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。

●NTT西日本子会社から約900万件の個人情報流出…元派遣社員が10年間持ち出し

https://www.itmedia.co.jp/news/articles/2310/17/news121.html
https://www.nttbizsol.jp/newsrelease/20231017140000952.html

このニュースをザックリ言うと･･･

- 10月17日(日本時間)、NTT西日本グループ会社のNTTビジネスソリューションズ社(以下・BS社)およびNTTマーケティングアクトProCX社(以下・ProCX社)より、ProCX社が利用するコールセンターシステムで扱われていた顧客情報が、当該システムの運用保守業務を請け負うBS社から流出していたと発表されました。

- 被害を受けたのは、ProCX社が59のクライアントから預かっていた顧客情報約900万件(氏名・住所・電話番号等、クレジットカード情報81件含む)とされています。

- BS社で当該システムの運用保守業務を行っていた元派遣社員(既に退職)が2013年3月～2023年7月にかけて、保守作業端末に顧客情報をダウンロード、端末にUSBメモリーを接続して保存し、不正に持ち出していたとされています。

AUS便りからの所感等

- NTTグループでは3月にもNTTドコモにおいて業務委託先の元派遣社員の不正持ち出しによる個人情報最大596万件の流出が発生しており(AUS便り 2023/07/26号参照)、今回の流出においてもドコモに関連する顧客情報約72,000件が含まれていたとしています。

- 各社では、保守作業端末にて顧客情報のダウンロードや外部媒体の接続が可能となっていたことに加え、セキュリティリスクが大きいと想定される振る舞いの検知、各種ログ等の定期的なチェックができていなかったことを流出の原因とし、それぞれについて対策を行うとしています。

- BS社からの不正持ち出しが始まった翌年2014年7月にベネッセにて個人情報流出事案(被害個人情報最大3,504万件)が発覚、持ち出しの手口についても今回とほぼ共通していたもので、この時点で今回出された対策をとるべく点検を行っていれば、以後の流出は阻止できた可能性もあったと思われます。

ITmedia NEWS

派遣社員が"クライアントの顧客情報"900万件を不正持ち出し　NTT西グループ

2023年10月17日 15時18分 公開　[ITmedia]

NTT西日本グループのNTTマーケティングアクトProCX（大阪市）は10月17日、マーケティング業務を代行するためにクライアントから預かっていた顧客情報900万件が不正に持ち出されたと発表した。コールセンター用システムの運用保守を依頼していたNTTビジネスソリューションズ（同）の元派遣社員が、第三者に情報を流出させていたという。

派遣社員が"クライアントの顧客情報"900万件を不正持ち出し

少なくとも、NTTマーケティングアクトProCXがクライアント59社から預かっていた顧客情報（氏名、住所、電話番号など）が持ち出された。元派遣社員はコールセンター用システムの管理者用アカウントを悪用。データが保存されていたサーバにアクセスし、情報を持ち出したという。

●国際語ドメイン名の悪用・飾り文字を含んだURLによるなりすましフィッシングに注意喚起

https://gigazine.net/news/20231020-malvertising-attack-punycode-keepass/
https://www.malwarebytes.com/blog/threat-intelligence/2023/10/clever-malvertising-attack-uses-punycode-to-look-like-legitimate-website
https://internet.watch.impress.co.jp/docs/news/1539912.html
https://www.antiphishing.jp/news/alert/decourl_20231017.html

このニュースをザックリ言うと･･･

- 10月18日(現地時間)、セキュリティベンダーのMalwarebytes社より、Google検索の広告においてパスワード管理ツール「KeePass」のダウンロードサイトを騙るフィッシングサイトの表示が確認されたとして注意喚起が出されています。

- 公式サイトが「keepass.info」であるのに対し、1文字目が英字ではない「keepass.info」というドメイン名でサイトが用意され、KeePassのインストーラーに偽装したマルウェアをダウンロードするとのことです。

- 一方10月17日(日本時間)には、フィッシング対策協議会より、Amazon等を騙るフィッシングにおいて、URL中の英字が罫線で囲まれたような飾り文字となっている事例が確認されたとしています。

AUS便りからの所感

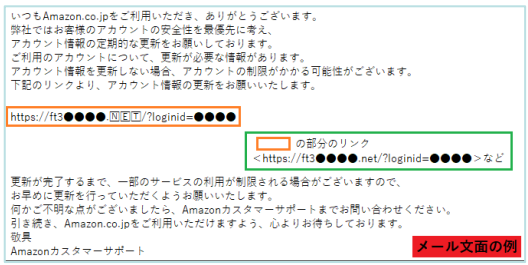
- keepassのフィッシングは、英数字以外の文字を使用する「国際化ドメイン名(IDN)」を悪用したもので、似たような事例としてGIMPの偽サイト(AUS便り2022/11/01号参照)等がGoogle検索の広告に現れるケースが報告されています。

- 飾り文字を含むURLは通常のテキストのチェックでは検出が困難な一方、ブラウザー上ではクリック時に飾り文字を削除して扱われるため、アンチウイルスやブラウザー等のアンチフィッシング機能でも同様にURLの正規化を行ってのチェックを行う必要があるでしょう。

- このようなフィッシング等の攻撃の手口があることを常に把握するよう情報収集を行い、アンチウイルス・UTMによる防御も確実に実行しつつ、メールや広告に表示されたURLを安易にクリックしない等慎重に行動することが肝要です。

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

URL に飾り文字などが含まれたフィッシング (2023/10/17)



●「Google Play プロテクト」、ストア外でインストールするAndroidアプリもスキャン実施へ

https://gigazine.net/news/20231020-real-time-scan-app-install/
https://security.googleblog.com/2023/10/enhanced-google-play-protect-real-time.html

このニュースをザックリ言うと･･･

- 10月18日(現地時間)、Googleより、Android端末を有害なアプリから保護する「Google Play プロテクト」において同社公式のGoogle Playストア以外からインストールするアプリについてもスキャンする機能を搭載すると発表されました。

- インストールしようとするアプリが未知のものだった場合、アプリをスキャンするかインストールを中断するか求められるようになり、スキャンの結果有害なものと判断された場合は中断を促す画面が表示されるとのことです。

- スキャン機能は現在インド等で展開され、数か月以内に全ての地域に拡大される予定としています。

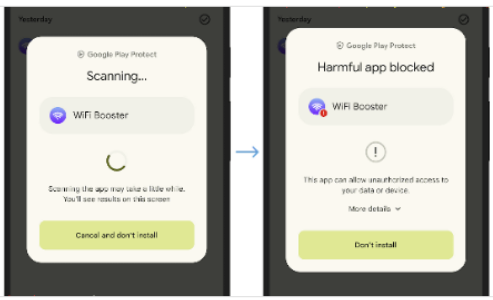
AUS便りからの所感

- Google Play プロテクトでは、これまでもWebサイト等からアプリ(apkファイル)を直接ダウンロードする場合に「既存の驚異リスト」をもとに警告を出していたものの、未知の脅威に対応できない場合があったとしています。

- スキャン機能が追加された後も、くれぐれもメール・SMSでアプリのダウンロード・インストールを誘導してくるもの等には騙されず、ソーシャルネットワーク上での評判・報告等をもとにインストールを行うことを推奨致します。

2023年10月20日 16時00分　セキュリティ

Google Play以外で配布される野良アプリのインストール時に危険性をスキャンする機能が登場



Googleが、Google Play以外の場所からAndroid用のアプリを直接ダウンロードしてインストール際に、アプリの危険性をスキャンする機能を発表しました。

GIGAZINE