— AUS（アルテミス・ユーザ・サポート）便り 2016/05/23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。

●機密情報が匿名FTPサーバで公開されている恐れ･･･LACより注意喚起

http://internet.watch.impress.co.jp/docs/news/20160513_757285.html
http://www.lac.co.jp/security/alert/2016/05/13_alert_01.html

このニュースをザックリ言うと･･･

- 5月13日（日本時間）、国内大手セキュリティベンダーのラック社より、国内の約3,400の組織・個人について、インターネットに接続されているサーバで取引先情報・社員の個人情報等の機密情報が意図せず公開されているとみられるケースを複数確認したとして、警告が発表されました。

- 問題となっているのは、FTPサーバによるファイル保管において、ID・パスワードが不要な匿名FTP（anonymous(アノニマス) FTP）によるサーバへのアクセスが可能なケースであり、営業秘密に該当し得る「請求書」や「見積書」の他、「年賀状送り先一覧」「従業員名簿」および「メールのバックアップ」といった個人情報も閲覧可能だったとされています。

- 同社では2006年にも同様の注意喚起を行っていますが、こういった問題の背景として、「過去に使っていたFTPサーバが放置されている」「社員が自宅などで作業するため個人でFTPサーバを設置している」等を挙げています。

- また、このような不正な公開により「取引先から情報管理の責任を問われる」「標的型攻撃に悪用される」といった恐れがある他、万が一、匿名FTPでのデータ書き込みが可能な設定の場合には、第三者によるファイル置き場として利用される恐れもあるとしており、その上で、FTPサーバの設置・運用状況を確認し、不適切な設定でないか、そもそも業務に必要か等の洗い出しを行うことを呼び掛けています。

AUS便りからの所感等

- FTPは1970年代から使われている古典的なファイルアップロード・ダウンロードの手法であり、今日ではより新しくセキュアな手段の方をまずは検討すべきでしょうし、例えば、クラウドストレージの利用でも、対策を十分に講じ適切に使用する限りではよほど安全という見方もあります。

- 通常使わないサービスやアクセス経路を「有効なままにしない」ことはサーバをセキュアに保つための基本的で重要なポイントであり、この他、VPS等であればOSのファイアウォール機能を有効にすること、社内ネットワーク上のサーバは可能な限り前面にUTM等の設置を行うことも大切です。


INTERNET Watch

10年経っても根絶されず――匿名FTPサーバーで請求書や従業員名簿を公開していないか、改めて確認を

(2016/5/13 14:31)

株式会社ラックは13日、ID・パスワード不要で誰もがログインできる匿名FTPサーバー上で、取引先一覧などの重要情報が公開されている例が複数確認されたと発表した。権限設定のミス、サーバーの放置などが原因とみられ、ネットワーク管理者に改めて注意を呼び掛けている。

/pub/eigyou/share/ のインデックス

名前	サイズ	更新日
親ディレクトリ		
A社御向けご提案/		2016/04/03 19:27:00
B社御向けご提案/		2016/04/04 22:29:00
提案資料.xlsx	203.0 kB	2016/04/03 19:29:00
原価一覧.xlsx	30.2 MB	2016/04/04 22:57:00
s-IR.gz	37.7 kB	2016/04/28 1:12:00

匿名FTPサーバーで内部情報を公開してしまっている例(イメージ)

今回ラックが確認したのは、ファイル保管用のFTPサーバーの中でも、パスワード入力せずにアクセスできる匿名FTPサーバーによる事例。インターネット利用者であれば事実上、誰でもファイルをダウンロードできてしまうため、個人情報・社内情報などを保存する場所としては適さない。

ラックによると、約3400の国内組織ないし個人の情報が公開状態となっていた。その大部分は公開しても差し支えない情報だったが、請求書や見積書、年賀状送り先一覧、従業員名簿、メールのバックアップといった情報が含まれるケースもあったという。なお、管理が不十分な匿名FTPサーバーを公開していたのは、個人以外では中小企業がほとんどで、大企業や政府系機関では確認できなかったとしている。


LAC 株式会社ラック

注意喚起情報

匿名FTPサーバで重要情報が公開されていることへの注意喚起

2016年05月13日

いいね！ シェア ツイート

本注意喚起をダウンロードして読む方は PDF版

ラックではこのほど、インターネットに接続されたサーバから、取引先情報や社員の個人情報などが意図せず公開されているとみられるケースを複数確認しました。情報管理のあり方が厳しく問われる昨今、組織の内部情報に外部の誰もがアクセスできる状態を放置すれば、取引の縮小や停止、社会的信用の低下を招き、経営危機に直結する事態にも発展しかねません。経営層の方々は以下の情報を参考に、自組織でアクセス管理が不十分なサーバが公開状態になっていないか早急に確認することをお勧めします。

内部情報が公開状態となっているのは、ファイルをやり取りするための「ファイル転送サーバ（FTPサーバ）」のうち、パスワードを入力せずに外部からアクセスできる「匿名FTPサーバ（anonymous FTPサーバ）」です。匿名FTPサーバ自体はインターネット黎明期から存在する情報共有手段の一つですが、近年は他の手段の多様化により利用されなくなりつつあります。

情報が公開状態となっていたのは国内の約3400組織・個人で、大部分は公開しても差し支えないとみられる情報でしたが、中には営業秘密に該当し得る請求書や見積書のほか、年賀状送り先一覧、従業員名簿、メールのバックアップといった個人情報も含まれていました。

●マルウェア作者が狙うOfficeの脆弱性は4年前のもの･･･Sophos

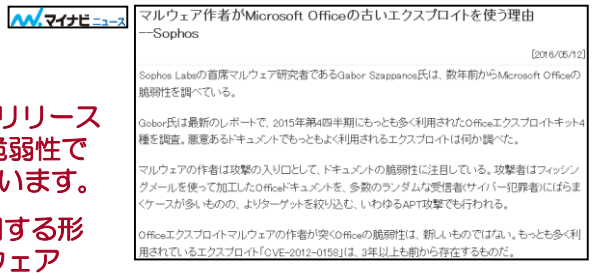
http://news.mynavi.jp/news/2016/05/12/106/

このニュースをザックリ言うと･･･

- 5月5日（現地時間）、大手セキュリティベンダーの英Sophos社の首席マルウェア研究者Gabor Szappanos氏より、Microsoft Officeの脆弱性を狙うマルウェアの傾向に関する見解がブログで発表されました。

- 2015年第4四半期に最も多く利用されたOfficeに対するエクスプロイトキット（さまざまな脆弱性を攻撃するためのパッケージ化されたプログラム）4種を調査したところ、最もターゲットにされていた脆弱性は「CVE-2012-0158」（2012年4月に発表された「MS12-027」でパッチがリリースされていたもの）であり、全体の48%を占めていたとのことです。

- Gabor氏は、こういった既にパッチが出ている古い脆弱性を狙うエクスプロイトが依然多く使われる理由を「かなりの比率で機能するから」としており、防御策として「パッチをすぐに当てる」「セキュリティソフトウェアを最新のものに更新する」「迷惑メールの添付ファイルを開かない」「簡素化したドキュメントビューアの利用を検討する」ことを挙げています。


マイナビニュース
マルウェア作者がMicrosoft Officeの古いエクスプロイトを使う理由
―Sophos
[2016/05/12]
Sophos Labsの首席マルウェア研究者であるGabor Szappanos氏は、数年前からMicrosoft Officeの脆弱性を調べている。
Gabor氏は最新のレポートで、2015年第4四半期にもっとも多く利用されたOfficeエクスプロイトキット4種を調査、悪意あるドキュメントでもっともよく利用されるエクスプロイトは何か調べた。
マルウェアの作者は攻撃の入り口として、ドキュメントの脆弱性に注目している。攻撃者はフィッシングメールを使って加工したOfficeドキュメントを、多数のランダムな受信者(サイバー犯罪者)にばらまくケースが多いものの、よりターゲットを絞り込む、いわゆるAPT攻撃でも行われる。
Officeエクスプロイトやマルウェアの作者が突くOfficeの脆弱性は、新しいものではない。もっとも多く利用されているエクスプロイト「CVE-2012-0158」は、3年以上も前から存在するものだ。

AUS便りからの所感等

- CVE-2012-0158はOffice 2003～2010に対しパッチがリリースされている他、Office以外からも利用されるコンポーネントの脆弱性であることから、SQL Server 2000～2008等にも影響するとされています。

- あくまで推測ですが、Office2013以降は個々のパッチを適用する形ではなくなったことで、最新の状態である可能性が高いとマルウェア作者は判断し、Office2010以前に的を絞っているのではとも考えられ、一方でOffice2003以前のバージョンは既にサポート期限が切れており、これもまたマルウェアの格好の餌食となる恐れがあります。

- 可能な限りサポートされているバージョンを使用し、全てのパッチを適用した状態を保つようにすることが最も大事であり、加えてアンチウイルスやUTMによる防御を重ねて実施することも重要です。

●Amebaに不正ログイン5万件･･･リスト型攻撃受け、全ユーザにパスワード変更呼び掛け

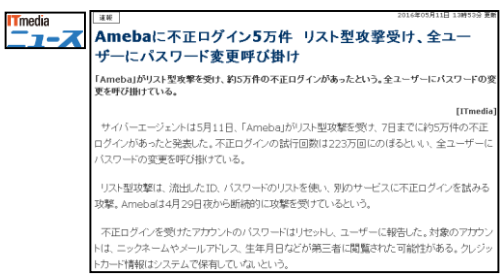
http://www.itmedia.co.jp/news/articles/1605/11/news108.html

このニュースをザックリ言うと･･･

- 5月11日（日本時間）、サイバーエージェント社は、同社が運営するサービス「Ameba」が不正ログインの被害を受けたと発表しました。

- いわゆる「リスト型攻撃」によるログイン試行が4月29日夜から5月7日夕方まで約220万回実行されており、うち50,905件のアカウントについてログインされた模様ではあるものの、アカウントの登録情報の改ざんは確認されなかったとのことです。

- 同社では被害を受けたアカウントのパスワードリセットを行い、ユーザに対し再設定を依頼するメールを送っている他、被害を受けなかったユーザに対してもパスワードの変更を推奨しています。


ITmedia ニュース
速報
Amebaに不正ログイン5万件 リスト型攻撃受け、全ユーザーにパスワード変更呼び掛け
「Ameba」がリスト型攻撃を受け、約5万件の不正ログインがあったという。全ユーザーにパスワードの変更を呼び掛けている。
[ITmedia]
サイバーエージェントは5月11日、「Ameba」がリスト型攻撃を受け、7日までに約5万件の不正ログインがあったと発表した。不正ログインの試行回数は223万回にのぼるといい、全ユーザーにパスワードの変更を呼び掛けている。
リスト型攻撃は、流出したID、パスワードのリストを使い、別のサービスに不正ログインを試みる攻撃。Amebaは4月29日夜から断続的に攻撃を受けているという。
不正ログインを受けたアカウントのパスワードはリセットし、ユーザーに報告した。対象のアカウントは、ニックネームやメールアドレス、生年月日などが第三者に閲覧された可能性がある。クレジットカード情報はシステムで保有していないという。

AUS便りからの所感等

- リスト型攻撃による大規模な不正ログイン事件は2014年5月以降多くのサービスで断続的に発生していて、当AUS便りでも度々取り上げておりますが、Amebaは2014年6月にも、約38,000件のアカウントに不正ログインされる被害を受けています。

- 関連する出来事としては、ロシア人クラッカーがGmailやYahoo!等のメールアカウントとパスワードの情報約2億7200万件を流出させたと報じられたものの、ほとんどは古いデータであり、パスワード変更済みで無効なものだったという一幕もありました（http://gigazine.net/news/20160506-big-data-breache-found-major-email-service/）。

- ともあれ、こういった事件のたびに申し上げていることですが、万が一あるサービスでアカウント流出が発生した場合に、他のサービスにまで連鎖的に不正ログインされないためにも、推測されにくいパスワード、サービス毎に少しでも異なるパスワードを用いることが重要です。