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。

●ランサムウェア「vvvウイルス」への感染報告相次ぐ･･･Flash Player等の更新は確実に

http://internet.watch.impress.co.jp/docs/news/20151207_734143.html
http://internet.watch.impress.co.jp/docs/news/20151208_734342.html
http://blog.trendmicro.co.jp/archives/12632

このニュースをザックリ言うと･･･

- 12月6日（日本時間）以降、ランサムウェア「CrypTesla（TeslaCrypt）」の感染報告が日本国内で多く報告されています。

- 感染により、PC上のファイルが暗号化されてしまい、その際ファイルに「.vvv」という拡張子が追加されることから「vvvウイルス」という通称で呼ばれています。

- トレンドマイクロ社では、主な感染経路として、12月1日以降vvvウイルスが添付されたメールを全世界で19,000通以上確認している他、イギリス大手紙サイトが改ざんされてvvvウイルスが埋め込まれた事例も取り上げています（他にも「不正な広告から感染する」という説もあります）。

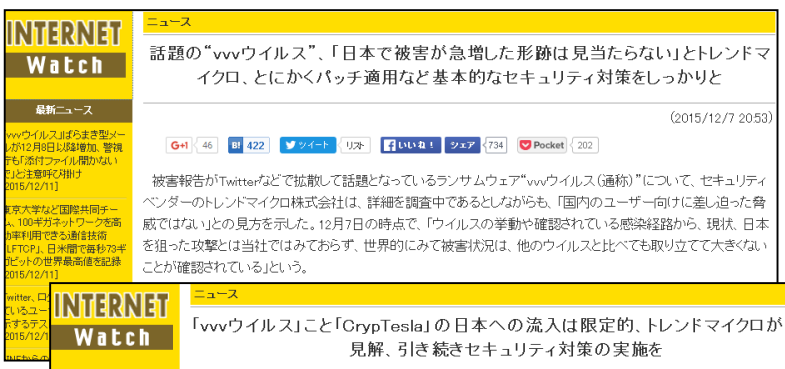
- 一方で、こういったメールやサイト改ざんによる国内への流入は限定的としており、「わかりやすい特徴を持つ脅威ほど、実際の影響に関わらずネット上で大げさに伝わる」とはしているものの、「脆弱性対策等を怠りなくとること」「ランサムウェアによる攻撃の手口を把握して慎重に行動すること」「感染に備えて重要なファイルのバックアップをとっておくこと」を推奨しています。

AUS便りからの所感等

- 前述したサイトの改ざんでの感染において、10月に対策されたFlash Playerの脆弱性を突いていたとされていること等から、あらゆるマルウェアへの根本的な感染予防策となる「PCのOSと各種アプリケーションを最新バージョンに保つこと」はここでも有効となり得ますし、加えて「FlashやJavaプラグインを無効化する、ないし限定的に有効化すること」も効果的でしょう。

- もちろん、特にアップデートが完全に終わっていないPCへの感染等に対し、アンチウイルス・UTMによる防御は重要です。

- なお、ファイルのバックアップに関しては、ランサムウェアがバックアップ先まで暗号化してしまう可能性を考慮し、PCと常時接続されているようなバックアップシステムは避け、USB接続のHDDをバックアップ時にのみ接続する等の方法をとるべきともされています。


INTERNET Watch

ニュース

話題の“vvvウイルス”、「日本で被害が急増した形跡は見当たらない」とトレンドマイクロ、とにかくパッチ適用など基本的なセキュリティ対策をしっかりと

(2015/12/7 20:53)

G+1 46 B! 422 ツイート リスト いいね！ シェア 734 Pocket 202

被害報告がTwitterなどで拡散して話題となっているランサムウェア“vvvウイルス（通称）”について、セキュリティベンダーのトレンドマイクロ株式会社は、詳細を調査中であるとしながらも、「国内のユーザー向けに差し迫った脅威ではない」との見方を示した。12月7日の時点で、「ウイルスの挙動や確認されている感染経路から、現状、日本を狙った攻撃とは当社ではみておらず、世界的にみて被害状況は、他のウイルスと比べても取り立てて大きくないことが確認されている」という。


INTERNET Watch

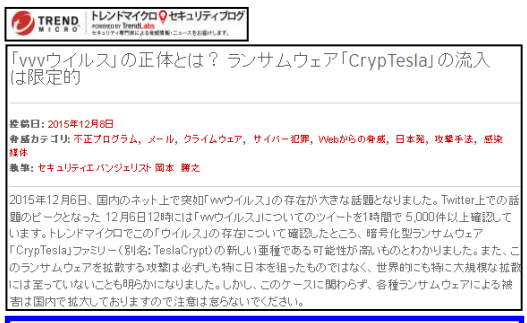
ニュース

「vvvウイルス」こと「CrypTesla」の日本への流入は限定的、トレンドマイクロが公式見解、引き続きセキュリティ対策の実施を

(2015/12/8 20:33)

G+1 6 B! 29 ツイート リスト いいね！ シェア 103 Pocket 31

トレンドマイクロ株式会社は8日、Twitterなどで被害情報が拡散されているランサムウェア「vvvウイルス」の見解について、同社公式ブログで公開した。同社によると、vvvウイルスは日本をターゲットにしたものではなく、日本への流入も限定的だとしている。


TREND MICRO トレンドマイクロ セキュリティブログ

「vvvウイルス」の正体とは？ ランサムウェア「CrypTesla」の流入は限定的

投稿日：2015年12月8日
脅威カテゴリ：不正プログラム，メール，クライムウェア，サイバー犯罪，Webからの脅威，日本発，攻撃手法，感染媒体
執筆：セキュリティエバンジェリスト 岡本 勝之

2015年12月6日、国内のネット上で突如「vvvウイルス」の存在が大きな話題となりました。Twitter上での話題のピークとなった 12月6日12時には「vvvウイルス」についてのツイートを1時間で 5,000件以上確認しています。トレンドマイクロでこの「ウイルス」の存在について確認したところ、暗号化型ランサムウェア「CrypTesla」ファミリー（別名：TeslaCrypt）の新しい亜種である可能性が高いものとわかりました。また、このランサムウェアを拡散する攻撃は必ずしも特に日本を狙ったものではなく、世界的にも特に大規模な拡散には至っていないことも明らかになりました。しかし、このケースに関わらず、各種ランサムウェアによる被害は国内で拡大しておりますので注意は怠らないでください。

vvvウイルスは、暗号化型ランサムウェア「CrypTesla（クリプトテスラ）」（別名：TeslaCrypt）ファミリーの亜種の可能性が高く、ほかの暗号化型ランサムウェアと同様、侵入したPC内のファイルを暗号化し、復号化と引き換えに身代金を要求する。この際、暗号化されたファイルを「.vvv」に変える特徴からvvvウイルスと呼ばれるようになった。

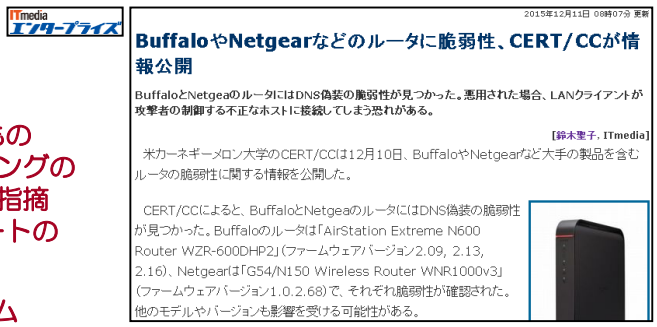
●ブロードバンドルータのDNS機能に脆弱性

http://www.itmedia.co.jp/enterprise/articles/1512/11/news059.html

このニュースをザックリ言うと・・・

- 12月10日（米国時間）、米CERT/CCより、複数メーカーのブロードバンドルータのDNSサービス機能に脆弱性が存在するとして警告が出されました。

- 問題が報告されているのは、Buffalo「AirStation Extreme N600 Router WZR-600DHP2（ファームウェアバージョン2.09, 2.13, 2.16）」、Netgear「G54/N150 Wireless Router WNR1000v3（ファームウェアバージョン1.0.2.68）」となっており、いずれも外部DNSサーバへの問合せ時に毎回同じUDP発信元ポートを用いるため、第三者が偽の応答パケットを送信することにより、不正なDNS情報をキャッシュさせられる可能性がある模様です。


ITmedia エンタープライズ

2015年12月11日 08時07分 更新

BuffaloやNetgearなどのルータに脆弱性、CERT/CCが情報公開

BuffaloとNetgeaのルータにはDNS偽装の脆弱性が見つかった。悪用された場合、LANクライアントが攻撃者の制御する不正なホストに接続してしまう恐れがある。

[鈴木聖子, ITmedia]

米カーネギーメロン大学のCERT/CCは12月10日、BuffaloやNetgearなど大手の製品を含むルータの脆弱性に関する情報を公開した。

CERT/CCによると、BuffaloとNetgeaのルータにはDNS偽装の脆弱性が見つかった。Buffaloのルータは「AirStation Extreme N600 Router WZR-600DHP2」（ファームウェアバージョン2.09, 2.13, 2.16）、Netgearは「G54/N150 Wireless Router WNR1000v3」（ファームウェアバージョン1.0.2.68）で、それぞれ脆弱性が確認された。他のモデルやバージョンも影響を受ける可能性がある。

AUS便りからの所感等

- 不正なDNS情報をキャッシュさせようとする、いわゆる「DNSキャッシュポイズニング」攻撃は非常に古典的なものですが、発信元ポートが固定の場合にキャッシュポイズニングの標的とされやすいことは既にセキュリティ研究者によって指摘されており、多くのDNSサーバプロダクトでは発信元ポートのランダム化による対策が行われています。

- 今回問題があった各ルータについては、近日中にファームウェアのアップデートが行われるとみられますので、メーカーサイトを随時確認して対応することを推奨しますが、普段からの回避策としては、独自にDNSキャッシュサーバを立てるか、ISPが提供するDNSサーバを利用することが挙げられます。

- この他、UTMの機能次第では、万が一キャッシュポイズニングが発生した場合の不正なサイトへの誘導を検知することも期待できるでしょうが、UTM自体に脆弱性が存在する可能性についても注意し、こちらについてもメーカー情報を随時確認すべきです。

●「SQL Server 2005」が2016年4月にサポート終了

http://cloud.watch.impress.co.jp/docs/news/20151202_733351.html

このニュースをザックリ言うと・・・

- 12月2日（日本時間）、日本マイクロソフト社より、同社の「SQL Server 2005」が2016年4月12日にサポート期限が切れることを受けて、最新状況と移行支援策等に関する説明会が行われました。

- 同社によれば、2015年12月現在、国内で約12万台のSQL Server 2005が稼働しており、うち約7万台が会計パッケージソフト等に組み込まれた無償版とみられています。
（また、これらのうち32%が会計、16%が人事のシステムで利用されているとのことです。）

- 同社では移行等に関する情報ポータルを立ち上げており、全国400社のパートナー企業とともに告知と移行支援を行っていくとしています。


クラウド Watch

2015年12月11日

日ヒューレット・パッカード、またな「HPE 3PAR StoreServ」ソリューション
[2015/12/11]

生、自動仕訳サービス「YAYOI SMART CONNECT」強化、データ取得がよりシンプルに
[2015/12/11]

スク、Synology製の2ドライNAS「DiskStation DS216j」発売
[2015/12/11]

TT Com、インドで国内ネットークサービスを提供

ニュース

「SQL Server 2005」は2016年4月12日サポート終了、早急な移行計画の策定を

日本では約12万台が稼働中、うち約7万台は会計ソフトなどに組み込まれている無償版

(2015/12/2 16:07)

G+1 11 B! 5 ツイート リスト いいね！ シェア 38 Pocket 12

日本マイクロソフト株式会社は2日、「Microsoft SQL Server 2005」が2016年4月12日（日本時間）にサポートを終了することについて、最新状況と移行支援策に関する説明会を開催した。

SQL Server 2005は、2005年12月に提供を開始したデータベース製品。メインストリームサポート期間の5年間と、延長サポート期間の5年間を経て、2016年4月12日にサポート終了となり、以降はセキュリティ更新プログラムの提供も行われなくなるため、マイクロソフトでは新しい環境への移行を呼び掛けている。

AUS便りからの所感等

- 2005よりも後のバージョンのSQL Serverとしては2008・2008 R2・2012・2014があり、例えば2014のサポート期限は2024年7月となっていますが、2014へアップグレードを行った後も、約8年後にさらなるアップグレードが必要となる段階で慌てることなく、適宜スムーズなアップグレードを行えるよう計画しておくべきでしょう。

- 2016年からはマイナンバー制度の開始により、全従業員等のマイナンバーをデータベースに保存するといった状況も発生し、なおのこと機密情報・個人情報を保存するデータベースサーバについて、特に内部からの不正アクセスによるセキュリティ侵害を警戒する必要があります。

- DBサーバへの不正アクセスの防止および内部からの情報流出の検知のため、UTMをはじめとする各種ソリューションについても併せて導入を検討することを推奨します。