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。

●マッチングアプリ会員約171万件分の個人情報、不正アクセスで流出か…免許証画像等

https://www.itmedia.co.jp/news/articles/2105/21/news135.html
https://www.net-marketing.co.jp/news/5873/

このニュースをザックリ言うと･･･

- 5月21日(日本時間)、ネットマーケティング社より、同社運営のマッチングアプリ「Omiai」のサーバーが不正アクセスを受け、会員の個人情報に関するデータ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、2018年1月31日～2021年4月20日に年齢確認審査書類を提出した会員(退会済み含む)最大1,711,756件分の年齢確認書類(運転免許証・健康保険証・パスポート・マイナンバーカードの表面等)の画像データおよびそれに記載された個人情報(氏名・住所・生年月日・顔写真・年齢確認書類毎の登録番号)とのことです(クレジットカード情報は保有していなかったため、対象外とのことです)。

- 4月28日に会員情報を管理するサーバーに対する不正アクセスの痕跡が確認され、調査の結果、同20日～26日の間にデータが複数回外部へ流出していた可能性が高いことが判明したとのことです。

AUS便りからの所感等

- 年齢確認審査のために提出された個人情報を含む画像が、審査完了後も長期間保有されていたことは、それ自体が不正アクセスと流出によるリスクを抱えていたと言え、またプライバシーポリシーにおいて「退会後も会員情報を10年間保持する」という記載があったこと等についてもネット上では指摘されています。

- 一般論とはなりますが、流出しては困るセンシティブな情報についてはできる限り最初から収集しないこと、必要に応じ収集し保有しているものについても、不要となり次第適切にサーバー上等から破棄するようルールとシステムの整備を行うこと、また不正アクセスとデータの外部への流出を食い止めるため、UTMの導入等により出口対策も含めた監視等を行うことが重要です。

- また、運転免許証の画像やそれを手に持っている自分の顔等をスマートフォンのカメラで撮影して本人確認を行う「eKYC」が近年銀行口座開設において普及しつつある中、このような画像が流出し、免許証等の書類の偽造に悪用されることを懸念する声も散見されており、こちらについても、本物の書類かどうかを確認するための別の方法が検討されるのか等の動向が注目されるところです。

ITmedia NEWS

マッチングアプリ「Omiai」に不正アクセス　免許証など本人確認書類の写し約171万件が流出した可能性

2021年05月21日 16時59分 公開　[ITmedia]

印刷　769　Share　B!　45

メディア事業を手掛けるネットマーケティング（東京都港区）は5月21日、婚活マッチングサービス「Omiai」の情報を管理するサーバが不正アクセスを受け、最大で171万1756件の会員情報が流出した可能性があると発表した。

Omiaiの公式サイト

漏えいした可能性があるのは、2018年1月31日から2021年4月20日までにOmiaiで本人確認を行ったユーザーが、年齢確認書類として提出した運転免許証、健康保険証、パスポート、マイナンバーカード表面の画像データ。21日時点では流出した可能性がある情報の悪用は確認していないとしている。

●「気をつけてよ！写真がネットに載ってるじゃん」SMSからのフィッシングに注意喚起…知り合いの番号から送信も

https://internet.watch.impress.co.jp/docs/news/1326239.html
https://twitter.com/IPA_anshin/status/1395250775702396928
https://www.ipa.go.jp/security/anshin/mgdayori20200220.html

このニュースをザックリ言うと･･･

- 5月20日(日本時間)、IPAより、知り合いを騙るSMSによるフィッシング(スミッシング)の相談が寄せられているとして注意喚起が出されています。

- SMSは「気をつけてよ！写真がネットに載ってるじゃん、気まずいな！」といった文面とともにURLが貼られているもので、URLのタップにより、Androidでは不審アプリのインストール、iPhoneではApple IDを入力させる偽サイト等に誘導されるとしています。

- IPAでは、従来から報告されていた宅配便の不在通知を騙るスミッシングの文面変化版であるとし、また知り合いの電話番号から送られてくるケースもあるとして、URLのタップ、不審なapk(Androidアプリ)ファイルのダウンロードおよび偽サイトでのApple ID情報の入力を行わないよう呼び掛けています。

AUS便りからの所感

- SMSが知り合いの電話番号から送られてくるケースについては、その知り合いが同様の手口でAndroid端末に不審なアプリをインストールしたことにより、アドレス帳の連絡先を読み取られたことによるものとされています。

- Twitter上では、これより前に発生した別のフィッシングでApple ID情報を入力してしまい、使用していたクレジットカードを不正利用された等の事例も報告されています。

- 報告されているフィッシングの多くが特定のダイナミックDNSサービス(動的なグローバルIPアドレスに固有のホスト名を関連付けられるサービス)を使用しており、そのサービスのドメイン名を含むURLについては警戒するという自衛策も考えられますが、これに当てはまらないドメイン名を使用するフィッシングも当然ながら多いため、基本的には前述したIPAが呼び掛けるような回避策をとり、またネット上での報告を随時注視することがより肝要です。

●Windows10の5月度アップデートで修正された脆弱性を突くコード公開、アップデート適用を

https://news.mynavi.jp/article/20210518-1889939/
https://www.ipcert.or.jp/at/2021/at210024.html
https://msrc.microsoft.com/update-guide/ja-JP/vulnerability/CVE-2021-31166
https://forest.watch.impress.co.jp/docs/news/1323816.html

このニュースをザックリ言うと･･･

- 5月12日(日本時間)、マイクロソフト(以下・MS)より、5月度の月例セキュリティアップデートがリリースされていますが、同17日にはそのアップデートで修正された脆弱性の一つ「CVE-2021-31166」(以下・当該脆弱性)のPoC(攻撃コードの一例)がGithubで公開されました。

- 当該脆弱性はHTTPプロトコルスタック(HTTP.sys)に存在し、攻撃者が細工したパケットを送信することにより、Webサーバーとして稼働するWindowsサーバーのクラッシュや乗っ取りが可能とされています。

- 同12日の時点で、特に当該脆弱性について、悪用が容易でワームが開発される恐れもあり、優先して対応を実施することを強く推奨するとの注意喚起がJPCERT/CC等からも出されています。

AUS便りからの所感

- HTTP.sysはIIS以外のWebサービス、例えばWindows Remote Management(WinRM)やWeb Services on Devices API(WSDAPI)等でも利用される場合があり、Windowsサーバーにおいてはデフォルトで80番(HTTP)や443番(HTTPS)のみならず、5985番(WinRM)や5357番(WSDAPI)に外部からアクセス可能な場合にも攻撃を受ける恐れがあるとの情報があります。

- 当該脆弱性はWindows 10 バージョン2004/20H2およびWindows Server バージョン 2004/20H2にのみ影響しますが、5月度のセキュリティアップデートでは他にも多岐にわたる脆弱性が修正されていること、また前のバージョンとなるWindows 10 バージョン1909は(法人向けエディションを除き)4月度のアップデートを最後にサポートが終了しており、引き続きセキュリティアップデートのサポートを受けるためにバージョン2004/20H2(あるいは21H1)へのアップグレードが必要となることにも注意してください。