一方で、このような警告を出すツールやシステムに対し、ユーザーが度々の警告に慣れ切ってしまい、時にはこれを無視して安全でない操作を強行してしまう恐れもあることにも、注意・配慮は必要でしょう。

個人情報流出事故を防止可能になったOutlookアドイン「おかん for Outlook」v2.7.0.0

一斉配信メールの宛先をBCCに強制変換。文頭・文末へ定型文の自動追加機能も

石山裕規　2022年5月20日 06:45

（株）のらねこは5月17日、無料で使える「Microsoft Outlook」用の誤送信防止アドイン「おかん for Outlook（Outlook Okan）」の最新版v2.7.0.0を公開した。本バージョンでの主な変更点は、全ての宛先を強制的にBCCに変換する機能が追加されたこと。