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。

●日本人ユーザーからの漏洩パスワード、頻出は「123456」「password」「qwerty」等

https://www.sankei.com/article/20241105-3KGXN4X5EBEKNPAUC3NFCAWG4M/
https://www.soliton.co.jp/news/2024/006192.html

このニュースをザックリ言うと･･･

- 10月30日(現地時間)、ソリトンシステムズ社より、「日本人のパスワードランキング2024最新版」が発表されました。

- 2024年1月～8月に発生した国内外276件の情報漏洩事案において日本人ユーザー(メールアドレスが.jpドメインのもの)が設定していたとみられるパスワードを分析した結果を示しています。

- 最も頻繁に使用されていたパスワードは「123456」で、以下5位まで「password」「123123」「qwerty」「111111」となっています。

- ソリトン社によるランキングの発表は2022年2月以来2年半ぶりで、またパスワード管理ツール「NordPass」等を提供するNord Security社が発表している同様のランキング(2023年版)も紹介されています。

AUS便りからの所感等

- 他のパスワード管理ツールの開発元やセキュリティ企業・機関からも発表されているランキングも含め、上位に入るパスワードに長年共通する傾向は「数字の羅列」「password・iloveyou等簡単な単語やフレーズ(および数字を足しただけのもの)」「キーボード上で並んでいる文字列」等となっています。

- また、NordPassによるランキングでは「ユーザー本人の名前」「趣味に関連した単語(アイドル・サッカーチーム等)」が多く用いられるという分析結果も出ています。

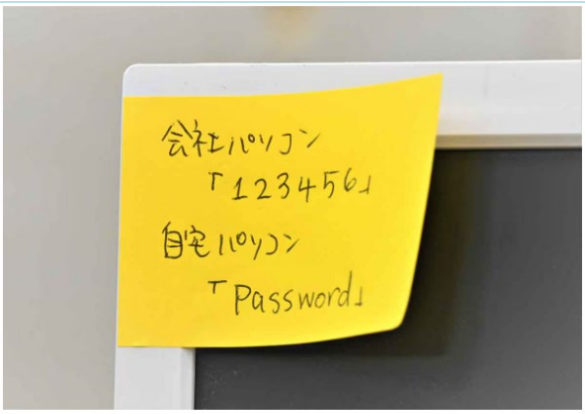
- ランキングに載っている、あるいは上記のパターンに合致するようなパスワードは、攻撃者がアカウント奪取のため真っ先に試す可能性が高いことから、Webやそれ以外のサービスで実際に使っていないか確認し、より推測されにくく比較的長い(例えばNordPassでは20文字を推奨しています)パスワードを各サービス毎に使い回すことなく設定し、所有する全てのアカウントの保護に努めることが肝要です。

産経新聞 THE SANKEI NEWS

漏洩パスワード、最も多い文字列は「123456」　配列なぞった「qwerty」も4位

2024/11/5 17:24

奥原 慎平　経済 | IT



「123456」「password」など簡単なパスワードは漏洩のリスクが高い

情報通信会社「ソリトンシステムズ」は日本人ユーザーによるとみられるパスワードの漏洩（ろうえい）実態を調査し、最も多かった「123456」、2位は「password」、3位は「123123」だったと公表した。同社は「誰でも推測できるパスワードは機能として安全ではない。簡単なパスワードを設定できないようにしてほしい」と改めて訴えている。

●マイニングマルウェアによる負荷でサービス停止…脆弱性を突かれた可能性も

https://www.nikkei.com/article/DGXZQOUC298QS0Z21C24A0000000/
https://corporate.demae-can.co.jp/pr/news/20241029_1830.html

このニュースをザックリ言うと･･･

－10月29日(日本時間)、デリバリーサービス「出前館」より、システムがマルウェアに感染し、同26日以降サービスを一時停止していたと発表されました。

－発表では、感染したのは暗号資産(仮想通貨)のマイニングを行うマルウェア「RedTail」とされ、これによりサーバーに高負荷が発生したことが原因としています。

－10月25日に一部のサーバーで高負荷が確認されたことから一旦サービスを停止、当該サーバーをネットワークから切り離して再開したものの、翌26日に別のサーバーで同様の事象が発生したため、再度サービスを停止した際にマルウェアの感染を確認したとしており、安全性の確認の上で同29日から再開しています。

AUS便りからの所感

－現時点で情報漏洩はないとはいえ、高負荷の発生により、サービスの停止に至ったということで、「可用性」の毀損という意味でのセキュリティインシデントとなります。

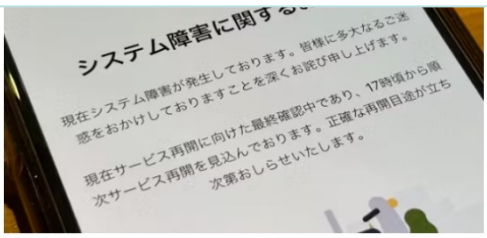
－RedTailは、ApacheやPHPあるいはメーカー製アプライアンス等の複数の脆弱性を悪用してサーバーに感染するとされ、うちPHPの脆弱性「CVE-2024-4577」(Windows版のみ影響)については7月にこれを狙う攻撃に関する注意喚起がIPAから出されていました(https://www.ipa.go.jp/security/security-alert/2024/alert_20240705.html)。

－今回の件で特定の脆弱性が原因となったという発表はされていませんが、複数台のサーバー構成のうち、1台でも未対策の脆弱性を突かれマルウェアに侵入されれば、他のサーバーにも瞬く間に感染を広げる恐れがあるため、全てのサーバーについてOSから各種ソフトウェアまで随時最新バージョンに保ち、またサーバー間での横展開による侵入等を防ぐようなネットワーク構成とすることが重要です。

日本経済新聞

出前館、マルウエア感染で3日間停止　「情報流出はなし」

専門店・EC　＋フォローする
2024年10月29日 19:18



一時サービスが利用できない状態だった（出前館のスマホアプリ画面）

出前館は29日、マルウエア（悪意あるプログラム）に感染し、料理宅配サービスを一時停止していたことを明らかにした。注文などを管理するサーバーに高負荷がかかったことから26日午後にサービスを停止した。マルウエアを削除しセキュリティーを高めたうえで、29日午後に再開した。「顧客情報の流出はない」（同社）という。

● Chromeブラウザーに脆弱性…アップデートは毎週水曜日に確認を

https://forest.watch.impress.co.jp/docs/news/1637044.html
https://chromereleases.googleblog.com/2024/11/stable-channel-update-for-desktop.html

このニュースをザックリ言うと･･･

－11月6日(日本時間)、Google Chromeブラウザーのセキュリティアップデート(v130.0.6723.116/.117)がリリースされました。

－2件の深刻な脆弱性が修正されており、悪用の報告はないものの、メモリ破壊・悪意あるコードの実行等に繋がる恐れがあるとされています。

－Chromeブラウザーは自動更新に対応しており、また「ヘルプ」→「Google Chromeについて」(あるいはchrome://settings/help)でバージョン情報が確認できるとともに、手動でアップデートが可能です(更新の完了にはブラウザーの再起動が必要です)。

AUS便りからの所感

－Chromeブラウザーでは7月以降、毎週水曜日(日本時間)にセキュリティアップデートのリリースが続いています。

－ブラウザーを開いたまま、かつ「Google Chromeについて」をしばらく開いていない場合、更新・再起動を促すメッセージが表示されますが、アップデートのリリースから数日のタイムラグを置いて表示されることがあり、その間に脆弱性を悪用される可能性も考えられることから、できる限り毎日バージョンを確認し、最新バージョンに保つよう心掛けるべきでしょう(日々ブラウザーを完全に終了させる使い方であれば最新バージョンとなっていると思われますが、安全のため確認するに越したことはありません)。

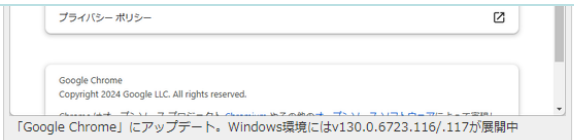
－またブラウザーのバージョンが古く、更新されるまでの間に攻撃を受けることを避けられるよう、アンチウイルス・UTM等による防御も確実に行いましょう。

Impress Watch

「Google Chrome」にセキュリティアップデート、UAF脆弱性を2件修正

Windows環境には修正版のv130.0.6723.116/.117が展開中

樽井 秀人　2024年11月6日 07:53



「Google Chrome」にアップデート。Windows環境にはv130.0.6723.116/.117が展開中

米Googleは11月5日（現地時間）、デスクトップ向け「Google Chrome」の安定（Stable）チャネルをアップデートした。現在、Windows/Mac環境にv130.0.6723.116/.117、Linux環境にv130.0.6723.116が展開中。Windows/Mac向けの拡張安定チャネルもv130.0.6723.117へとアップデートされる。

窓の杜からダウンロード