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。

●転職サイトに「パスワードリスト型攻撃」による不正ログイン…約21万人分の履歴書流出か

https://scan.netsecurity.ne.jp/article/2021/02/17/45201.html
https://tenshoku.mynavi.jp/info/2021/02/12

このニュースをザックリ言うと･･･

- 2月12日(日本時間)、マイナビ社より、同社が運営する転職者向け情報サイト「マイナビ転職」が不正ログイン攻撃を受けたと発表されました。

- 不正ログイン攻撃は1月17日～2月9日にいわゆる「パスワードリスト型攻撃」で行われたとされ、2000年以降同サイトに登録されていた212,816名分(退会者除く)のWEB履歴書にアクセスされた恐れがあるとのことです。

- 同社では2月9日に不正ログインを遮断した後、全ユーザーのパスワードリセットやreCAPTCHAの採用等の対応を行ったとのことです。

AUS便りからの所感等

- 外部サービスから奪取されたメールアドレス・パスワードのリストを用いての「パスワードリスト型攻撃」は既にWebサイトへの不正ログインと情報等の奪取における定番となっており、複数のサイトで同じパスワードを使い回さないよう啓発するキャンペーンも長年行われていますが、今も頻繁に不正ログインが発生する事例が報告されています。

- ボット等の機械的な不正ログインを抑制するために用いられるreCAPTCHAでは、近年画像認証の前にカーソルの動きで相手を判定する等、人間側の利便性を損なわない手法も提供している一方、組織的な人力でreCAPTCHAを通過しようとする攻撃者もいるとされ、いたちごっこは今後も続くとみられます。

- ユーザー側においては自衛のため、これまでの啓発に則って推測されにくいパスワードをサイト毎に生成し、場合によっては生成から保存までツールによる管理も視野に入れることを改めて心がけて頂ければ幸いです。

Impress Watch

マイナビ転職、約21万人のWeb履歴書に不正アクセス

劉 尭　2021年2月16日 14:13

株式会社マイナビは、総合転職情報サイト「マイナビ転職」において、Webサーバーへの外部からの不正ログインがあったと発表し、陳謝した。

2000年から現在に至るまでに「マイナビ転職」に登録したユーザーのうち、21万2,816名のWeb履歴書に対し、2021年1月17日～2月9日のあいだに不正アクセスが行なわれた。外部で不正に取得されたと思われるパスワードを使ったなりすましで、一部ユーザーのWeb履歴書へ不正ログインが行なわれた。

● Mac約3万台がマルウェア「Silver Sparrow」に感染…M1モデルもターゲットに

https://www.itmedia.co.jp/news/articles/2102/22/news064.html

このニュースをザックリ言うと・・・

- 2月18日(現地時間)、セキュリティ企業の米Red Canary社より、Mac PCに感染する新たなマルウェアが確認されたと発表されました。
- 「Silver Sparrow」と名付けられたマルウェアは、17日の時点で世界153ヶ国・29,139台のmacOSで感染が確認されており、特にアメリカ・イギリス・カナダ・フランス・ドイツでの被害が大きいとしています。
- また、従来のIntel Macの他、最近発売されたM1モデルのMacにも感染が確認されているとのことですが、現時点でランサムウェア的な行動などはとっておらず、目的は不明とされています。

AUS便りからの所感

- Macでは「Windowsと違いマルウェアには感染しない」と宣伝していた時期もありましたが、2017年には「Fireball」と呼ばれるアドウェアがWindowsだけでなくMacにも感染を拡大し(AUS便り 2017/6/12号参照)、また2019年にはPC1台あたりのマルウェア平均検出数においてMacがWindowsを上回ったという情報も出ています(https://japanese.engadget.com/jp-2020-02-12-mac-windows-2019-malwarebytes.html)。
- M1モデルのMacではデスクトップPCでシェアが高いx86ではなく、スマホ等で既に実績があるARMアーキテクチャを採用していますが、2月に入りこのモデルで初めてとなるマルウェアが確認されたばかりでした(https://gigazine.net/news/20210218-apple-m1-malware/)。
- Macユーザーにおいても決して油断することなく、Gatekeeper等あらかじめ備わっているセキュリティ機能を確実に有効にし、またUTM等による防御、不審なメールの添付ファイルを開かないといった慎重な行動など、Windows利用時と気を付けるべきことは何ら変わりはありません。

ITmedia NEWS

M1端末を含む3万台が感染　目的不明のMacマルウェア「Silver Sparrow」

2021年02月22日 09時41分 公開　[ITmedia]

米セキュリティ企業Red Canaryは2月18日（現地時間）、世界で少なくとも約3万台のMac（M1モデルを含む）で感染が確認された新マルウェアを発表した。今のところランサムウェア（データを人質に身代金を要求するマルウェア）のような動作はなく、目的は不明という。

感染したM1 Macで表示されるウィンドウ（画像：Red Canary、Image Credit：Jimmy Astle）

● 「Movable Type」に複数のクロスサイトスクリプティングの脆弱性

https://scan.netsecurity.ne.jp/article/2021/02/26/45248.html
https://jvn.jp/jp/JVN66542874/index.html
https://www.sixapart.jp/movabletype/news/2021/02/24-1100.html

このニュースをザックリ言うと・・・

- 2月24日(日本時間)、CMS(コンテンツ管理)ソフトウェア「Movable Type(以下MT)」の開発元より、MTにクロスサイトスクリプティング(以下XSS)の脆弱性が複数確認され、修正バージョンのリリースが発表されています(同日、IPA・JPCERT/CCからも注意喚起が出されています)。
- 脆弱性は管理画面等3つの画面に存在するとされ、サイトにログインしたユーザーの権限で不正な処理を実行するよう攻撃者に誘導される恐れがあります。
- 修正バージョンとしてMovable Type 7 r.4706およびMovable Type 6.7.6がリリースされており、アップデートが強く推奨されています。

AUS便りからの所感

- MTは2000年代前半からブログサイトの構築等で多く用いられており、WordPressに人気面で押されている状態が長く続いている現在でも、日本を中心に使われているとされています。
- XSSの影響範囲は発生する場所や悪用のための条件次第でまちまちであり、外部の攻撃者が他の訪問者のみならず、運営する管理者側を罠に仕掛けることが可能なケースも存在し得ます。
- MTやWordPressに限らず、多機能なCMSには頻繁な脆弱性の報告とアップデートのリリースが付き物と考え、速やかにアップデートを行う体制を随時整えておくこと、場合によってはサーバー上やUTMにおいて不正なアクセスを遮断するWAF機能を導入・有効にする等も検討することが、訪問者と管理者の双方を保護する意味で肝要です。

ScanNetSecurity by iid

Movable Typeに複数のクロスサイトスクリプティングの脆弱性

独立行政法人情報処理推進機構（IPA）および一般社団法人JPCERT コーディネーションセンター（JPCERT/CC）は2月24日、Movable Typeにおける複数のクロスサイトスクリプティングの脆弱性について「Japan Vulnerability Notes（JVN）」で発表した。