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。

●go.jp下のサブドメインに「乗っ取り」の恐れ…ネットワーク研究者による「保護」も

http://www.e-ontap.com/blog/?date=20241223
https://www3.nhk.or.jp/news/html/20250109/k10014688801000.html
https://www3.nhk.or.jp/news/html/20250110/k10014689801000.html
https://www.itmedia.co.jp/news/articles/2501/21/news187.html
https://jprs.jp/tech/security/2025-01-21-danglingrecords.html

このニュースをザックリ言うと･･･

- 12月23日(日本時間)、ネットワーク研究者である中京大学の鈴木常彦教授より、総務省のサイトで使われていた「kyufukin.soumu.go.jp」と、厚生労働省のサイトで使われていた「oshigoto.mhlw.go.jp」の各サブドメインを「悪意ある乗っ取りから保護」したとするブログ記事が発表されました。
- 各サイトは既に運用が終了していたものですが、DNSの設定上の問題による「乗っ取り」が可能な状況にあったとし、鈴木氏自身の「保護」措置により、同氏が用意したWebサイトが表示される状態となっていました。
- 前述のサイトはいずれも1/8までに対策され表示されなくなっていましたが、同氏は他にも10近くのgo.jp下などのサブドメインについて保護措置を行ったとしています。
- 1月9日・10日にはNHKでもこの問題が報じられ、国土交通省のあるサブドメインが実際に攻撃者の乗っ取りを受けて海外のオンラインカジノにつながる広告サイトとなっていたことが明らかとなった他、同21日には.jpドメインを管理するJPRS社からも注意喚起が出されています。

AUS便りからの所感等

- 問題となったサブドメインは、DNSのCNAMEレコードやNSレコードで参照していた外部サーバーが解約等で空いている状態(Dangling Record等と呼ばれる)となり、第三者が同じサーバー名で契約を行うことにより、「偽サイト」の設置や、Let's EncryptによるHTTPSサーバー証明書の発行等が可能となっていた模様です。
- JPRSの注意喚起では、前述した手口の事例を取り上げるとともに、サービスを終了したWebサイト等のためのDNS設定(CNAME・NSレコード等)を削除・変更することや、ツール等を用いての削除・変更漏れの検知・修正等を推奨していますが、サービス自体が継続中でも、参照する外部サーバー等に変動があった場合、使わなくなったサーバーへの参照は削除するよう注意してください。
- 「可能な限り新規ドメイン名の取得ではなく既存のドメイン名下に置く」ことは当欄でも度々推奨していましたが、その際にも別途(これまで考慮していなかったような)必要な技術的対策があることに留意すべきです。

NHK

国交省 過去に使ったドメイン オンラインカジノ広告に一時流用

2025年1月10日 17時16分

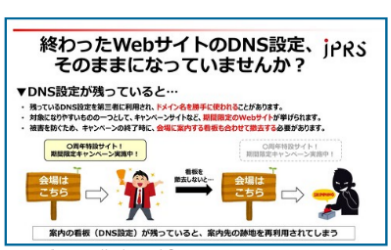
総務省など複数の中央省庁の一部ウェブサイトに、セキュリティー上の不備があった問題で、国土交通省が過去に使ったウェブサイトのドメインがタイのオンラインカジノにつながる広告サイトに一時流用されていたことがわかりました。外部からの指摘で、現在は修正されていますが、専門家は、「信頼性が高い政府機関のドメインが、不正なサイトに使われたことは非常に大きな問題だ」としています。

ITmedia NEWS

期間限定のWebサイト、DNS設定をそのままにしていない？　サブドメインを乗っ取られるリスク　JPRSが注意喚起

2025年01月21日 19時37分 公開　[松浦立樹，ITmedia]

期間限定のWebサイトでDNS設定をそのままにしていないか？――.jpドメインのレジストリである日本レジストリサービス（JPRS）は1月21日、サブドメインの管理方法に関する注意喚起を発表した。期間限定のキャンペーンサイトなどの公開後、DNS設定を残したままだと、第三者に悪用されサブドメインを乗っ取られる可能性があるという。



JPRS、サブドメインの管理方法に注意喚起

レンタルサーバやCDNなどの事業者のサービスを利用して、自身のドメイン名のサブドメインで新たにWebサイトを公開できる。その際、事業者のサーバを参照するDNS設定を自身のドメイン名の権威DNSサーバに追加することで、Webサイトを提供できる状態になる。

● 12月フィッシング報告件数は232,290件、20万件の大台一気に突破

https://www.antiphishing.jp/report/monthly/202412.html

このニュースをザックリ言うと・・・

－1月17日(日本時間)、フィッシング対策協議会より、12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。

－12月度の報告件数は232,290件で、11月度(https://www.antiphishing.jp/report/monthly/202411.html)の178,593件から53,697件増加しています。

－フィッシングサイトのURL件数は120,415件で12月度(77,109件)から43,306件増加、悪用されたブランド件数は107件で12月度(94件)から13件増加となっています。

－ブランド別で最も多いAmazonを騙るフィッシングの割合は全体の約16.3%と減少、次いで10,000件以上の報告を受けたえきねっと、PayPay、佐川急便、国税庁、マスターカード、Apple、三井住友カード、JAバンク、JCBと合わせて約73.7%、さらに1,000件以上報告された27ブランドまで含めると約96.8%を占めたとのことです。

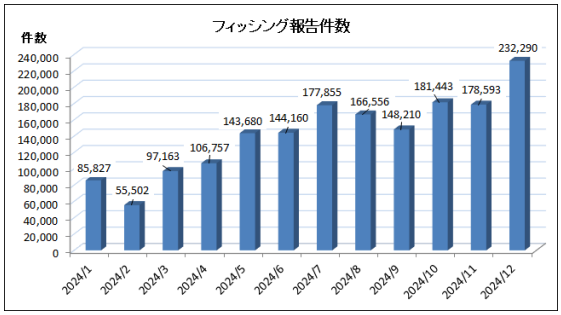
AUS便りからの所感

－報告件数はついに20万件の大台を突破、フィッシングサイトのURL件数も10万件越えでそれぞれ過去最多を更新しています。

－毎月の発表によれば、フィッシングメールの大量送信を行うIPアドレスにはDNS PTRレコード(IPアドレスからの逆引き)が設定されていないケースが多く(今月度は全体の約97.5%を占めているとのことです)、大手メールサービスでは既にこのようなアクセス元からのメールを受信しない設定となっているものもあるとされ、自組織のメールサーバーにおいても受信しない設定を採用することは、フィッシング・スパムメールの大幅な遮断に有用とみられます(ただし実際の取引先からのメールを誤って遮断しないよう、サーバー管理者において慎重に確認する必要はあるでしょう)。

－同協議会からの特定のフィッシングへの注意喚起は最近では12月上旬に3件あったのみですが、日本データ通信協会の迷惑メール相談センターには日々20件前後のフィッシングメールが掲載されており(https://www.dekyo.or.jp/soudan/contents/news/alert.html)、利用しているサービスについて不審なメールを受信した際はこういった情報等と文言が一致するか確認するとともに、本物のサービスのサイトへは事前に登録したブラウザーのブックマークやスマホアプリからアクセスする等、慎重に行動することを日々心掛けましょう。

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



● LinkedInへのコンタクトから暗号資産流出へ…警察庁、JPCERT/CC等注意喚起

https://www.yomiuri.co.jp/national/20241223-OYT1T50182/
https://www.npa.go.jp/bureau/cyber/koho/caution/caution20241224.html
https://blogs.jpcert.or.jp/ja/2025/01/initial_attack_vector.html

このニュースをザックリ言うと・・・

－12月24日(日本時間)、警察庁より、5月にDMMビットコイン社から約482億円分のBitcoinが流出した事件について、北朝鮮の攻撃者グループ「TraderTraitor」が関与したものだったと発表されています。

－DMMビットコイン社から暗号資産取引の管理を委託されていた業者の社員に対し攻撃者がビジネス特化型SNS「LinkedIn」で接触し、技術の確認名目を騙ってマルウェアを実行させ、システムに侵入したとされています。

－1月10日にはJPCERT/CCより、本件を受けてさらに技術的な解説を含めた注意喚起が出されています。

AUS便りからの所感

－JPCERT/CCの注意喚起では大きく3つの攻撃事例を紹介した上で、「主に英語を使用する」「やり取りをLinkedInから(SkypeやWhatsApp等に)変更するように要求してくる」「ファイルをダウンロード・実行させようとし、また実行したかどうか等を執拗に確認してくる」等の特徴があるとしています。

－警察庁では1月に別の攻撃者グループによる攻撃についての注意喚起も行っており、やはり巧妙に相手を安心させた上でマルウェアを送り付け実行させる手口となっています(AUS便り 2025/01/16号参照)。

－今回の事案について安易に「暗号資産に関わっていないから」等と対岸の火事で済ませるのではなく、発表された事例にできる限り目を通し、不審な相手からの連絡に常に注意を払うこと、アンチウイルス・UTM等によるマルウェア感染等への防御を固めることが重要です。

讀賣新聞オンライン

ＤＭＭビットコインの４８２億円流出、北のハッカー集団「ＴＴ」関与と特定…ＦＢＩと警察庁

2024/12/24 07:00　保存して後で読む

暗号資産「ビットコイン」をイメージしたもの＝ロイター

暗号資産交換会社「ＤＭＭビットコイン」（東京）から５月、約４８２億円相当のビットコインが流出した事件で、警察庁や米連邦捜査局（ＦＢＩ）は２４日、北朝鮮のハッカー集団「トレイダートレイター（ＴＴ）」によるサイバー攻撃と特定したと公表した。同社の暗号資産取引を管理する委託先の社員が、ヘッドハンティングを装って接触してきた人物に社員権限を盗まれていたという。

ＴＴは朝鮮人民軍偵察総局に属するハッカー集団「ラザルス」の一部とされ、国内での被害確認は初めて。攻撃元を名指しで非難する「パブリック・アトリビューション」を日本政府が行うのは８例目で、警察庁サイバー特別捜査部と警視庁が不正アクセス禁止法違反容疑で調べている。