— AUS（アルテミス・ユーザ・サポート）便り 2017/11/06号 —
https://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。

●新型ランサムウェア「Bad Rabbit」発生…国内企業サイトも改ざんで拡散元に

https://internet.watch.impress.co.jp/docs/news/1088055.html
https://internet.watch.impress.co.jp/docs/news/1088502.html
https://www.ipa.go.jp/security/ciadr/vul/20171026-ransomware.html

このニュースをザックリ言うと･･･

- 10月24日（現地時間）、新型のランサムウェア「Bad Rabbit」の感染がロシア・ウクライナや東ヨーロッパで確認されたとして、セキュリティベンダー等より警告が出されています。

- Bad Rabbitは、Windowsの共有フォルダ等に関連する「SMB」プロトコル経由での感染と、Webサイトの閲覧によりFlash Playerのインストーラーに偽装したマルウェア（install_flash_player.exe）が自動的にダウンロードされる「ドライブバイダウンロード攻撃(以下・DBD攻撃)」により、被害が急速に広がったとされています。

- 被害の多くはロシアで発生している一方で日本国内でも被害が報告されており、愛知県のアイカ工業社のWebサイトにおいて、Bad Rabbitの拡散が目的とみられる改ざんが発生していたことも発表されています。

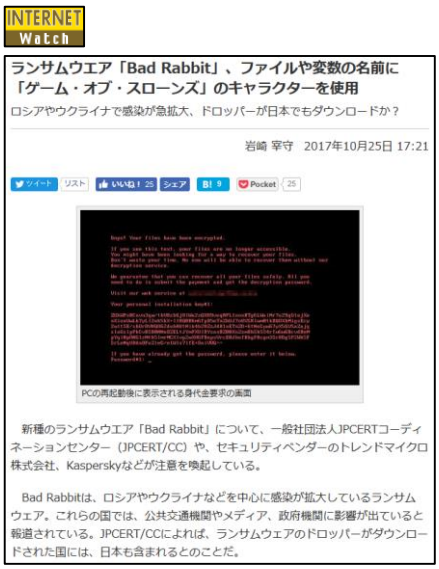
AUS便りからの所感等

- Bad Rabbitは、2016年に発生した「Petya」の亜種とされている一方、DBD攻撃のようにPetyaにはなかった攻撃経路を持つ等、別物とみてよい程の改造がされています。

- 今回のようなDBD攻撃については、不審なサイトからダウンロードしたインストーラーや、ダウンロードフォルダにいつの間にか置かれていたインストーラーを実行しないよう注意することが肝心です。

- OSやブラウザでデフォルトのダウンロード先となっているフォルダから独自のフォルダへ変更すること、またそういったフォルダにファイルを置きっぱなしにせず整理すること、等は自衛策の一つとして有効でしょう。

- Webサイトの改ざんについては、管理者のPCを踏み台にして侵入した可能性も考えられますので、UTMの設置等により、出口対策を考慮したネットワーク構成とすることが不審な外部への通信を遮断するためにも望ましいと言えます。


INTERNET Watch

ランサムウェア「Bad Rabbit」、ファイルや変数の名前に「ゲーム・オブ・スローンズ」のキャラクターを使用

ロシアやウクライナで感染が急拡大、ドロッパーが日本でもダウンロードか？

岩崎 宰守　2017年10月25日 17:21

PCの再起動後に表示される身代金要求の画面

新種のランサムウェア「Bad Rabbit」について、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）や、セキュリティベンダーのトレンドマイクロ株式会社、Kasperskyなどが注意を喚起している。

Bad Rabbitは、ロシアやウクライナなどを中心に感染が拡大しているランサムウェア。これらの国では、公共交通機関やメディア、政府機関に影響が出ていると報道されている。JPCERT/CCによれば、ランサムウェアのドロッパーがダウンロードされた国には、日本も含まれるとのことだ。


INTERNET Watch

ランサムウェア「Bad Rabbit」配布目的で、国内企業サイトが改ざん被害

日本への攻撃は全体の3%か？

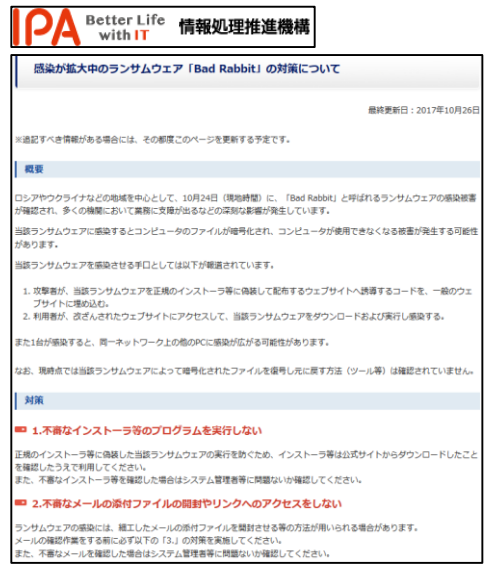
岩崎 宰守　2017年10月27日 13:07

10月24日に感染が拡大したランサムウェア「Bad Rabbit」の配布を目論んだとみられるウェブサイト改ざん被害が、アイカ工業株式会社（愛知県清須市）のウェブサイトで発生した。

Bad Rabbitは、ウェブサイトからAdobe Flashのインストーラーを偽装した「install_flash_player.exe」をダウンロードさせて感染を広げる。

アイカ工業では、25日12時17分にサイトを閉鎖。サイトを管理する外部委託会社やセキュリティベンダーとともに調査を進めたところ、ウェブサーバー内のファイル1つが外部の何者かによって書き換えられ、その後、修復された痕跡があることが、26日15時30分までに判明したという。

AICA
現在ホームページを閉鎖しております。


IPA Better Life with IT 情報処理推進機構

感染が拡大中のランサムウェア「Bad Rabbit」の対策について

最終更新日：2017年10月26日

※追記すべき情報がある場合には、その都度このページを更新する予定です。

概要

ロシアやウクライナなどの地域を中心として、10月24日（現地時間）に、「Bad Rabbit」と呼ばれるランサムウェアの感染被害が確認され、多くの機関において業務に支障が出るなどの深刻な影響が発生しています。

当該ランサムウェアに感染するとコンピュータのファイルが暗号化され、コンピュータが使用できなくなる被害が発生する可能性があります。

当該ランサムウェアを感染させる手口としては以下が確認されています。

1. 攻撃者が、当該ランサムウェアを正規のインストーラ等に偽装して配布するウェブサイトへ誘導するコードを、一般のウェブサイトに埋め込む。
2. 利用者が、改ざんされたウェブサイトにアクセスして、当該ランサムウェアをダウンロードおよび実行し感染する。

また1台が感染すると、同一ネットワーク上の他のPCに感染が広がる可能性があります。

なお、現時点では当該ランサムウェアによって暗号化されたファイルを復号し元に戻す方法（ツール等）は確認されていません。

対策

1.不審なインストーラ等のプログラムを実行しない

正規のインストーラ等に偽装した当該ランサムウェアの実行を防ぐため、インストーラ等は公式サイトからダウンロードしたことを確認したうえで利用してください。
また、不審なインストーラ等を確認した場合はシステム管理者等に問題ないか確認してください。

2.不審なメールの添付ファイルの開封やリンクへのアクセスをしない

ランサムウェアの感染には、細工したメールの添付ファイルを開封させる等の方法が用いられる場合があります。
メールの確認作業をする前に必ず以下の「3.」の対策を実施してください。
また、不審なメールを確認した場合はシステム管理者等に問題ないか確認してください。

●Webサイト売買サービスから顧客情報14612件が流出

http://itpro.nikkeibp.co.jp/atcl/news/17/103002551/

このニュースをザックリ言うと・・・

- 10月30日（日本時間）、GMOインターネット社より、同社が運営するWebサイト売買サービス「サイトM&A」が不正アクセスを受け、顧客情報が流出したことが発表されました。

- 被害を受けたのは今年5月17日までに登録した会員1万4612件についての情報で、氏名・ユーザ名・法人名・住所・生年月日・電話番号・メールアドレス・登録案件・問い合わせおよび査定内容とされており、クレジットカード情報は含まれていないとのことです（「サイトM&Aマーケット」の方に登録したユーザについては影響はないとされています）。

- 9月14日に顧客情報が外部サイトで閲覧可能な状態になっているとの通報があったことから発覚しており、調査の結果、サーバの脆弱性を悪用しての不正アクセスを受けた可能性が高いと判断したとのことです。

AUS便りからの所感等

- 流出した個人情報はインターネット上の様々な場所にアップロードされた他、Amazonの電子書籍サイト「Kindle Store」で一時販売されていた等の情報もあります。

- GMO社では流出した顧客情報の削除を各方面へ依頼しているとのことで、Kindle Storeからは削除されていますが、一旦流出した個人情報が悪意を以て拡散される行為を根絶するには長い時間がかかることでしょう。

- 同社では、システムを新たに構築し直すと同時に、第三者のセキュリティ専門機関によるチェックを受け、さらにWebアプリケーションファイアウオール（WAF）などの対策を導入したとされておりますが、導入されたセキュリティ対策が適切に機能しているか、以後も定期的にチェックを行うこともまた重要です。

●「WannaCry」被害の英病院、パッチ適用の警告を無視していた

https://japan.zdnet.com/article/35109537/

このニュースをザックリ言うと・・・

- イギリス国民保健サービス（NHS）関連の病院でランサムウェア「WannaCry(WannaCrypt)」への感染が発生し、システムダウンに見舞われたと5月13日（現地時間）に発表された件について、システムへのパッチ適用を求める警告がありながら、多くの病院が実行していなかったことが英会計検査院（NAO）より発表されています。

- 発表によれば、NHSのデータおよびIT部門であるNHS Digitalより、WannaCryのような攻撃を予防するため、3月～4月を通してさまざまな組織に緊急アラートを発し、システムにパッチを適用するよう警告が出されていましたが、それ以前の2014年にも、英保健省と内閣府から、2015年4月までにWindows XP等からの移行を完了する計画の策定が勧告されていたとのことです。

- こういった警告・勧告にも拘らず、NHS内部ではXP等が使われ続け、結果としてNHS関連病院の3分の1がWannaCryの被害を受けたとされています。

AUS便りからの所感等

- Windows XPのサポートは2014年4月に終了していますが、3年が経過しようとしていた今年3月でも依然として利用が多かったことから、WannaCryが悪用するSMBv1の脆弱性のパッチ（MS17-010）がXP向けにもリリースされたという経緯があります。

- サポートが終了したOSにおいては、このようなパッチのリリースはあくまで特例に過ぎないこと、移行へのコストを渋ることによりマルウェアへの感染でそれ以上の損害費用が発生し得ること、等を十分考慮し、それでもそういった古いOSを使い続けるのであれば、データの損失や周辺への感染を最小限に留めるため、データバックアップやUTM等による隔離等の十分な対策をとる必要があります。