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。

●PayPalをかたるフィッシング、フィッシング対策協議会が警告

https://internet.watch.impress.co.jp/docs/news/1172171.html
https://www.antiphishing.jp/news/alert/paypal_20190228.html

このニュースをザックリ言うと・・・

- 2月28日（日本時間）、フィッシング対策協議会より、PayPalをかた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。

- メールは、
◆件名が「[大切] PayPal アカウントでの不審なログインアクティビティ - ケース ID#英数字」
◆本文には「誰かログインードがPayPalアカウントに登録されました」(原文ママ)等と記載
◆「検証が必要」と書かれたリンクをクリックするとPayPalの偽のログイン画面に誘導されます。

- 同協議会ではこのようなフィッシングサイトでメールアドレス・パスワード・個人情報・クレジットカード情報などを絶対に入力しないよう呼びかけている他、PayPalでもフィッシングメールに対する注意を呼びかけるページを以前から用意しており、個人情報や運転免許証番号等をメールで確認することはないとしています。
（https://www.paypal.com/jp/webapps/mpp/support/phishing）

AUS便りからの所感等

- メールに記載されたリンクのURLはTwitterでURLの圧縮に用いられる「https://t.co/●●」となっており、そこから「https://セキュリティ更新.●●●●.jp/」（https://xn--dckta5b5b2j4a1907fbec.●●●●.jp/ と表示される場合あり）にリダイレクトする形をとっています。

- フィッシングサイトが日本語ではなく英語が表示されることを除けば比較的本物に近いデザインとみられるため、前述のようにメールで一箇所不自然な文章があることや、サイトのURLが本物のように「paypal.com」ドメインではなく日本語文字を含むドメインを使用しているところ等で不審に思わないとだまされてしまう可能性もあり、ブラウザやセキュリティソフトおよびUTMによるアンチフィッシング機能の有効化、およびあらかじめブックマークに登録してそこからアクセスする等による回避策をとることは大切です。

- なお本物のPayPalサイトではEV-SSL証明書を使っていますが、なぜかChromeではアドレスバーに企業名が表示されない（IE・Edge・Firefoxでは表示）ことに注意してください。


INTERNET Watch

PayPalかたりユーザー情報を詐取するフィッシングメール拡散中、件名は「[大切] PayPal アカウントでの不審なログインアクティビティ」

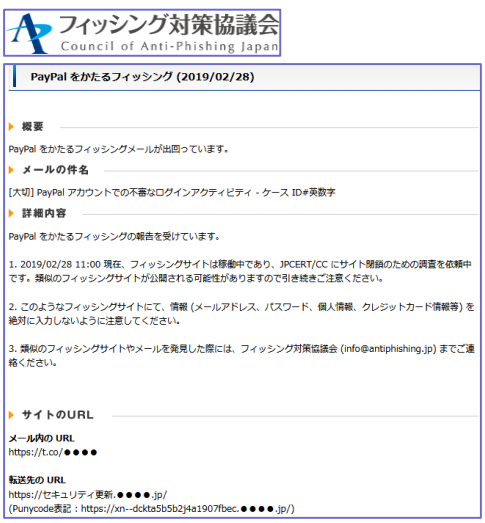
磯谷 智仁　2019年2月28日 14:37

ツイート リスト　いいね！79　シェア　B! 2　Pocket 2

PayPal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注意を促している。

メールの件名は「[大切] PayPal アカウントでの不審なログインアクティビティ - ケース ID#英数字」。本文では「誰かログインードがPayPalアカウントに登録されました。」（原文ママ）などとして、ユーザー情報を確認するように促し、PayPalのログイン画面を模した偽サイトへ誘導する。誘導先の偽サイトは2月28日11:00時点で稼働中だ。

PayPal


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

PayPal をかたるフィッシング (2019/02/28)

▸ 概要

PayPal 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

[大切] PayPal アカウントでの不審なログインアクティビティ - ケース ID#英数字

▸ 詳細内容

PayPal をかたるフィッシングの報告を受けています。

1. 2019/02/28 11:00 現在、フィッシングサイトは稼働中であり、JPCERT/CC にサイト閉鎖のための調査を依頼中です。類似のフィッシングサイトが公開される可能性がありますので引き続きご注意ください。

2. このようなフィッシングサイトにて、情報 (メールアドレス、パスワード、個人情報、クレジットカード情報等) を絶対に入力しないように注意してください。

3. 類似のフィッシングサイトやメールを発見した際には、フィッシング対策協議会 (info@antiphishing.jp) までご連絡ください。

▸ サイトのURL

メール内の URL
https://t.co/●●●●

転送先の URL
https://セキュリティ更新.●●●●.jp/
(Punycode変記：https://xn--dckta5b5b2j4a1907fbec.●●●●.jp/)

●ChromeのPDFリーダー機能に脆弱性か…PCの情報等を外部に送信の可能性

https://www.itmedia.co.jp/news/articles/1902/20/news077.html

このニュースをザックリ言うと・・・

- 2月26日（現地時間）、セキュリティ企業のEdgeSpot社より、Google ChromeのPDFリーダー機能に存在する未修正の脆弱性を突くPDFファイルが2018年12月から確認されているとして注意喚起が出されています。

- 発表によれば、この不正なPDFファイルをPC上に保存した状態でChromeで開いた場合、PCのIPアドレス・OS・Chromeのバージョンおよび PDFファイルのローカルディスク上のパスといった情報がユーザの許可なく外部に送信されるとのことです。

- Googleでは12月の時点で報告を受けており、4月下旬に修正を予定しているとのことです。

AUS便りからの所感等

- 2月12日にAcrobat Reader等で修正された脆弱性とは異なるものとされ、Chrome以外（Acrobat ReaderやFirefox等）の場合や、外部Webサイト上のPDFファイルを直接表示する場合には問題は発生しないとの情報があるため、攻撃者はWebサイト上のリンクをクリックしたらそこでPDFを直接表示する形ではなく、一旦ダウンロードさせてから開かせようとする形をとることが考えられます（メールに添付する等も考えられます）。

- PDFリーダーはAcrobat Reader以外にも数多く存在し、またChrome以外の各種Webブラウザ（IE除く）にも備わっていますので、PDFファイルを読む手段を普段から複数用意しておくことはセキュリティリスクの回避の面でも有用と言えますが、常に最新のバージョンを利用することや、アンチウイルスやUTMによる防御も併せて行っていくことも忘れてはいけません。


ITmedia エンタープライズ

Google Chromeに脆弱性か、ユーザー追跡の不審なPDF発見

Google Chromeで問題のPDFファイルを開くと、そのユーザーの情報が、本人の知らないうちに外部に送られてしまう可能性があるという。

2019年03月01日 10時00分 公開 [鈴木聖子，ITmedia]

印刷 71 25 B! 14

セキュリティ企業のEdgeSpotは2月26日、米GoogleのWebブラウザ「Chrome」の未解決の脆弱性を突くPDFファイルが出回っているのを見つけたと伝えた。Google Chromeをローカルビューワとして使って問題のPDFファイルを開くと、そのユーザーの情報が、本人の知らないうちに外部に送られてしまう可能性があるとしている。

EdgeSpotによると、問題のPDFは2018年12月ごろから大量に検出されるようになった。Adobe ReaderなどのPDF閲覧ソフトで開いた場合は不審な挙動は確認されなかったが、Google Chromeで開くと不審な上りトラフィックが検出され、調べた結果、ユーザー情報が密かに外部のドメインに送信されていることが分かったという。

●「WinRAR」「Explzh」に脆弱性…原因は古い圧縮フォーマット

https://forest.watch.impress.co.jp/docs/news/1170860.html

このニュースをザックリ言うと・・・

- 2月20日（現地時間）、セキュリティベンダーのチェック・ポイント・ソフトウェア・テクノロジーズ社より、圧縮・解凍ソフト「WinRAR」に19年前から脆弱性が存在していたと発表されました。

- WinRARが扱う圧縮形式の一つ「ACE」の処理に問題があり、細工したACE形式（.ace拡張子）の圧縮ファイルを展開することにより、PC上の任意のフォルダにファイルが展開される可能性があるとされています。

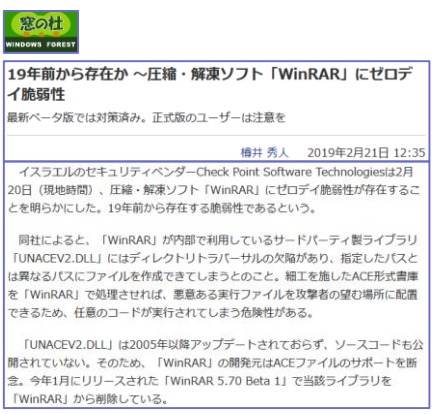
- 2月28日にWinRARの修正バージョン5.70がリリースされた他、別の圧縮・解凍ソフトウェア「Explzh」でも影響を受けるとされたことから、バージョン7.74でACE形式のサポートを打ち切っています。

AUS便りからの所感等

- 不正なアーカイブファイルを開くことにより、想定外の場所にファイルが展開される、いわゆる「ディレクトリトラバーサル」の脆弱性は、以前から様々な形式の圧縮ファイル形式で報告・対策されています。

- ACE形式は、ZIPや7z形式等に比べ今や利用される機会は皆無に等しく、そのため脆弱性の発見が遅れていたことが考えられますが、こういった修正される可能性が低いとみられるファイル形式やそれを処理するソフトウェアの脆弱性は攻撃者にとって格好の標的であり、またアンチウイルス・UTM等が今後対応するかどうかも未知数です。

- このような攻撃から少しでも回避できるよう、普段から使用している圧縮・解凍ソフトについては最新に保ち、ベンダーからのセキュリティ情報に注意を払い、不審な添付ファイルを持つメールは展開せずに削除することを心がけましょう。


窓の杜 WINDOWS FOREST

19年前から存在か ～圧縮・解凍ソフト「WinRAR」にゼロデイ脆弱性

最新ベータ版では対策済み。正式版のユーザーは注意を

樽井 秀人 2019年2月21日 12:35

イスラエルのセキュリティベンダーCheck Point Software Technologiesは2月20日（現地時間）、圧縮・解凍ソフト「WinRAR」にゼロデイ脆弱性が存在することを明らかにした。19年前から存在する脆弱性であるという。

同社によると、「WinRAR」が内部で利用しているサードパーティ製ライブラリ「UNACEV2.DLL」にはディレクトリトラバーサルの欠陥があり、指定したパスとは異なるパスにファイルを作成できてしまうとのこと。細工を施したACE形式書庫を「WinRAR」で処理させれば、悪意ある実行ファイルを攻撃者の望む場所に配置できるため、任意のコードが実行されてしまう危険性がある。

「UNACEV2.DLL」は2005年以降アップデートされておらず、ソースコードも公開されていない。そのため、「WinRAR」の開発元はACEファイルのサポートを断念。今年1月にリリースされた「WinRAR 5.70 Beta 1」で当該ライブラリを「WinRAR」から削除している。