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。

●Appleをかたるフィッシングメールが出回る、「アカウントがロックされる」などとして偽サイトでApple ID詐取

http://internet.watch.impress.co.jp/docs/news/1032714.html
https://www.antiphishing.jp/news/alert/apple_20161201.html

このニュースをザックリ言うと･･･

- 12月1日（日本時間）、フィッシング詐欺に関する調査・啓発を行っているフィッシング対策協議会より、Appleをかたり、Apple IDやクレジットカード情報等を詐取しようとするフィッシングメールが出回っているとして警告が出されています。

- フィッシングメールの件名は7つ（下図参照）が確認されており、それぞれに共通した文面とともに、6つの偽サイト（下図参照）へ誘導するものとなっています。

- 同協議会では、発表の時点でフィッシングサイトが稼働中として、サイト閉鎖のための調査をJPCERT/CCに依頼するとともに、今後類似したサイトが公開される恐れがあるとしており、こういったサイトでアカウント情報を絶対に入力しないよう、また同様のサイトやメールを見かけた場合は協議会へ連絡するよう呼び掛けています。

AUS便りからの所感等

- Apple IDを狙うフィッシング詐欺は7月にも確認されており（AUS便り 2016/08/08号参照）、これはSMSによる英語のメッセージでしたが、日本語によるより洗練された内容のフィッシングが出回ることは時間の問題だったと言えます。

- Apple IDはiPhoneアプリ購入時に必須になる他、iCloudのアカウントでもあり、それを奪取されるとクラウドに保存したデータを読み出される可能性がありますが、二段階認証の設定等による保護は万が一のID奪取の際に有効です。

- 実際のフィッシングサイトのURLは十分注意すればそれと認識できるものですが、そういうように人間の判断だけに依存するよりは、可能な限りブラウザやUTM等のアンチフィッシング機能と組み合わせることによる防御が効果的でしょう。

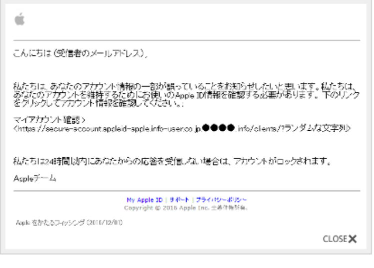
INTERNET Watch

ニュース

Appleをかたるフィッシングメールが出回る、「アカウントがロックされる」などとして偽サイトでApple ID詐取

岩崎 宰守　2016年12月1日 11:47

ツイート リスト いいね！ 121 シェア B! 12 Pocket 41



Appleをかたるフィッシングメールが出回っているとして、フィッシング対策協議会が1日、注意を呼び掛ける緊急情報を出した。誘導先となっている偽サイトは、同日9時30分現在も稼働中だとしており、アカウント情報（Apple ID、パスワードなど）や個人情報を含む請求先情報、クレジットカード情報などを絶対に入力しないよう注意を呼び掛けている。

フィッシング対策協議会 Council of Anti-Phishing Japan

Apple をかたるフィッシング (2016/12/01)

概要

Apple をかたるフィッシングメールが出回っています。

メールの件名

誰かがあなたのアカウントを使用しようとしていると思われま
私たちは24時間以内にあなたからの応答がない場合は、アカウントがロックされます。
お使いのApple IDはiCloud上にログインするために使用されてきました
あなたのアカウントのApple IDが別のデバイスから開かれました！
アカウントがロックされます：201926
アカウントがロックされます！
アップルIDがロックされました。

サイトのURL

https://secure-account.appleid-apple.info-user.co.jp.●●●●.info/ランダムな文字列
https://d17oy1vhnax1f7.●●●●.net/items/ランダムな文字列/AppIe-ID(●●●●).info_rmation.html
https://secure3.store.apple.com.b9cfe.●●●●.info/sign_in/
http://appleid.apple.co.jp.data.verification.status.●●●●.info/
http://appleid.apple.co.jp.verify.id.xse.●●●●.info/
http://scurty.accont-i-cl0ud.informati.●●●●.com/clients/

●画像に偽装したファイルでマルウェアに感染、ランサムウェア拡散に使用か

http://www.itmedia.co.jp/enterprise/articles/1611/27/news031.html

このニュースをザックリ言うと・・・

- 11月24日（現地時間）、大手セキュリティベンダーであるチェックポイント社より、画像ファイルに偽装したファイルからマルウェアに感染させようとする攻撃手法が確認されたとして警告が出されています。

- 同社が「ImageGate」と名付けたこの攻撃では、攻撃者がSNSに偽装ファイルをアップロードし、ユーザにPC上へダウンロードさせて開かせることにより、マルウェアをPC上で実行させるという手順をとっており、偽装ファイルは実際には「.hta」「.js」および「.svg」の拡張子を持っています。

- 少なくとも9月上旬以降にFacebook等の主要なSNSでこの手法による攻撃を確認している他、11月14日の週には、この手法により、ランサムウェア「Locky」へ感染させる攻撃が発生していたとしています。

- 同社では、「Webサイトで画像をクリックしてファイルのダウンロードが開始された場合、ファイルを開かない」「SNSサイト利用時は画像を表示だけにとどめる」「特に特殊な拡張子を持つ画像ファイルは決して開かない」よう注意を促しています。

ITmedia エンタープライズ

2016年11月28日 06時30分 更新

画像でマルウェアに感染させる「ImageGate」攻撃、ランサムウェア拡散に使用か

攻撃者は悪質なコードを埋め込んだ画像をSNSなどにアップロードし、ユーザーに画像をダウンロードさせることでマルウェアに感染させるという。

[ITmedia]

画像ファイルに悪質なコードが埋め込んでソーシャルメディア経由でマルウェアに感染させる新たな攻撃手法が報告された。発見したセキュリティ企業のCheck Point Software Technologiesは、この攻撃を「ImageGate」と命名。ランサムウェアの拡散に利用されているという。

同社によると、この攻撃では悪質なコードが埋め込まれた画像を攻撃者がSNSサイトにアップロードする。さらに攻撃者は、SNSサイトの設定を利用してユーザーに画像ファイルをダウンロードさせ、ファイルをクリックした瞬間にマルウェアが実行されてしまう。

AUS便りからの所感等

- 「ImageGate」と名付けられ「新たな攻撃手法」とされていますが、根本となるのは「実際には .hta, .js といった拡張子を持つファイル」を用いることであり、古典的手法が再び注目されたということでしょう。

- .svg拡張子のファイルはベクターイメージの画像ファイルである一方、XMLファイルでもあるという側面を持ち、リンクやJavaScriptを埋め込むことも可能であり、ブラウザ上でsvg画像を表示する限り、仮にスクリプトが実行されたとしても影響範囲は制限されるでしょう。

- 今回の攻撃手法に限って言えば、ブラウザ上で表示するだけでマルウェアに感染することはありませんが、アンチウイルスやUTMによりそういったファイルのダウンロードを食い止められる体制を作ることが重要です。

●資生堂子会社に不正アクセス、個人情報42万人分が流出か

http://www.itmedia.co.jp/enterprise/articles/1612/02/news106.html

このニュースをザックリ言うと・・・

- 12月2日（日本時間）、資生堂より、同社子会社イプサが運営する「イプサ公式オンラインショップ」が不正アクセスを受け、クレジットカード情報を含む個人情報が流出した可能性があると発表されました。

- 対象となるのは、同サイトの登録会員最大421,313人分の氏名・生年月日・電話番号・メールアドレス・住所・パスワード・購入履歴等、および2011年12月14日～2016年11月4日のクレジット決済56,121件についてのカード番号・名義・住所・有効期限とされています。

- 11月4日に決済代行会社からの連絡で流出が発覚しており、詳細な原因等については、2017年1月末をめどに調査報告書が発表される予定とのことですが、資生堂グループの他のショッピングサイトについては、システムが完全に分離しているため、直接の影響はないとのことです。

ITmedia エンタープライズ

2016年12月02日 16時37分 更新

クレジットカード情報も約5万件流出の恐れ：

資生堂子会社に不正アクセス、個人情報42万人分が流出か

大手化粧品メーカー、資生堂の子会社「イプサ」の公式オンラインショップに、不正アクセスがあったことが発覚。最大で約42万人分の個人情報と、約5万件のクレジットカード情報が流出した可能性がある。

[ITmedia]

大手化粧品メーカーの資生堂は12月2日、子会社の「イプサ」が運営する公式オンラインショップが外部から不正アクセスを受け、最大42万1313人分の個人情報および、最大5万6121件のクレジットカード情報が流出した可能性があると発表した。

2016年11月4日に、決済代行会社から「イプサの公式オンラインショップが攻撃を受け、クレジットカード情報が流出している可能性がある」と連絡を受け、情報漏えいが発覚。同日18時30分頃に、同サイトのクレジットカード決済を停止した。その後、対策本部の設置や、第三者機関への調査依頼、そして警察や経済産業省への報告を行ったという。

AUS便りからの所感等

- サイトの登録会員情報、特にメールアドレスとパスワードの流出により、他のWebサイトでこれを悪用した不正ログインが実行される可能性は非常に高く、同じID（アカウント名やメールアドレス）とパスワードの組み合わせで、複数のサイトが芋づる式に不正ログインの攻撃を受けることはこれまで度々言及していることです。

- 流出した情報のうちクレジットカード情報については、パスワード・セキュリティコードは含まれていないことから、従来は悪用は困難とみられていましたが、つい最近、一部クレジットカードにおいてカード番号からセキュリティコードを割り出せたという研究結果も出てきています（http://itpro.nikkeibp.co.jp/atcl/idg/14/481709/120600279/）。

- ともあれ究極的には、カード情報の入力等を決済代行会社が提供するサービスの上で行い、自前ではカード情報を保持しないシステムであることが望ましく、万が一の流出時のリスクを抑える一助となるでしょう。