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。

●宅ふぁいる便が不正アクセス被害…約480万件のアカウント・個人情報流出

http://www.itmedia.co.jp/enterprise/articles/1901/28/news084.html

このニュースをザックリ言うと･･･

- 1月26日（日本時間）、ファイル送信サービス「宅ふぁいる便」を運営するオージス総研社より、同サービスのサーバが不正アクセスを受け、登録ユーザ（退会済み含む）約480万件のアカウント情報（メールアドレスとパスワード）および個人情報が流出したと発表されました。

- 流出が確認された個人情報は、各ユーザから回答を受けた「氏名(ふりがな含む)」「生年月日」「性別」「職業」「居住地(都道府県名)」「(アカウント情報以外での)メールアドレス」、この他2012年まで収集していた情報として「居住地と勤務先の郵便番号」「配偶者・子供の有無」も含まれているとのことです。

- パスワードのハッシュ化を行っていなかったことから、同じアカウント情報を使用している他のサービスへの「リスト型攻撃」による不正ログインに利用される可能性があるとされ、同社ではユーザに対し、宅ふぁいる便で使用していたものと同じパスワードを使用していた場合は別のパスワードへの変更、また同サービスを装い「パスワードの再発行」や「口座番号の確認」等を行おうとするフィッシングに注意するよう呼びかけています。

- なお、今回被害を受けた「宅ふぁいる便」「宅ふぁいる便プレミアム」「宅ふぁいる便ビジネスプラス」は1月23日以降サービスを停止しています（2月1日現在）が、「オフィス宅ふぁいる便」はこれらとはサーバ・システム等が独立しているため影響は受けていないとのことです。

AUS便りからの所感等

- 1月17日に、多数のWebサイトから流出した約8億件に上るアカウント情報がハッキングフォーラムに掲載されていたことが発覚した（AUS便り 2019/01/28号参照）ばかりでの発生で、「日本国内」での「ユーザアカウント情報」の流出としては稀に見る規模のものとなっており、リスト型攻撃による不正ログイン被害の発生は時間の問題と思われます。

- 同社は、宅ふぁいる便がパスワードをハッシュ化して保存していなかったことを認識、対策を計画していたところに不正アクセスが発生したと証言している他、退会済みユーザの情報についても後日問合せを受ける場合があるため残していたとしています。

- パスワードをハッシュ化して保存することはシステム構築の段階で最低限行っておくべきことの一つとされていますが、Webサービスの運営者においては、速やかに同様の問題がないか確認し、パスワードのハッシュ化の対策等を実施すること、また第三者による外部・内部からのセキュリティ監査を検討することを強く推奨致します。

- またユーザ企業等の管理者においては、マルウェア等によるアカウント情報の奪取をアンチウイルスやUTMによって可能な限り防ぐようにすることはもちろんですが、安易に「こういうサービスを使っているから漏えいした」と結論付けて「今後同様のサービスの利用を禁止する」といった姿勢に出るのではなく、2段階認証等のセキュリティ機能を備えているサービス（Google DriveやDropbox等）の利用を推奨あるいは企業として登録・提供し、アカウント保護のためのセキュリティ機能の活用を啓発する方向性も視野に入れるべきでしょう。


ITmedia エンタープライズ

480万件流出の「宅ふぁいる便」不正アクセス、郵便番号など漏えい情報を新たに追加

「宅ふぁいる便」の不正アクセスについて、オージス総研が第3報を発表。新たに居住地や勤務先の郵便番号や、配偶者や子供の有無といった情報についても、漏えいが確認されたという。

2019年01月28日 14時00分 公開 [ITmedia]

印刷 426 989 B! 55

大容量ファイル送信サービス「宅ふぁいる便」の一部サーバが不正アクセスを受け、約480万件の顧客情報が流出したインシデントで、オージス総研は1月28日に第3報を公表。漏えいしたデータについて、新たに郵便番号などの情報が含まれていたと発表した。

同社が第2報までで流出したと発表していたのは、ログイン用のメールアドレスとパスワード、氏名、生年月日、性別、業種・職種、居住地（都道府県のみ）。第3報ではこれに加え、ログイン用とは別のメールアドレスのデータ（ダウンロードやファイル開封の通知先として、任意で登録）や、職業ジャンルといった情報が加わった。

●警察庁が「Mirai」とみられる攻撃とリモートデスクトップへの攻撃に注意喚起

https://www.npa.go.jp/cyberpolice/important/2019/201902011.html

このニュースをザックリ言うと・・・

- 2月1日（日本時間）、警察庁より、同庁のインターネット定点観測システムにて2018年11月以降に増加が観測されているアクセスについてのレポートが発表されています。

- 1つ目はTCPポート32764番および37215番に対するアクセスで、前者はCisco社のルータで2014年に発表された脆弱性を、後者はHuawei社製ルータで2017年に発表された脆弱性を悪用する目的のものとされ、パケットの特徴からIoTマルウェア「Mirai」の亜種によるものとみられています。

- 2つ目はWindowsのリモートデスクトップが使用するTCPポート3389番に対するアクセスで、パケット発信元PC上のリモートデスクトップにアクセス可能なものも多く確認されたとのことです。

AUS便りからの所感等


@police

32764/TCP 及び37215/TCP に対するMirai ボットの特徴を有するアクセスの増加等について

2019年2月1日
警察庁

- 32764/TCP 及び37215/TCP に対するMirai ボットの特徴を有するアクセスの増加
- リモートデスクトップサービスを標的としたアクセスの増加

詳細

32764/TCP 及び37215/TCP に対するMirai ボットの特徴を有するアクセスの増加等について(PDF形式：980KB)

- Miraiは2016年にネットワークカメラ等多数のIoT機器を乗っ取り、DDoS攻撃のためのネットワークを構築したボット型マルウェアであり、2017年に確認された「Satori」をはじめとした亜種等も未だに多く活動しています。

- 警察庁も各種攻撃への対策として挙げていますが、「OSやファームウェアを最新に保つ(自動アップデート機能があれば活用)」「機器を直接インターネットに接続せず、ルータやUTMを用いて必要最低限のポート・IPアドレスからのアクセスに限定する(VPNを用いての接続も検討)」「リモートデスクトップについてはログオン可能なユーザを制限する」「ユーザ名・パスワードは初期設定から必ず変更する」「サポートが切れた製品を使っている場合はより新しいサポート中の製品へ更新する」ことを推奨致します。

●DNS設定の改ざんによるドメイン名ハイジャックに注意喚起

https://scan.netsecurity.ne.jp/article/2019/01/30/41896.html

このニュースをザックリ言うと・・・

- 1月22日（現地時間）以降、米国政府のサイバーセキュリティに関連する複数の組織より、DNSインフラをハイジャックする攻撃が広範囲で行われているとして、対策を行うよう相次いで注意喚起が出されています。

- 攻撃は、あるサイトへアクセスしようとするユーザを偽のサーバに誘導することを目的としており、第三者のDNSサーバが偽装されている場合に問題に気がつきにくい恐れがあるとされています。

- 同28日にはJPドメインを管理するJPRS社からも同様に情報が公開されており、日本国内での同様の攻撃はまだ増加していないとしながらも、DNSの安全性と信頼性に対する重大な脅威であることを鑑み、国内全てのドメイン名登録者・DNSサービス提供者・ドメイン名登録事業者に対し、対策および設定の確認を強く推奨しています。

AUS便りからの所感等


ScanNetSecurity

脆弱性と脅威 ／ 脅威動向

DNS設定の改ざんによるドメイン名ハイジャックに注意喚起（JPRS）

JPRSは、「米国国土安全保障省によるDNS設定の改ざんに関する緊急指令の公開について」とする緊急情報を公開した。

株式会社日本レジストリサービス（JPRS）は1月28日、「米国国土安全保障省によるDNS設定の改ざんに関する緊急指令の公開について」とする緊急情報を公開した。これは1月22日、米国国土安全保障省（DHS）のサイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）が「Mitigate DNS Infrastructure Tampering（参考訳：DNSインフラストラクチャ改ざんの軽減）」という緊急指令（Emergency Directive 19-01）を公開したことを受けたもの。

シェア　ツイート

もっと「株式会社日本レジストリサービス（JPRS）」のニュース

PowerDNS RecursorにDNSSEC検証の回避など複…
PowerDNS RecursorにDoS攻撃を受ける脆弱性（J…
PowerDNS RecursorおよびAuthoritative Serverに…

編集部にメッセージを送る

- 攻撃方法としては「DNSプロバイダに設定されたAレコード(ドメイン名に対応するIPアドレス情報)」や「レジストラ(ドメイン名登録業者)経由で設定されたNSレコード(ドメインを管理するDNSサーバの情報)」を不正に書き換えること等が挙げられており、この攻撃が成功した場合、対象ドメイン名宛に送られてくるメールを詐取することや、SSL証明書を攻撃者が不正に発行すること等も可能となるでしょう。

- 2014年に国内で.comドメイン名のハイジャックがあった際にJPRSが発表した資料では、例えばドメインの登録者に対し「レジストリロックの設定の実施」や「情報の不正な書き換えに対する検知と対応」を推奨しています。

- 特に後者については、通知メールの連絡先メールアドレスとして「登録者が受け取れる有効なアドレス」「複数の担当者等が受け取れるメーリングリスト」「登録しているドメインと別のドメインのアドレス」を指定することと、届いたメールを定期的にかつ確実に確認できる体制をとることを挙げています。