— AUS（アルテミス・ユーザ・サポート）便り 2017/07/03号 —
http://www.artemis-jp.com

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。

●「メルカリ」Web版にて最大54,180人分の個人情報露呈か

http://news.mynavi.jp/news/2017/06/24/033/
https://www.mercari.com/jp/info/20170622_incident_report/

このニュースをザックリ言うと･･･

- 6月22日（日本時間）、メルカリ社（東京都港区に本社を置く日本の企業で、フリマアプリ「メルカリ」のサービスを運営している）より、同社が運営するフリーマーケットアプリ「メルカリ」のWeb版サイトにおいて不具合が発生し、一部ユーザの個人情報が第三者から閲覧可能な状態になっていたことが発表されました。

- 発表によれば、不具合は同日朝にWeb版サイトでのサーバの切り替えを実施した際に発生したものとされ、外部からの不正アクセス等による流出ではないとされています。

- ユーザから他者の情報が表示されているという問合せを受けたことにより、システムの切り戻しが行われています。

- 不具合が発生していた同日9:41-15:05の間にサイトにアクセスした最大54,180人のユーザについて、個人情報が第三者から閲覧可能な状態となっており、うち最大29,396人については、直接的に個人を特定し得ると考えられる情報（住所・氏名・メールアドレス）が露呈していたとのことです。

AUS便りからの所感等

- 不具合の原因は、パフォーマンス改善のためキャッシュサーバの切り替えを行った際の設定不備によるもので、あるユーザがWeb版サイトにアクセスした際に表示された内容がキャッシュされ、そのキャッシュが他のユーザのアクセスに対して表示されてしまったこととされています。

- DDoS攻撃への対応策としても注目されているCDN（Contents Delivery Network）等において、画像やスクリプト等のデータのキャッシュは重要な技術の一つである一方、一つ設定を誤ることでキャッシュが使用されずトラフィックの軽減が図られなかったり、あるユーザのためだけに表示されるべきデータのキャッシュが他者に表示されたりすることがあり、今回のように個人情報流出の恐れもあるという点で、その運用には仕様を理解した上で適切な設定がなされる必要があると言えます。

マイナビニュース

「メルカリ」Web版で個人情報流出、閲覧された可能性のある2つのケース公開

[2017/06/24]

メルカリは6月22日、同社が提供するフリマアプリ「メルカリ」Web版において一部ユーザーの個人情報が他者から閲覧できる状態になっていたと発表した。同社は、今回の個人情報流出の原因はすでに判明しており、対応も完了しているとしている。

今回の個人情報流出は、2017年6月22日にWeb版のメルカリにおいて、パフォーマンス改善のためキャッシュサー
報が他者から閲覧でき

同社は個人情報流出が
の究明。問題を解消し
洩、不正アクセス等に
ていない」としている
iOS/Androidアプリ版

同社によると、個人情
にメルカリWeb版にア
れる情報(住所・氏名・
は29,396名。

■ケース1

- 障害発生時間帯(6/22 9:41-15:05)にログインした状態でWeb版のメルカリにアクセスし、その時に閲覧したページが、キャッシュサーバーに保存された。(この際、複数存在するキャッシュサーバーのひとつに保存される)
- ユーザーがアクセスした後、1時間以内に、アクセスしたURLと完全に一致するURLに第三者がアクセスし、その際上記で保存されたサーバーと偶然同じサーバーに接続された。

■ケース2

- ユーザーが購入者側である取引において、取引中の相手が上記ケース1に該当した。
- 対象の商品が匿名配送を利用していなかった。

また、閲覧できる可能性のあったユーザー情報は次の通り。

- 直接的に個人を特定し得る可能性がある情報
  住所、氏名、メールアドレス(アドレス内に氏名情報が含まれていた場合)
- その他のユーザー情報(他の情報と組み合わせることで個人の特定は可能だが、単体で直ちに悪用されるとは考えにくいもの)
  銀行口座番号・クレジットカードの下4桁と有効期限(登録しているユーザーのみ)、購入・出品履歴、ポイント・売上金、お知らせ、やることリスト

mercari

Web版のメルカリにおける個人情報流出に関するお詫びとご報告 ※6/23追記あり

2017.06.22

2017/6/23 15:40追記

この度は、お客さまをはじめ多くの関係者の皆様に多大なるご迷惑とご心配をおかけいたしましたことを、深くお詫び申し上げます。
調査の結果、新たに判明した事項につきまして、下記の通りご報告いたします。
なお、本件はID・パスワード
報漏洩、データ改竄は確認さ

1.情報が閲覧できる状態にな

A) 直ちに個人を特定できる情
できる状態になっていた可能

B) 上記のうち、直接的に個人
閲覧できる状態になっていた

1.経緯
2017年6月22日（木）、Web版のメルカリにおけるパフォーマンス改善のためキャッシュサーバーの切り替えを行って以降、一部のお客さまの情報について、他者から閲覧できる状態になっていたことがお客さまからの問い合わせで発覚しました。発覚後、Web版のメルカリをメンテナンス状態とし、原因の究明と問題の解消を行うとともに、経緯や対象範囲の確認を行いました。現在は対応を完了しており、通常通りご利用いただけます。

■時系列
9:41 キャッシュサーバーの切り替えを実施（問題発生）
14:41 カスタマーサポートにてお客さまからの問い合わせ（「マイページをクリックしたら他人のアカウントのページが表示された」旨）を確認し、社内へ報告
15:05 キャッシュサーバーの切り替えを中止し、従来の設定へ戻す
15:16 Web版のメルカリをメンテナンスモードへ切り替え
15:38 キャッシュサーバーへのアクセスを遮断し、問題を完全解消
15:47 Web版のメルカリメンテナンスモードを終了

2. 対象サービス
Web版のメルカリ（日本/US）
※iOS/Androidアプリ版のメルカリをご利用のお客様につきましては対象外となります。

●「2017．6支払依頼書」の添付ZIPファイルに注意、ウイルス付きメールが拡散中…警視庁が警戒を呼び掛け

http://internet.watch.impress.co.jp/docs/news/1067443.html

このニュースをザックリ言うと・・・

- 6月27日（日本時間）、警視庁と日本サイバー犯罪対策センター（JC3）より、「2017．6支払依頼書」という件名などで、ウイルスが添付されたメールが同日より拡散しているとして警告が出されています。

- 警告では以下の2種類のメールが挙げられており、いずれも文書ファイルに偽装したウイルスが添付されています。

① 件名が「請求書ほか」、本文が「お世話になっております。御請求書は、御社様宛に送付になります。」で始まり、「2017-(数字).zip」が添付

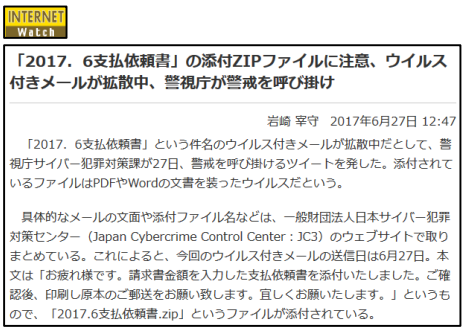
② 件名が「2017．6支払依頼書」本文が「請求書金額を入力した支払依頼書を添付いたしました。」で始まり、「2017．6支払依頼書.zip」が添付

- これらのメールは、国内のオンラインバンキングやクレジットカード利用者を狙うマルウェア「URSNIF(gozi)」への感染を意図したものであるとされ、以前から不定期に様々な件名・文面で拡散しています。

AUS便りからの所感等

- マルウェアへの感染を効果的に防ぐには、手元のPCにおけるOS・各種ソフトウェア・そしてアンチウイルスのパターンファイルを最新に保つこと、そういったメールの受信を遮断するためのUTMの設置、そしてどんな内容のマルウェア添付メールが広まっているか随時情報収集すること、これらの組み合わせが大事です。

- 最近の状況を鑑み、JC3では、確認されたウイルス添付メールの件名・添付ファイル名といった特徴をまとめたインデックスページ（https://www.jc3.or.jp/topics/vm_index.html）を用意しています。


INTERNET Watch

「2017．6支払依頼書」の添付ZIPファイルに注意、ウイルス付きメールが拡散中、警視庁が警戒を呼び掛け

岩崎 宰守　2017年6月27日 12:47

「2017．6支払依頼書」という件名のウイルス付きメールが拡散中だとして、警視庁サイバー犯罪対策課が27日、警戒を呼び掛けるツイートを発した。添付されているファイルはPDFやWordの文書を装ったウイルスだという。

具体的なメールの文面や添付ファイル名などは、一般財団法人日本サイバー犯罪対策センター（Japan Cybercrime Control Center：JC3）のウェブサイトで取りまとめている。これによると、今回のウイルス付きメールの送信日は6月27日。本文は「お疲れ様です。請求書金額を入力した支払依頼書を添付いたしました。ご確認後、印刷し原本のご郵送をお願い致します。宜しくお願いたします。」というもので、「2017.6支払依頼書.zip」というファイルが添付されている。

●約2億人分にのぼる米有権者の個人情報漏えいが発覚…全人口の62%分

https://japan.cnet.com/article/35102966/

このニュースをザックリ言うと・・・

- 6月19日（現地時間）、米セキュリティ企業のUpGuard社より、アメリカ全人口の62%にあたる1億9800万人分の有権者のものと思われる個人情報がインターネット上の公開サーバ上に保存されていたと発表されました。

- データは調査会社Deep Root Analyticsが共和党からの委託で収集していたもので、有権者の個人情報の他、思想・宗教に関するプロファイルデータも含まれていたとされています。

- UpGuard社は、6月12日にクラウドストレージサービス「Amazon S3」のサーバに1.1テラバイトにおよぶ当該データが保存されていたことを発見、同14日に公開停止されたとのことで、Deep Root社によれば同1日の時点で設定ミスにより外部からアクセス可能な設定になっていましたが、UpGuard社によるアクセスまでの間他者による不正アクセスはなかったとのことです。

AUS便りからの所感等

- 保存されていた個人情報の数はアメリカの全有権者に相当するものとされており、センシティブな情報も含まれていたことから、悪意のある第三者がアクセスし、データが拡散していたならば、インターネット史上類を見ない騒ぎになっていたと思われます。

- 個人情報収集にあたり必要のない情報まで無闇に収集することは、万が一の流出の際の被害をより大きなものとするでしょう。

- 機密情報をクラウドに保存することへの抵抗は依然強いですが、組織ネットワークの中であろうと外であろうと、第三者からのアクセスを遮断するよう適切なアクセス制御が設定されていることが大事なのには変わりはなく、オンプレミスで保存している情報についても内部ネットワークを経由しての不正アクセスを考慮し、UTM等を用いたネットワーク構成をとることが肝要です。


cnet Japan

約2億人分にのぼる米有権者の個人情報漏えいが発覚

Zack Whittaker（ZDNet.com） 翻訳校正：編集部　2017年06月20日 07時16分

UPDATE 米国の大量の有権者データが、保護されていない公開サーバ上で見つかっていたことが判明した。10年以上前に遡る米国の全登録済み有権者のものと思われる個人情報や有権者のプロファイリングデータが含まれていたという。

これだけ大量の有権者情報が公開されたことは、知り得る限りでこれまでになかったとされている。

1億9800万人分の米国有権者情報を含む全政党からの複数のデータベースが、共和党のデータ分析を行う企業Deep Root Analyticsが所有する「Amazon S3」の公開ストレージサーバ上で見つかった。

UpGuardのサイバーリスクアナリストであるChris Vickery氏がこの公開サーバを発見し、データを確認した。同氏の責任ある情報開示に基づき、このサーバは14日、報道される前に保護されたという。