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。

●テレビ・ラジオ局Webサイトから個人情報流出相次ぐ、のべ110万件弱

http://itpro.nikkeibp.co.jp/atcl/news/16/042101194/
http://itpro.nikkeibp.co.jp/atcl/news/16/042301210/

このニュースをザックリ言うと・・・

- 東京のテレビ局とFMラジオ局のWebサイトから、個人情報の流出が2日間に相次いで発生し、それぞれのWebサイトにて「お詫び」が発表されました。

- 4月21日（日本時間）、日本テレビは、同社Webサイトが不正アクセスを受け、番組へのメッセージ投稿者やプレゼント応募者の個人情報（氏名、住所、電話番号、メールアドレス等）約43万件が流出した恐れがあると発表しました。

- 翌4月22日、FMラジオ局のJ-WAVEは、同様にWebサイトへの不正アクセスにより、約64万件の個人情報が流出した恐れがあると発表しました。

- いずれのケースも、Webサイトからのメッセージ投稿フォームに存在していた「OSコマンドインジェクション」の脆弱性を突かれたものとなっている模様です。

AUS便りからの所感等

- OSコマンドインジェクションとは、Webアプリケーションに対し細工したリクエストを送信することにより、Webサーバ上で任意のOSコマンドを不正に実行する攻撃であり、クロスサイトスクリプティング等と同様に古典的な脆弱性で、また任意のコマンドの実行により、今回のようなサーバ上に保存されている機密情報・個人情報の流出以外にも、第三者への攻撃の踏み台への悪用等の様々な行為が可能となる、非常に危険な脆弱性となります。

- 例えば、スクリプト言語で書かれたWebアプリケーションから、複雑な処理等を別のコマンドに実行させようとする場面で、安全でないコマンドの呼び出し方をしたり、リクエストの内容を十分にチェックしていなかった場合に脆弱性が存在し得ます。

- なお、今回のケースでは、不正アクセスの発生から検知・調査・発表まで比較的迅速に行われているようです。

- Webアプリケーションファイアウォール（WAF）やそれを搭載したUTMによる不審なリクエストの検知・遮断により、こういった攻撃から防御できることもあり、また、Webサーバから第三者への想定外のアクセスを防止する出口対策も重要でしょうが、根本的な対策としては、Webアプリケーションの脆弱性の修正が最終的には不可欠となります。


ニュース　日経コンピュータ

日テレWebサイトに不正アクセス、約43万件の個人情報流出の恐れ

2016/04/21
清嶋 直樹＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

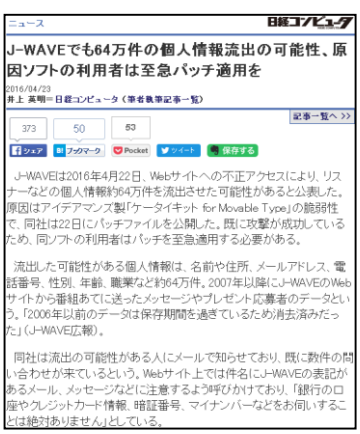
50　13　28

シェア　ブックマーク　Pocket　ツイート　保存する

日本テレビ放送網は2016年4月21日、同社のWebサイトが不正アクセス攻撃を受け、保有する個人情報のうち約43万件が流出した恐れがあると発表した。同社のニュース番組でも報じた。

日本テレビの説明によれば、4月20日13時頃から、ソフトウエアの脆弱性を突く不正アクセスがあった。ログ解析の結果、OSに対する不正な命令文を外部から紛れ込ませる「OSコマンドインジェクション」による攻撃だと判明した（関連記事：インジェクション系攻撃への防御の鉄則）。

流出した可能性がある個人情報は、氏名・住所・電話番号・メールアドレスなどで、約43万件分。バラエティー番組「踊る！さんま御殿！！」の視聴者からの「テーマ募集」への応募や、その他番組の視聴者プレゼントの応募に際して入力されたものなど、十数番組に関する応募情報に流出の可能性があるという。21日未明までに当該ソフトウエアを削除し、データを別の安全な保存場所に移動させるなどの対策を講じた。


ニュース　日経コンピュータ

J-WAVEでも64万件の個人情報流出の可能性、原因ソフトの利用者は至急パッチ適用を

2016/04/23
井上 英明＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

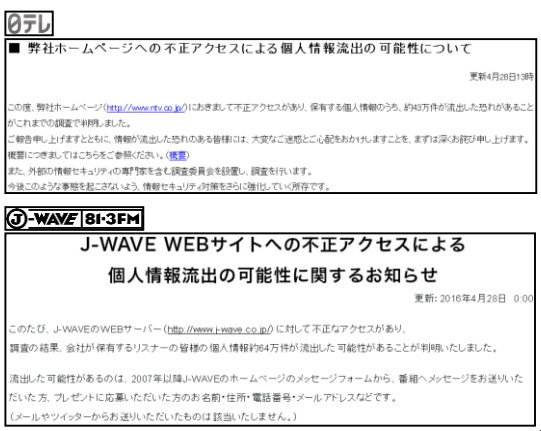
373　50　53

シェア　ブックマーク　Pocket　ツイート　保存する

J-WAVEは2016年4月22日、Webサイトへの不正アクセスにより、リスナーなどの個人情報約64万件を流出させた可能性があると公表した。原因はアイデアマンズ製「ケータイキット for Movable Type」の脆弱性で、同社は22日にパッチファイルを公開した。既に攻撃が成功しているため、同ソフトの利用者はパッチを至急適用する必要がある。

流出した可能性がある個人情報は、名前や住所、メールアドレス、電話番号、性別、年齢、職業など約64万件。2007年以降にJ-WAVEのWebサイトから番組あてに送ったメッセージやプレゼント応募者のデータという。「2006年以前のデータは保存期間を過ぎているため消去済みだった」（J-WAVE広報）。

同社は流出の可能性がある人にメールで知らせており、既に数件の問い合わせが来ているという。Webサイト上では件名にJ-WAVEの表記があるメール、メッセージなどに注意するよう呼びかけており、「銀行の口座やクレジットカード情報、暗証番号、マイナンバーなどをお伺いすることは絶対ありません」としている。


日テレ

■ 弊社ホームページへの不正アクセスによる個人情報流出の可能性について

更新4月28日13時

この度、弊社ホームページ（http://www.ntv.co.jp/）におきまして不正アクセスがあり、保有する個人情報のうち、約43万件が流出した恐れがあることがこれまでの調査で判明しました。
ご報告申し上げますとともに、情報が流出した恐れのある皆様には、大変なご迷惑とご心配をおかけしますことを、まずは深くお詫び申し上げます。
概要につきましてはこちらをご参照ください。（概要）
また、外部の情報セキュリティの専門家を含む調査委員会を設置し、調査を行います。
今後このような事態を起こさないよう、情報セキュリティ対策をさらに強化していく所存です。

J-WAVE 81・3FM

J-WAVE WEBサイトへの不正アクセスによる
個人情報流出の可能性に関するお知らせ

更新：2016年4月28日　0:00

このたび、J-WAVEのWEBサーバー（http://www.j-wave.co.jp/）に対して不正なアクセスがあり、
調査の結果、会社が保有するリスナーの皆様の個人情報約64万件が流出した可能性があることが判明いたしました。

流出した可能性があるのは、2007年以降J-WAVEのホームページのメッセージフォームから、番組へメッセージをお送りいただいた方、プレゼントに応募いただいた方のお名前・住所・電話番号・メールアドレスなどです。
（メールやツイッターからお送りいただいたものは該当いたしません。）

●落ちているUSBの約半数がPCに接続される･･･米での実験結果

http://www.gizmodo.jp/2016/04/post_664461.html

このニュースをザックリ言うと･･･

- 2015年4月末、米イリノイ大学において297個のUSBメモリを放置し、どれだけが拾われ、あるいはPCに接続されるかという実験が行われ、先日その結果に基づく論文が発表されました。

- USBメモリにはHTMLファイルが入っており、それを開くと実験である旨のメッセージが表示され、アンケート入力画面にアクセスする仕組みになっていたとのことです。

- 実験の結果、約半数にあたる45%のUSBメモリが誰かに拾われており（PCに接続され）、アンケート結果によれば、回答者の16%がアンチウイルスソフトでUSBメモリをスキャンした一方、使用しているPCのセキュリティ機能で保護してくれると考えていた人が8%いた、等とされています。

AUS便りからの所感等

- 不審なUSBメモリからのマルウェア感染は、メモリ上のファイルを開くだけでなく、接続時に発生するドライバの自動インストールにおいても発生する恐れがあります。

- 一見USB端子からは充電しか行わないように見えるケースでも油断はできず、2014年11月には、中国製のUSBで充電する電子タバコからマルウェアに感染したケースが報告されています（AUS便り 2014/12/01号参照）。

- こういった問題もあり、USBメモリ等を使わない、PCのUSBポートを塞ぐ等の防御策をとっている企業も多く、マルウェアの侵入を効果的に阻止し、安全にUSBデバイスを取り扱えるようOSレベルでのセキュリティ機能の向上が行われるまでは、せめてアンチウイルスによる感染の防御、万が一のマルウェア感染時に外部にデータが流出しないようUTMによる出口対策を行っておくべきでしょう。

GIZMODO

USBが落ちていたら、こっそり拾う？ 中も見ちゃう？

ふと足下を見ると、見慣れないUSBがあって、何かしらとコンピュータに繋いでみる…。

いえいえそんな情弱なことはしませんという人も、セキュリティ上ダメ、ゼッタイ。という人も…。これが結構やっちゃうみたいですよ。

実験が行なわれたのは、イリノイ大学アーバナ・シャンペーン校。297個のUSBを、教室や駐車場、カフェなど校舎内に撒き散らすという実験が行なわれました。USBの中身は、ノートや写真など、かなりプライベートなドキュメントに見せかけたHTMLファイルの数々。

ネットに接続されたコンピュータでそのままファイルを開くと、画面上では実験のネタバレが明かされ、そのままアンケート調査への回答を求められることになります。アカデミックな研究でも有り、且つドッキリのようなこの実験。さぁ一体どんな結果になったでしょう…？

●バングラデシュ中央銀行が不正送金被害･･･システムにはファイアウォール設置せず

http://japan.zdnet.com/article/35081781/

このニュースをザックリ言うと･･･

- 今年2月、バングラデシュ中央銀行のシステムが不正アクセスを受け、保有していたニューヨーク連邦準備銀行の口座から現金が外部へ不正送金される事件が発生しました。

- 攻撃者はターゲットとなる口座から9億5100万ドルの不正送金を試み、全額の送金こそ阻止されたものの、8100万ドルがフィリピンの口座へ送金されてしまった模様です。

- バングラデシュ警察によれば、同銀行のシステムには「ファイアウォール」と呼べるものが存在せず、世界中の銀行や金融機関との取引に用いられる国際銀行間通信協会（SWIFT）のシステムとの接続には中古の安価なスイッチ（ネットワークスイッチ）が使用されている状況だったとのことです。

AUS便りからの所感等

- 一国の中央銀行のシステムがこれほどお粗末なものでは、おそらく攻撃を受けていたことや、通常は有り得ないような不審な送金があったことにも自分たちでは気付かないでいた可能性もあり、事実、不正送金を食い止められたのも、いくつかの送金経路の途中の銀行で送金先口座のスペルミスがあったことに気付かれたことがきっかけでした。

- 不正アクセスを自分たちで検知し、侵入あるいは侵入されてからの行動を遮断するためにも、システム・ネットワークへのUTM等セキュリティ機器の導入は決して怠ってはならないことと言えます。

ZDNet Japan

バングラデシュ中銀の不正送金被害--中銀の粗末なセキュリティ、SWIFTソフトに侵入の可能性が明らかに

Charlie Osborne（ZDNet.com）翻訳校正：編集部 2016年04月26日 11時59分

バングラデシュ中央銀行が保有するニューヨーク連邦準備銀行の口座から8000万ドルが盗み出された事件で、バングラデシュ中央銀行のセキュリティが無防備であったこと、そして、ハッカーが国際銀行間通信協会（Society for Worldwide Interbank Financial Telecommunication：SWIFT）のソフトウェアに不正侵入した可能性があることが分かってきた。

バングラデシュ警察の犯罪捜査部門におけるForensic Training Instituteの責任者Shah Alam氏が米国時間4月22日付のReutersの記事で語ったところによると、同銀行のコンピュータシステムにはファイアウォールと呼べるものが存在せず、世界中の銀行や金融機関との取引に用いられるSWIFTのシステムとの接続には中古の安価なスイッチが使用されていたという。

攻撃が実行に移されたのは2016年2月のことだった。サイバー犯罪者のグループは、同銀行の従業員とトランザクションの動きを監視するために、中央処理システムに監視系のトロイの木馬を感染させ、数週間にわたって情報を収集していたと考えられている。