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。

●Windows Server 2003サポート終了がもたらすリスク、内部のサーバも狙われる危険性

http://cloud.watch.impress.co.jp/docs/news/20150623_708315.html
http://blogs.mcafee.jp/mcafeeblog/2015/06/5-windows-serve-07fb.html
http://blogs.mcafee.jp/mcafeeblog/2015/06/windows-server--43e4.html

このニュースをザックリ言うと･･･

- 6月23日（日本時間）、大手セキュリティベンダーの米マカフィー社が今年7月15日にサポート終了予定のWindows Server 2003（以下、Win2003）に関して、サポート切れに伴うリスク、およびやむを得ず運用を継続する際の注意点等について同社ブログで説明しています。

- 記事では、Win2003に関連する新たな脆弱点について、今年3月には17件が発表されるなど、現在も発見・発表され続けている事実や、2014年4月にサポートが終了したWindows XPについて、その直後にInternet Explorerの脆弱点が発覚した例を挙げ、Win2003についても攻撃者がサポート切れのタイミングを見計らって未修正の脆弱点を攻撃する可能性を指摘しています。

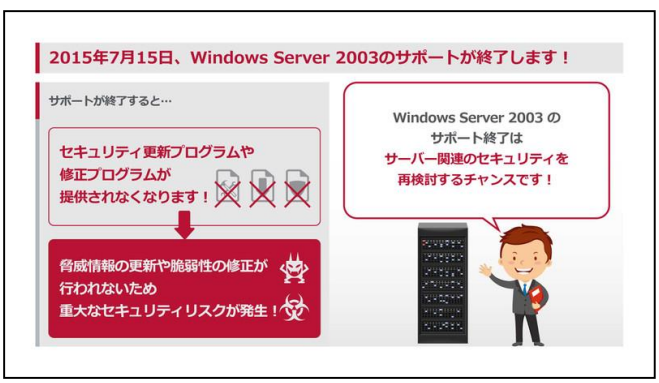
- 一方で、現実問題として「どうしても移行が間に合わない」というケースに対し、同社では「後継環境に移行する場合」「やむを得ず当面Win2003を継続利用する場合」「新旧の環境が混在する場合」の3パターンに関して、安全に運用するためのソリューションを提供するとしています。

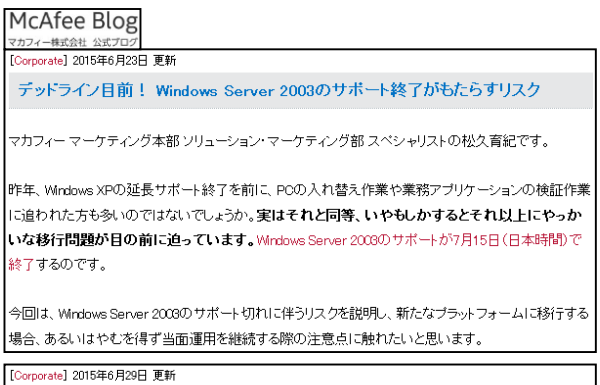
AUS便りからの所感等

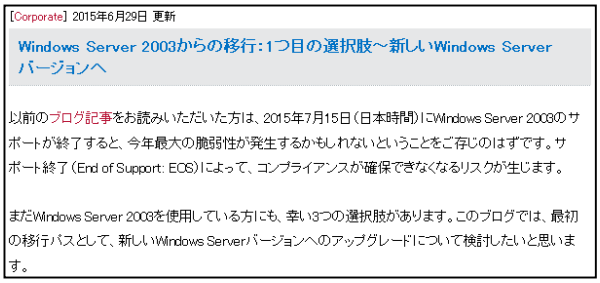
- ブログでも先月多く報じられた標的型攻撃による事件が引合いに出されているとおり、単に「外部ネットワークからのアクセスが制限できていれば大丈夫」とする認識はもはや危険です。

- サポートが終了したサーバは最終的に必ず新しいものに移行するようにし、それまでの運用にあたっては社内LANからの遮断、もしくは可能な限り相互通信を制限するようなネットワーク構成にすべきです。

- あるいは、どうしても社内LANとの通信が必要なサーバについて、その間にUTMを設置しての隔離も検討に値するかと思われます。







●標的型メール攻撃：組織的に日本狙い撃ち　同種ウイルスメール横行　似た表題、中国語フォント

http://mainichi.jp/shimen/news/20150628ddm041040153000c.html

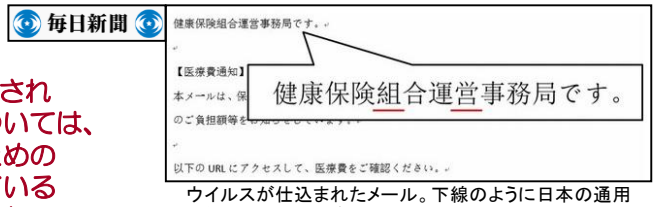
このニュースをザックリ言うと･･･

- 日本年金機構の事件、もしくはそれ以前からの日本の組織を対象とした一連の標的型攻撃について、中国国内の攻撃者が組織的に日本を狙ったものである可能性が複数の専門家から挙がっています。

- セキュリティベンダーのカスペルスキー社は、昨秋以降に出回っているマルウェアが添付された攻撃メールの共通点として、「医療費通知のお知らせ」「健康保険のお知らせ」など類似のタイトルが付いている点を挙げており、PCに感染したマルウェアに指令を出すサーバについても攻撃者が乗っ取ったものとされる約80台を確認しているとのことです。

- また、情報セキュリティ会社のマクニカネットワークス社が攻撃メールを分析した結果、中国語フォントが用いられており、かつ作成日時は平日のオフィス稼働時間帯に集中し、春節（中国の旧正月）等の休日に作成されたものはほとんどなかったとしており、組織的に目的をもって作られた可能性を示唆しています。

AUS便りからの所感等



ウイルスが仕込まれたメール。下線のように日本の通用字体とは違う文字が使われている。

- 対象組織に特化した内容のためアンチウイルス等で遮断されにくいとされる標的型攻撃ですが、今回の一連の攻撃については、攻撃メール特有の特徴が解析され、効果的に遮断を行うためのパターンが作られる点が少なからず期待されると見られている一方、攻撃者もそういった怪しまれる特徴を潰し、攻撃対象のユーザが添付ファイルを開きやすい内容の攻撃メールを洗練していくことでしょう。

- やはり「感染しないように」ではなく「万が一感染したときの被害を最小限に抑えられるように」へ意識を移行し、ユーザ側への啓発だけでなく、アンチウイルス・UTMの活用、ネットワーク構成の見直し等、より新しい対策をとっていくことが重要です。

●その秘密の質問の答えは第三者に推測されてしまうかもしれません…IPAが注意喚起

https://www.ipa.go.jp/security/txt/2015/07outline.html

このニュースをザックリ言うと･･･

- 7月1日（日本時間）、独立行政法人情報処理推進機構（IPA）が毎月行っている「今月の呼びかけ」の7月号が発表され、Webサービスにログインするパスワードを忘れた際の「パスワードリマインダ」で利用される「秘密の質問」に関する安全性への懸念が指摘されています。

- 呼びかけでは、Googleが5月に発表した調査結果において「それ単体でアカウント復旧の仕組みとして使用するには安全性も信頼性も十分ではない」としたこと等が挙げられた他、パスワードリマインダの中にパスワードを画面上に表示するものもあり、秘密の質問に対し正しい解答を当てた攻撃者にそのまま不正利用されてしまう恐れもあるとしています。

- IPAでは、秘密の質問を利用する際の対策として「秘密の質問への答えは第三者に推測されにくい内容にする」「『本来の答え』に自分しか知らない『共通フレーズ』を追加する」ことを呼びかけています。

AUS便りからの所感等

「秘密の質問」が攻撃の対象となることも

- 秘密の質問にまつわるセキュリティインシデントとしては、2013年5月に「Yahoo! JAPAN」約150万ユーザについて、ハッシュ化されたパスワードと一緒に秘密の質問とその回答が流出し、当時システム上の問題があったことから、容易に不正ログインにつながる状態になっていたことが挙げられます。

- ユーザ側の対策の一つとして挙げられる「『本来の答え』に自分しか知らない『共通フレーズ』を追加する」は、複数のサービスでパスワードが共通のアカウントが連鎖的に不正ログインの被害を受ける事件が多発した際において、安全なパスワードを設定する方法の一つとして挙げられていたものの応用とも言えますし、この他には完全にランダムな文字列を設定する手段も有効でしょう。