— AUS（アルテミス・ユーザ・サポート）便り 2015/05/11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。

●日本人を狙う「ランサムウェア」、一週間に60件の感染確認

http://www.jiji.com/jc/zc?k=201505/2015050400137&g=soc
http://blog.trendmicro.co.jp/archives/11378

このニュースをザックリ言うと・・・

- 4月27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ランサムウェア（感染したPCのファイルを人質に金銭等を要求するマルウェア）の一種「TROJ_CRYPWALL.XXQQ」について、同社ブログで警告しています。

- これは昨年登場したランサムウェア「CryptoWall(クリプトウォール)」の亜種ですが、特筆すべき特徴として、日本語メッセージが機械翻訳のような不自然なものではないこと、また感染したPCの環境に応じて表示する言語を変える多言語対応型であることが挙げられており、「日本におけるランサムウェアのひとつの転換点になる」可能性もあると述べられています。

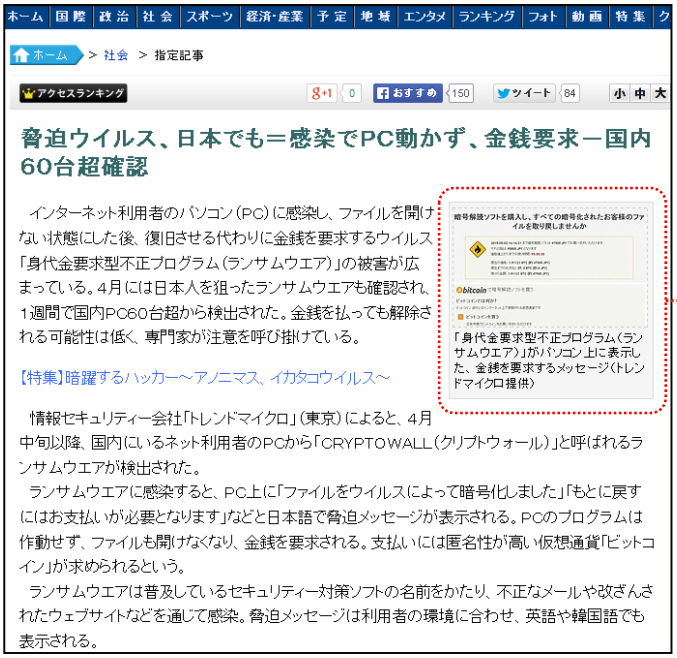
- ブログでは、現時点でまだ広く被害が拡散している状況ではないとしていますが、4月17日前後から国内PCへの感染が一週間に60件近く確認されている模様です。

AUS便りからの所感等

- 同社によれば、日本語メッセージを表示するランサムウェアはこれまで2014年3月以降に2種しか確認されておらず、国内での本格的な感染も確認されていなかったとのことですが、今回の「TROJ_CRYPWALL.XXQQ」ではメッセージ以外にも感染成功率を上げるためのいくつかの工夫がなされていたものと推測されます。

- ランサムウェアについては当便りでも度々言及していますが、PC上のファイルが暗号化等で人質にとられ、かつ「身代金」を支払ってもファイルが確実に復旧できるという保証はないことを考えれば、事実上ファイルが破壊されることに等しいと言えます。

- ランサムウェアを含めた各種マルウェアの感染を防ぐためにも、基本的な対策としてPCのOSと各種アプリケーションを最新に保つこと、かつ、アンチウイルス・UTMの導入による防御が重要となります。


ホーム | 国際 | 政治 | 社会 | スポーツ | 経済・産業 | 予定 | 地域 | エンタメ | ランキング | フォト | 動画 | 特集

ホーム > 社会 > 指定記事

アクセスランキング

脅迫ウイルス、日本でも＝感染でPC動かず、金銭要求－国内60台超確認

インターネット利用者のパソコン（PC）に感染し、ファイルを開けない状態にした後、復旧させる代わりに金銭を要求するウイルス「身代金要求型不正プログラム（ランサムウエア）」の被害が広まっている。4月には日本人を狙ったランサムウエアも確認され、1週間で国内PC60台超から検出された。金銭を払っても解除される可能性は低く、専門家が注意を呼び掛けている。

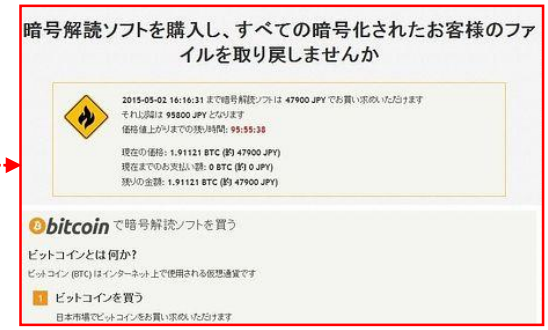
【特集】暗躍するハッカー～アノニマス、イカタコウイルス～

情報セキュリティー会社「トレンドマイクロ」（東京）によると、4月中旬以降、国内にいるネット利用者のPCから「CRYPTOWALL（クリプトウォール）」と呼ばれるランサムウエアが検出された。

ランサムウエアに感染すると、PC上に「ファイルをウイルスによって暗号化しました」「もとに戻すにはお支払いが必要となります」などと日本語で脅迫メッセージが表示される。PCのプログラムは作動せず、ファイルも開けなくなり、金銭を要求される。支払いには匿名性が高い仮想通貨「ビットコイン」が求められるという。

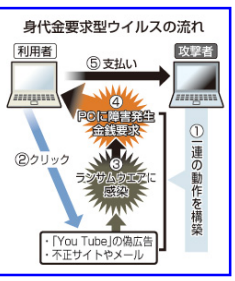
ランサムウエアは普及しているセキュリティー対策ソフトの名前をかたり、不正なメールや改ざんされたウェブサイトなどを通じて感染。脅迫メッセージは利用者の環境に合わせ、英語や韓国語でも表示される。

「身代金要求型不正プログラム（ランサムウエア）」がパソコン上に表示した、金銭を要求するメッセージ（トレンドマイクロ提供）



「身代金要求型不正プログラム（ランサムウエア）」がパソコン上に表示した、金銭を要求するメッセージ（トレンドマイクロ提供）

ランサムウエア　インターネット利用者を狙い、金銭を脅し取るサイバー犯罪で使われるウイルス。ランサムは英語で身代金を意味し、「身代金要求型不正プログラム」とも呼ばれる。感染すると、パソコンに保存されている重要なファイルやデータを利用できないよう暗号化し、解除する代わりに金銭の支払いを求める。情報セキュリティー会社「トレンドマイクロ」によると、ランサムウエアは複数の種類が確認され、欧州や南米、米国などの4000の機関や企業で被害が出ているという。（2015/05/04-15:05）



●企業がターゲットのマルウェア拡散…Dropboxからダウンロード、不正なマクロ実行を誘導

http://www.itmedia.co.jp/enterprise/articles/1504/30/news114.html
http://blog.trendmicro.co.jp/archives/11397

このニュースをザックリ言うと・・・

- 4月30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オンラインストレージ・ファイル同期サービス「Dropbox」等を利用して拡散する等の特徴を持つマルウェア「BARTALEX」について、同社ブログで警告を出しました。

- BARTALEXは、企業間の電子決済に関する通知に偽装したメールを送信し、メール上のリンクからDropbox上に保存されているWordファイルをダウンロードさせ、不正なマクロを有効にするよう仕向けることにより、PCに感染するという手口をとっている模様です。

- また、マクロを悪用するという古い手口が依然有効であることについても指摘し、マクロやその他スクリプトの実行について、不要なものは無効にする等の基本的な対策を社員に教育することを呼びかけています。


2015年04月30日 17時14分 更新

マクロ悪用のサイバー攻撃、今度はDropboxを使用

Microsoft Officeのマクロ機能を悪用するマルウェア感染攻撃で、攻撃者が不正ファイルの配布にDropboxを利用していることが分かった。

[ITmedia]

印刷／PDF　ツイート 130　いいね！ 69　チェック　g+1 0　Pocket 31　通知

PR Box World Tour Tokyo アーロン・レヴィ来日講演 6/17(水)
PR 「ライオン」のデータ統合・システム連携の事例を紹介！

Microsoft Officeのマクロ機能を悪用するサイバー攻撃が増える中、トレンドマイクロは4月30日、マルウェア感染にDropboxを使う新たな手口を確認したとブログで伝えた。取引や決済などに関するメールを企業へ送り付け、文中のリンクからマルウェアを設置したDropboxのページにユーザーを誘導する。

同社によると、企業に送り付けられるメールは、米国で企業間の電子決済などに使われる「Automated Clearing House」（ACH）の通知を装ったものが多く、ACH以外にもFAXの受信通知や請求書、明細書、宅配などの通知を装ったメールもある。受信者に仕事関係のメールと思い込ませる狙いがあるようだ。

AUS便りからの所感等

- 今回のケースに関して言えば、マルウェア本体へのアクセスを誘導する不審なメールはUTM等の導入により、アンチウイルスもしくはアンチスパム機能で遮断されることが期待されます。

- ともあれ、どれか一つの対策のみではなく、セキュリティの教育・啓発を含めたあらゆるアプローチからの多重防御が肝心となるでしょう。

●東京電力のXP継続利用計画に「待った」、4月にOS更新完了

http://www.itmedia.co.jp/news/articles/1504/22/news051.html
http://www.yomiuri.co.jp/it/20150421-OYT1T50005.html

このニュースをザックリ言うと・・・

- 4月20日（日本時間）、東京電力（以下東電）が昨年4月にサポートが切れているWindows XPの継続利用を計画していたことに対して指摘を受け、同月までにOS更新を完了していたことが新聞で報じられました。

- 今回および昨年7月時点の報道によれば、当初東電は36億円のコストカットの名目で約48,000台のXP搭載PCを2018年まで利用しすることを計画していましたが、電力という重要なインフラがサイバー攻撃の標的になる可能性から、内閣官房情報セキュリティセンターが2013年10月以降OS更新に関する注意喚起を再三行い、また会計検査院も3月下旬の報告書において同様の指摘を行っていました。

- 東電はこれらの指摘を受けて2015年上半期までにOS更新を行う方針に転換し、今回あらためて「OS更新を完了した」との発表をしました。

AUS便りからの所感等

- 会計検査院の報告書では、東電は当初「OSによらないセキュリティ対策を実施することにより、更新時期をサポート終了後まで繰り延べることは可能」と判断していたとのことですが、東電のような大企業ですらXPをサポート切れから4年以上使い続けるという計画をとろうとしていたわけですから、中小企業ではなおのこと、同様の意識・判断で使い続けようとしているところは決して少なくはないと見受けられます。

- 今日行われる攻撃の多くはOSよりもPCにインストールされた周辺のアプリケーションを狙う傾向にあり、そういったアプリケーションの中にはXPのサポートを続けるものも珍しくなく、またアンチウイルス・UTMによる防御も当分は効果があるでしょう。

- それでも、「サポートが切れたOS自体に残っている脆弱性はもう修正されない」ということは決して忘れることなく、OSの更新を必ず計画的に行うことがまさかの攻撃からPCとネットワークを守るセキュリティ対策として重要となります。