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。

●JR西日本、特別列車運行ダイヤ情報サイトが改ざん クレジットカード情報詐取サイトへ誘導

https://www.yomiuri.co.jp/national/20190903-OYT1T50283/

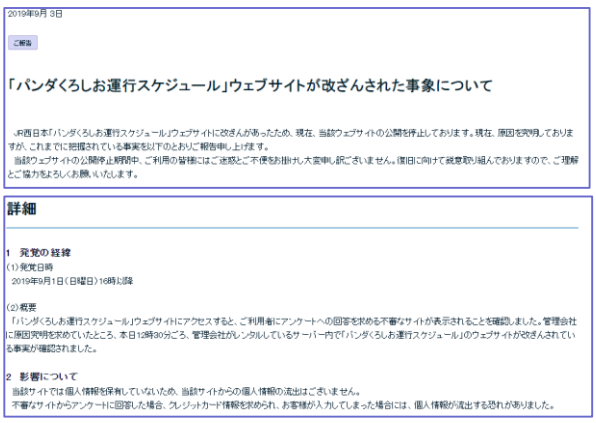
https://www.westjr.co.jp/press/article/2019/09/page_14812.html

このニュースをザックリ言うと・・・

- 9月3日(日本時間)、JR西日本より、「特急くろしお」の特別列車「パンダくろしお」の運行ダイヤを掲載するWebサイトが改ざんされていたと発表されました。
- 改ざんは同1日16時以降に発覚したもので、同2日17時頃に閉鎖するまでの間、サイトへのアクセスにより、アンケートを装ってクレジットカード番号などの入力を求める外部のサイトにリダイレクトする恐れがあったとのことです。
- 当該サイトでは個人情報を保持しておらず、サイト自体からの個人情報の流出はなかったとする一方、フィッシングサイトのアンケートに回答した場合には個人情報が流出した可能性があるとしています。

AUS便りからの所感等

- Webサイトの改ざん自体は今も世界中で多く発生していますが、目的は「閲覧者へのマルウェア感染」「外部との不審な通信を行うボットの埋め込み」あるいは今回のような「フィッシングサイトへの誘導」等様々です。
- また今回のケースに類似した例としては、今年5月にも東京都教育委員会のサイトが同様の改ざん被害を受けています。(AUS便り 2019/5/27号参照)
- 改ざんが発生した経路は現時点で不明ですが、これも「プログラムの脆弱性を突かれた」「管理画面やWeb以外のサービスから不正ログインされた」あるいは「管理者のクライアントPCがマルウェアに感染し踏み台にされた」等多くのケースが考えられ、各々について確実にセキュリティ対策を行っておくこと、改ざんの発生を速やかに検知できるサービス等を導入すること、また万が一の改ざん発生からの復旧についてもバックアップ等の準備を行っておくことを推奨致します。
- 閲覧する側としても、Webブラウザーやアンチウイルスあるいはは UTM等のセキュリティ機能によって防御するとともに、不審なサイトへの誘導やポップアップの表示についてネット上での報告がないか調べる慣習をつけることが肝要です。


2019年9月3日

ご報告

「パンダくろしお運行スケジュール」ウェブサイトが改ざんされた事象について

JR西日本「パンダくろしお運行スケジュール」ウェブサイトに改ざんがあったため、現在、当該ウェブサイトの公開を停止しております。現在、原因を究明しておりますが、これまでに把握されている事実を以下のとおりご報告申し上げます。
当該ウェブサイトの公開停止期間中、ご利用の皆様にはご迷惑とご不便をお掛けし大変申し訳ございません。復旧に向けて鋭意取り組んでおりますので、ご理解とご協力をよろしくお願いいたします。

詳細

1 発覚の経緯
(1)発覚日時
2019年9月1日(日曜日)16時以降

(2)概要
「パンダくろしお運行スケジュール」ウェブサイトにアクセスすると、ご利用者にアンケートへの回答を求める不審なサイトが表示されることを確認しました。管理会社に原因究明を求めていたところ、本日12時30分ごろ、管理会社がレンタルしているサーバー内で「パンダくろしお運行スケジュール」のウェブサイトが改ざんされている事実が確認されました。

2 影響について
当該サイトでは個人情報を保有していないため、当該サイトからの個人情報の流出はございません。
不審なサイトからアンケートに回答した場合、クレジットカード情報を求められ、お客様が入力してしまった場合には、個人情報が流出する恐れがありました。

●企業の半数近くがまだ「Windows 7」を利用…サポート終了は2020年1月

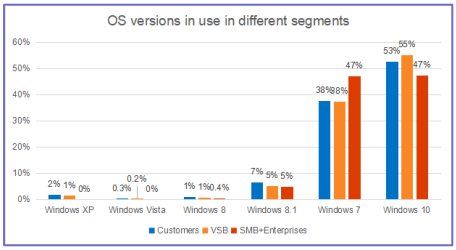
https://japan.cnet.com/article/35142049/
https://usa.kaspersky.com/about/press-releases/2019_consumers-still-use-unsupported-and-near-end-of-life-os

このニュースをザックリ言うと・・・

- 8月26日(現地時間)、セキュリティベンダーのカスペルスキー社より、企業の半数近くが依然としてWindows 7(以下Win7)を使用しているという調査結果が発表されました。
- 調査結果によれば、中小～大企業のPCでWindows 10(以下Win10)を使用している割合は約47%である一方、Win7の割合も同じく約47%となっています。
- また零細企業でもWin10の55%に対しとWin7は38%、同じく消費者のPCでもそれぞれ53%と38%という結果が出ています。

AUS便りからの所感等

kaspersky



- 当AUS便りでも度々言及しているとおり、Win7は2020年1月14日に一般のサポート終了を予定しており、2023年1月まで提供される有償の延長サポートも大企業向けエディションに限られています(AUS便り 2018/9/18号参照)。
- 調査結果を取り上げたCNETの記事では、2017年5月に発生したワーム「WannaCry」の影響を最も受けたのがWin7であることや、Win7以前で確認され、本来サポートが終了しているWindows XPにもパッチが提供された脆弱性「BlueKeep」の例が挙げられ、2020年以降にこういった致命的な脆弱性等が発生したとしても無防備になるとしています。
- 組織内でWin7を使用しているPCを把握するとともに、それぞれのPCについて、サポート終了前にWin10へのアップデートや新しいPCへの移行を行うか、あるいは移行できないものについてはアンチウイルス・UTMによる厳重な防御を行うとともに隔離したネットワークに配置ないしオンラインから切断するか、今からでも処置について計画すべきです。

●Google Playから「広告を見終わるまで閉じられない」アドウェア85個削除…計800万回以上ダウンロード不正ログイン

https://japan.cnet.com/article/35141476/
https://news.mynavi.jp/article/20190819-879228/
https://blog.trendmicro.co.jp/archives/22313

このニュースをザックリ言うと・・・

- 8月16日(米国時間)、トレンドマイクロ社より、Google公式のアプリストア「Google Play」においてアドウェア「AndroidOS_Hidenad.HRXH」が組み込まれた85個のAndroid向けアプリを確認したと発表されました。
- 問題のアプリは「Magic Camera: Make Magical Photos」「Blur Photo Editor」「BackgroundReplacement」「Find the difference: smart detective」「Color House2019」等といったゲームアプリや写真ツールで、インストールしたデバイス上で広告を頻繁に(5分間隔等)表示する上、広告を最後まで見ないと画面を閉じられない等の特徴があったとのことです。
- アプリは同社の報告によって既に削除されており、計800万回以上ダウンロードされたとみられています。

AUS便りからの所感等


図1:アドウェアが埋め込まれた不正アプリの例

- アプリは自らがアンインストールされにくくするよう、インストールされた30分後に密かに自分のアイコンをショートカットに差し替える等、巧妙な手口をとるとされています。
- トレンドマイクロ社をはじめセキュリティベンダーがAndroid向けセキュリティツールを場合によっては無償でも提供していますが、これを使用するか否かに拘らず大切なのは、事前にアプリストアでのレビューやSNS等での評判を参考としつつ、インストールするAndroidアプリを最小限に留めることにより、可能な限りマルウェアからの脅威を回避することです。

TREND MICRO

- Android 8.0以降では、アプリによるショートカット作成時に確認を求める機能により気付きやすくなっているとのことで、こういった機能を持つより新しいバージョンへのアップデートもまた、不正なアプリに対する根本的な対策として重要となってくるでしょう。