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。

●モバイルキャリアへの「リスト型攻撃」で回線不正契約…中高生逮捕

https://www.yomiuri.co.jp/national/20250226-OYT1T50205/
https://www.asahi.com/articles/AST2W3PLJT2WUEFT00KM.html
https://network.mobile.rakuten.co.jp/information/news/other/3300/
https://piyolog.hatenadiary.jp/entry/2025/02/28/050112

このニュースをザックリ言うと･･･

- 2月27日(日本時間)、警視庁より、「楽天モバイル」の回線を不正に契約した容疑で中学～高校生3人を逮捕したと発表されました。
- 容疑者達は2023年12月以降、いわゆる「リスト型攻撃」によって楽天モバイルのサイトに不正ログイン、少なくとも約2,500回線を不正に契約し、売却によって計750万円分の暗号資産(仮想通貨)を得たとされています。
- リスト型攻撃にはメッセージアプリ「Telegram」上で購入した約33億件のID・パスワードのリストを用い、また不正契約を行うプログラムは生成AIによって作ったとしています。
- 同日には楽天モバイルからも発表があり、身に覚えのない回線登録に注意するよう呼び掛けられています。

AUS便りからの所感等

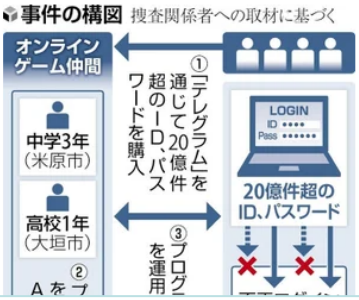
- 発表を受けての新聞等各社の報道は、攻撃ツールの開発における生成AIの使用に注目が集まっている一方、攻撃自体は従来のリスト型攻撃の大規模な事例と言えます。
- リスト型攻撃はユーザーに対し推奨されるパスワード設定の考え方を大きくシフトさせるきっかけとなりましたが、他のサービスで流出したものと同じID・パスワードをユーザーが使用することを完全にやめさせるのは不可能であり、多要素認証やパスキー等、ID・パスワードのみに依存しないログイン手順の採用も急務とされます。
- 楽天モバイルは1つのIDで最大15回線を契約可能、かつ追加契約には本人確認不要という仕様に攻撃者が目を付けたとされ、このような大手サービス、こと携帯電話回線の発行を行う事業者においては、前述した多要素認証等の採用、不正ログインの試行へのより厳格な対応、ユーザー自身へのログイン通知等によるユーザーの積極的な保護が肝要でしょう。

読賣新聞オンライン

生成ＡＩ悪用し楽天モバイルに不正アクセス、１０００件以上の回線入手し転売か…容疑で中高生３人逮捕

2025/02/27 05:00 #生成ＡＩ #ＣｈａｔＧＰＴ 保存して後で読む

携帯大手「楽天モバイル」のシステムに自作プログラムで不正ログインし、通信回線を契約したとして、警視庁が１４～１６歳の中高生３人を不正アクセス禁止法違反と電子計算機使用詐欺の疑いで逮捕したことがわかった。対話型生成ＡＩ（人工知能）サービス「チャットＧＰＴ」で作業の効率化や処理速度の向上を図っており、ＳＮＳで購入した２０億件超の情報を基にログインを試み、入手した回線を転売していたという。



未成年者による生成ＡＩを悪用した大規模な不正アクセス事件は、極めて異例だ。

逮捕されたのは、滋賀県米原市の中学３年（１５）、岐阜県大垣市の高校１年（１６）、東京都立川市の中学３年（１４）の男子生徒。調べに、一人の生徒は「２０２３年１２月以降、１０００件以上の回線を契約した」などと説明している。

●顧客約18,000社の情報漏洩、別のネットワーク装置から侵入か

https://www.itmedia.co.jp/news/articles/2503/05/news185.html
https://www.ntt.com/about-us/press-releases/news/article/2025/0305_2.html

このニュースをザックリ言うと･･･

- 3月5日(日本時間)、NTTコミュニケーションズ社より、同社社内システムが不正アクセスを受け、顧客情報が流出した可能性があると発表されました。

- 被害を受けたのは、同社法人向けサービスのユーザー17,891社の契約番号・顧客名(契約名)・担当者名・電話番号・メールアドレス・住所およびサービスの利用に係る情報とされています。

- 2月5日に顧客情報を保存していた装置Aへの不審なアクセスを検知、調査の結果、社内ネットワークにあった別の装置Bが外部から不正アクセスを受け、そこから装置Aにアクセスされたことが同15日に判明したとしています。

AUS便りからの所感

- 外部から侵入を受けた装置等の詳細は公表されておらず、今回のケースに該当するかは不明ですが、VPN装置が脆弱性を突かれる、あるいは推測されやすいID・パスワードを設定していたアカウントから不正ログインされる事例は頻繁に報告されており、脆弱性を塞ぐため装置のOS・ファームウェアを最新バージョンに保つこと、また全てのアカウントに強力なパスワードを設定することが重要です。

- またサーバーへの不正アクセス時は、VPN装置を踏み台とするだけでなく、各クライアントPCへマルウェアを感染させるケースも決して珍しくなく、その観点からもアンチウイルス等による防御の強化もまた決して疎かにしてはいけないでしょう。

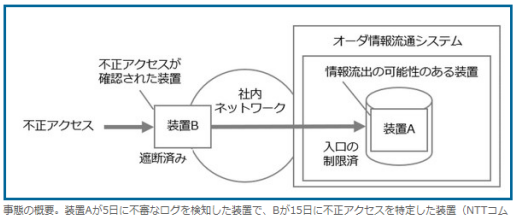
ITmedia NEWS

NTTコム、顧客約1万8000社の情報漏えいか　社内システムに不正アクセス

2025年03月05日 17時28分 公開　[ITmedia]

NTTコミュニケーションズは3月5日、社内システムに不正アクセスを受け、法人向けサービスのユーザー1万7891社の情報が漏えいした可能性があると発表した。

ユーザー企業の契約番号、契約名、担当者名、電話番号、メールアドレス、住所、サービスの利用に関する情報が漏えいした可能性がある。対象サービスの詳細は明らかにしていない。NTTドコモが提供する法人向けスマートフォン・携帯電話サービスは対象外という。



事態の概要。装置Aが5日に不審なログを検知した装置で、Bが15日に不正アクセスを特定した装置（NTTコムの発表から引用）

● Chromeバージョン134リリース、古い拡張機能無効化へ

https://forest.watch.impress.co.jp/docs/news/1667833.html
https://forest.watch.impress.co.jp/docs/serial/yajiuma/1667861.html

このニュースをザックリ言うと･･･

- 3月5日(日本時間)、GoogleよりChromeブラウザーのメジャーアップデートとなるバージョン134(Windowsではv134.0.6998.35/36)がリリースされました。

- AI関連機能等の新機能の他、14件の脆弱性も修正されています。

- 一方で拡張機能について、新しい仕様「Manifest v3」に対応していないものが無効化され、Google公式の拡張機能ストアからの新規インストールもできなくなっている模様です。

AUS便りからの所感

- 無効化の対象とされた拡張としては恐らく「uBlock Origin(https://chromewebstore.google.com/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm)」あたりが最も著名な一つとされ、代替としては「uBlock Origin Lite(uBlock Originと同じ開発者)」や「AdGuard 広告ブロッカー」が挙げられています。

- またインプレス「やじうまの杜」では、「はてなブックマーク」の拡張が動かなくなったという日本人ユーザーからのX(旧・Twitter)での報告が取り上げられています(厳密にははてなブックマークについて新旧2種類の拡張機能が提供され、古い方が今回無効化の対象とされています)。

- インストールしていた拡張が無効にされた場合でも、拡張機能の管理画面において「この拡張機能を残す」を選択し、明示的に有効にすることは可能ですが、将来のバージョンで完全に使用できなくなる可能性があることには注意してください。

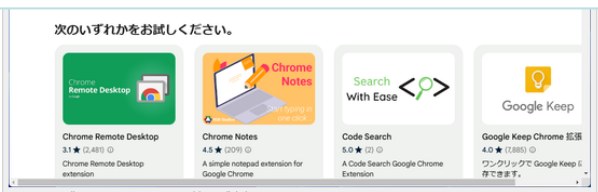
- 無効化された拡張機能の「Manifest v3に対応したバージョン」を称する偽物が公式の拡張機能ストアに登録された事例も報告されており(AUS便り 2025/01/09号参照)、ストアで検索して出てきたものを安易にインストールせず、SNSでの報告等を十分に確認することは今回に限らずあらゆる拡張機能の利用時に重要です。

Impress Watch

「はてブ」のChrome拡張機能が突如利用不能になり戸惑いの声 ～回避策（裏ワザ）あり

「拡張機能のベスト プラクティスに沿わないため、ご利用いただけなくなりました」

樽井 秀人　2025年3月6日 06:45



「はてなブックマーク」の拡張機能が突如利用できなくなる

「はてなブックマーク」（はてブ）のGoogle Chrome拡張機能が突如利用できなくなったと、一部で話題になっています。「Chrome ウェブストア」で確認してみると「この拡張機能は、Chrome 拡張機能のベスト プラクティスに沿わないため、ご利用いただけなくなりました」というメッセージとともにインストール不能となっています。