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。

●厚労省新型コロナ相談窓口サイトの独自ドメイン名、ネットオークションで第三者に落札

https://www.itmedia.co.jp/news/articles/2404/16/news159.html
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000211289_00014.html

このニュースをザックリ言うと･･･

- 4月3日、厚生労働省が運営していた、新型コロナウイルス感染症に関する「都道府県の外国人用相談窓口」サイト(以下・同サイト)で使用していたドメイン名「covid19-info.jp」(以下・同ドメイン名)が無関係のサイトに使われているとして、同省より注意喚起が出されています。

- 同ドメイン名については、2023年9月の時点で、ドメイン名管理業者によるオークションにかけられ、約322万円で落札されていたことがメディアで報じられており、今回投資に関するブログとみられるWebサイトの設置が確認された模様です。

- 厚労省では、2023年5月31日に同サイトに関する委託業務終了とともに同ドメイン名の運用も終了、以後は当該ドメイン名およびこれを用いたWebやメールは同省と無関係としています。

AUS便りからの所感等

- 厚労省からの発表は、同ドメイン名が失効してオークションにかけられたとみられる2023年9月にも行われており、今回は2回目となっています。

- 同サイトは2020年9月に設置された後、2021年1月に厚労省の「mhlw.go.jp」ドメイン下に移転しており、以後「covid19-info.jp」ドメインはリダイレクトのために用いられていた模様です。

- 同ドメイン名の失効は委託業者が更新しなかったためとされていますが、サイト閉鎖からドメイン名失効までわずか3ヶ月と、周知徹底のための期間が十分だったとは言い難く、厚労省を騙る巧妙なフィッシングサイト等が設置されて問題となっていた恐れがあります。

- つい最近まで使用されていたようなドメイン名が十分な期間を経ずに失効してしまい、第三者に登録されてしまう「ドロップキャッチ」の事例は政府機関・地方自治体あるいは大手企業に至るまで度々報じられており、事前事後の対策として、一時的なイベントのために専用のドメイン名を(jpやcom等で)新規に登録するよりも、既存のドメイン名の下にサブドメイン名を作るよう検討すること、またイベントやサービスの終了後も5年・10年といった可能な限り長期間ドメイン名を維持するよう計画すること等が推奨されます。

ITmedia NEWS

厚労省、新型コロナ相談窓口のドメイン、FX勧誘サイトに転用されていた

2024年04月16日 16時57分 公開　[岸潤隆徳，ITmedia]

厚生労働省が新型コロナウイルス感染症に関する情報を在留外国人向けに提供するために開設したWebサイトのドメイン（covid19-info.jp）が、FX（外国為替証拠金）取引の勧誘とみられるWebサイトに転用されていることが分かった。

24年4月16日時点の「covid19-info.jp」

厚生労働省は、新型コロナウイルス感染症の流行を受け、2020年9月1日に多言語に対応する「都道府県の外国人用相談窓口」を開設し、23年5月31日まで運用していた。委託業務終了とともに、ドメインの利用も終了したという。

● 3月のフィッシング報告件数は97,163件、フィッシングサイト件数も急増

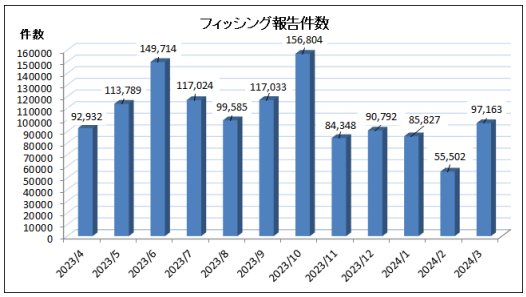
https://www.antiphishing.jp/report/monthly/202403.html

このニュースをザックリ言うと・・・

- 4月10日(日本時間)、フィッシング対策協議会より、3月に寄せられたフィッシング報告状況が発表されました。
- 3月度の報告件数は97,163件で、2月度(https://www.antiphishing.jp/report/monthly/202402.html)の55,502件から41,661件増加しています。
- フィッシングサイトのURL件数は44,228件で2月度(23,988件)から20,240件増加、悪用されたブランド件数は87件で2月度(70件)から17件増加となっています。
- 最も多く報告されたのは東京電力とAmazonを騙るフィッシングでそれぞれ報告数全体に対する約15.9%、次いで報告が多かったイオンカード、三井住友カード、メルカリ、ETC利用照会サービスと合わせて約66.7%、さらに1,000件以上報告された15ブランドまで含めると約90.5%を占めたとのことです。

AUS便りからの所感

フィッシング対策協議会
Council of Anti-Phishing Japan



- 同協議会では2月度報告件数発表時、件数の落ち込みを「旧正月の前後にあたるため」と分析していましたが、実際に2023年11月度～2024年1月度に近い水準まで回復しています。
- フィッシングサイトURL件数は4か月連続の増加、かつ2022年9月(53,612件)以来の4万件越えとなっており、サイトへのリダイレクト用に短縮URLおよびCloudflare Workersで付与できるサブドメインを悪用する傾向も続いています(全体の約61.1%)。
- Gmailが@gmail.com(および @googlemail.com)宛にメールを送信する相手にSPF・DKIM・DMARCの設定等のメールセキュリティ要件を満たすよう要請する「メール送信者のガイドライン(https://support.google.com/a/answer/81126?hl=ja)」は2月1日に適用され、既にガイドライン未対応のメールに対し一時的なエラーによる受信遅延の措置がとられており、以後も受信拒否が段階的に拡大されるとのことですが、最大手のメールサービスである以上「対応しなくてよい」ということはほぼ有り得ず、またその他の取引相手をフィッシングから保護する意味でも、全ての組織でドメイン名・メールサーバーにおける対応が必須と言えます。

●ターミナルソフト「PuTTY」に脆弱性、特定形式の秘密鍵が容易に復元される恐れ…他のソフトにも影響あり

https://forest.watch.impress.co.jp/docs/news/1584589.html
https://www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/vuln-p521-bias.html

このニュースをザックリ言うと・・・

- 4月16日(日本時間)、SSHに対応するターミナルソフト「PuTTY」に脆弱性(CVE-2024-31497)が確認され、修正バージョン0.81がリリースされています。
- 脆弱性は、PuTTYバージョン0.68～0.80において521-bit ECDSAのSSH秘密鍵を用いての認証処理に問題があったというもので、攻撃者に秘密鍵を推測され、容易に復元される恐れがあるとされています。
- PuTTY開発元からは、バージョン0.81へのアップデートとともに、521-bit ECDSAの秘密鍵は破棄し(サーバー上に登録している公開鍵も)、秘密鍵を作り直すよう呼び掛けています。
- 内部でPuTTYを使用しているツールにも脆弱性の影響があるとされ、ファイル転送ソフト「WinSCP」「FileZilla」やバージョン管理ツール「TortoiseGit」ではそれぞれ修正バージョンがリリースされています。

AUS便りからの所感

Impress Watch

「PuTTY」に秘密鍵が復元できてしまう深刻な脆弱性 ～「WinSCP」など他ツールにも影響

v0.81への更新と鍵の再生成を

樽井 秀人　2024年4月16日 12:55

リモートログオンクライアント「PuTTY」の最新版v0.81が、4月15日に公開された。たった60個ほどの署名からNIST P-521秘密鍵を復元できてしまう脆弱性（CVE-2024-31497）を修正したセキュリティアップデートとなっている。

この脆弱性が影響するのは、「PuTTY 0.68」から「PuTTY 0.80」までのバージョン。ECDSA署名では一度だけ利用される秘密の番号（nonce）を必要とするが、「PuTTY」を含む一部のプログラムではこれが十分にランダムではないため、公開されている署名を少し集めるだけで、ローカルのオフライン環境で秘密鍵を算出できてしまう可能性がある。

- 脆弱性の影響を受ける秘密鍵は、例えばPuTTY等に付属するputtygenで作成した場合、鍵の種類として「ECDSA」かつ「nistp521」を指定したもの(Pageantに鍵を追加した際には「NIST p521」と表示され、サーバー上の ~/.ssh/authorized_keys に追加する公開鍵は「ecdsa-sha2-nistp521」で始まるものとなります)が該当する一方、ECDSA以外の秘密鍵(RSAやEd25519)、またECDSAでもnistp256・nistp384を指定していた秘密鍵については影響は受けないとされています。
- 秘密鍵の作り直し、あるいは今後作成する場合には、長年使用されてきたRSA鍵が強度の問題の指摘からOpenSSHの新しいバージョンで非推奨となっていることもあり、Ed25519鍵を作成することを推奨致します。