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。

●「7pay」で不正利用被害多発…新規登録とチャージ停止

https://www.itmedia.co.jp/news/articles/1907/03/news140.html
https://www.itmedia.co.jp/news/articles/1907/04/news079.html
https://www.itmedia.co.jp/news/articles/1907/04/news116.html

このニュースをザックリ言うと･･･

- 7月3日（日本時間）、セブン＆アイ・ホールディングス傘下のセブン・ペイ社より、同社が1日に開始したモバイル決済サービス「7pay」において不正アクセスおよび商品の不正購入が確認されたと発表されました。

- ユーザアカウントが第三者に乗っ取られ、登録されていたクレジットカードから電子マネーへのチャージが行われたとしており、7payの新規登録およびクレジットカードとデビットカードによるチャージが一時停止されています。

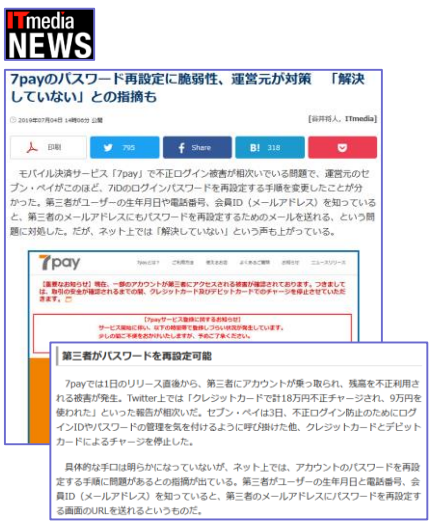
- 同4日の時点で、不正利用の被害者数は約900人、被害額は約5,500万円に上るとみられています。

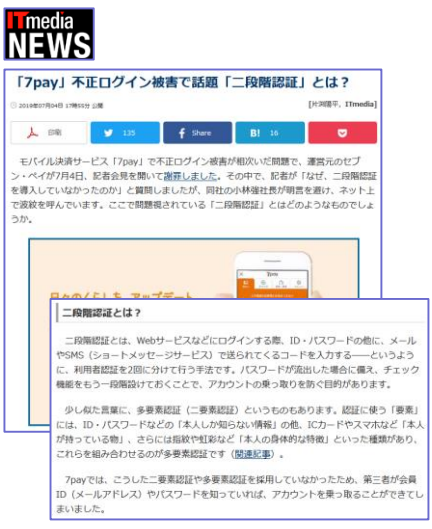
AUS便りからの所感等

- 当初は「リスト型攻撃」の可能性が考えられ、セブン・ペイ社ではログインIDやパスワードの管理に注意するよう呼び掛けていましたが、パスワードリセット機能において「①第三者のメールアドレスにリセットのためのメールを送信することが可能だった」ことや、メールアドレス・生年月日・電話番号の入力が必要とされていたところ「②生年月日を入力しなかったユーザについてはデフォルトの特定の生年月日が指定可能だった」こと、またSMS等を用いた「③二段階認証の機能がなかった」こと等から、攻撃者にとってアカウントを乗っ取りやすい状況にあったことが判明しています。

- 特に、前述①の仕様は、7payも連携していたセブン＆アイグループの通販サイト「オムニ7」に存在していたとされる問題であり、新たに作られたアプリ等のみならず、既存のWebサイトにあったセキュリティ上の問題が目を付けられ悪用されたという面が特徴的と言えます。

- QRコード決済については、昨年リリースされブームとなった「PayPay」でも、外部で奪取されたクレジットカード情報が勝手に登録される事例があり（AUS便り 2018/12/25号参照、現在は対策）、今年3～4月にはキャッシュレス推進協議会により「不正利用防止ガイドライン」が策定されていましたが、今回の7payの事例では、ガイドラインが遵守されていなかったとして経済産業省から指摘を受ける事態になっており、根幹となるスマホアプリあるいはWebサイトにおいて、ガイドラインに沿って必要なセキュリティ機能を実装することの重要性が今後改めて問われることとなるでしょう。





●「OneDrive」を悪用したフィッシング詐欺に注意、偽ログイン画面で認証情報を詐取

https://internet.watch.impress.co.jp/docs/news/1193011.html

このニュースをザックリ言うと・・・

- 6月27日（日本時間）、フィッシング対策協議会より、マイクロソフトのオンラインストレージサービス「OneDrive」を悪用したフィッシングメールが確認されているとして注意喚起が出されています。

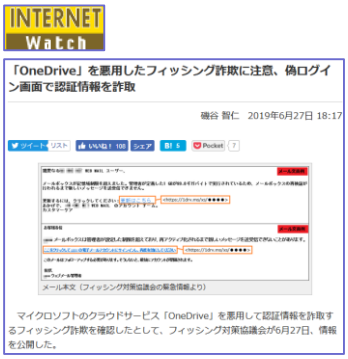
- メールは、「メールボックスは管理者が設定した制限を超えており、再アクティブ化されるまで新しいメッセージを送受信できないことがあります」等と偽り、制限を解除するためのログインページをかたるフィッシングサイトへ誘導するものとなっています。

- 同協議会では、フィッシングサイトはOneDrive上に存在していることからURLも正規サービスのものとなっており、かつメールに記載されたリンクもOneDriveで使用される短縮URL（https://1drv.ms/●●●●）であることに注意すること、そしてこのようなフィッシングサイトにてメールアドレス・パスワード等を絶対に入力しないこと、を呼び掛けています。

AUS便りからの所感等

- 6月25日にセキュリティベンダーのFireEyeが発表したレポートでも、このような信頼されるストレージサービスやファイル共有サービスを攻撃用ファイルの保存先として利用し、リンクを電子メールに記載する攻撃が増えているとしており、OneDriveはDropboxに次いで頻繁に使われるようになっているとのことです。

- URLが有名なオンラインストレージサービスのものであることから、ブラウザ等のアンチフィッシング機能は回避される可能性が高いため、現時点で取り得るその他の防御策で補完すること、例えば攻撃手法についての情報を随時入手し、今回のような「オンラインストレージ上にログイン画面らしきフォームがある」ケースは怪しいと判断できるようになることが重要でしょう。


INTERNET Watch

「OneDrive」を悪用したフィッシング詐欺に注意、偽ログイン画面で認証情報を詐取

確谷 智仁　2019年6月27日 18:17

マイクロソフトのクラウドサービス「OneDrive」を悪用して認証情報を詐取するフィッシング詐欺を確認したとして、フィッシング対策協議会が6月27日、情報を公開した。

●「NOTICE」調査結果発表、9,000万IP中147件に注意喚起

http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00033.html

このニュースをザックリ言うと・・・

- 6月28日（日本時間）、総務省とNICT（国立研究開発法人情報通信研究機構）より、国内の脆弱なIoT機器について調査・注意喚起を行うプロジェクト「NOTICE」の実施状況が発表されました。

- 国内約9,000万IPアドレスに対する調査の結果、外部からID・パスワードが入力可能だった対象は約31,000～約42,000件、うち延べ147件については、容易に推測可能なID・パスワードによるログインが可能だったため、ISP経由で注意喚起を行ったとしています。

- また、これとは別に、マルウェアに感染していると検知した機器に対し注意喚起を行う取り組みも6月中旬から行い、1日あたり112～155件が注意喚起の対象となっているとのことです。

AUS便りからの所感等

- その多くは調査の範囲ではログイン可能ではなかったとはいえ、恐らくは管理画面が外部に見えていたとみられる機器が2,000～3,000件に1件存在していた計算となっていますが、管理者各位には管理下のあらゆる機器について外部から管理画面にアクセス可能か各自で診断を行っていただき、可能だった場合にはできる限り設定変更やUTMによる遮断等による対策をとることを推奨致します。

- 総務省では、上記の注意喚起件数について「現時点で数は少ない状況と考えられる」としながらも、今後も機器へのマルウェア感染活動が見込まれるとして、引き続き適切なID・パスワードの設定、ファームウェアの最新版へのアップデート等のセキュリティ対策の徹底に努めるよう呼び掛けており、次回の発表の際には注意喚起対象等の割合がより低くなっていることを期待したいものです。


総務省 MIC Ministry of Internal Affairs and Communications

報道資料

令和元年6月28日

総務省
国立研究開発法人情報通信研究機構
一般社団法人ICT-ISAC

脆弱なIoT機器及びマルウェアに感染しているIoT機器の利用者への注意喚起の実施状況

近年、IoT機器※1を悪用したサイバー攻撃が増加していることから、利用者自身が適切なセキュリティ対策を講じることが必要です。
総務省、国立研究開発法人情報通信研究機構（NICT）及び一般社団法人ICT-ISACは、インターネットプロバイダと連携し、脆弱なID・パスワード設定等のためサイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取組「NOTICE（National Operation Towards IoT Clean Environment）」並びにNICTのNICTERプロジェクト※2によりマルウェアに感染していることが判明した機器の利用者への注意喚起を行う取組を実施しています。
今般、これまでの実施状況を取りまとめましたので公表します。

1　経緯等

あらゆるものがインターネット等のネットワークに接続されるIoT/A時代が到来し、それらに対するサイバーセキュリティの確保は、安心・安全な国民生活や社会経済活動確保の観点から重要な課題となっています。
IoT機器が増加する一方で、IoT機器を狙ったサイバー攻撃は近年増加傾向にあります。センサーやウェブカメラなどのIoT機器は、機器の性能が限定されている、管理が行き届きにくい、ライフサイクルが長いなど、サイバー攻撃に遭われやすい特徴を持っています。セキュリティ対策に不備のあるIoT機器は、マルウェアに感染しサイバー攻撃に悪用されるおそれがあります。諸外国においては、IoT機器を悪用した大規模なサイバー攻撃（DDoS攻撃）によりインターネットに障害が生じるなど、深刻な被害が発生していることから、我が国においても2020年オリンピック・パラリンピック東京大会などを控え、対策の必要性が高まっています。
このような状況を踏まえ、NICTの業務にサイバー攻撃に悪用されるおそれのある機器の調査等を追加[5年間の時限措置]する「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」が平成30年11月1日（木）に施行されました。