— AUS（アルテミス・ユーザ・サポート）便り 2019/09/17号 —
https://www.artemis-jp.com

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。

●Facebookユーザー4億1,900万件超の電話番号流出か… 公開状態のデータベース発見

https://www.itmedia.co.jp/news/articles/1909/05/news075.html

https://gigazine.net/news/20190905-facebook-phone-number-database/

https://jp.techcrunch.com/2019/09/05/2019-09-04-facebook-phone-numbers-exposed/

このニュースをザックリ言うと･･･

- 9月4日(現地時間)、米国のネットメディアTechCrunchより、Facebookユーザー4億1,900万件以上のID(Facebook ID)とそれに紐付いた電話番号のデータが公開状態にあったと報じられました。
- オランダのセキュリティ研究者が所有者不明のデータベースを発見したことにより発覚したもので、8月末にアップロードされたものとみられており、連絡を受けたTechCrunchがWebホストに問合せた後にデータベースにはアクセスできなくなった模様です。
- Facebookからは2016年以降ユーザー情報の流出が相次いで発生しており、最近の例としては、4月に約5億4,000万件のアカウント情報を収集していたサードパーティー(外部企業)のデータベースが公開状態にあったことが発覚したケースが挙げられます(AUS便り 2019/4/15号参照)。

AUS便りからの所感等

- Facebookによれば、データは2018年4月に携帯電話番号でユーザーを検索する機能を終了した時点のものとのことで、またその多くは重複しており、実際の件数は約半分と主張しています。
- 記事に掲載されたデータのスクリーンショットを見る限り、Facebook ID(ユーザーを識別する数字)と電話番号の他には、ログイン時のメールアドレスやパスワードは含まれていないとみられる一方、誕生日・性別・住所(空欄もあり)およびユーザー名(いわゆるページID)が含まれていた模様で、例えばパスワードリセット機能を悪用することにより、メールアドレスの一部を割り出すこと等が可能とされています。
- 個人情報を含むデータベースを保存する場所が、たとえクラウド上であろうと社内のサーバー(オンプレミス)であろうと、どちらかがより安全であると確実に言えるものではなく、アクセス制限やデータベース自体のパスワード等による保護は両方のケースで必要不可欠ですし、それ以外にもそれぞれのケースで必要な対策を十分に洗い出し、確実に実行することが肝要です。

●警察を騙る詐欺サイトに注意喚起…2017年にも日本向けサイト確認

https://blog.trendmicro.co.jp/archives/22425

このニュースをザックリ言うと・・・

- 9月11日(日本時間)、トレンドマイクロ社より、警察などの法執行機関や政府機関を騙り「罰金」を要求するというランサムウェアがとる手口の一つ「ポリスランサム」を真似た詐欺サイトが海外で活発化しているとして注意喚起が出されています。
- 同社によれば、現時点でカタール内務省版とフランス警察版の詐欺サイトを確認しており、いずれも共通したデザインで、クレジットカード情報を詐取するものとなっている模様です。
- 同社では2017年にも、警察庁を騙る日本語のサイトが確認されたこともあり、注意喚起を行っていましたが、今回そのときと共通した手口がみられ、日本語のサイトも再び登場することが予測されることから、改めて注意喚起を出したとしています。

AUS便りからの所感等

- 2017年に確認された詐欺サイトと共通した特徴として、サイトアクセス時にサイレンを鳴らす、ブラウザーのウィンドウを全画面表示させた上で、ウィンドウのボタンやWindowsのタスクバー等を画像で偽装することにより、それらをクリックしても有効でないと思い込ませる手口をとっていることが挙げられています。
- 詐欺サイトの表示を遮断するため、Webブラウザーやセキュリティソフト・UTMのアンチフィッシング機能を有効にする他に、こういった詐欺サイトに遭遇した際に慎重に行動できるよう、随時その手口に関する情報収集を行うことが重要と言えます。

●顧客情報67,000件超を記録したノートパソコンを紛失-

https://cybersecurity-jp.com/news/33305

http://www.zetton.co.jp/company/IR/docs/ir_20190906.pdf

このニュースをザックリ言うと・・・

- 9月6日(日本時間)、外食チェーン店を経営する株式会社ゼットンより、同社顧客情報が記録されている業務用ノートPCを紛失したと発表されました。
- 同社社員が8月30日に立ち寄った小売店舗で紛失したもので、同社が運営する計20店舗で2017年12月～2019年8月(一部期間)に予約をした利用者最大67,280件の氏名・企業名、電話番号およびメールアドレスの全部または一部が含まれているとのことです。
- 発表の時点で当該PCは発見されていないものの、遠隔操作によりパスワードを複雑なものに変更、かつ社内ネットワークへのアクセスを遮断する措置をとったとしています。

AUS便りからの所感等

- 同社がとったとする措置が攻撃者に破られる可能性がどれほどあるかは不明ですが、インシデント発生後の個人情報流出を可能な限り阻止する体制が整っていたことは一定の評価ができるものと思われます。
- ノートPC等の紛失・盗難に対し遠隔で対応するソリューションとしては、他にもHDD/SSDを消去するもの等が存在しており、万が一に備え導入を検討することは大切である一方、個人情報を随時(クラウド上あるいはVPNで接続した社内ネットワーク上の)サーバーから参照し、可能な限りPC上に残さない形をとることもまた一考に値するでしょう。