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。

●請求書に偽装したマルウェア添付のメール、国内銀行のアカウント狙いか

http://internet.watch.impress.co.jp/docs/news/20141212_680078.html
http://blog.trendmicro.co.jp/archives/10558

このニュースをザックリ言うと･･･

- 12月10日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社は、オンラインショッピングなどの請求書に偽装してマルウェアに感染させようとする攻撃メールが8日以降急増していることを同社ブログで発表しました。

- メールに添付された文書ファイルに請求書の画像が貼り付けられており、これをダブルクリックすることにより、マルウェアが実行される仕組みとなっています。

- マルウェアが外部のサーバからダウンロードするファイルには、プロキシの自動設定に使用されるファイルもあり、これに国内銀行15行のドメイン情報が含まれていることから、それらの銀行のオンラインバンキングサイト等へのアクセスを傍受するようプロキシ設定を変更する意図があるとされています。

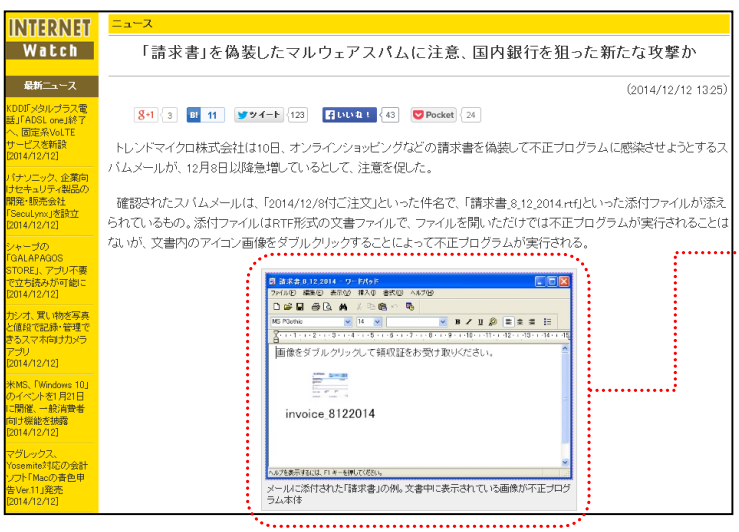
- 同社では、ショッピング等の機会が増える年末を狙った同様の攻撃が増える可能性を指摘し、見慣れない様式の請求書メールなどが添付された不審なメールを開かないよう呼びかけています。

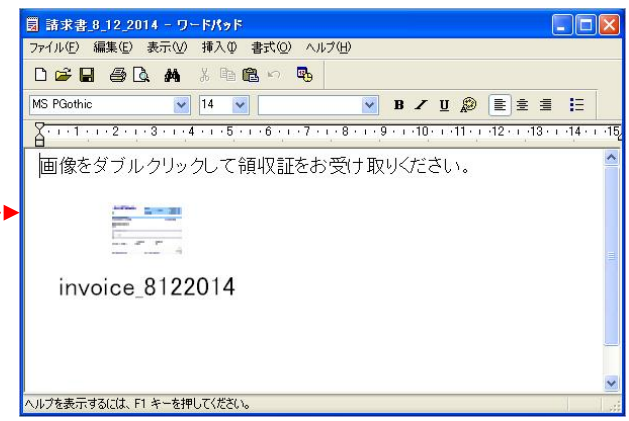
AUS便りからの所感等

- 今回確認されたメールには、年月日が逆順につながった形式の日本では一般的ではない形式の日付が書かれていることから、日本のユーザが騙される可能性はそう高くはないと思われます。

- 今後、こういった部分にも違和感がなく、また各銀行から出されるメールのフォーマットに寸分違わずそっくりなメールが送信されるようなことがある場合、攻撃が成功する可能性は非常に高くなると思われます。

- メールを受信したユーザによる判断でマルウェアに感染してしまう可能性を抑制するためにも、アンチウイルス・UTMによる受信メールの確実なチェックが重要になります。





メールに添付された「請求書」の例。
文書中に表示されている画像が不正プログラム本体

●破壊的なマルウェアを使った攻撃発生、FBIが全米の企業に警告。ソニー・ピクチャーズへの攻撃に関連か？

http://www.itmedia.co.jp/news/articles/1412/03/news056.html

このニュースをザックリ言うと･･･

- 12月2日（米国時間）、米国のセキュリティ情報サイト「Krebs on Security」は、社内のコンピュータの全情報を消去してしまうマルウェアによる攻撃が発生しているとして、米連邦捜査局（FBI）が全米の企業に対し注意を呼びかけていると発表しました。

- マルウェアに感染したPCはHDDのマスターブートレコード（MBR）を含む全データを消去され、起動することやデータの復旧が困難な状態に陥る模様です。

- 11月24日（米国時間）にソニー子会社の米ソニー・ピクチャーズ・エンタテインメント社が組織的なクラッキングを受け、機密情報や新作映画の動画等が流出するといった被害を受けており、FBIは明言はしていないものの、この事件に関与しているマルウェアである可能性が高いとされています。

AUS便りからの所感等

- マルウェアが日本企業の子会社を狙った犯行で使われたとみられること等から、米国のみならず日本国内の企業に対してもマルウェアが送信され、広く拡散する可能性は十分に考えられます。

- こういったセンセーショナルな話題が伝えられるマルウェアのみならず、密かに感染していくマルウェアについて万全に対応するため、アンチウイルスの導入・UTMの設置による防御を確実に行っておくべきでしょう。

●国内出版社のWebサーバが改ざん･･･VPS管理画面からサーバを初期化される

http://www.sakura.ad.jp/news/sakurainfo/newsentry.php?id=1002
http://internet.watch.impress.co.jp/docs/news/20141209_679479.html

このニュースをザックリ言うと･･･

- 12月6日、IT関連の書籍・雑誌の出版で知られる技術評論社のWebサーバが攻撃を受け、訪問者が他のWebサイトにリダイレクトするよう改ざんされていたことが明らかになりました。

- このWebサーバは国内の大手VPSサービス「さくらのVPS」を利用していましたが、サーバ管理用のアカウント情報をフィッシングによって奪取され、管理画面からOSを上書きインストールされたことが原因としています。

- VPSの管理画面は「ユーザIDとパスワード」でのログインの他に「VPSのIPアドレスとパスワード(先程のパスワードとは別)」でのログインも可能となっており、前者について対策は行ったものの、後者への対策が間に合わず、こちらの経路からログインされた模様です。

AUS便りからの所感等

- 攻撃者が侵入できたのは管理画面までで、サーバ内の管理者権限の奪取はできなかったようですが、その状態でサーバを乗っ取るため、OSを上書きインストールするという方法をとったとみられています。

- 特定のターゲットに向けられる、いわゆるスピア型によるフィッシング攻撃は、アンチウイルスやUTMのみでは万全に防止できない可能性もあるため、管理するユーザ側の慎重な行動、例えばあらゆる重要なアカウントについて確実に把握し、十分に強力なパスワードを設定する、等の対策をとることが肝心です。