

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。

●マクロ悪用のマルウェアが急増、Microsoftが注意呼び掛け

<http://www.itmedia.co.jp/enterprise/articles/1501/06/news034.html>
<http://blogs.technet.com/b/mmpc/archive/2015/01/02/before-you-enable-those-macros.aspx>



このニュースをザックリ言うと…

- 1月2日（現地時間）、米Microsoft社が「Microsoft Office」のマクロ機能を悪用してマルウェアに感染させようとするメールが2014年12月から急増しているとして注意を呼びかけています。
- 具体的には、メールに添付されたマルウェアを開かせる際、Officeの通知を装い、「この文書のコンテンツを表示するために『コンテンツを有効にする』ボタンを押してください」など具体的な指示を出し、マクロを有効にするよう仕向けるといいう手口をとっているとのこと。
- 現在、Microsoftが警告する手口は英文のメールでのみ行われており、検出数もアメリカ・イギリスが突出していますが、日本でも少なからず検出がある模様です。
- Microsoftでは、「領収書や請求書などのファイルはほとんどの場合、マクロを必要としない」として、署名のない・信頼できない相手からのマクロを実行しないよう警告しています。

AUS便りからの所感等

- 不審な添付ファイルを開かないこと、添付ファイルに仕込まれた悪意のあるスクリプトやマクロを実行しないことは、非常に当たり前すぎるセキュリティ対策の一つであり、また、その度に警告が発生するとすると、逆に注意を怠り、今回のように巧妙に普段は実行できないようなマクロを実行するよう誘導する手口に引っかかる可能性も見逃せないものとなっています。
- アンチウイルス・UTMの利用は、ユーザへこういったメールが届かないようにするために必要な最低限の対策ですが、万が一それをかいくぐって手元に届いたメールをユーザが適切に処理できるよう、今回のような手口の存在を周知させる等の啓発も随時大事になってくるでしょう。

記事一覧 ITマネジメント ビックデータ モバイル ソーシャル 海外速報 セキュリティ デイルパート 用語事典 ホワイトペ

ITmedia エンタープライズ > セキュリティ > マクロ悪用のマルウェアが急増、Microsoftが注意呼...

2015年01月06日 08時10分 更新

マクロ悪用のマルウェアが急増、Microsoftが注意呼び掛け

ユーザーをだまして手作業でマクロを有効にするよう仕向けるといいう手口が急増。この手口を使うマルウェアは日本でも検出されているという。

[鈴木聖子, ITmedia]

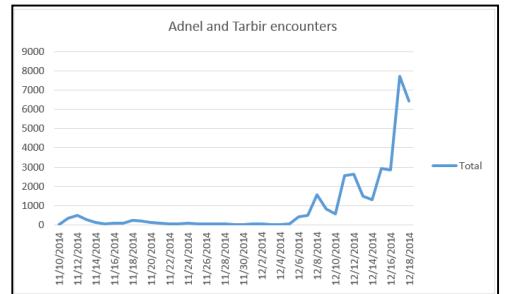
印刷/PDF ツイート 41 いいね! 29 チェック 8+1 2 Pocket 6 通知

バチカン図書館CIO来日 約4千万ページのデジタル文庫化事業
データの共有、生産性とセキュリティは両立できるか？

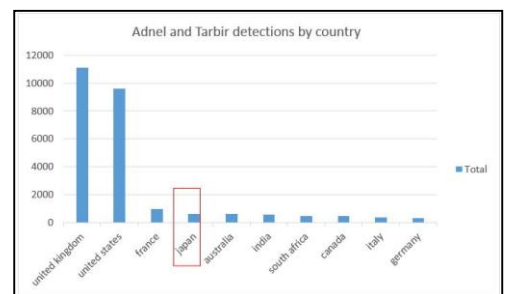
Microsoft Officeのマクロ機能を悪用してマルウェアに感染させようとする手口が急増しているとして、米Microsoftが注意を呼び掛けている。

マクロは複数の手順を記憶して自動的に実行させる機能で、デフォルトでは無効になっている。しかし最近になって、ユーザーをだまして手作業でマクロを有効にするよう仕向け、悪質なコードを実行できる状態にさせてしまう攻撃が浮上しているという。

Microsoftによると、この手口を使ったスパムメールは2014年12月に入って急増した。マルウェア「W97M/Adnel」「O97M/Tarbir」の検出数は米国と英国が突出しているが、日本などでも検出されている。



この手口を使ったスパムメールは2014年12月に入って急増した



国別の感染状況 (Microsoftより)

●SOHOルータに数百万台の乗っ取りを可能にする脆弱性

<http://news.mynavi.jp/news/2014/12/25/176/>
<https://jvn.jp/vu/JVNVU96446762/>




このニュースをザックリ言うと…

- 12月24日(現地時間)、大手セキュリティベンダーの米CheckPoint社が一般家庭や小規模企業で広く使用されている複数のメーカー、モデルのSOHOルータに影響する脆弱性を発見したと発表しました。
- 脆弱性は、これらルータの管理画面で利用される組み込みWebサーバプログラムに存在するもので、WAN側からこれにアクセス可能な設定になっている場合、ルータを乗っ取られる可能性があるとのこと。
- CheckPoint社では、この脆弱性を放置した場合、世界中の数百万台のルータが攻撃者に乗っ取られ、さらにはルータと同一LAN上にあるデバイスが攻撃を受け、データを盗まれる可能性があるとしています。

AUS便りからの所感等

- ルータを外部から簡単に管理できるよう、管理画面へ外部から直接アクセス可能な設定にするケースが散見されますが、大抵はIPアドレスでの制限もなく、不特定多数からアクセス可能にするものです。
- 管理画面に認証がかかっていたとしても、管理画面を表示するプログラムに脆弱性があれば認証なしでルータを乗っ取られる可能性があり、昨年騒ぎになったShellshockについても、機器OSにLinuxを、管理画面にbashによるCGIを利用しているケースでは有効となってしまいます。
- このように、管理画面に外部から直接アクセス可能な設定にするのは決して奨められるものではなく、別の手段で内部LANにログインし、そこを経由して管理画面に入る方がアクセス元の監視等の意味からも安全と考えます。


公開日:2014/12/22 最終更新日:2015/01/06
JVNVU#96446762 複数のブロードバンドルータに、脆弱性が存在するバージョンの Allegro RomPager を使用している問題
概要 複数のブロードバンドルータのファームウェアには、脆弱性が存在する古いバージョンの Allegro RomPager を使用している問題が存在します。
影響を受けるシステム • Allegro RomPager 434 より前のバージョンを実装したファームウェア
本脆弱性の影響を受ける可能性がある製品に関する詳しい情報は、Check Point Software Technologies の アドバイザリ に記載されています。

●大規模なサイバー攻撃への防御方法とは？ - WatchGuard社

<http://news.mynavi.jp/news/2014/12/26/032/>
http://www.watchguard.co.jp/press_news/2014/12/it-1.html



このニュースをザックリ言うと…

- 12月24日(現地時間)、XTM・FireboxといったUTM等で知られる大手セキュリティベンダーの米WatchGuard社が先日発生したソニー・ピクチャーズへの大規模なサイバー攻撃等を教訓とした「IT担当者が早急に対策を講じるべき緊急提案」を発表しました。
- 同社は「最前線の防御体制を強化する5つのアクション」として、①「ファイアウォールとアンチウイルスは(細かい防御において)万全ではない」としたうえで、②「(入口だけではなく)出口対策」③「標的型攻撃対策」④「スピアフィッシングの攻撃を特定・報告するように従業員をトレーニングする」⑤「セキュリティ対策として不適切である可能性のあるWebサイトに関する情報を素早く提供するレピュテーションサービスを活用する」ことを挙げています。
- 同様に「サイバー攻撃に遭遇した際に被害を最小限に抑える7つのアクション」として①「感染した場合に備えておく」②「すべてを暗号化する」③「ネットワークをセグメント化し、最少権限の原則を適用する」④「二要素認証を利用する」⑤「情報漏えい防止対策によりデータ流出を抑止し、アラートを発信する」⑥「キルチェーン(複数の段階で行われる攻撃手順)を意識し、外部のコマンド&コントロール(攻撃指令を出す)ホストとの接続を防御する」⑦「可視化および分析ソリューションにより感染を把握する」ことを挙げています。

AUS便りからの所感等

- アンチウイルスやUTMによる防御は決して欠かすことの出来ない最低限の対策の一つである一方、それだけで100%攻撃を防御できるわけではないことは度々言及していることです。
- 先に挙げた各種アクションを検討し、可能なものから実行し、多重防御によるセキュリティ侵害・情報漏洩等の効果的な防止を意識していくことを強く推奨致します。