— AUS（アルテミス・ユーザ・サポート）便り 2016/04/25号 —
http://www.artemis-jp.com

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。

●ゴールデンウィークにおける情報セキュリティに関する注意喚起、IPAが呼びかけ

http://www.ipa.go.jp/security/topics/alert280420.html

このニュースをザックリ言うと・・・

- 4月20日（日本時間）、独立行政法人情報処理推進機構（IPA）より、ゴールデンウィークを迎えるにあたり、情報セキュリティに関する注意喚起が発表され、以前に発表した「長期休暇における情報セキュリティ対策」をはじめとするセキュリティ対策に関する資料も示しています。

- システム管理者が長期間不在になることにより、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまう可能性、および従業員等が友人や家族と旅行に出かけた際のSNSへの書き込み内容から思わぬ被害が発生、場合によっては関係者にも被害が及ぶ可能性を指摘しています。

- 前述の資料では、組織内のシステム管理者やユーザに対し、休暇前・休暇中および休暇明けにとるべき対策のポイントを挙げており、例えば管理者に対しては、休暇前に「緊急連絡体制の確認」「使用しないサーバ機器の電源OFF」、休暇明けに「パッチの適用」「アンチウイルスパターンファイルの更新」「サーバの各種ログの確認」を呼びかけています。

- また、ユーザに対しては、業務対応等の理由で機器やデータを持ち出す必要がある場合、休暇前の「持ち出しルールの確認と遵守」、休暇中の「厳重な管理」および休暇明け時にはやはり「パッチの適用」「アンチウイルスパターンファイルの更新」そして「持ち出した機器やUSBメモリ等のウイルスチェック」を行うよう呼びかけています。

AUS便りからの所感等

- IPAの呼びかけは、「いつもとは違う状況になる」ことで通常時には生じにくい様々な問題にも早く確実に対応することへの注意を促すものとなっています。

- 通常は目立った行動をせず、休暇期間中を狙って、動作中のPC等で活動するマルウェアは決して珍しいものではありませんし、休暇明けにPCを開いてみたらあらゆるファイルがランサムウェアによって暗号化されていた、といった事態も有り得ない話ではありません。

- 今回の呼びかけでは、マルウェアによる脅威以外にも、「PCがWindows10に自動的にアップグレードしてしまい元のOSに戻すまで数時間パソコンを操作できない状況に陥った」という相談例も紹介されており、システムの可用性を考えるならばこれについても事前の対策は必要なものです。

- 以上の意味でも、UTMによるネットワークの防御、ソフトウェアのアップデートやアンチウイルス等を用いてのPCの防御、あるいは全てのユーザに対する随時のセキュリティ教育や情報の共有、いずれも必要不可欠なものと言えるでしょう。

●今度は「Amazon-co-jp .pw」に「amanozn .com」・・・Amazonを騙るフィッシングサイト確認

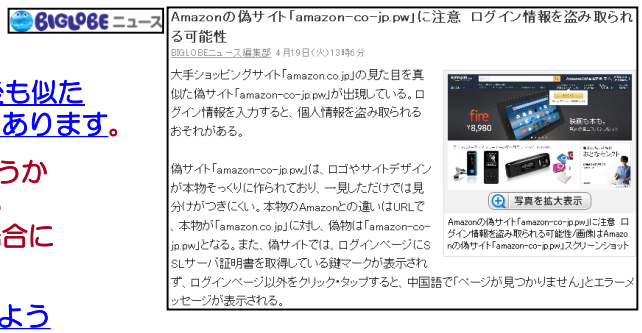
http://news.biglobe.ne.jp/it/0419/blnews_160419_7805521660.html

このニュースをザックリ言うと・・・

- 4月18日（日本時間）頃より、Amazon.co.jpを騙る新たなフィッシングサイトの存在がTwitter等で報告されています。

- １つは「amazon-co-jp .pw」というドメインで、ログインページが「https://」ではない、中国語のエラーメッセージが表示される、といった特徴があったとされています。

- 他にも「amanozn .com」というドメインのサイトも確認されており、「アカウントが一時的に停止されました」とするフィッシングメールでの誘導を行っていた模様です。


BIGLOBEニュース

Amazonの偽サイト「amazon-co-jp.pw」に注意 ログイン情報を盗み取られる可能性

BIGLOBEニュース編集部 4月19日(火)13時6分

大手ショッピングサイト「amazon.co.jp」の見た目を真似た偽サイト「amazon-co-jp.pw」が出現している。ログイン情報を入力すると、個人情報を盗み取られるおそれがある。

偽サイト「amazon-co-jp.pw」は、ロゴやサイトデザインが本物そっくりに作られており、一見しただけでは見分けがつきにくい。本物のAmazonとの違いはURLで、本物が「amazon.co.jp」に対し、偽物は「amazon-co-jp.pw」となる。また、偽サイトでは、ログインページにSSLサーバ証明書を取得している鍵マークが表示されず、ログインページ以外をクリック・タップすると、中国語で「ページが見つかりません」とエラーメッセージが表示される。

写真を拡大表示

Amazonの偽サイト「amazon-co-jp.pw」に注意 ログイン情報を盗み取られる可能性/画像はAmazonの偽サイト「amazon-co-jp.pw」スクリーンショット

AUS便りからの所感等

- 4月22日現在、各サイトとも閉鎖された模様ですが、今後も似たようなドメインでのフィッシングが行われる可能性は十分にあります。

- Amazon.co.jpでは「Amazon.co.jp からのEメールかどうかの識別について」（※）にて、フィッシングメールに関する注意点と、万が一メールのリンクをクリックしてしまった場合にコンピュータを保護する手順について示しています。

- ブラウザのブックマークから正規のサイトへアクセスするよう心がけることにより、フィッシングサイトへアクセスする可能性を抑制することが期待できますし、この他にも、ブラウザ・アンチウイルスソフトやUTM等のアンチフィッシング機能も有効化し、さらに防御を固めることを推奨します。

（※）https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=201304810

●WindowsやNASのファイル共有に影響する脆弱性

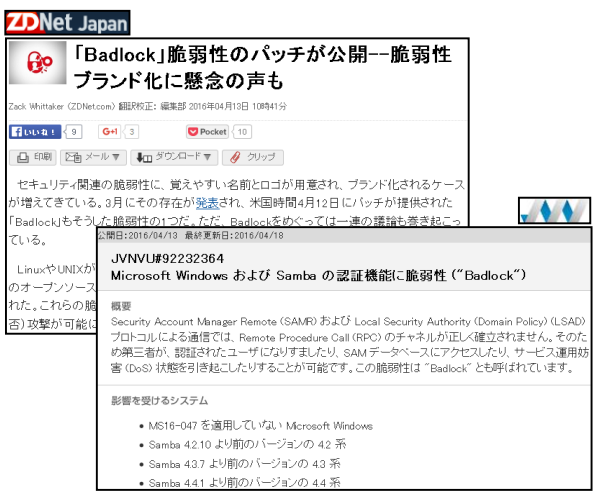
http://news.mynavi.jp/news/2016/04/08/046/
http://jvn.jp/vu/JVNVU92232364/

このニュースをザックリ言うと・・・

- 4月12日（米国時間）、Windows、および、NASのファイル共有機能等を提供するサーバソフトウェア「Samba」において、共通する脆弱性の存在が明らかになり、それぞれ修正パッチがリリースされました。

- WindowsではMSセキュリティ情報「MS16-047」でセキュリティパッチがリリースされ、またSambaについても修正バージョンがリリースされています。

- いわゆる中間者攻撃によるユーザのなりすまし、あるいはサービス拒否攻撃等が可能になる複数の脆弱性は、まとめて「Badlock」と呼称され、3月末の時点で、発見者により、パッチがリリースされるこの日に詳細を発表することが予告されていました。


ZDNet Japan

「Badlock」脆弱性のパッチが公開--脆弱性ブランド化に懸念の声も

Zack Whittaker（ZDNet.com）翻訳校正：編集部 2016年04月13日 10時41分

いいね！ 9 G+ 3 Pocket 10

印刷 メール ダウンロード クリップ

セキュリティ関連の脆弱性に、覚えやすい名前とロゴが用意され、ブランド化されるケースが増えてきている。3月にその存在が発表され、米国時間4月12日にパッチが提供された「Badlock」もそうした脆弱性の1つだ。ただ、Badlockをめぐっては一連の議論も巻き起こっている。

LinuxやUNIXが
のオープンソース
れた。これらの脆
否）攻撃が可能に

公開日:2016/04/13 最終更新日:2016/04/18

JVNVU#92232364
Microsoft Windows および Samba の認証機能に脆弱性（“Badlock”）

概要

Security Account Manager Remote (SAMR) および Local Security Authority (Domain Policy) (LSAD) プロトコルによる通信では、Remote Procedure Call (RPC) のチャネルが正しく確立されません。そのため第三者が、認証されたユーザになりすましたり、SAM データベースにアクセスしたり、サービス運用妨害 (DoS) 状態を引き起こしたりすることが可能です。この脆弱性は “Badlock” とも呼ばれています。

影響を受けるシステム

- MS16-047 を適用していない Microsoft Windows
- Samba 4.2.10 より前のバージョンの 4.2 系
- Samba 4.3.7 より前のバージョンの 4.3 系
- Samba 4.4.1 より前のバージョンの 4.4 系

AUS便りからの所感等

- 脆弱性の存在する箇所からみるに、攻撃の多くは内部LAN上にて行われる可能性が高いとみられます。

- Windows、Sambaをインストールしているlinux等において、アップデートを行うのはもちろん、NASの多くはSambaを採用しているとみられますので、ベンダーサイトにおいて対策の要・不要やファームウェアのアップデートを確認する必要があるでしょう。

- また、ファイルサーバの不要なポートにアクセスされないよう、クライアントPC等と同一のLANではなく、UTM等を隔てた別のセグメントに配置することも検討すべきでしょう。