— AUS（アルテミス・ユーザ・サポート）便り 2022/11/22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。

●8年前閉鎖の経産省事業サイト、ドメイン名を第三者が取得して偽サイト設置か

https://www.itmedia.co.jp/news/articles/2211/21/news085.html
https://www.meti.go.jp/press/2022/11/20221118005/20221118005.html

このニュースをザックリ言うと･･･

- 11月18日(日本時間)、経済産業省より、同省が2011年度に実施していた「コンテンツ緊急電子化事業」特設サイトのドメイン名が第三者に取得されていることが確認されたとして、注意喚起が出されています。

- 当該事業は2013年3月で終了し、2014年7月にサイトも閉鎖されていましたが、「meti.go.jp」下のものではない独自の「.jp」ドメイン名を使用しており、2021年付で海外の第三者に登録されていることが確認されています。

- さらに、このドメイン名において元のサイトをコピーしたとみられる偽サイトが設置され、無関係な外部サイトへのリンクが張られていた模様で(11月22日時点ではサイトにアクセスできなくなっています)、同省からは、マルウェアに感染する恐れがあるため、サイトにアクセスしないよう呼び掛けられています。

AUS便りからの所感等

- アーカイブサイトにおける当該ドメイン名のサイトの記録では、少なくとも2015年8月にはドメインパーキングに、2016年3月の時点で(現在の持ち主とは別のものとみられる)第三者に登録され、無関係な内容のサイトが存在していたようですが、今年10月に現在の登録者が、恐らくはこのアーカイブサイトから過去のコンテンツを取得して偽サイトを立ち上げていたとみられます。

- 一時的なイベント等のために取得した独自ドメイン名が失効した後で第三者に取得される「ドロップキャッチ」により、閉鎖したWebサイトが不審なページに変わったりする例は枚挙にいとまがありませんが、今回は元のサイトのコンテンツを悪用する偽サイトが同じドメイン名で稼働するという悪質な事例となっています。

- また、過去に配布されたチラシ・ポスターに記載されたURL(およびそれを変換したQRコード)から、不審なサイトにアクセスしてしまうという事例も報告されたことがあります。

- ドロップキャッチによるセキュリティリスクを考慮し、可能であれば既存のドメイン名の下にサブドメインを作るよう検討すること、独自にドメイン名を取得した場合はサイト閉鎖後も5年・10年以上の長期間あるいは無期限で保持するよう計画すべきでしょう。

ITmedia NEWS

経産省「コンテンツ緊急電子化事業」偽サイトに注意 事業終了後、第三者が「.jp」ドメイン取得　ウイルス感染のおそれ

2022年11月21日 11時59分 公開　[岡田有花，ITmedia]

経済産業省は11月18日、同省が過去に保有していた「コンテンツ緊急電子化事業」特設サイトのURLから、同事業と無関係なサイトへのリンクが張られているとして注意を呼び掛けた。アクセスすると、ウイルス感染などの恐れがあるとしている。

コンテンツ緊急電子化事業（緊デジ）は2011年度の事業で、既に終了している。特設サイトは「.jp」ドメインで作られ、14年に閉鎖されていた。

このドメインを第三者が取得し、緊デジのWebサイトのデザインを再現した上で、無関係なサイトへのリンクを貼り付けたようだ。

●ランサムウェア感染で個人情報流出か…パスワード総当たり攻撃受ける

https://scan.netsecurity.ne.jp/article/2022/11/21/48522.html
https://www.thers.ac.jp/news/2022/11/20221118-jimu.html
https://www.thers.ac.jp/news/upload/20221118_jimu.pdf

このニュースをザックリ言うと･･･

- 11月18日(日本時間)、名古屋大学と岐阜大学を運営する国立大学法人・東海国立大学機構より、同機構がランサムウェアによる攻撃を受け、個人情報が漏えいした可能性があると発表されました。

- 被害を受けたのは、名古屋大学および岐阜大学に在籍歴がある教職員・学生最大4万人分の個人情報(氏名・所属・身分・生年月日・性別・学生番号・職員番号および機構アカウント情報)とされています。

- 10月18日に不正アクセスによるパスワード総当たり攻撃を受けており、ネットワークの遮断とパスワードの初期化を実施しています。

AUS便りからの所感

- 機構外からネットワークアクセス制限が要求される個所において、設定に不備があったのが不正アクセスを受けた原因としています。

- パスワード総当たり攻撃を受けて不正ログインが成功したアカウントがあること、流出した他のアカウント情報にも暗号化されたパスワードが含まれており、すぐに復号できるものではないとしているものの、暗号化の強度次第では現実的な時間で復号が行われる可能性もあること、また初期化されたパスワードのルール次第では第三者に推測される恐れもあることが懸念され、今回のような事態では必ずパスワード変更を行い、また使用していたパスワードを他のサービスでも使い回していないか確認する必要があるでしょう。

- ランサムウェアにより一部データが改変されたものの、復旧可能のため業務への支障は出ていないとのことで、データバックアップ等の備えは行っていたとみられ、またアクセス制限設定の不備があったとしても、不審なログイン試行を遮断する機構があれば防げていた可能性があり、そういった各種防御策を多重に実施することはあらゆる場面でセキュリティを維持するためにも重要と言えます。


インシデント・事故／インシデント・情報漏えい

東海国立大学機構にパスワード総当たり攻撃でアカウント情報流出の可能性、設定不備が原因

東海国立大学機構は11月18日、同機構への不正アクセスによる個人情報流出について発表した。日本語に加え英文での案内も行っている。

シェア　ツイート　送る

東海国立大学機構は11月18日、同機構への不正アクセスによる個人情報流出について発表した。日本語に加え英文での案内も行っている。

これは10月18日に、同機構で機構アカウントを管理するために運用する機構統合認証システムの一部に対し、第三者から不正アクセスによるパスワード総当たり攻撃があり、サーバがランサムウェアに感染し、データの一部が改変され、機構が保有する個人情報が漏えいした可能性が判明したというもの。機構外からネットワークアクセス制限が要求される個所の設定に不備があったことが原因。

漏えいの可能性があるのは2022年5月以降に岐阜大学に所属していた、或いはしている教職員と2021年7月以降に名古屋大学に所属していた、或いはしている学生・教職員 最大4万人の氏名、所属、身分、生年月日、性別、学生番号・職員番号、機構アカウント、機構アカウントを認証するための暗号化されたパスワード、機構メールアドレス、機構 ID を含む個人情報。現時点で悪用の事実は確認されていない。

トップページ
全７枚
拡大写真

●転送設定ミスで10ヶ月間メールが外部に流出か…「gmail.com」入力ミス

https://www.itmedia.co.jp/news/articles/2211/21/news144.html
http://www.saitama-u.ac.jp/news_archives/2022-1118-1029-16.html

このニュースをザックリ言うと･･･

- 11月21日(日本時間)、埼玉大学より、教員によるメール転送設定ミスが原因で、個人情報2,000超が流出していた可能性があると発表されました。

- 流出が発生していたのは2021年5月6日～2022年3月3日にかけての4,890件のメールで、同大学の教職員・学生及び学内関係者のべ2,122件の個人情報(氏名・学生番号・メールアドレス等)が含まれていたとされています。

- 教員が所有する「***@gmail.com」のメールアドレスへの転送設定の際、誤って「***@gmai.com」と入力していたことが原因としています。

AUS便りからの所感

- 「@gmai.com」の誤入力によるメール流出は2021年3月に京都市立芸術大学で発生しており(AUS便り 2021/04/05号参照)、このような著名なドメイン名からの誤送信やWebアクセス等を狙って似たようなドメイン名を取得する手口は「タイポスクワッティング」、それによって取得されたドメイン名を含めた似通ったドメイン名は「ドッペルゲンガー・ドメイン」と呼ばれることがあります。

- 「@gmai.com」はGMailが登場するよりはるかに前の1991年に登録されている模様ですが、登録している企業などの実態は確認されない一方、メールを受信するためのMXレコードが設定されています。

- ユーザー側で入力ミス(他にもメーラー上でBcc: ではなくCc: にアドレスを入力する等)を完全に防止するには限界があり、メーラー自身やアドオンあるいはメールサーバー等に対するソリューションとして提供される誤送信防止機能の導入による対策を強く推奨致しますが、一方でタイポスクワッティングを狙ったドメイン名や「@gmai.com」のような実害が度々発生しているものについては、メールサーバーの設定で遮断するよう設定するのも検討に値するでしょう。


「gmail」ドメインを「gmai」と誤記、10カ月気付かず2000件超の情報漏えいか　埼玉大が「ドッペルゲンガー・ドメイン」の毒牙に

2022年11月21日 18時37分 公開　[ITmedia]

埼玉大学は11月21日、教員によるメールの転送ミスが原因で、個人情報2000件超が漏えいしていた可能性があると発表した。本来「@gmail.com」のドメインに送るはずだったメールを、約10カ月にわたって「@gmai.com」のドメインに自動転送し続けていたという。

埼玉大学（公式サイトから引用）

2021年5月6日から22年3月3日にかけて、4890件のメールを誤配信していた。一連のメールには、教員の氏名・メールアドレスなどが485件、学生の氏名、学生番号、メールアドレスなどが849件、学外関係者の氏名、メールアドレスなどが788件含まれていたという。漏えいした可能性がある情報の悪用は確認していない。