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。

●ネットバンキング不正送金、法人顧客の被害増大が明らかに

http://www.zenginkyo.or.jp/news/2014/11/27150000.html
http://security-t.blog.so-net.ne.jp/2014-12-01

このニュースをザックリ言うと・・・

- 11月17日、全国銀行協会（全銀協）が会員の金融機関191行を対象にした、2005年度～今年9月の「インターネットバンキングによる預金等の不正払戻し」等に関するアンケート結果を発表しました。

- 個人顧客における年度別の被害件数および被害額は、2011年度以降は年々件数が増え、2013年度は年間984件・12億5000万円となり、今年度は第1四半期（4～6月）にて441件・4億4800万円、第2四半期（7～9月）は237件・1億7500万円と推移しています。

- 一方、法人顧客については2013年度に35件・1億8300万円だったものが、今年度は第1四半期で48件・1億9800万円、第2四半期は23件・2億1900万円となっており、半年間で既に71件・4億1700万円の被害が報告されています。

AUS便りからの所感等

- アンケート結果からは、昨年度～今年度にかけて件数・被害額ともに急激に上昇していることが伺え、特に法人顧客については、今年度の半年だけでも昨年度の年間被害の2倍に匹敵するペースとなっているようです。

- アンケートでは明言されていないものの、新たなマルウェアの投入が増加されていったことによる被害の拡大と見て良いでしょう。

- UTMの設置によるマルウェア侵入の防止、またインターネットバンキングを利用するPCにおいてはアンチウイルスの導入はもちろん、金融機関から提示されるクライアント向けセキュリティツールがあればその導入を検討すること、これらの対策全てが不正送金被害の効果的な防止の一助となることでしょう。

●1200のサイバー攻撃サイトに日本国内から3万8000ものアクセス - トレンドマイクロ調査

http://www.itmedia.co.jp/enterprise/articles/1411/29/news009.html
http://news.mynavi.jp/news/2014/12/02/202/

このニュースをザックリ言うと・・・

- 11月28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がWebサイトの改ざんを起点とするサイバー攻撃の最新情報について、同社ブログにて解説を行っています。

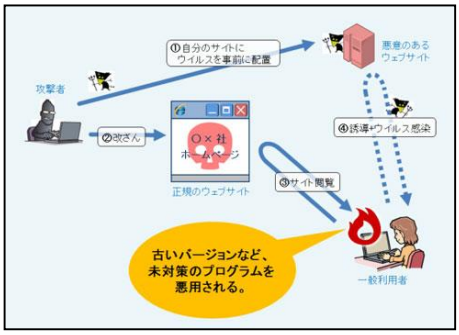
- 記事によると、2014年10月の1ヶ月間に、1200ドメイン以上の攻撃者が用意したWebサイトに対し、日本国内から約3万8000件のアクセスがあり、またこれらのサイトの8割が「Rig Exploit Kit」というマルウェアのツールキットを使用していたとのことです。

- 攻撃者が用意したWebサイトにはPCのOSやアプリケーション情報を収集するスクリプトが仕込まれており、脆弱性のある古いアプリケーションがインストールされていればさらなる攻撃を行い、またアンチウイルスがインストールされている場合は攻撃しない、といった処理を行っている模様です。

AUS便りからの所感等

- 今回明らかになったPCへの攻撃の傾向は、訪問者に対し無差別に攻撃を仕掛けることで目立ってしまうことを避け、古いバージョンを入れている、さらにはアンチウイルスソフトも入れてないような「格好のターゲット」を目立つことなく密かに待ち受けることが狙いであると分析されているようです。

- 攻撃者に対し隙を見せないようにするためにも、UTMの導入のみならず、個々のクライアントPCにおけるアンチウイルスの導入、およびOSとアプリケーションのアップデート、これら全ての対策が重要となってきます。



Webサイトを訪問したユーザーをマルウェアに感染させる「ドライブ・バイ・ダウンロード攻撃」の仕組み

●人目に付かず監視活動を行う最悪のスパイツール「Regin」 - Symantecが解説

http://www.symantec.com/connect/ja/blogs/regin
http://news.mynavi.jp/news/2014/11/30/025/

このニュースをザックリ言うと・・・

- 11月27日（日本時間）、大手セキュリティベンダーのシマンテック社がこれまでにない技術力を持つ高度なスパイツール「Regin」について、同社ブログにて解説を行っています。

- Reginはバックドア型マルウェアの一種で、暗号化された複数のパーツによって5段階に分けてダウンロードされることにより、アンチウイルス等からの検出を回避する仕組みをとっています。

- 2008年から2011年まで活動した後に休止し、その後2013年に新しいバージョンが確認されており、ロシアやサウジアラビアを含む10ヶ国で主に感染が確認されているとのことです。

AUS便りからの所感等

- 各パーツを単にダウンロードしてファイルとして保存するだけではなく、Windowsのレジストリ上に次のパーツをダウンロードする等のコードを保存する等、巧妙な手口がとられています。

- 現時点でReginが日本で活発に活動しているという情報はなく、また幸いにも、Reginの行動の仕組み自体はセキュリティベンダー各社で分析が進んでおり、各社のアンチウイルス・UTMにおいて、侵入・感染を根元から経つ、あるいは感染したPC上での本格的な活動を食い止められるようになることが期待できます。