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。

●押収されたプロキシサーバに506万件の個人情報

http://www.asahi.com/articles/ASH4K318RH4KUTIL003.html
http://www.47news.jp/CN/201504/CN2015041701001304.html
http://www3.nhk.or.jp/news/html/20150417/k10010051521000.html

このニュースをザックリ言うと・・・

- 4月17日（日本時間）、警視庁は、同庁が昨年11月に摘発した不正アクセス禁止法違反事件で都内サーバ管理会社から押収したプロキシ(中継)サーバに、「のべ約785万件、重複を省いたものでも約506万件のID・パスワードを含めた個人情報」が保存されていたことを発表しました。

- 当該サーバからは、保存された個人情報を入力してショッピングサイトや無料通信アプリに不正ログインを試みる「攻撃ツール」も発見され、約5万9千件の個人情報についてログインに成功し、不正に買い物等を行ったとみられています。

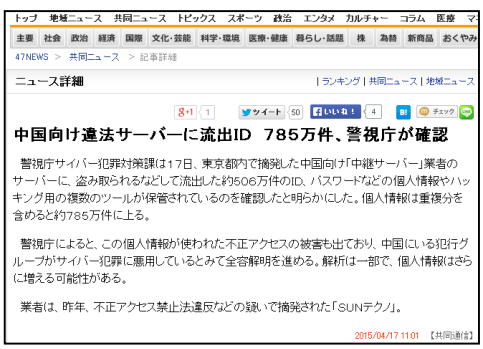
- 警視庁では、不正ログインに成功したアカウントは「同じパスワードを複数のサイトで使い回していたもの」とみて、パスワードの使い回しを避けるよう呼びかけています。

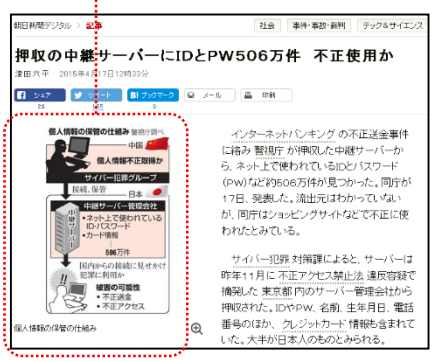
AUS便りからの所感等

- 個人情報を詐取されたケースの多くは、今回呼びかけられているパスワードの使い回しを狙われたものや、偽のフォームを表示するWebサイトやマルウェアによるものと考えられ、いずれも昨年あるいはそれ以前から度々報道で取り上げられています。

- 前者のケースについては、特に金銭が絡むサービス等の重要なアカウントについて、それぞれ異なる推測されにくいパスワードを設定することが重要であり、場合によってはパスワード管理ツールの導入も検討に値するでしょう。

- 後者のケースについては、マルウェアの感染あるいはフィッシングサイトへのアクセス遮断のため、アンチウイルスやUTMの導入が重要であり効果的です。





●Windowsサーバをダウンさせる脆弱性の攻撃コード出回る、速やかにパッチ適用を

https://www.ipa.go.jp/security/ciadr/vul/20150415-ms.html
https://technet.microsoft.com/library/security/MS15-034

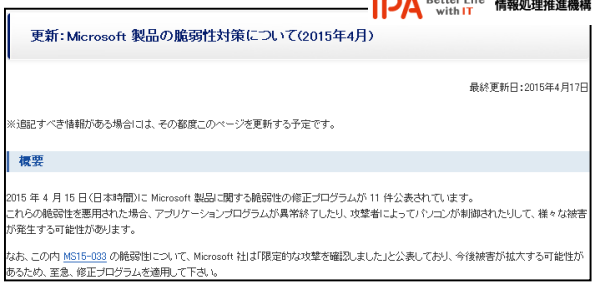
このニュースをザックリ言うと・・・

- 4月15日（日本時間）に発表された定例のマイクロソフトセキュリティ情報において、Windowsサーバをダウンさせること等が可能な脆弱性「MS15-034」の存在が明らかになりました。

- この脆弱性は、HTTP.sysというWindowsのコンポーネントに存在し、例えばIISによるWebサービスが稼働しているサーバに対し、細工したリクエストを送信することにより、BSOD（ブルースクリーン）を発生してOSをダウンさせる、あるいはサーバを乗っ取ることが可能になるとされています。

- マイクロソフトでは、この脆弱性を「緊急」レベルと位置付け、早急なパッチの適用を呼びかけるとともに、「カーネルキャッシュを無効化する」という回避策を提示しています。

- また、IPA等も、今回のセキュリティ情報の中からこの脆弱性に対して特別に警告を出しており、既に脆弱性を狙った攻撃コードがインターネット上に出回っている等としています。


IPA Better Life with IT 情報処理推進機構

更新：Microsoft 製品の脆弱性対策について(2015年4月)

最終更新日：2015年4月17日

※追記すべき情報がある場合には、その都度このページを更新する予定です。

概要

2015 年 4 月 15 日(日本時間)に Microsoft 製品に関する脆弱性の修正プログラムが 11 件公表されています。
これらの脆弱性を悪用された場合、アプリケーションプログラムが異常終了したり、攻撃者によってパソコンが制御されたりして、様々な被害が発生する可能性があります。

なお、この内 MS15-033 の脆弱性について、Microsoft 社は「限定的な攻撃を確認しました」と公表しており、今後被害が拡大する可能性があるため、至急、修正プログラムを適用して下さい。

AUS便りからの所感等

- 今回発表された脆弱性は、IISではなくWindowsに存在しており、SQL Server等、WebサービスのためにHTTP.sysを利用するプロダクトが影響を受ける可能性があるとみられ、多くのケースにおいてパッチの適用が必要と考えられます。

- 他のセキュリティパッチも含め適用は速やかに行われるべきですが、それまでに行われ得る攻撃を遮断するため、特に不正な攻撃パターンに対応したUTMによる防御が有効となるでしょう。

●大企業の87%は情報侵害の早期検知体制が不十分、RSA調査

http://itpro.nikkeibp.co.jp/atcl/news/15/041501315/
http://japan.emc.com/about/news/press/japan/2015/20150415-1.htm

このニュースをザックリ言うと・・・

- 4月15日（日本時間）、セキュリティベンダーのEMCジャパンRSA事業本部は、昨年12月から今年2月までに世界の大企業170社に対して行った、セキュリティの脅威に早期対応する体制作りに関するアンケート調査結果を発表しました。

- サイバー攻撃による問題発生の検知と対処、いわゆる「インシデントレスポンス」について、「企業公認の体制を備えている」と回答した企業は30%、さらにその中で「体制の更新や見直しを実施している」企業は57%という結果となっており、全体では87%の企業が体制作りが不十分であるという結論になっています。

- また、セキュリティ脅威の削減や検知のためのインテリジェンス（役に立つ情報や仕組み）を用意しているかの調査では、「セキュリティ警告ログの収集および分析手法」を備えている企業は45%、「全てのパケットを収集するネットワークフォレンジックを常時実施」している企業は42%、といった結果が出ています。


ニュース

大企業の87%は情報侵害の早期検知体制が不十分、RSA調査

2015/04/15
日川 佳三＝ライター（筆者執筆記事一覧）

記事一覧へ >>

EMCジャパンRSA事業本部は2015年4月15日、セキュリティの脅威に早期対応する体制作りについて世界の大企業170社にアンケート調査した結果を発表した（写真）。これによると、大手企業の87%が、そもそも体制を整えていないか、または体制の維持管理が不十分だった。

写真●EMCジャパンRSA事業本部

AUS便りからの所感等

- 「セキュリティの侵害は万が一にも発生してはならない」という視点にだけ囚われ、その「万が一」が発生した際の速やかな沈静化に意識が及ばないというのは本末転倒であると言えます。

- インシデントレスポンスへの対応のためには、ネットワーク構成の一からの見直しや、全く新しい機器の導入を検討するだけでなく、既存のネットワーク機器で活用されていない機能がないか確認することも重要です。

- 例えばUTMについても、単に外部からの攻撃だけでなく、内部からの不正なアクセス先へのアクセスを遮断することや、そういったアクセスのログを分析する機能をフルに活用することがより強固なセキュリティの確立と今後の改善の一助となることでしょう。