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。

●電話注文時の注文書・メモ画像、ランサムウェアが暗号化…クレジットカード情報流出か

https://cybersecurity-jp.com/news/81275
https://www.nihonsakari.co.jp/news/p/356
https://www.nihonsakari.co.jp/news/p/341

このニュースをザックリ言うと･･･

- 3月30日(日本時間)、酒造メーカーの日本盛株式会社より、同社サーバーが不正アクセスを受け、一部ユーザーのクレジットカード情報等が流出した可能性があると発表されました。

- 被害を受けたとされるのは、電話による通信販売で2016年10月6日～2022年9月16日に注文を行った利用車の一部にあたる23人分のクレジットカード情報(番号・有効期限・氏名)とされています。

- 不正アクセスは2022年9月16日に発生し、ランサムウェアによって暗号化された画像データの中にカード情報が記載されていたことが確認され、流出の可能性ありとして今回の発表となった模様です。

- 同社はECサイトも運営していましたが、クレジットカード情報を保持しない設定となっていたこと、またこちらに対する不正アクセスの痕跡がなかったことから、ECサイトからのカード情報流出はなかったとされています。

AUS便りからの所感等

- 同社からの第一報は不正アクセス発生直後の2022年9月20日で、次いで10月25日の続報において、VPN装置の脆弱性を突いての侵入とランサムウェアによる暗号化があったことが発表されていましたが、今回注文書やカード情報のメモの画像情報が暗号化の被害を受けたことが明らかになっています。

- ECサイトでの被害がなかった一方、電話による通信販売において「カード情報が記載されたデータファイルについてはサーバーには保存しない」というルールが遵守されなかったことが情報流出の可能性に繋がっています。

- PCからサーバー・ネットワーク機器までセキュリティアップデートを確実に行うことはもちろん、くれぐれも「内部ネットワークに侵入されなければ大丈夫」等と油断することなく、流出時に問題となるような情報や一時的なデータファイルが用済みになった後も誰にも意識されずPCやサーバーに保存されてしまう等のないよう、適切に管理・破棄する為のルールを徹底することが肝要です。

Cyber Security.com

日本盛がランサムウェア感染の続報発表、23名のカード情報流出か

画像：日本盛株式会社より引用

日本盛株式会社は2023年3月30日、同社がランサムウェアに感染した問題について、暗号化されたデータのなかに通信販売で同社に注文したユーザー23名のクレジットカード情報が流出した可能性がある旨、続報を発表しました。

日本盛株式会社は2022年9月20日、同社が管理運用する複数のサーバーがランサムウェアに感染し、内部データが暗号化されるなどの被害が生じ、電話注文およびECサイトを停止したと明かしていました。今回の続報は同社が実施した外部調査機関に調査結果を踏まえたもので、攻撃者は同社のVPN機器の脆弱性を利用して不正アクセスを仕掛けたことや、暗号化被害を受けたデータのなかに通信販売（電話）により購入した一部ユーザ

●3月度フィッシング報告件数は77,056件、昨年の水準に回復

https://www.antiphishing.jp/report/monthly/202303.html

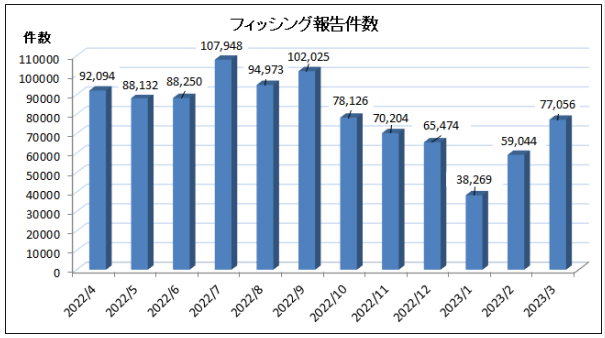
このニュースをザックリ言うと･･･

- 4月6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77,056件で、2月度(https://www.antiphishing.jp/report/monthly/202302.html)の59,044件から18,012件増加しています。
- フィッシングサイトのURL件数は14,343件で2月度(9,994件)から4,349件増加、フィッシングに悪用されたブランド数は110件で2月度(89件)から21件増加となっています。
- Amazonを騙るフィッシングは全体の約22.1%と割合の減少傾向が続き(2月度28.0%)、以下三井住友信託銀行・三井住友銀行・えきねっと・イオンカードを騙るものと合わせて全体の約58.0%を占めたとのことです。
- 同協議会の調査用メールアドレスへ配信されたフィッシングメールの約74.6%が中国の通信事業者からの配信とされる一方、日本国内の通信業者からの配信も約19.9%を占めているとのことです。

AUS便りからの所感

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

- 2023年1～2月度における同協議会の分析のとおり、1月度に38,269件まで落ち込んだのは旧正月だったことによるようで、2ヶ月でその倍にまで回復し、2022年10～12月度の水準に戻っています。
- 同協議会からは3月末にマイナポイント事務局を騙るフィッシングの注意喚起が(AUS便り 2023/04/04号)、また4月上旬だけでも住信SBIネット銀行・厚生労働省・総務省・三菱UFJ信託銀行等のフィッシングについての注意喚起が出ています。
- ユーザーPCのアンチウイルスやUTMによるアンチフィッシング機能に加え、自組織のメールサーバーにおいてもSPFやDMARCによるメールのなりすましチェックを行うとともに、中小零細企業であってもEmotet等による取引相手へのなりすましメール送信等が行われる恐れがあることを鑑み、自社ドメインにSPF・DMARCレコードの設定と適切な運用を行うよう心掛けましょう。



●よく使用されるパスワードの半数がAIで1分以内にクラック…米セキュリティ企業発表

https://pc.watch.impress.co.jp/docs/news/1492292.html
https://japan.zdnet.com/article/35202432/
https://www.homesecurityheroes.com/ai-password-cracking/

このニュースをザックリ言うと･･･

- 4月7日(現地時間)、セキュリティ企業の米Home Security Heroes社より、AIを用いてのパスワードのクラックに関する調査結果が発表されました。
- AIツール「PassGAN」に対し、実際に流出したパスワードを学習させ、よく使われるとされる約1,568万通りのパスワードのクラックを試したところ、そのうち51%が1分以内で推測されるとの結果が出ています(また、1時間以内で65%を、1日以内で71%を、1ヶ月以内で81%を推測できたとしています)。
- 同社では安全なパスワードの要件として「アルファベット大文字・小文字・数字・記号を組み合わせる」「15文字以上」等を挙げており、「パスワードを使い回さない」ことも推奨しています。

AUS便りからの所感

Impress Watch

- この他、アルファベット大文字・小文字・数字・記号を組み合わせたパスワードでも8文字であれば7時間、7文字なら6分、6文字ならわずか4秒で推測される、また数字だけのパスワードは18文字でも10ヶ月で推測される、等の結果が出ています。
- 今やパスワード管理ツールによるパスワードの生成ないし保存も広く行われるようになっており、それゆえそこで生成する際は記号までを含めた十分に長いものを選ぶべきであり、またWebサービス等を提供する側もそれを受け入れるようなパスワードポリシーとすることが重要です。
- 同社は前述した推奨事項の他に「定期的なパスワードの変更」も推奨していますが、変更はパスワードやハッシュデータが流出した場合に行うべきであり、むしろそれらの流出をどれだけ速やかに感知して変更等の対応ができるかも大事でしょう。

AIによるパスワードの解析時間をセキュリティ会社が公開。8桁なら7時間以内に解析完了

関根 慎一　2023年4月10日 14:54

米国のセキュリティ企業Home Security Heroesは、AIを用いたパスワードのクラックにかかる時間についての調査結果を発表した。

調査ではAIによるパスワードの生成/解析ツールとして「PassGAN」を例に挙げ、実際に漏洩したパスワードリストを学習/解析させたうえで1,568万個のパスワードを評価した結果、「一般的なパスワード」のうち51%を1分以内、65%を1時間以内、71%を1日以内、81%を1カ月以内に推測できたとしている。