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。

●日本を狙った複数の「ランサムウェア」が確認される

http://internet.watch.impress.co.jp/docs/news/20141216_680615.html
http://www.symantec.com/connect/blogs/torlocker

このニュースをザックリ言うと･･･

- 12月16日（日本時間）、大手セキュリティベンダーのシマンテック社が「TorLocker」と呼ばれるランサムウェア（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）の亜種について、同社ブログで日本のユーザに対し警告しています。

- 同社によれば、日本はアメリカに次いでランサムウェアの被害を受けている国ではあるものの、今回確認されたランサムウェアは日本語のメッセージをポップアップ表示する等、日本のユーザを明確に標的とする点が特徴であるとのことです。

- また、最近の事例として、日本の出版社のサイトがクラックされて不正なWebサイトにリダイレクトされる、あるいはブログサイトが改ざんされて偽のFlash Playerのダウンロードサイトにされるというケースが紹介されており、これらもランサムウェアへの感染を狙ったものとされています。

AUS便りからの所感等

- 「ランサムウェア」という名前や、PC上のファイルが人質にとられるという攻撃は一見独特ですが、つまるところ、一旦感染したらPC上のファイルを破壊されることと同然のことであり、復旧できる可能性を信じて要求に安易に乗るべきではありません。

- シマンテック社も推奨していることであり、かつマルウェアに感染しないための基本となりますが、OSやアプリケーションを最新に保つこと、アンチウイルスとUTMによる防御を確実に行うことがやはり重要となるでしょう。


INTERNET Watch

ニュース

日本を狙った複数の"ランサムウェア"が活動中、ファイルを人質に身代金要求～「俺は君の20年後を見ている」などと脅迫

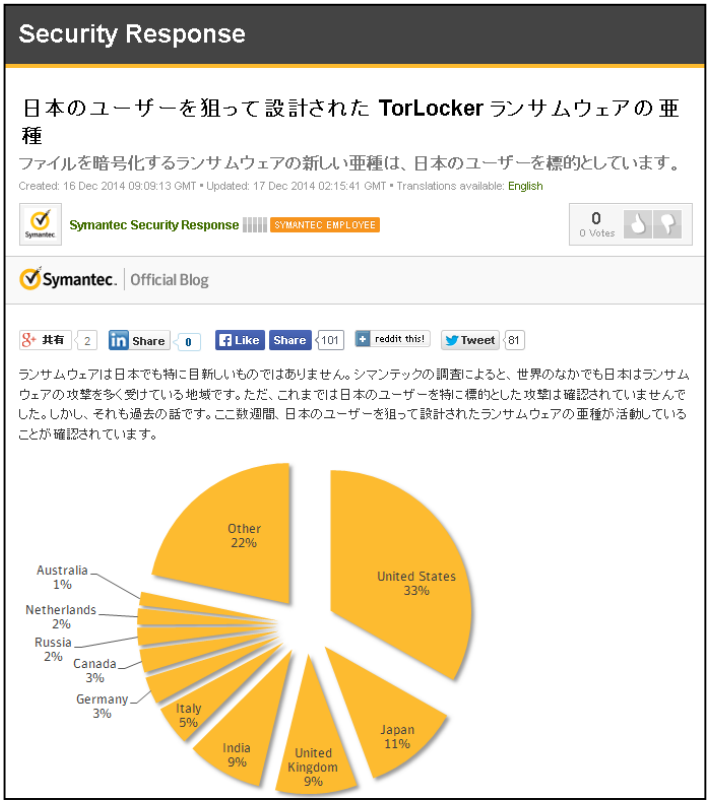
(2014/12/16 21:21)

ランサムウェア「TorLocker」において、特に日本のPCユーザーを狙って設計された日本語ローカライズ版の亜種が複数確認されているという。株式会社シマンテックが同社公式ブログの12月16日付記事で伝えている。

ランサムウェアが「TorLocker」の日本語ローカライズ版亜種によって表示されるポップアップウィンドウ（シマンテック公式ブログより）

ランサムウェアとは、感染したPC内のファイルを勝手に暗号化して開けないようにすることで人質にとり、復号化したければ身代金を支払えと要求してくるウイルスのこと。シマンテックによると、こうしたランサムウェアによる攻撃件数の国別内訳で日本は11%を占めており、米国の33%に次いで2番目（2014年11月のデータ）。世界の中でも日本はランサムウェアの攻撃を多く受けている地域だが、これまでは日本のユーザーを特に標的とした攻撃は確認されていなかったとシマンテックでは説明している。

ランサムウェアとは、感染したPC内のファイルを勝手に暗号化して開けないようにすることで人質にとり、復号化したければ身代金を支払えと要求してくるウイルスのこと。シマンテックによると、こうしたランサムウェアによる攻撃件数の国別内訳で日本は11%を占めており、米国の33%に次いで2番目（2014年11月のデータ）。世界の中でも日本はランサムウェアの攻撃を多く受けている地域だが、これまでは日本のユーザーを特に標的とした攻撃は確認されていなかったとシマンテックでは説明している。


Security Response

日本のユーザーを狙って設計された TorLocker ランサムウェアの亜種

ファイルを暗号化するランサムウェアの新しい亜種は、日本のユーザーを標的としています。

Created: 16 Dec 2014 09:09:13 GMT • Updated: 17 Dec 2014 02:15:41 GMT • Translations available: English

Symantec Security Response SYMANTEC EMPLOYEE 0 Votes

Symantec. Official Blog

共有 2 Share 0 Like Share 101 reddit this! Tweet 81

ランサムウェアは日本でも特に目新しいものではありません。シマンテックの調査によると、世界のなかでも日本はランサムウェアの攻撃を多く受けている地域です。ただ、これまでは日本のユーザーを特に標的とした攻撃は確認されていませんでした。しかし、それも過去の話です。ここ数週間、日本のユーザーを狙って設計されたランサムウェアの亜種が活動していることが確認されています。

●ラックが2014年のサイバー事件・事故を総括

http://itpro.nikkeibp.co.jp/atcl/news/14/121702300/

このニュースをザックリ言うと・・・

- 12月16日、国内大手セキュリティベンダーのラック社が2014年のサイバー事件・事故を総括する報道陣向けの説明会を開催しました。

- 今回の発表では、
①最近発生したソニーピクチャーズからの情報流出のような「サイバー犯罪のO2O(オンライン・ツー・オフライン)」が鮮明になったこと
②国内においてベネッセ等の印象的な内部犯行による事件が多かったこと
③影響の大きい脆弱性に「Heartbleed」「ShellShock」といったニックネームが付けられていたこと
等が挙げられています。

- また、今年露見した三つの重大な課題として、「脆弱性対応のスキームの破たん」「標的型攻撃の常態化」「内部犯行の被害の表面化」が挙げられており、例えば一番目については「バージョンアップによる機能の増加が新しい脆弱性を抱えるというリスク」について指摘した上で、自組織で使用しているソフトウェアにおいて公表された脆弱性がどう影響するか把握し、パッチの適用か、運用でのカバーかの判断を行うこと、またパッチの適用までの間はWAF(Webアプリケーションファイアウォール)による一時的防御も重要であると説明しています。

AUS便りからの所感等

- 例えば、Linuxディストリビューションの安定版でインストールされる各ソフトウェアパッケージでは、最新バージョンを常に追いかけるということはせず、以前のバージョンをベースに独自にセキュリティパッチを当てていくといった形で対応することがあります。

- もし、ディストリビューションが提供するパッケージに必要な機能がない等の理由で、別途最新のバージョンを独自に導入するのであれば、脆弱性が修正され次第その対策バージョンへ更新し続けていくという運用を常時責任をもって行うことに注意すべきでしょう。

●「Wordpress」に感染するロシア製マルウェア

http://www.gizmodo.jp/2014/12/wordpress.html

このニュースをザックリ言うと・・・

- 12月15日（米国時間）、セキュリティベンダーのSucuri社がブログツール「Wordpress」に感染するロシア製マルウェア「SoakSoak」について警告しています。

- SoakSoakは、Wordpressプラグイン「Slider Revolution」の脆弱性を突いて感染するものとされており、有料ながら非常に人気の高いプラグインであることから、Wordpressを導入している10万以上のサイトが感染している模様ですが、感染後どういった行動をするのかは不明とのことです。

AUS便りからの所感等

- 前述した別のニュースでも挙げられていますが、利用している全てのソフトウェアに脆弱性が存在しないか把握しておくことは、自らがマルウェアの拡散に加担する加害者とならないためにも、セキュリティリスクのマネジメントにおいて欠かせないものです。

- もちろん、ユーザ側にとっても、サイトの閲覧によってPCがマルウェアに感染する可能性を防ぐため、各種ソフトウェアを最新に保ち、アンチウイルス・UTMを導入することは重要です。

セキュリティ , ニュース , 犯罪

謎のロシア製マルウェアがWordpressのサイトを狙って拡散中

2014.12.16 20:00

Wordpressでサイトを運用している方、ご注意！

ロシア製のマルウェア、「**SoakSoak**」が急激に広まっています。日曜日から確認されたものだけでも、すでに約**10万以上**のサイトに影響が及んでいると見られ、グーグルはすでに1万1,000サイトをブロックしました。

セキュリティ関連企業**Sucuri**の指摘によると、これは、スライドショーを簡単に作れることで大変人気のあるプラグイン「**Slider Revolution**」の脆弱性を狙ったものとのこと。Slider Revolutionの開発チームは、少なくとも9月にはこの脆弱性を知っていたのにその対策を怠っていたとも指摘しています。

Sucuriはまた、このマルウェアの根絶は**とても難しい**とも指摘しています。なぜなら、Slider Revolutionはその人気のためテーマに最初から入っていることも多く、自身のサイトにSlider Revolutionが入っていることを**そもそも知らない人が多い**ためです。さらに悪いことに、この脆弱性を回避するにはプラグインの更新が必要なのですが、あらかじめテーマに入っているSlider Revolutionは自動アップデートの対象にならないため、手動で更新する必要があるとのことです。