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。

●Androidスマホ等を狙うランサムウェアが日本上陸と発表･･･シマンテック

http://ascii.jp/elem/000/001/144/1144829/
http://www.symantec.com/connect/ja/blogs/android-32

このニュースをザックリ言うと･･･

- 4月4日（日本時間）、大手セキュリティベンダーのシマンテック社より、Androidデバイス（スマートフォン・タブレット等）に感染するランサムウェア「Android.Lockdroid」が日本に上陸したと発表がありました。

- Android.Lockdroidは3月11日に初めて確認され、ヨーロッパで広く拡散しているもので、アダルトサイトの広告のリンクをクリックしただけで感染する場合があり、またシステムアップデートと称して管理者権限を要求するものもあるとされています。

- 感染後の身代金要求メッセージは、各国の警察機関やインターポールを名乗って罰金支払いを命じるものとなっていますが、アジア諸国については日本語のメッセージ（日本にはない「国土安全保障省」を名乗ります）のみが確認されており、同社では、日本のユーザを標的にして他のアジア諸国向けの脅威をテストしている段階と推測しています。

- 同社では、「モバイル向けセキュリティソリューションを導入する」「アプリは信頼できるソースだけからインストールする」「モバイルアプリがリクエストする許可の種類に注意する」「デバイスのバックアップをまめに作成する」「ソフトウェアは最新の状態に保つ」ことを推奨しています。

AUS便りからの所感等

- 3月にMac OS X初の完全体なものとされる「KeRanger」が発見される（「AUS便り2016/03/22号」参照）等、ランサムウェアについても、これまでに現れた様々なマルウェアと同様、OS・デバイスの種類に関わらず脅威となりつつあります。

- シマンテック社が推奨するように、スマートフォンに対してもPCと同様にセキュリティソフトウェアを導入することや、各種行動に注意を払うことは重要ですし、併せて可能な限りUTMへのVPN接続を経由しての外部接続を活用すべきでしょう。

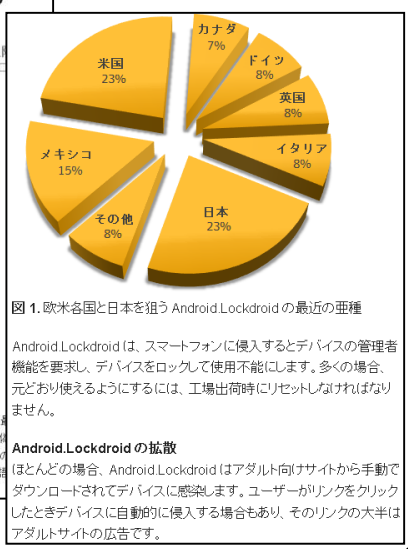


図 1. 欧米各国と日本を狙う Android.Lockdroid の最近の亜種

Android.Lockdroid は、スマートフォンに侵入するとデバイスの管理者機能を要求し、デバイスをロックして使用不能にします。多くの場合、元どおり使えるようにするには、工場出荷時にリセットしなければなりません。

Android.Lockdroid の拡散

ほとんどの場合、Android.Lockdroid はアダルト向けサイトから手動でダウンロードされてデバイスに感染します。ユーザーがリンクをクリックしたときデバイスに自動的に侵入する場合もあり、そのリンクの大半はアダルトサイトの広告です。

●「Mobage」アカウント10万件以上に不正ログイン･･･1月上旬から発生か

http://internet.watch.impress.co.jp/docs/news/20160401_751350.html

このニュースをザックリ言うと･･･

- 4月1日（日本時間）、株式会社ディー・エヌ・エー（DeNA）より、同社が運営するゲーム・SNSサイト「Mobage」の最大104,847アカウントが不正ログインの被害を受けていたことが発表されました。

- 不正ログインは、海外の同一端末とみられるIPアドレスから、少なくとも1月9日から4月1日にかけて行われており、ユーザのニックネーム・生年月日・性別・都道府県名等のプロフィール、およびお気に入りゲームのリスト等を閲覧された可能性、またはメールアドレスを変更された可能性があるとされています。

- 同社では、他社サービスから流出したアカウント情報が試行されたものとみており、不正ログインやメールアドレス変更が行われた各アカウントに対し、パスワードの初期化やメールアドレスの復旧と、個別連絡の対応を行っています。


INTERNET Watch
ニュース
「Mobage」に不正ログイン発生、最大10万4847アカウントで、1月上旬から継続
(2016/4/1 21:46)
株式会社ディー・エヌ・エー(DeNA)は1日、同社が運営するサービス「Mobage」において、第三者による不正ログインが行われていたことを公表した。
不正ログインが確認されたアカウントは、最大で10万4847件。ニックネーム、生年月日、性別などの登録プロフィールやお気に入りゲームのリストなどを閲覧された可能性があるという。ただし、氏名を含む個人情報やクレジットカード情報の閲覧は確認されておらず、また、仮想通貨などの不正購入も確認されていないとしている。
他社サービスから流出した可能性のあるID・パスワードによって、同じID・パスワードの組み合わせを使い回していたアカウントが不正ログインを受けてしまったものとみられてる。

AUS便りからの所感等

- 他社サービスから流出したアカウント情報による不正ログインの問題については、警視庁が摘発したサーバからのべ1800万人分の流出したアカウント情報が発見されたことが3月25日に発表された（「AUS便り 2016/04/04号」参照）ばかりであり、決して対岸の火事とは言えません。

- 有名サービス・小規模なサービスの区別なく、異なる、かつ推測されにくいパスワードを設定することを改めて推奨致します。

- アカウント情報を詐取するマルウェアの感染や、万が一感染を許した後の外部へのアカウント情報の送信を防御・検知するために、アンチウイルスやUTMの導入もまた必要でしょう。

●古いバージョンのWordPressとDrupalがパナマ文書漏洩に関与か

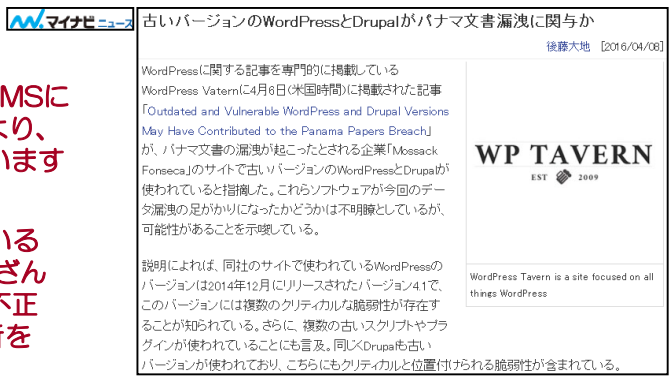
http://news.mynavi.jp/news/2016/04/08/046/

このニュースをザックリ言うと･･･

- 4月6日（米国時間）、WordPressに関する記事を掲載する「WordPress Tavern」より、「パナマ文書」と呼ばれる機密文書の流出元となったパナマの法律事務所Mossack Fonsecaのサイトで、脆弱性のあるバージョンのコンテンツ管理システム（CMS）を使用していたと発表がありました。

- 当該サイトで使用されていたCMSは、WordPressの他にもDrupalが挙げられており、いずれも複数のクリティカルな脆弱性が明らかになっているバージョンを使用していたとのことです。

- WordPress Tavernでは、これらが今回のデータ漏洩の足がかりになったかどうかは不明瞭としながらも、可能性があることを示唆している模様です。


マイナビニュース
古いバージョンのWordPressとDrupalがパナマ文書漏洩に関与か
後藤大地 [2016/04/08]
WordPressに関する記事を専門的に掲載しているWordPress Vatern(4月6日(米国時間)に掲載された記事「Outdated and Vulnerable WordPress and Drupal Versions May Have Contributed to the Panama Papers Breach」が、パナマ文書の漏洩が起こったとされる企業「Mossack Fonseca」のサイトで古いバージョンのWordPressとDrupalが使われていると指摘した。これらソフトウェアが今回のデータ漏洩の足がかりになったかどうかは不明瞭としているが、可能性があることを示唆している。
説明によれば、同社のサイトで使われているWordPressのバージョンは2014年12月にリリースされたバージョン4.1で、このバージョンには複数のクリティカルな脆弱性が存在することが知られている。さらに、複数の古いスクリプトやプラグインが使われていることにも言及。同じくDrupalも古いバージョンが使われており、こちらにもクリティカルと位置付けられる脆弱性が含まれている。
WP TAVERN EST 2009
WordPress Tavern is a site focused on all things WordPress

AUS便りからの所感等

- WordPressやDrupal等の知名度の高いPHPベースのCMSについては、2月にもセキュリティ専門機関JPCERT/CCより、PHPファイルを改ざんされる危険性について取り上げています（「AUS便り 2016/02/29号」参照）。

- 使用しているCMSを含め、それがインストールされているOS等を最新のバージョンに保つこと、かつファイルの改ざん等を目的としたSQLインジェクションや管理ページへの不正ログイン等攻撃の兆候を見出すためにアクセスログの分析を行うことは重要です。

- この他にも、情報流出の被害を最小限に食い止めるためのサーバ・ネットワーク構成の見直しは検討に値しますし、特に、CMSを社内サーバで運用している場合は、内外からの不正アクセスを検知・遮断するため、サーバをUTMによって仕切られたDMZ下に配置すると効果的でしょう。