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。

●日本法人サイトの移転でドメイン名失効、第三者取得で偽サイト立ち上げ

https://www.itmedia.co.jp/news/articles/2407/09/news103.html
https://news.sap.com/japan/?p=17521

このニュースをザックリ言うと･･･

- 7月3日(日本時間)、大手ソフトウェア企業SAP社の日本法人SAPジャパン社より、同社のサイトに使用していたドメイン名「sapjp. com」が第三者に取得され、なりすましサイトに悪用されているとして注意喚起が出されています。

- Google等サーチエンジンで「SAPジャパン」等を検索した結果に上記ドメイン名のサイトが含まれるケースが確認されており、同社では、クリックにより不審なサイトへ誘導されたり、マルウェア等がダウンロードされたりして、思わぬ被害が発生する可能性があるとしています。

- 現在の同社サイトのURLは「https://www.sap.com/japan/ 」「https://news.sap.com/japan/ 」等であり、なりすましサイトに関しては関係各所に削除対応等の申し入れを行っているとし、sapjp. comのサイトにはアクセスしないよう呼び掛けています。

AUS便りからの所感等

- sapjp. comは6月頃までに一旦失効し、現在は登録者やWebサーバーがロシア関連のものとなっていますが、失効前にあった本物のサイトのコンテンツを複製してなりすましを行っており、これによりサーチエンジンの上位に表示されている模様です。

- 2024年前半の半年程度、sapjp. com から現サイトへのリダイレクト措置がとられていた模様ですが、ドメイン名の失効までには明らかに期間が短く、いわゆる「ドメインドロップキャッチ」による悪用には格好のターゲットであったと考えられます。

- ドメインドロップキャッチの対策として、使用しなくなったドメイン名はサイト移転やサービス終了等の後も10年程度は保持することが推奨されます。

- 広告ブロック等を行うWebブラウザー向け拡張「uBlock Origin」ではsapjp. comへのアクセスに警告を出すようになっており、このような拡張機能やブラウザー自体・アンチウイルス・UTMによるサイトブロック機能を有効にし、可能な限りリスクのあるWebサイトへのアクセスを回避するよう心掛けましょう。

ITmedia NEWS

SAPジャパンの偽サイト「sapjp.com」に注意　過去に保有していたドメインを第三者が取得、なりすまし被害に

2024年07月09日 10時23分 公開　[ITmedia]

SAPジャパンは、同社が以前保有していたサイトが第三者企業によって取得され、なりすましサイト化している事例を確認したと発表した。「sapjp.com」というドメインのサイトは偽サイトだとして、アクセスしないよう注意を呼び掛けてる文書を、7月3日付で公表した。

SAPジャパン公式サイトのURLは「https://www.sap.com/japan/」、ニュースセンターは「https://news.sap.com/japan/」。このドメイン以外で同社のコンテンツを掲載しているサイトは、無断転載によるなりすましサイトという。

この度、弊社が以前保有していたサイトが第三者企業によって取得され、なりすましサイトとしてインターネット上で表示される事例が確認されました。当該サイトには、弊社の著作物が無断で掲載されており、著作権侵害の状態にあります。これらのサイトと弊社は一切関係がございません。

偽サイトの具体事例

現在、GoogleやYahoo等の検索エンジンにて弊社に関連したキーワードで検索をした場合、検索結果になりすましサイトが表示され、クリックすると不審なサイトへ誘導される可能性や、気付かぬうちにお使いのパソコン等に有害なソフトウェア等がダウンロー

●「史上最大のパスワード漏洩」か…100億件のパスワード情報がハッキングフォーラムに投稿

https://gigazine.net/news/20240708-10-billion-passwords-leak-rockyou2024/
https://cybernews.com/security/rockyou2024-largest-password-compilation-leak/

このニュースをザックリ言うと・・・

- 7月4日(現地時間)、リトアニアのセキュリティニュースメディアCyberNewsより、9,948,575,739件に上るパスワード情報からなるテキストファイルがハッキングフォーラムに投稿されたと報じられました。

- テキストファイルが「rockyou2024.txt」というファイル名であることから、CyberNewsでは今回の事案を「RockYou2024」と呼称しています。

- 2021年に約84億件の流出パスワードが投稿された「rockyou2021.txt」があり、「rockyou2024.txt」はこれに約15億件の追加を行った更新版である可能性が指摘されています。

- Cybernewsでは、攻撃者がこのファイルを利用したブルートフォース攻撃を行う可能性があるとして、「漏洩に関係したアカウントについてパスワードリセットを行い、強固で他のサービスと共有していないパスワードを設定する」「可能な限り多要素認証(MFA)を利用する」「パスワードマネージャーソフトによるパスワード生成・管理を行う」ことを推奨しています。

AUS便りからの所感

- Cybernewsでは、RockYou2024で流出したパスワードかどうか確認するためのWebサイトも用意していますが、入力したパスワードがサーバーに送信される仕様となっている点には注意が必要です(同様のサイトである「Have I Been Pwned」ではパスワードのハッシュ値を生成して照合する方法をとっており多少安全ですが、現時点でRockYou2024のデータが追加されているかは未確認です)。

- 近年はリモートデスクトップやSSHさらにはVPNに対する不正ログインも情報漏洩のみならずマルウェア感染等重大な問題のきっかけとなるケースが多発しており、MFAの利用が推奨されているのと同様、クライアント証明書等による認証が備わっているものについては、パスワードのみの認証とせず必ずこれを使用してください。

GIGAZINE

2024年07月08日 11時31分　セキュリティ

100億件ものパスワード情報がインターネット上で流出、「史上最大のパスワード漏えい」との指摘も

2024年7月4日、ハッキングフォーラム上に約100億件ものパスワード情報を含むファイルが投稿されました。セキュリティメディアのCybernewsは「史上最大のパスワード漏えい」として、今回のデータ漏えいについて報じています。

RockYou2024: 10 billion passwords leaked in the largest compilation of all time | Cybernews
https://cybernews.com/security/rockyou2024-largest-password-compilation-leak/

ハッキングフォーラム上に「rockyou2024.txt」というテキストファイルが投稿され、このテキストファイルの中身を調査したCybernewsの研究者により、ファイルには99億4857万5739件もの固有のパスワード情報が含まれていることが明らかになりました。なお、「rockyou2024.txt」を投稿したのは、2024年5月下旬にアカウント登録した、「ObamaCare」というユーザーです。

● Microsoft月例のセキュリティアップデートリリース、Win11 22H2サポートは10月まで

https://forest.watch.impress.co.jp/docs/news/1607079.html
https://msrc.microsoft.com/blog/2024/07/202407-security-update/
https://forest.watch.impress.co.jp/docs/news/1606718.html

このニュースをザックリ言うと・・・

- 7月10日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対する月例のセキュリティアップデートがリリースされています。

- Windowsの最新バージョンはWindows 10 22H2 KB5040427(ビルド 19045.4651)および11 23H2 KB5040442(ビルド 22631.3880)となります。

- なお、Windows 11 22H2については、3か月後となる10月9日の月例アップデートでサポートが打ち切られるため、23H2へバージョンアップするよう呼び掛けられています。

AUS便りからの所感

- MSから今回発表された脆弱性では、SharePoint ServerやリモートデスクトップライセンスサービスPC等に関する計5件が最も深刻なものとされており、これ以外ではHyper-VとMSHTMLの脆弱性について既に悪用が確認されているとしています。

- 日本時間での第2水曜日(1日が水曜日の場合は第3水曜日)はMSをはじめとする各社からのセキュリティアップデート発表が集中、また来週7月17日にはOracleからもJavaやMySQL等に対する4半期毎のセキュリティアップデートがリリースされます。

- 運用している各種プロダクトについて定期的なアップデートのスケジュールが定まっているものについては把握しておき、OSや機器のファームウェアあるいは各種アプリケーションに至るまで確実にバージョンアップないしアップデートの適用を行うことが根本的な対策であり、併せてそれまでに発生する攻撃に対してもアンチウイルス・UTM等によって防御を固めることも重要です。

Impress Watch

2024年7月の「Windows Update」がリリース、「Copilot in Windows」が単体アプリに

「Critical」5件、ゼロデイ2件を含む139件の脆弱性に対処

樽井 秀人　2024年7月10日 09:10

2024年7月のセキュリティ更新プログラム

米Microsoftは7月9日（現地時間）、すべてのサポート中バージョンのWindowsに対し月例のセキュリティ更新プログラムをリリースした（パッチチューズデー）。現在、「Windows Update」や「Windows Update カタログ」などから入手可能。Windows以外の製品も含め、今月のパッチではCVE番号ベースで139件の脆弱性が新たに対処されている。