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。

●「ツイッターで偽の広告」マクドナルドが注意呼びかけ

http://web.archive.org/web/20170630164958/www3.nhk.or.jp/news/html/20170630/k10011036271000.html
http://nlab.itmedia.co.jp/nl/articles/1706/29/news141.html

このニュースをザックリ言うと･･･

- 6月30日（日本時間）、日本マクドナルド社より、同社がツイッター上で行っているキャンペーンをかたる偽の広告が確認されたとして警告が出されました。

- 同社では同28日からハンバーガーの割引券を提供する「バーガーツイート診断」キャンペーンを行っていました（現在は終了）が、29日に、不正なアプリとの連携を行う偽の広告が拡散していることを確認したとのことです。

- 同社では、「w.mdj.jp/」で始まるURLが表示されて“いない” ツイートは偽の広告でありアクセスしないこと、またアプリ認証画面で許可する内容を確認するよう呼び掛けています。

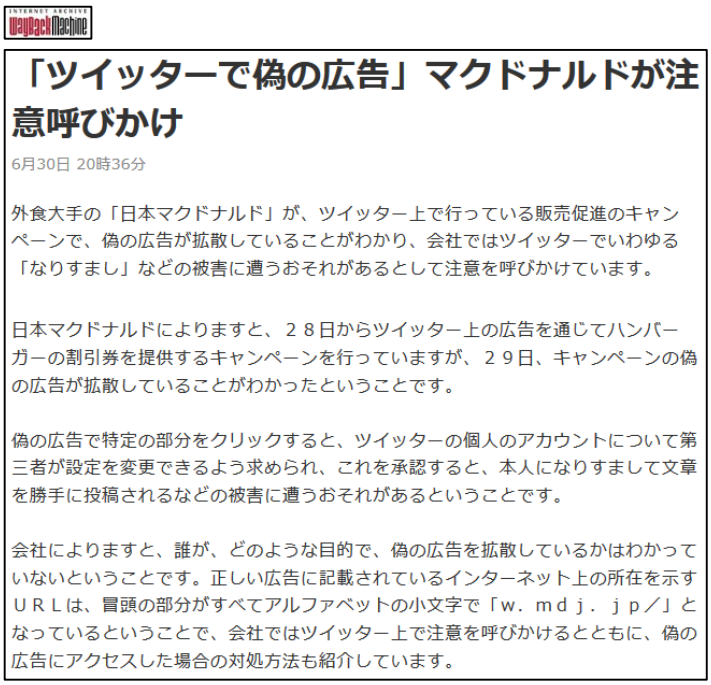
AUS便りからの所感等

- Twitterユーザに便利な機能を提供すると偽って不正なアプリと連携させ、スパムツイートを投稿させるケースが手を変え品を変え確認されています。

- 当AUS便りでも、例えばあるユーザが何人からブロックされているかを調査するアプリをかたりスパムを拡散するケース等を取り上げています（2017/2/20号参照）。

- 悪意のあるアプリによっては、こういったツイートやDMの勝手な送信だけでなく、プロフィールの書き換えやDMを覗き見られる可能性もあります（なお、アカウントのパスワードが奪取・変更されることは仕様上ありません）。

- どんなアプリであっても、連携の際には要求される権限を明示した上で承諾が求められますので、信頼できるアプリかどうかTwitter上等の情報から判断することと、必要最小限のアプリとのみ連携するようにしましょう。



「ツイッターで偽の広告」マクドナルドが注意呼びかけ

6月30日 20時36分

外食大手の「日本マクドナルド」が、ツイッター上で行っている販売促進のキャンペーンで、偽の広告が拡散していることがわかり、会社ではツイッターでいわゆる「なりすまし」などの被害に遭うおそれがあるとして注意を呼びかけています。

日本マクドナルドによりますと、２８日からツイッター上の広告を通じてハンバーガーの割引券を提供するキャンペーンを行っていますが、２９日、キャンペーンの偽の広告が拡散していることがわかったということです。

偽の広告で特定の部分をクリックすると、ツイッターの個人のアカウントについて第三者が設定を変更できるよう求められ、これを承認すると、本人になりすまして文章を勝手に投稿されるなどの被害に遭うおそれがあるということです。

会社によりますと、誰が、どのような目的で、偽の広告を拡散しているかはわかっていないということです。正しい広告に記載されているインターネット上の所在を示すＵＲＬは、冒頭の部分がすべてアルファベットの小文字で「ｗ．ｍｄｊ．ｊｐ／」となっているということで、会社ではツイッター上で注意を呼びかけるとともに、偽の広告にアクセスした場合の対処方法も紹介しています。

2017年06月29日 23時14分 更新

マクドナルド「バーガーツイート診断」に便乗したスパムツイートに公式が注意喚起　正規URLからアクセスするよう呼びかけ

アプリ連携の解除方法を説明しています。

[高原れい，ねとらぼ]

316 ツイート　70 いいね！　70 シェア　2 B! Bookmark　7 Pocket　2 G+1

日本マクドナルドは6月29日、現在実施中の「バーガーツイート診断」に便乗したスパムツイートの存在を確認。同診断に偽装したURLに注意するよう呼びかけています。

●Flash Playerの半数超が古いバージョンのまま…割合は前年より増加

http://internet.watch.impress.co.jp/docs/column/security/1068807.html

このニュースをザックリ言うと・・・

- 6月5日（現地時間）、米Duo Security社より、約460万台のデバイスにおけるOS・ブラウザ・プラグインの更新状況等の調査レポート「The 2017 Duo Trusted Access Report」が発表されました。

- レポートによれば、「Flash Player」のインストール状況について、53%が古いバージョンのままとされており、この数値は前年の42%よりも10%以上増えているとのことです。

- 上記結果をブラウザ毎で見てみると、Internet Explorer（IE）向けFlash Playerは58%が古いままであるのに対し、Google Chromeに同梱されるものは65%が最新の状態になっているとされています。

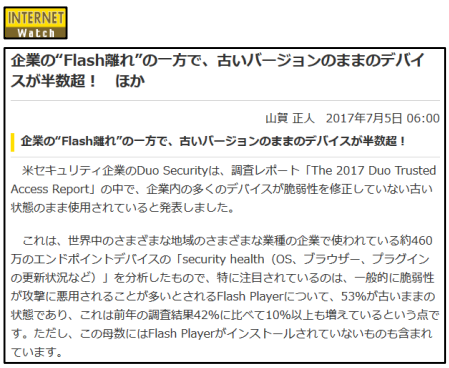
- 一方で、「Flash Playerをインストールしていないデバイス」の割合が前年の19%から25%に上昇しているという調査結果も出ています。

AUS便りからの所感等

- Flash Playerは、JavaやAdobe Readerと同様、長年の間脆弱性を悪用され続けてきたプラグインです。

- Webブラウザの機能向上により、Flashに依存せずHTML5を用いる形に転換するWebサービスも増えてきていることもあり、各ブラウザにおいてはFlashコンテンツを自動再生させない方向に徐々に進んでいます。

- Chrome以外のブラウザ（FirefoxおよびWindows7上のIE等）の場合はFlash Playerが自動更新されているかをコントロールパネルから適宜確認し、Windows10上のIE/Edgeの場合はWindows Updateで更新されますので、これも無効にしていないか注意が必要です。


INTERNET Watch

企業の“Flash離れ”の一方で、古いバージョンのままのデバイスが半数超！　ほか

山賀 正人　2017年7月5日 06:00

企業の“Flash離れ”の一方で、古いバージョンのままのデバイスが半数超！

米セキュリティ企業のDuo Securityは、調査レポート「The 2017 Duo Trusted Access Report」の中で、企業内の多くのデバイスが脆弱性を修正していない古い状態のまま使用されていると発表しました。

これは、世界中のさまざまな地域のさまざまな業種の企業で使われている約460万のエンドポイントデバイスの「security health（OS、ブラウザー、プラグインの更新状況など）」を分析したもので、特に注目されているのは、一般的に脆弱性が攻撃に悪用されることが多いとされるFlash Playerについて、53%が古いままの状態であり、これは前年の調査結果42%に比べて10%以上も増えているという点です。ただし、この母数にはFlash Playerがインストールされていないものも含まれています。

- Flash Playerを最新に保ち、かつアンチウイルスやUTMで攻撃を防御する体制にしておくのが重要です。

●老舗の圧縮・解凍ソフト「Lhaz」「Lhaz+」に脆弱性、修正版が公開

http://forest.watch.impress.co.jp/docs/news/1068510.html

このニュースをザックリ言うと・・・

- 7月1日（日本時間）、Windows用圧縮・解凍ソフト「Lhaz」「Lhaz+」に脆弱性が確認され、最新バージョンがリリースされました。

- 開発者によれば、Lhazのインストーラー、およびLhazで作成した自己解凍アーカイブにおいて、DLL（動的ライブラリ）を読み込む際の検索処理に問題があり、不正なDLLファイルによってPCを完全にコントロールされる恐れのある脆弱性が存在したとのことです。

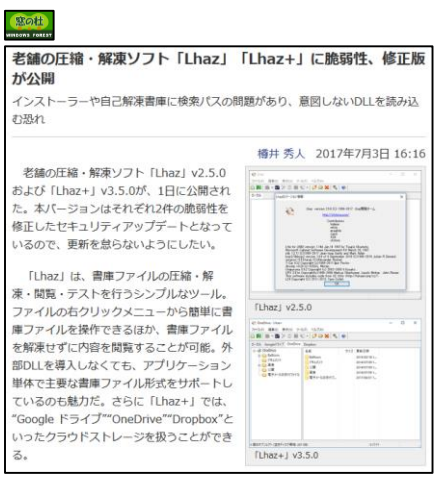
- 脆弱性はLhaz 2.4.0以前およびLhaz+ 3.4.0以前に存在し、それぞれ修正版の2.5.0/3.5.0がリリースされており、アップデートが推奨されています。

AUS便りからの所感等

- 問題とされている脆弱性は、5月下旬にIPA等から発表された、いわゆる「DLLインジェクション攻撃」とされるものです（AUS便り 2017/6/5号参照）。

- 今回においてはソフトウェアのインストーラーのみならず、これらのソフトで生成される自己解凍アーカイブにも問題が発見されており、即ち古いバージョンで自己解凍アーカイブを作成していた場合に二次災害が広がる可能性もあったと言えます。

- 企業によっては、暗号化機能も持った自己解凍アーカイブの利用を義務付けるところもあるようですが、これに慣れきったところでうっかりマルウェアを実行してしまう恐れがあるという指摘もあり、利用については賛否両論があります。


窓の杜 WINDOWS FOREST

老舗の圧縮・解凍ソフト「Lhaz」「Lhaz+」に脆弱性、修正版が公開

インストーラーや自己解凍書庫に検索パスの問題があり、意図しないDLLを読み込む恐れ

橋井 秀人　2017年7月3日 16:16

老舗の圧縮・解凍ソフト「Lhaz」v2.5.0および「Lhaz+」v3.5.0が、1日に公開された。本バージョンはそれぞれ2件の脆弱性を修正したセキュリティアップデートとなっているので、更新を怠らないようにしたい。

「Lhaz」は、書庫ファイルの圧縮・解凍・閲覧・テストを行うシンプルなツール。ファイルの右クリックメニューから簡単に書庫ファイルを操作できるほか、書庫ファイルを解凍せずに内容を閲覧することが可能。外部DLLを導入しなくても、アプリケーション単体で主要な書庫ファイル形式をサポートしているのも魅力だ。さらに「Lhaz+」では、“Google ドライブ”“OneDrive”“Dropbox”といったクラウドストレージを扱うことができる。

「Lhaz」v2.5.0

「Lhaz+」v3.5.0

- Lhazで自己解凍アーカイブを作成することがない限りは脆弱性のあるファイルを拡散してしまうことはないでしょうが、必ず最新版にアップデートしておきましょう。