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。

●デジタル庁よりメールアドレス400件流出…報道機関向けメールでアドレスをCc: に記載

https://www.itmedia.co.jp/news/articles/2111/25/news142.html

このニュースをザックリ言うと・・・

- 11月24日、デジタル庁より、メール送信時にミスがあり、メールアドレスが他者に流出する事象が発生していたと発表されました。

- 同庁から報道機関向けにプレスリリースを送信した際、報道各社の担当者のメールアドレス約400件を、送信されたメールには表示されない「Bcc: 」ではなく「Cc: 」に記載したことにより、メール受信者がこれらのメールアドレスを読み取ることが可能な状態となっていたとのことです。

- 同庁では誤送信したメールの破棄を報道各社に求めており、「今後は厳重に注意し、再発防止に努める」とコメントしているとのことです。

AUS便りからの所感等

- 400件という大量のメールアドレスをメーラーに手動で入力するという方法は、潜在的にミスが発生するリスク、そしてミスが発生した場合の被害も大きいものとなりますし、一方で複数回に分割するやり方でもまた同様で、ミスの発生率はさらに上がる恐れがあります。

- デジタル化推進を担うべく鳴り物入りで始まったばかりのデジタル庁が、今日においてプレスリリースの発信手段についてもより安全で先進的なシステム等がある中、古典的なEメールによる送信を用いたことや、ミスが発生した原因およびそれへの対策等、ネット上では様々な点に対し疑問を呈する声が挙がっています。

- 安全な同報メール送信のためには、メーリングリストやメール配信サービス等の利用、また可能であれば多数のアドレスが記載された長大なTo: やCc: ヘッダーを含むメールを許可せずUTM等で遮断・警告を返すような仕組みの採用、あるいはどうしてもメーラーで対応せざるを得ない場合は、メーラー自身やアドオンで誤送信防止機能が提供されていればそれを利用する等、人間側の注意のみに依存しない各種システムの導入によって解決されるべきでしょう。

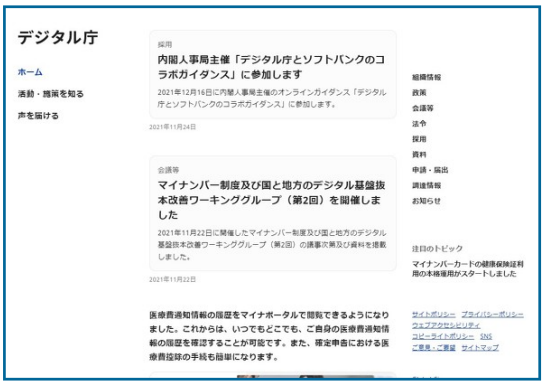
ITmedia NEWS

デジタル庁がメール誤配信　CC・BCC設定ミスで約400件のアドレスが公開状態に

2021年11月25日 15時55分 公開　[谷井将人，ITmedia]

印刷　458　Share　B!　19　5

デジタル庁は11月24日、報道関係者へのメールを配信する際に、宛先の記載ミスにより約400件のメールアドレスを誤送信したと明らかにした。



デジタル庁のWebサイト

同庁は24日午後2時40分「デンマーク外務省とデジタル分野での協力に関する覚え書きを結んだ」という内容のメールを報道陣向けに送信した。その際、第三者から確認できないBCCに記載するべき送信先メールアドレスをCCに記載。メールを受け取った報道陣から全てのメールアドレスが閲覧できる状態になっていた。

●トロイの木馬仕込まれたゲームアプリ、Androidユーザー930万人がダウンロード

https://news.mynavi.jp/article/20211125-2198828/
https://news.drweb.co.jp/show/?i=14360&lng=ja

このニュースをザックリ言うと・・・

- 11月23日(現地時間)、アンチウイルス製品ベンダーのロシアDoctor Web社より、HUAWEI AppGallery(ファーウェイ社製スマートフォン向けアプリストア)においてトロイの木馬「Android.Cynos.7.origin」が組み込まれたゲームアプリを発見したと発表されました。

- Android.Cynos.7.originはアプリインストール時に電話管理権限を要求し、許可されると、ユーザーの携帯電話番号や位置情報、端末の仕様等といった情報を収集するよう設計されているとのことです。

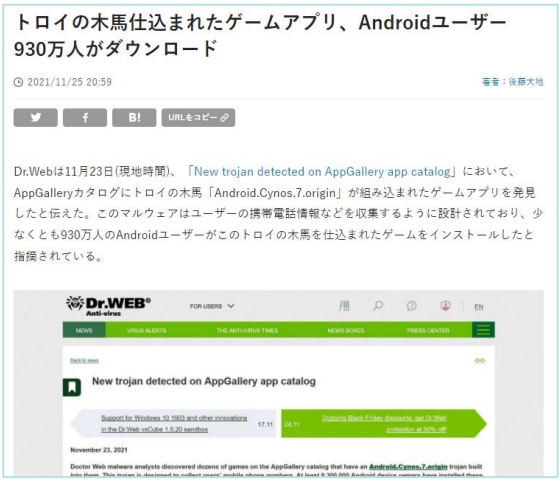
- 発表によれば、ロシア語圏を中心とした190のゲームにこのマルウェアが組み込まれていることがAppGallery上で確認され、合計で930万人以上のユーザーにダウンロードされたとしていますが、現在は報告によってアプリは削除されているとのことです。

AUS便りからの所感

- Android向けアプリストアとしてはGoogle公式のGoogle Playストアがあり、端末を有害なアプリから保護する「Google Play プロテクト」を提供しているものの、やはりそこでもマルウェアを含んだアプリは時々発見されており、Doctor Web社もそういったアプリを報告・削除させています(AUS便り 2021/07/13号参照)。

- Androidアプリでは、インストール時や最初の実行時に権限をユーザーに要求する必要があり、マルウェアによる端末の即座の乗っ取りを防ぐには、不自然に多くの権限が要求された場合にそれをすぐに許可せず、インストールしてはいけないアプリ等でないか、アプリストア・SNS等での評価・評判を参考として判断するべきです。

- Google PlayストアやAppGalleryのようなメーカー提供のストアでも前述のようにマルウェアを含んだアプリに遭遇し得るとはいえ、それ以外の場所からのインストールはさらにその恐れが高くなることには注意が必要です。


トロイの木馬仕込まれたゲームアプリ、Androidユーザー930万人がダウンロード

2021/11/25 20:59　著者：後藤大地

Dr.Webは11月23日(現地時間)、「New trojan detected on AppGallery app catalog」において、AppGalleryカタログにトロイの木馬「Android.Cynos.7.origin」が組み込まれたゲームアプリを発見したと伝えた。このマルウェアはユーザーの携帯電話情報などを収集するように設計されており、少なくとも930万人のAndroidユーザーがこのトロイの木馬を仕込まれたゲームをインストールしたと指摘されている。

●セキュリティ対策をしていないSNSユーザー、Instagramが第1位

https://news.mynavi.jp/article/20211126-2199724/
https://mmdlabo.jp/investigation/detail_2009.html

このニュースをザックリ言うと・・・

- 11月25日(日本時間)、モバイル専門の市場調査等を行うMMD研究所より、同社が実施した「個人の情報セキュリティリテラシーに関する調査」の結果が発表されました。

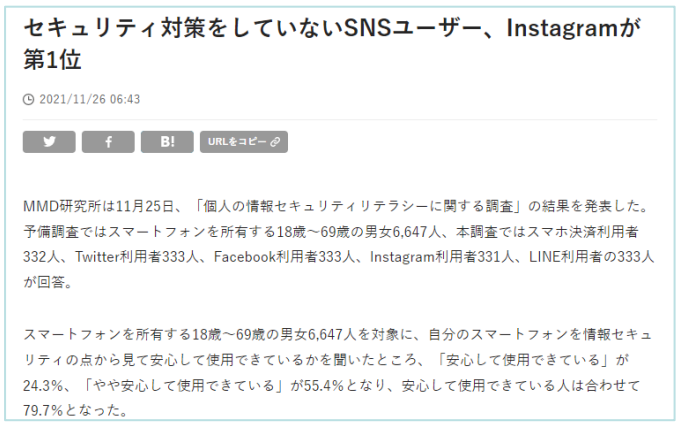
- スマートフォンを所有する18歳～69歳の男女6,647人を対象にした「情報セキュリティの点から見て自分のスマートフォンを安心して使用できているか」という質問への回答は、「安心して使用できている」24.3%、「やや安心して使用できている」55.4%で、安心して使用できている人は合わせて79.7%となっており、また「自分のスマートフォンで情報セキュリティ対策を行っている」と答えたのは87.0%で、具体的な対策では「怪しげなメールや添付ファイルは開かない」62.0%、「不審なサイトを閲覧しない」55.3%等となっています。

- また、スマホ決済・Twitter・Facebook・Instagram・LINEの利用者それぞれ約333人ずつに対し「セキュリティ対策を行っているか」を質問したところ、「対策している」と答えた割合が高かったのはスマホ決済(85.8%)・Twitter(80.2%)・Facebook(73.0%)・LINE(71.2%)・Instagram(68.9%)の順で、Instagramは「対策していない」と答えたのが31.1%と最も多かったとしています。

AUS便りからの所感

- スマホ決済については大きな金銭的被害が出てニュースで取り上げられた事件が大手サービスも含めいくつか発生したことによりユーザーがより注意を払うようになったこと、Twitterは最初期から一定以上の情報リテラシーを持つユーザーが多く集まっていたことが対策率の高さに繋がっている一方、Instagram・LINE・Facebookはより幅広く一般的なユーザーが利用していることが要因と推測されます。

- Instagramユーザーをはじめとした「情報セキュリティを意識するのが面倒」と考える層に対し、分かりやすく、普段から実行しやすいセキュリティ対策の啓発を行えるかが、今後のセキュリティ対策率を底上げする鍵となるものと考えられます。


セキュリティ対策をしていないSNSユーザー、Instagramが第1位

2021/11/26 06:43

MMD研究所は11月25日、「個人の情報セキュリティリテラシーに関する調査」の結果を発表した。予備調査ではスマートフォンを所有する18歳～69歳の男女6,647人、本調査ではスマホ決済利用者332人、Twitter利用者333人、Facebook利用者333人、Instagram利用者331人、LINE利用者の333人が回答。

スマートフォンを所有する18歳～69歳の男女6,647人を対象に、自分のスマートフォンを情報セキュリティの点から見て安心して使用できているかを聞いたところ、「安心して使用できている」が24.3%、「やや安心して使用できている」が55.4%となり、安心して使用できている人は合わせて79.7%となった。