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。

●「ドコモ口座」で使用していたドメイン名が失効、オークションに… ドコモ402万円で買い戻しか

https://www.itmedia.co.jp/news/articles/2309/25/news165.html
https://www.itmedia.co.jp/news/articles/2309/26/news117.html
https://www.watch.impress.co.jp/docs/series/suzukij/1534421.html
https://news.yahoo.co.jp/expert/articles/94066560a4a5f9eae4c552610da74665218cbb56
https://www.onamae.com/auc/jp/detail/183604

このニュースをザックリ言うと･･･

- 9月25日(日本時間)、NTTドコモがかつて使用していたドメイン名「docomokouza.jp」が、ドメイン名業者・お名前.comのオークションに出品されていることが、複数のネットメディアより相次いで報じられました。

- ドメイン名は2021年10月に終了した決済サービス「ドコモ口座」のもので、2023年7月いっぱいで失効していたものとされています。

- オークションは9月1日～9月25日に実施され、ドメイン名は4,023,000円で落札されましたが、その後NTTドコモがこのドメイン名を取り戻したことが明らかになっています。

AUS便りからの所感等

- NTTドコモでは、運営する各サービスのURLを「docomo.ne.jp」下のサブドメインに移行し、過去使用していたドメイン名も整理する作業を進めていましたが、「社内管理の不手際」で当該ドメイン名が失効したとしており、落札についても同社が行ったとする情報があるようです。

- 当該ドメイン名はサービス終了から2年弱での失効でしたが、オークションページによれば現在も外部1,500箇所以上からリンクされていた模様で、これらのリンク元からアクセスが来ることを見越し、自分たちが運営するWebサイトへのアクセス流入を期待する業者の入札により、落札価格が高騰するケースは決して珍しくはありません。

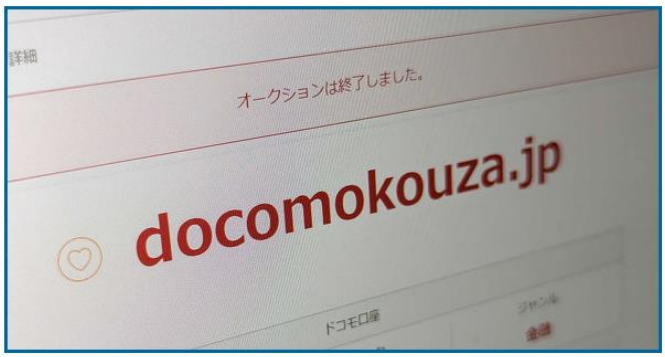
- ネット上に引き続き外部からのリンクが残るのみならず、本やチラシにURLやQRコードが掲載されることをも鑑み、Webサイト等立ち上げにおいて独自ドメイン名を取得する場合は、最終的にサイトを閉鎖した後も、使用しなくなったドメイン名を可能な限り維持することを最初から計画に入れることも必要でしょう。

ITmedia NEWS

「ドコモ口座」のドメイン、ドコモが取り戻す　出品の経緯をGMO含め聞いた

2023年09月26日 12時50分 公開　[山川晶之，ITmedia]

2021年に終了した、NTTドコモのウォレットサービス「ドコモ口座」のドメイン「docomokouza.jp」が、GMOインターネットのドメイン登録サービスでオークションに掛けられていた件について、ドコモは原因を「社内管理の不手際」と説明した。加えて、出品されていたドメインはドコモが取り戻しており、現在同社の管理下にあることも明かした。



「お名前ドットコム」に出品されていた「ドコモ口座」のドメイン

●マツダ・NHK、不正アクセスで個人情報流出

https://www.itmedia.co.jp/news/articles/2309/15/news138.html
https://newsroom.mazda.com/ja/publicity/release/2023/202309/230915a.pdf
https://nordot.app/1079294579822707100
https://www.nhk.or.jp/info/otherpress/pdf/2023/20230926.pdf

このニュースをザックリ言うと・・・

- 9月15日(日本時間)、自動車メーカーのマツダ社より、同社サーバー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。

- 不正アクセスが発覚したのは7月24日で、被害を受けたのは、同社・グループ会社・協力会社の社員および取引先担当者の計104,732件分の個人情報(ID・暗号化済みのパスワード・氏名・メールアドレス・会社名・部署・役職・電話番号)とされています。

- 同26日には、NHKより、同放送センターのサーバーが7月31日に不正アクセスを受け、同協会職員・スタッフおよび委託業務従事者の計23,435人分の個人情報(氏名・メールアドレス・部署・役職・内線番号・ID・ハッシュ化済みのパスワード)が流出した可能性があると発表されています(こちらは受信契約者情報および取材に関する情報は含まれていないとしています)。

AUS便りからの所感

- それぞれの不正アクセス発生は一週間の間隔ですが、同一の攻撃者か否か、マツダの発表において原因が「アプリケーションサーバーの脆弱性が悪用された」とされていたものについて、NHKでも同様かといった点は現在不明です。

- 大手企業・組織で不正アクセス・情報流出が相次ぐ形とはなりましたが、大きく報じられないながらも中小組織でも同様の事案は相次いでいるとみてよく、またくれぐれも「自組織が攻撃対象となることはない」等と思わず、サーバー・ネットワーク側でOS・アプリケーションを最新に保ち、またUTM等での防御を固めること(WAFの設置により、不正アクセスを受けながらも情報流出が防御できた例もあります)、クライアント側でもアンチウイルス等による確実な防御を行うことが肝要です。

ITmedia NEWS

マツダ、個人情報10万件超を漏えいか　社内サーバに不正アクセス

2023年09月15日 15時12分 公開　［松浦立樹，ITmedia］

マツダは9月15日、サーバ機器に不正アクセスを受け、個人情報が漏えいした可能性があると発表した。対象の個人情報は10万件超。同社は「関係者の皆さまには多大なるご迷惑とご心配をおかけすることとなり、深くおわび申し上げます」と謝罪している。

●Googleの広告からMac上で仮想通貨奪取を行うマルウェアに感染する事例が報告

https://pc.watch.impress.co.jp/docs/news/1529613.html
https://www.malwarebytes.com/blog/threat-intelligence/2023/09/atomic-macos-stealer-delivered-via-malvertising

このニュースをザックリ言うと・・・

- 9月6日(現地時間)、セキュリティベンダーのMalwarebytes社より、Google検索の広告からフィッシングサイトに誘導され、マルウェアに感染する事例が報告されています。

- 挙げられている事例は、チャート分析ツール「TradingView」の偽サイトからMacに感染するマルウェア「Atomic Stealer(AMOS)」をダウンロードさせるものとなっています。

- 偽のTradingViewを実行することにより、Macのユーザーパスワードが延々と要求され、入力すると仮想通貨ウォレット等のデータが奪取されるとしています。

AUS便りからの所感

- 偽のTradingViewは、macOSのセキュリティ機構であるGatekeeperを巧妙に回避するような特殊なインストール手順を提示する模様です。

- macOSでのソフトウェアの導入においては、不審なインストール手順を要求するような、偽物である可能性が高いパッケージによるインストールは決して行わず、Mac App Storeから正式なソフトウェアをインストールするよう心掛けるべきです。

- マルウェア入りパッケージをダウンロードさせる手法としては、Google検索結果の上位に表示される以外にも、公式のWebサイトを不正アクセスで改ざんし、偽サイトへ誘導するケースもあります(AUS便り 2023/09/20号参照)。

Impress Watch

Google検索の広告経由でMacに感染して仮想通貨などを奪うマルウェア

浅井 淳志　2023年9月7日 15:55

TradingViewのWebサイトを装った広告ページ(出典:Malwarebytes)

アンチマルウェアソフトの開発を手掛ける米Malwarebytesは、Google検索の広告経由でフィッシングサイトに誘導し、Atomic Stealer(AMOS)と呼ばれるマルウェアをダウンロードさせる事象を公式ブログにて紹介し、ユーザーに注意を促している。

AMOSは、2023年4月に登場した、主に暗号資産を標的とするmacOS用の情報窃取型マルウェア。ブログでは、チャート分析ツール「TradingView」のWebサイトになりすました偽サイトに誘導し、AMOSを含んだファイルをダウンロードさせる事象が紹介されている。