— AUS（アルテミス・ユーザ・サポート）便り 2014/11/25号 —

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。

●社内で見つかる「遠隔操作ウイルス」、1年で7倍増に

http://www.itmedia.co.jp/enterprise/articles/1411/20/news134.html
http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20141117022557.html

このニュースをザックリ言うと・・・

- 11月20日、大手セキュリティベンダーのトレンドマイクロ社が2014年第3四半期（7～9月）のセキュリティ動向を発表し、いわゆる「標的型攻撃」がこれまでの官公庁や特定業種のみならず、業種・規模に関係なく、様々な法人が保有する「顧客情報」をターゲットにしていることが明らかになりました。

- 同社に対し法人から寄せられたマルウェア解析依頼のうち、遠隔操作型マルウェア（バックドア）の割合は29.5%で、2013年第3四半期の4.2%の7倍にものぼっています。

- 同時期の日本からのフィッシング詐欺サイトへのアクセスブロック数は61万2000件で、第1四半期の27万4000件、第2四半期の13万4000件からこれも大きく跳ね上がっており、2014年社会問題化しつつあるネットバンキングの不正送金被害も続いているとのことです。

AUS便りからの所感等

- ひとたび内部ネットワークのPCに遠隔操作ウイルスを仕掛けられると、攻撃者が外部から侵入してくる余地、また内部から攻撃者のサイトに接続し、指令のもとPCを操作される余地が生じてしまいます。

- アンチウイルス・UTMの設置により、外部からの接続、内部から外部への不審な接続、そして何よりもマルウェアからの感染を食い止めることが重要でしょう。


記事一覧 | ITマネジメント | ビッグデータ | モバイル | ソーシャル | 海外速報 | セキュリティ | ディルバート | 用語事典 | ホワイトペ

ITmedia エンタープライズ ＞ 社内で見つかる「遠隔操作ウイルス」、1年で7倍増に...

2014年11月20日 18時04分 更新

社内で見つかる「遠隔操作ウイルス」、1年で7倍増に

トレンドマイクロによると、企業から解析依頼のあった不正プログラムに占める遠隔操作型の割合が1年で7倍も増加したという。

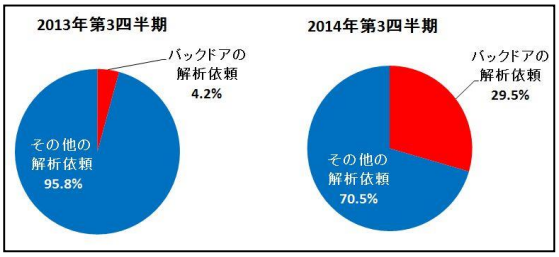
[ITmedia]

印刷／PDF | ツイート 43 | いいね！ 90 | チェック | 8+1 0 | Pocket 6 | 通知

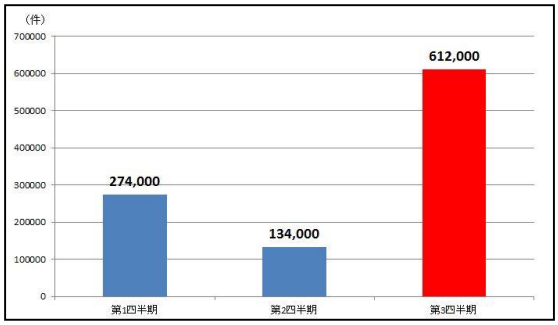
PR 業界内レベルが分かる！セキュリティ対策を今すぐチェック
PR ドSの幼馴染、小悪魔上司に、メイド服の総務部員？？

トレンドマイクロが11月20日に発表した2014年第3四半期のセキュリティ動向によれば、企業や組織から機密情報を盗むことなどを目的にした遠隔操作型の不正プログラムの割合が急増。同社は、標的型サイバー攻撃で狙われる組織の業種や規模は関係ない状況だと警鐘を鳴らしている。

法人顧客が同社に解析を依頼した不正プログラムの内訳をみると、遠隔操作型（バックドア型）が占める割合は、前年同期の4.2%から今期は29.5%と、約7倍に増えた。サイバー攻撃者は、不正プログラムに感染させたコンピュータを遠隔操作して機密情報を盗み出すことから、この増加ぶりは、既に多くの企業の内部に不正プログラムが侵入している実態をうかがわせる。



国内の法人から解析依頼における遠隔操作型不正プログラム（バックドア）の割合（トレンドマイクロより）



日本からのフィッシング詐欺サイトへのアクセスブロック数（同）

●IPA、「やりとり型攻撃」について警告

http://internet.watch.impress.co.jp/docs/news/20141121_677215.html
http://www.ipa.go.jp/security/topics/alert20141121.html

このニュースをザックリ言うと・・・

- 11月21日、独立行政法人情報処理推進機構（IPA）がいわゆる「標的型攻撃」の一種である「やりとり型」攻撃について警告を出しました。

- やりとり型攻撃は、事前に無害なメールをやり取りし、その後にウイルスが添付されたメールを送信することが特徴です。

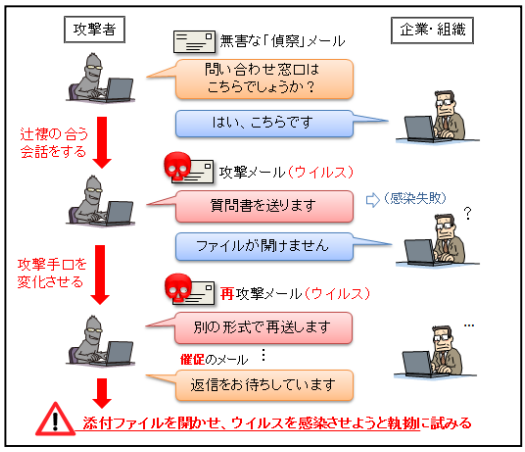
- IPAでは、以前からこの攻撃が行われていたことを感知していましたが、今年8月から10月にかけて再び国内の複数の組織に対して攻撃が行われたことを確認し、特に外部向け窓口の担当者に対し注意を呼びかけています。

AUS便りからの所感等

- IPAのページでは、攻撃者がウイルス入りの添付ファイルを複数回送信し、「返信をお待ちしています」と催促する等、ユーザが添付ファイルを開くよう仕向ける手口について紹介されています。

- 事前に無害なメールのやり取りを行うことにより、不審な発信元からのメール受信を拒絶するようなアンチSPAM機構を回避する狙いもあると思われます。

- 最低限、アンチウイルス・UTMの設置は不可欠ですが、このような攻撃の存在に注意し、「誤検出なのでは?」と安易にウイルスチェックをせずにメールを受信すること等のないよう、ユーザ側も慎重に行動することが求められます。



「やりとり型」攻撃のイメージ

●プロキシサーバ運営業者逮捕、国産ルータからのアカウント情報奪取も

http://itpro.nikkeibp.co.jp/atcl/news/14/112001989/
http://www.yomiuri.co.jp/it/20141120-OYT1T50012.html

このニュースをザックリ言うと・・・

- 11月19日、インターネット上の不正行為の際にアクセス元を秘匿する目的でプロキシサーバを運営していたことにより、都内のサーバ運営会社2社等が摘発されました。

- 前述のサーバ運営会社は、ISPユーザ1500人分のアカウント情報を悪用してISPに不正アクセスしていたことが明らかになっており、不正アクセス禁止法違反容疑が適用されています。

- これらのアカウント情報は、大手コンピュータ周辺機器メーカー「ロジテック」社の無線LANルータから、ファームウェアの脆弱性を突いて奪取されたものとみられています。

AUS便りからの所感等

- ルータ等のネットワーク機器はPCに比べてその存在を意識されることが少ないためか、PCのOSに相当するファームウェアの更新が疎かになることがあります。

- 今回悪用されたとみられる脆弱性も2012年5月に発表され、ファームウェアの修正版が既にリリースされていたもので、2年半の間アップデートを行わなかったルータがターゲットにされた模様です。

- 社内のPCと同様、ルータ等のネットワーク機器についてもその存在を確実に把握し、適宜メーカーサイトにおいて脆弱性が発表されていないか確認する等の運用を怠らないことが重要です。