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。

●大学の教育研究施設HP、不正なWordPressプラグインインストールされ閉鎖…迷惑メール送信も

https://scan.netsecurity.ne.jp/article/2022/12/06/48591.html
https://www.pu-toyama.ac.jp/news/news_outline/2022/12/01/15392/

このニュースをザックリ言うと･･･

- 12月1日(日本時間)、富山県立大学より、同大学DX教育研究センターのWebサイトが不正アクセスを受け、管理者権限を乗っ取られたとして、当該サイトを閉鎖したと発表されました。

- 11月21日に当該サイトへのアクセス、管理画面へのログインができない事象があり、外部レンタルサーバー事業者に問合せた結果、11月12日に不正なプラグインがインストールされたことにより、WordPressが正常に実行されなくなっていたことが確認されたとしています。

- 不正アクセスにより、同14日に32,255件の迷惑メールが送信されたことも明らかになっている一方、当該サーバーには外部公開情報のみが保管されており、個人情報の漏洩は確認されていないとのことです。

AUS便りからの所感等

- 発表において、レンタルサーバー上でWordPressを使用していたことが示唆されているものの、不正アクセスの詳しい経路には触れられておらず、WordPressに対し本体やプラグインの脆弱性を悪用された、管理画面からブルートフォース等による不正なログインを実行された可能性、あるいはWordPress以外の経路(FTP・SSH等)からの不正ログインの可能性等も考えられます。

- 各種サービスやWebサイトの管理画面へのログインにおいてID・パスワードによるログイン試行を無制限に実行可能なケースでは、特に簡単なパスワードが設定されていた場合、たちどころに不正ログインが成功してしまう恐れがあるため、不審なログイン試行の記録や遮断を行う機能を有効にする、あるいはそういった機能を提供するプラグイン等の導入は欠かせません(WordPressにも有償・無償に拘わらず多くのセキュリティプラグインがサードパーティーから提供されています)し、VPSであればインストールされているOSからアプリケーションに至るまで最新のバージョンであるよう管理する体制も必須となります。

- また可能であれば、Webサーバーと個人情報等重要なデータを保存するサーバーを分離することや、サーバーが乗っ取られた場合にそこを踏み台に他のサーバーにアクセスされないよう、サーバー自体の設定やUTM等での隔離によりアウトバウンドアクセスの適宜フィルタリングをすること等も検討に値するでしょう。

ScanNetSecurity by iid

インシデント・事故／インシデント・情報漏えい

2022.12.6 Tue 8:05

富山県立大学 DX教育研究センターホームページに不正アクセス、プラグインをインストールされる

公立大学法人富山県立大学は12月1日、DX教育研究センターホームページへの不正アクセスについて発表した。

シェア　ツイート　送る

トップページ

全２枚

拡大写真

公立大学法人富山県立大学は12月1日、DX教育研究センターホームページへの不正アクセスについて発表した。

これは同学が外部レンタルサーバ上で公開しているDX教育研究センターホームページに第三者から不正アクセスがあり、管理者権限を有するユーザーアカウントが乗っ取られたことが11月22日に判明したというもの。

11月21日午前に、当該サイトにアクセスできないこと、管理者画面にログインできないことを担当者が確認し、同日午後に外部レンタルサーバ事業者に状況を問い合わせ、11月12日に不正なプラグインがインストールされたことでWordPressが正常実行されなかった旨の回答が翌11月22日にあった。また11月14日には32,255件のメール送信の踏み台となったことを、11月29日にメール送信の痕跡から確認している。

● W杯ライブ配信を騙りクレカ情報詐取等のフィッシング、警視庁が注意喚起

https://twitter.com/MPD_cybersec/status/1599598433173737472

このニュースをザックリ言うと・・・

- 12月5日(日本時間)、警視庁サイバーセキュリティ対策本部より、FIFAワールドカップ等スポーツイベントのライブ配信を騙るフィッシングが確認されているとして注意喚起が出されています。

- 同対策本部のTwitterアカウントでは、ライブ配信の視聴は正規サイトから行うよう、またセキュリティソフトやアプリは最新に保つよう呼び掛けられています。

AUS便りからの所感

- ワールドカップやオリンピック等スポーツイベントから、地震・台風といった事故・災害あるいは新型コロナウイルス感染症に至るまで、世界が注目する大きな出来事には必ず便乗したサイバー犯罪が起こり得ます。

- また、例えば7月に発生したKDDIの通信障害の際も、ユーザーへの返金に便乗したフィッシングが発生し、注意喚起が出る事態となっています。

- 非公式で安価に何らかのサービスが受けられるようなものを安易に検索して素性の知れないサイトに軽率に個人情報・クレジットカード番号等を入力することは決して行わないようにし、また不審な宣伝や通知を騙ったSMSやメールを受け取った際にも、セキュリティ関連団体・組織からの注意喚起、本物の業者からのメールやSMSの運用に関するポリシーを確認し、無闇にリンクをクリックしない等に注意してください。

● Webブラウザ登録のルート認証局の一つ、米諜報機関との関係が報じられMS・Mozillaが無効化

https://gigazine.net/news/20221202-mozilla-microsoft-stop-trusting-trustcor/
https://gigazine.net/news/20221110-trustcor-systems-with-government-ties/

このニュースをザックリ言うと・・・

- 11月8日(現地時間)、米ワシントンポスト等より、主要なWebブラウザー等に登録されているルート認証局の一つTrustCorが米国の諜報機関や法執行機関と関係を持ち、認証システムを濫用していた疑いがあると報じられています。

- TrustCorは、米政府機関に通信傍受サービス等を提供していた米Packet Forensics社と、複数のAndroidアプリに個人情報を収集するコードを提供したとされるパナマのMeasurement Systems社との関係が取りざたされている他、エンドツーエンドの暗号化をうたって提供しているサービスMsgSafe.ioについてもTrustCorが内容を読み取れる状態だったと研究者から指摘される等しています。

- Firefox開発元のMozillaおよびWindows・Edge開発元のMicrosoftが、一連の報道を受け、TrustCorが新たに発行する証明書を信頼しないことを決定したことが11月30日に報じられています。

AUS便りからの所感

- 証明書は、Webサイトが正規のものであることを証明する以外にも、いわゆるコードサインニングによるソフトウェアへの署名と検証等にも用いられます。

- ルート証明書を提供する認証局が攻撃者に対して不正な証明書を発行したことにより、ルート証明書が無効化されたケースはこれまでも何度か発生しており、最も大規模なものとしては、Symantec社が所有していた複数の大手認証局について証明書発行プロセスの問題が指摘され、各ブラウザーにおいて証明書を信頼しない措置がとられた件が挙げられます。

- 組織内で独自に認証局を立ち上げ、随時証明書を発行するケースも多々あると思われますが、これについてもくれぐれも証明書発行のための秘密鍵等を奪取されないよう、厳密な管理を行うよう心掛けてください。

GIGAZINE

2022年12月02日 07時00分　セキュリティ
MicrosoftとMozillaがアメリカ諜報機関との関係が報じられたルート認証局「TrustCor」の証明書を信頼しないことを決定

ブラウザは通信の安全性を確認ためにデジタル証明書を利用しており、その根幹をなすルート証明書を発行しているのが、上位の認証局による認証を受けず正当性を自ら証明できるルート認証局です。そんなルート認証局の1つである「TrustCor」が、アメリカの諜報機関や法執行機関とのつながりがあることが指摘され、Firefoxを開発するMozillaとEdgeを開発するMicrosoftが、TrustCorからの新たな証明書を信頼しないことに決定したと報じられました。

concerns about Trustcor
https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/oxX69KFvsm4/m/WJXUELicBQAJ

Mozilla, Microsoft yank TrustCor's root certificate authority after U.S. contractor revelations - The Washington Post
https://www.washingtonpost.com/technology/2022/11/30/trustcor-internet-authority-mozilla/