— AUS（アルテミス・ユーザ・サポート）便り 2016/05/30号 —
http://www.artemis-jp.com

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。

●「vvvウイルス」活動終了宣言、後継？のランサムウェア「CryptXXX」にも注意を

http://www.itmedia.co.jp/enterprise/articles/1605/26/news136.html
http://blog.trendmicro.co.jp/archives/13384

このニュースをザックリ言うと･･･

- 5月19日（日本時間）、スロバキアのアンチウイルスベンダーであるESET社は、「vvvウイルス」「CrypTesla」等の別名で知られるランサムウェア「TeslaCrypt」の作者が暗号解除のためのマスターキーを公開し、活動終了を宣言したと発表しました。

- また、同社ではこのマスターキーをもとに、TeslaCryptに暗号化されたファイルを復元するツールをリリースしています。

- 一方で5月26日、大手セキュリティベンダーのトレンドマイクロ社は、4月半ばに登場したランサムウェア「CryptXXX」の亜種として、TeslaCryptの挙動を模倣するものが確認されたとして警告しています。

- TeslaCryptと同様、この亜種も改ざんされたWebサイトや不正な広告から感染するものとされている他、感染時の新たな特徴として、画面をロックし、支払いサイトへのアクセス以外の行動を妨害することが挙げられています。

AUS便りからの所感等

- トレンドマイクロ社によれば、2016年1月～3月期における国内のランサムウェア被害報告件数は870件で、2015年1年間の報告件数800件を早くも上回る勢いとされています（http://www.itmedia.co.jp/enterprise/articles/1605/25/news124.html）。

- 同社は、ランサムウェアによるデータ暗号化を回避するためのバックアップ方法として、「3つのコピーを保存」「2つの異なる種類の端末に保存」「そのうちの1つは他の2つとは異なる場所に保存」という『3-2-1ルール』を提案していますが、とにかく、バックアップデータまでも暗号化されないようにするのが肝要です（http://blog.trendmicro.co.jp/archives/11739）。

- 日々のWebへのアクセスやメールの扱い等について慎重であること、アンチウイルスやUTMによる防御を固めること、これらのいずれか片方だけではなく、両方を確実に行うことが効果的なランサムウェアあるいは各種マルウェア対策として不可欠です。

ITmedia エンタープライズ

2016年05月26日 17時46分 更新
終了宣言したランサムウェアに後継者？　より悪質な"更新版"が出現
活動終了を宣言した「CrypTesla」と同様の手口を使いながら、感染したユーザーに身代金を支払わせるための手段をより巧妙化させているという。

トレンドマイクロは5月
（検出名RANSOM_WAL
と同様の感染手法を使う
巧妙化しているという。

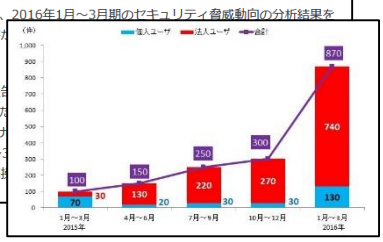
同社によるとCryptXX
や不正な広告にアクセス
コンピュータが仮想環境
停止。仮想環境でない場
させようとしても、暗号

2016年05月25日 14時38分 更新
ランサムウェア被害、3カ月で870件に　検出は8300台
トレンドマイクロによれば、2016年1月～3月のランサムウェア被害の報告件数は前年比8.7倍になった。

[ITmedia]

トレンドマイクロは5月25日、2016年1月～3月期のセキュリティ脅威動向の分析結果を発表した。ランサムウェア被害
な実態を報告している。

国内のランサムウェア被害報
（800件）を大きく上回る状況
同社によれば、2015年のランサ
用されたものの、2016年1月～
の攻撃メールが送信され、遠隔
ウェアも複数出現した。



TREND MICRO トレンドマイクロ セキュリティブログ

暗号化型ランサムウェア「CryptXXX」、「CRYPTESLA」の後継となるか

投稿日: 2016年5月26日
脅威カテゴリ: 不正プログラム，メール，スパムメール，サイバー犯罪，感染媒体
執筆: Trend Micro

2016年5月18日（米国時間）、暗号化型ランサムウェア「CRYPTESLA」（別名：TeslaCrypt、「RANSOM_CRYPTESLA」として検出）が活動を停止し、復号に必要なマスターキーが無料で公開されました。このランサムウェアに関連する脅威状況の一大事件の裏で、CRYPTESLA が利用していた手口を再利用しようとするサイバー犯罪者がいるようです。この事例に先立って、4月に、従来のランサムウェア「REVETON」の背後にいるサイバー犯罪者集団が新たに「Angler Exploit Kit(Angler EK)」および「BEDEP」を利用して暗号化型ランサムウェア「CryptXXX」（「RANSOM_WALTRIX」として検出）を拡散する報告がありました。

今回、CRYPTESLA の手口を模倣する CryptXXX の亜種（「RANSOM_WALTRIX.C」として検出）が確認されました。CRYPTESLA の無料復号ツールの公開によりユーザが身代金要求を無視できるようになった後で大幅に更新された亜種となり、この亜種は、ファイルを暗号化するだけでなくユーザがデスクトップにアクセスできないように画面をロックする機能も備えています。

■ 侵入経路

RANSOM_WALTRIX.C は、CRYPTESLA の拡散手口同様、改ざんされた Webサイトおよび Angler EK を組み込んだ不正広告経由で拡散します。

●業務用PC33台にマルウェア感染･･･岐阜市

http://www.gifu-np.co.jp/news/kennai/20160524/201605240846_27337.shtml

このニュースをザックリ言うと･･･

- 5月23日（日本時間）、岐阜市は、業務用PC全2,564台のうち33台がトロイの木馬等のウイルスに感染していたと発表しました。

- 同市によれば、12日にPCが不審な動作をしたことで調査したところ、計43種のウイルスを確認したとのことです。

- また、システムは2012年に導入されたそうですが、サーバにおいて、アンチウイルスソフトのパターンファイルが一切更新されていなかった模様とのことです。

- マイナンバーを含む住民情報システムの回線とは分離されているため、情報漏えいは発生していない模様で、ウイルスはパターンファイルの更新を行ったうえで駆除したとしております。

AUS便りからの所感等

- OSや各種ソフトウェアのバージョンと同様、アンチウイルスソフトのパターンファイルの更新は、新しく登場するマルウェアに対応するため必ず行わなければならないものです。

- アンチウイルスソフトのインストール直後、およびそれ以降も継続的にパターンファイルの更新状況を確認する必要があり、これはUTMについても同様のことが言えるでしょう。

- 社内のIT資産管理を行うソリューションの多くはそういった更新状況をチェックする機能がありますので、可能な限り導入することが望ましいでしょう。

岐阜新聞Web
パソコン33台ウイルス感染　岐阜市
2016年05月24日08:46

岐阜市は23日、市のパソコン端末33台がウイルスに感染していたと発表した。システムサーバーのウイルス対策ソフトが更新されていなかったのが原因。端末はサイバー攻撃対策が講じられており、住民情報を扱うシステムとは分離してあり、個人情報などの漏えいは確認されていないとしている。

市によると、12日に職員が端末の不審な動作を見つけ、ウイルス感染が発覚。対策ソフトの状態を確認したところ、端末は最新の状態になっていたが、サーバーが現在のシステムを導入した2012年1月から一度も更新されていなかったことが判明した。

20日までに端末約2560台を確認したところ、33台から43種のウイルスを検出、駆除した。大半が情報を盗み出すタイプだった。基盤を構築した日立製作所と調査したところ、設計段階からサーバーの更新機能に不備があった。

●文科省をかたる標的型攻撃メール、慶応大学に

http://www9.nhk.or.jp/kabun-blog/200/245719.html
http://www.sfc.itc.keio.ac.jp/ja/news_targeted_mail_20160524.html

このニュースをザックリ言うと･･･

- 5月24日（日本時間）、慶應義塾大学は、マルウェアが添付された標的型攻撃メールが文部科学省を装って大学職員6名に送信されたことを発表し、注意喚起をしています。

- メールは23日から24日にかけて計6通送信され、件名が『【文科省（ご連絡）】新学術領域研究の中間・事後評価について』、また実在する文科省担当者の名前が書かれており、この担当者が過去に送ったメールの本文が悪用された模様です。

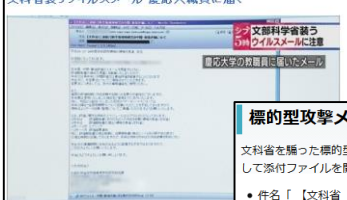
- また、メールアドレスに文科省のドメインの他、自民党佐賀県連のドメイン名も含まれている等、不審な点に職員が気付いたことにより発覚しており、同様のメールが他に発信される恐れがあるとして、文科省も全国の大学や研究機関に注意を呼びかけています。

AUS便りからの所感等

- 今回、一部の職員がメールを開封しましたが、セキュリティシステムが作動したことにより、情報漏えいは防がれた模様です。

- 標的型攻撃では、うっかり添付ファイルを開いてしまう恐れが特に強くなることから、そういったケースを想定しての「出口対策」もUTM等の活用により十分に行う必要があるでしょう。

NHK ONLINE
2016年05月26日（木）
文科省装うウイルスメール　慶応大職員に届く



文部科学省から発信されたように装ったウイル
数の職員に届き、文部科学省は同じようなメー
て、全国の大学や研究機関に注意を呼びかけ

慶應義塾 湘南藤沢 ITC

標的型攻撃メールに関する注意喚起

文科省を騙った標的型攻撃メールが確認されています。以下に類似するメールを受け取っても決して添付ファイルを開かないようご注意ください。

- 件名「【文科省（ご連絡）】新学術領域研究の中間・事後評価について」
- 宛先　業務用の個人アドレス宛
- 差出人 kenjo@mext.go.jp <*****-saga-saga-saga.com@saga-*****.com>のような差出人となっています。
- 添付ファイル　「中間-事後評価に係る様式20160524.zip」

このようなメールを受信しても添付ファイルは絶対に開かずに 速やかにネットワークケーブルを外し、ITC本部へご連絡ください。(内線：22185、22648)
最終更新日: 2016年5月26日