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アプリ開発キットにバックドア(※)、14,000種のアプリと1億人のユーザに影響か

http://itpro.nikkeibp.co.jp/atcl/news/15/110903653/
http://blog.trendmicro.co.jp/archives/12540

このニュースをザックリ言うと･･･

- 11月6日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、Android用ソフトウェア開発キット（SDK）である「Moplus」を利用したアプリにバックドアが仕掛けられている可能性があるとして、警告が発表されました。

- 問題となっているMoplusは、サーチエンジンサービス等を提供する中国バイドゥ（百度、Baidu）(※)社によるもので、当初トレンドマイクロ社はMoplusの脆弱性調査のために解析を行っていたところ、バックドア機能の存在を確認したとのことです。

- トレンドマイクロ社では、Moplusを組み込んだアプリを14,112種（うちBaiduの公式アプリ4,014種）確認、1億人のAndroidユーザが影響を受けるとしており、また、Moplusを利用して自動的・定期的にアプリをインストールさせる不正プログラム「ANDROIDOS_WORMHOLE.HRXA」の拡散も既に確認している模様です。

AUS便りからの所感等

- Moplusによるバックドアが有効になっているアプリを起動すると、スマートフォン上でサーバが立ち上がり、任意の攻撃者が指令を送信してスマートフォンを不正に操作することが可能になっていたとされています。

- セキュリティベンダー各社が提供するAndroid用アンチウイルスアプリを導入することを強く推奨するとともに、UTMを経由しての通信を行うことにより、端末への不正アクセスを遮断できる他、アプリから外部への不審な通信を捕捉できる可能性もあり、有効と言えるでしょう。

ニュース　日経コンピュータ

中国バイドゥのAndroid用SDKに外部操作可能なバックドア、約1億人に影響

2015/11/09
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 >>

トレンドマイクロは2015年11月6日、中国バイドゥ（百度、Baidu）が提供するAndroid用SDK（ソフトウエア開発キット）の「Moplus」に深刻なセキュリティ上の欠陥が確認されたとして、注意喚起する文書を出した。

Moplus SDKを利用して開発されたアプリを通じて、Android端末で特別なユーザー権限なしに「連絡先の追加」「偽メールの送信」「アプリのインストール」などを実行される恐れがあるという。約1億人のAndroidユーザーが影響を受けたとみられる。

トレンドマイクロは、「脆弱性について調査を進めたところ、Moplus SDK自体にバックドア機能が備わっており、必ずしもそれが脆弱性に由来または関連しているわけではないことが明らかになった」と説明している。バイドゥがMoplusに実装したのは、開発過程における不具合による「脆弱性」（欠陥）ではなく、意図的に外部操作を可能とする「バックドア」であるとの見方を示す。

IT用語辞典 e-Words

（※）バックドア【 backdoor 】

バックドアとは、裏口、勝手口という意味の英単語。ソフトウェアやシステムの一部として利用者に気付かれないよう秘密裏に仕込まれた、正規の利用者認証やセキュリティ対策などを回避してこっそり遠隔操作するための窓口のこと。

ネットワークを通じてシステムへの不正侵入に成功した攻撃者が、侵入に利用した脆弱性やアカウント情報などが失われても再び侵入できるよう設けることが多い。コンピュータウイルスが感染する際に、外部からの操作を受け入れるための窓口としてバックドアを設置する場合もある。

不正アクセスなどが確認された際に、悪用された個所の修正などに留まらず記憶装置の完全消去やOSの再インストールなどを行うべきとされるのは、バックドアを消去するためでもある。

また、システムの開発元や国家の情報機関などが、秘密裏に利用者の監視や情報の詐取などを行なうため、製品の開発時などにあらかじめバックドアを設ける場合もある。そのような事例では利用者側での対策は困難となる。

コトバンク

（※）百度　ばいどぅ　Baidu

中国最大手の検索サイト。中国では70%を超える圧倒的シェアを誇り、世界ランクでもGoogle、Yahoo!に次いで第3位につけている。ただし、13億人という中国の圧倒的な人口に支えられた数字で、国外での認知度は高いとは言えない。運営会社Baiduは、培われた2バイト文字(漢字)の検索技術を武器に、まずは日本市場でのシェア拡大を図っている。

会長兼CEOは、1968年北京市生まれのロビン・リー氏。留学先のアメリカでインフォシーク社の検索エンジンの設計、GO.comの画像検索エンジンの開発などに携わり、帰国後、2000年1月に百度公司(Baidu,Inc.)を設立した。同社の理念である「中国人のための中国語検索エンジン」(ロボット型)を大手ポータルサイトに提供し、翌01年にベータ版Baidu.comとして始動。わずか数年で中国最大の検索サイトに成長させた。05年には、米国ナスダック市場に上場。初日に記録的な高値をつけ、「中国のGoogle」として全米の注目を浴びた。

●国内70以上のサイトに身代金要求ウイルスが仕掛けられる

http://internet.watch.impress.co.jp/docs/news/20151102_728654.html

このニュースをザックリ言うと・・・

- 10月30日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、同29日以降に国内70以上のWebサイトが改ざんされているとして、同社ブログにて警告が発表されました。

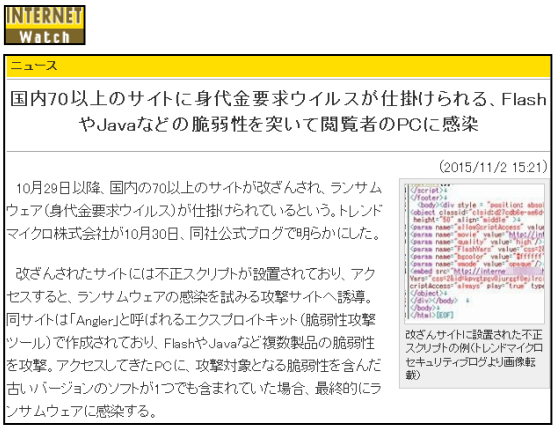
- 改ざんされたサイトは中小企業、各種学校、地域の団体、個人ページなど多岐にわたり、またいずれも同一の外部サーバからランサムウェア（感染したPCのファイルを人質に金銭等を要求するマルウェア）をダウンロードする不正なHTMLタグが埋め込まれていることから、全て同一犯による改ざんであると同社は推測しています。

- ランサムウェアはFlashやJavaなど複数の製品の脆弱性を攻撃する仕組みになっており、同社では既知の脆弱性への攻撃を100%防御するために、ブラウザを含め各種アプリケーションを最新バージョンに保つよう呼びかけています。

AUS便りからの所感等

- ランサムウェアへの感染によってファイルが暗号化されたら最後、犯人の要求に応じて身代金を支払う等を行ったとしてもファイルが確実に取り戻せる保証はなく、事実上ファイルが破壊されたに等しいことは当便りでも度々述べている通りです。

- 今回においては、未修正の脆弱性に対するゼロデイ攻撃を行うようなものは確認されていない模様ですが、過剰に安心することなく、上記の通りアプリケーションおよびOSを最新バージョンに保つ他、それができない場合やアップデートまでのタイムラグでの感染の可能性を少なからず抑制するため、アンチウイルスやUTMによる防御が効果的な対策となります。


INTERNET Watch

ニュース

国内70以上のサイトに身代金要求ウイルスが仕掛けられる、FlashやJavaなどの脆弱性を突いて閲覧者のPCに感染

(2015/11/2 15:21)

10月29日以降、国内の70以上のサイトが改ざんされ、ランサムウェア(身代金要求ウイルス)が仕掛けられているという。トレンドマイクロ株式会社が10月30日、同社公式ブログで明らかにした。

改ざんされたサイトには不正スクリプトが設置されており、アクセスすると、ランサムウェアの感染を試みる攻撃サイトへ誘導。同サイトは「Angler」と呼ばれるエクスプロイトキット(脆弱性攻撃ツール)で作成されており、FlashやJavaなど複数製品の脆弱性を攻撃。アクセスしてきたPCに、攻撃対象となる脆弱性を含んだ古いバージョンのソフトが1つでも含まれていた場合、最終的にランサムウェアに感染する。

改ざんサイトに設置された不正スクリプトの例(トレンドマイクロセキュリティブログより画像転載)

●国交省など8省庁、サポート切れソフト使用・・・会計検査院指摘

http://www.nikkei.com/article/DGXLASDG05H8P_W5A101C1CR0000/

このニュースをザックリ言うと・・・

- 11月6日（日本時間）、会計検査院が内閣に提出した「平成26年度決算検査報告」において、8省庁（内閣府(宮内庁)、総務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省）に対し、外部に公開しているサーバ上でサポート期間が終了しているソフトウェアを使用していたことを指摘、是正を指示したことを明らかにしました。

- 会計検査院が昨年4月に行った調査では、省庁の44の情報システムのうち21システムで同3月までにサポート期間が終了した4種類のソフトを使い続けており、中には約2年間サポート切れのまま使用され続けていたものもあったとのことです。

- また、対象となった各省庁は、今年7月までにソフトウェアの更新を完了するとともに、使用している各ソフトウェアのサポート期限情報を文書にまとめること等の処置をとったとのことです。

AUS便りからの所感等

- 会計検査院は以前にも、東京電力が既にサポート終了していたWindows XPを継続使用していたことを指摘しており、同社は今年4月までに更新を完了しています。

- 場合によっては、ソフトウェアの更新にかかる費用は莫大になり、実施に後ろ向きになるケースもあると思われますが、特に公開サーバについて攻撃への耐性を保ち、サーバへの侵入からの二次攻撃を抑止するためには、アンチウイルスやUTMの導入のみならず、ソフトウェアのアップデートが根本的な対策として重要となるでしょう。


日本経済新聞

Web刊 速報 ビジネスリーダー マーケット マネー テクノロジー ライフ スポーツ 映像 朝刊

全て 経済 企業 国際 政治 株・金融 スポーツ 社会 ニュース18時 その他ジャンル▼

速報

国交省など8省庁、サポート切れソフト使用　会計検査院指摘

2015/11/6 11:49

小 中 大 保存 印刷 リプリント ▼共有

国土交通省や厚生労働省など8省庁が、外部に公開するホームページ(HP)などでメーカーのサポート期限が切れたソフトウエアを使用していたことが6日、会計検査院の調べで分かった。ソフトの一部にはセキュリティー上の欠陥が確認されており、サイバー攻撃によるHPの改ざんや情報漏洩などの恐れがあったが、十分な対策が取られていなかった。

8省庁は他に総務省、経済産業省、文部科学省、農林水産省、環境省、宮内庁。各省庁は検査院の指摘を踏まえて7月までにソフトの更新などの対策を済ませた。これまでにサポート期限切れに伴う情報漏洩などの被害は確認されていないという。

検査院が昨年4月、インターネットに接続されている省庁の44の情報システムを調べたところ、21システムで同3月までにサポート期間が終了した4種類のソフトを使い続けていた。