

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。



Facebookユーザーの電話番号が掲載された大量データベースが流出

流出したデータベースには、米国ユーザー1億3,000万人、英国ユーザー1,000万人、ベトナムユーザー5,000万人の電話番号が含まれており、世界中のユーザーに関する最も大規模なデータベースと見られています。このデータベースはパスワードで保護されていたため、誰でもデータベースを閲覧してアクセスできませんでした。各記録にはユーザーのFacebook IDやアカウントにある電話番号が掲載されている。ユーザーの

情報提供・寄稿お待ちしております!

ITmedia NEWS

TechCrunch Tokyo 2019 SPONSORS

ITmedia NEWS



Facebookの4億人以上のユーザーIDと携帯番号を何者かがアップロード (削除済み)

© 2019年09月05日 11時01分 公開

[佐藤由紀子, ITmedia]

印刷 484 Share 30

人手不足の解消とコスト削減! ロボットの活用事例

米Facebookの4億人以上のユーザーFacebook IDとそれに紐付いた電話番号のデータが、パスワードのかかっていないデータベースに保存されていたと、米TechCrunchが9月4日(現地時間)、これを発見したセキュリティ研究者からの連絡に基づいて報じた。

オランダのセキュリティ企業GDI Foundationの研究者、サンヤム・ジャイナ氏が、オーナー不明のデータベースを見つけ、TechCrunchに連絡した。TechCrunchがWebホストに問い合わせたところ、データベースに接続できなくなったという。

TechCrunchは、分かっているFacebookユーザーの携帯番号をリスト内のFacebook IDと照合することで、このデータベース内のデータを多数検証した。中にはユーザー名、性別、在住する国まで分かるデータがあった。データベースに含まれていたのは、米国、英国、ベトナムのユーザーデータだった。

TechCrunchの問い合わせに対し、Facebookは「このデータセットは古いものであり、昨年4月に携帯番号でユーザーを検索する機能を終了した前のデータのようだ。データセットは既に削除されており、Facebookアカウントが侵害された証拠は確認されていない」と語った。

●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した。
- 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。



顧客情報6万7千件超を記録したノートパソコンを紛失 | 株式会社ゼットン

2019.09.10 2019.09.10

ノートパソコン遺失による個人情報漏洩の可能性に関するお詫びとお知らせ

この度、当社員が、業務用ノートパソコン1台を遺失する事故が発生いたしました。遺失した当該端末には、当社が運営する店舗にご予約をいただくお客様の個人情報(氏名・住所・電話番号・メールアドレス)が記録されており、また、当該端末には、当社が運営する店舗の予約システムに関する情報が記録されています。このように、お客様の個人情報を扱う業務において、個人情報を適切に管理することが求められており、今回の事故は、当社のセキュリティ体制の強化に努めています。本件に関する経緯及び対応につきまして、以下のとおりご報告申し上げます。なお、本件に関して第三者への個人情報の流出、不正利用の事実を確認されておりません。

紛失後に遠隔操作でセキュリティ対策

ノートパソコンは2019年8月30日に紛失され、発見に至っていません。同社は紛失が明らかになった後、遠隔操作でノートパソコンのパスワードを複雑なものに変更、さらに社内ネットワークへのアクセスを遮断するなど、可能な限り個人情報漏洩のリスクを低減する措置を講じています。

同社はインシデント発生を受け、今後個人情報漏洩の防止や従業員教育などを進めると発表。再発防止に向けた対策を実施すると考えます。

- ・ 同社運営店舗の予約システムに関する情報の記録が完了した状態
- ・ 紛失された端末の記録が完了した状態

2017年12月～2019年8月

2018年12月～2019年8月

2019年8月

最大67,280件

氏名・企業名、電話番号、メールアドレスの全部または一部

インターネット上の個人情報は個人情報漏洩のリスクを低減する措置を講じています