— AUS（アルテミス・ユーザ・サポート）便り 2016/02/29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。

●ランサムウェアで病院システムがダウン、身代金を支払って復旧

http://www.itmedia.co.jp/enterprise/articles/1602/18/news061.html
http://www.itmedia.co.jp/enterprise/articles/1602/19/news063.html

このニュースをザックリ言うと･･･

- 2月17日（現地時間）、米ロサンゼルス市内の病院「Hollywood Presbyterian Medical Center」のシステムがランサムウェアに感染してダウンする事態が発生していたと地元メディアが報じました。

- 同病院は2月5日の時点で「重大なIT問題」に見舞われたとして院内で非常事態を宣言しており、この時点で感染が発生していた模様で、これにより、「救急患者が別の病院に搬送された」「電子メールが使えずFAXが混雑状態になった」「電子カルテも使えず診察記録は手書きで記録している」等の事態となったとされています。

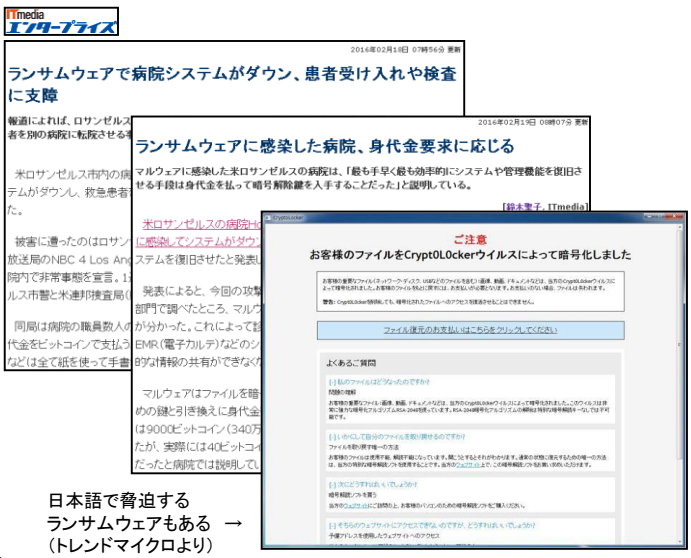
- ランサムウェアにより、多額の身代金をビットコイン（暗号通貨）(※)で支払うよう脅迫されていましたが、17日、病院側は結局17,000ドル（約190万円以上）相当のビットコイン支払いに応じ、システムが復旧したことを発表しています。

AUS便りからの所感等

- 病院のシステムダウンによるトラブル発生の事案としては、1月18日にもオーストラリアの病院で使用されていたWindows XPがウイルスに感染したケースが発生しており、このときも職員が手作業やFAX・電話でのやりとりを余儀なくされています（AUS便り2016/02/01号参照）。

- 身代金を支払うべきか否かについて、今回FBIは「身代金を払えば暗号化されたファイルにアクセスできるようになる、場合によっては要求に応じるよう被害者に助言することもある」としていた一方で、米セキュリティ機関のUS-CERT等のように「身代金を払ってもシステムを復旧できるとは限らない、要求に応じてはいけない」と指摘する声などそれぞれありますが、今回のようなケースや、分析により復号化が可能だったケースもあるとは言え、当便りでは、ランサムウェアへの感染は事実上ファイルを破壊されるも同然であると考えます。

- ランサムウェアの動向について随時情報収集を行い、万が一の感染による被害を最小限に抑えるためのシステム構成をとること、もちろんアンチウイルス・UTMの設置等によりとにかく感染しないよう防御を固めることが肝要です。



日本語で脅迫するランサムウェアもある →
（トレンドマイクロより）

コトバンク

（※）ビットコイン　びっとこいん　bitcoin

インターネット上で流通している電子マネー。通貨の単位はBTC。紙幣・硬貨は発行されていないため、「仮想通貨」「デジタル通貨」などとも呼ばれる。流通を管理する事業主体や国家もなく、中央銀行のようなものも存在しない。米ドルや円など現実通貨との交換は、ウェブ上の「取引所」を通して行われるが、決済は金融機関を通さないため、諸経費や手数料などが発生しない。そのため、小口の売買やP2P(個人同士)の取り引き、とりわけ国境を越えた送金・決済に利用されている。

2009年5月、サトシ・ナカモトと名乗る人物が論文でその原理を発表し、「非・中央集権」の仕組みに共感したハッカーたちが開発・普及させた。サトシ・ナカモトの正体は不明。通貨の発行は、ユーザーが高度な演算問題を解く「mining(採掘)」という作業などを通して行われる。ただし、その演算処理は発行量が増えるに従って複雑になり、また2100万BTC以上は創出できないように設計されている。当初は、IT(情報技術)の専門家やマニアが集う一部のネット空間で利用されていたが、次第に大手事業者が決済に採用するようになり、11～12年にかけて顕在化したキプロス金融危機の際には、「金」に近い安定した通貨として注目が集まった。現実通貨との交換レートは、需給関係や経済状況に左右され、投機の影響も受けやすいため、乱高下を繰り返している。こうした為替リスクに加え、資金洗浄など不正な取り引きの温床になっているという批判もある。しかし、手軽さや利便性の高さが人気で、開発からわずか4年の2013年4月には流通量10億ドルを超えるまでに成長した。

●glibcに脆弱性、Linuxを使用するネットワーク機器等に影響

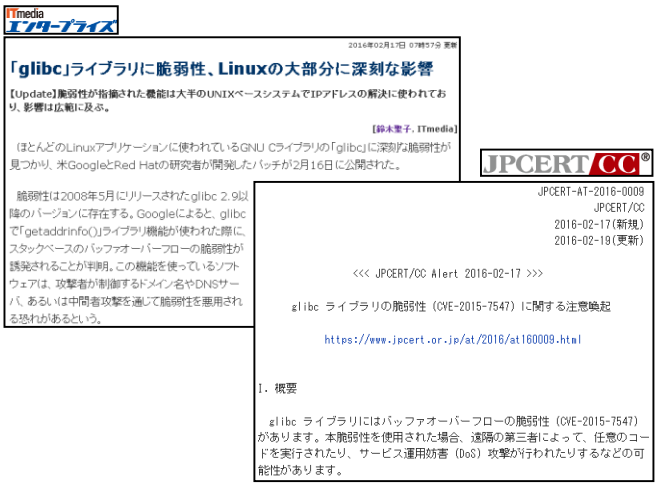
http://www.itmedia.co.jp/enterprise/articles/1602/17/news065.html

このニュースをザックリ言うと･･･

- Linuxの共有ライブラリ「glibc」にバッファオーバーフローの脆弱性「CVE-2015-7547」が見つかったとして、2月17日（日本時間）頃からJPCERT/CC・JPRS等が警告しています。

- 問題となっているのは、glibcに含まれるgetaddrinfo（ドメイン名のIPアドレスへの変換などを行うライブラリ関数）で、問合せ先のDNSサーバから2048バイト以上の長大なDNSレスポンスパケットを受信することにより、getaddrinfoを実行しているプログラムを乗っ取られる可能性があるとされています。

- 既にglibcに対するセキュリティパッチがリリースされ、Linuxの各種ディストリビューションでも提供されている他、Linuxベースのネットワーク機器においてもファームウェアのアップデートが提供されているところもあります。


ITmedia エンタープライズ

2016年02月17日 07時57分 更新

「glibc」ライブラリに脆弱性、Linuxの大部分に深刻な影響

【Update】脆弱性が指摘された機能は大半のUNIXベースシステムでIPアドレスの解決に使われており、影響は広範に及ぶ。

[鈴木聖子, ITmedia]

ほとんどのLinuxアプリケーションに使われているGNU Cライブラリの「glibc」に深刻な脆弱性が見つかり、米GoogleとRed Hatの研究者が開発したパッチが2月16日に公開された。

脆弱性は2008年5月にリリースされたglibc 2.9以降のバージョンに存在する。Googleによると、glibcで「getaddrinfo()」ライブラリ機能が使われた際に、スタックベースのバッファオーバーフローの脆弱性が誘発されることが判明。この機能を使っているソフトウェアは、攻撃者が制御するドメイン名やDNSサーバ、あるいは中間者攻撃を通じて脆弱性を悪用される恐れがあるという。

JPCERT CC®

JPCERT-AT-2016-0009
JPCERT/CC
2016-02-17(新規)
2016-02-19(更新)

<<< JPCERT/CC Alert 2016-02-17 >>>

glibc ライブラリの脆弱性（CVE-2015-7547）に関する注意喚起

https://www.jpcert.or.jp/at/2016/at160009.html

1. 概要

glibc ライブラリにはバッファオーバーフローの脆弱性（CVE-2015-7547）があります。本脆弱性を使用された場合、遠隔の第三者によって、任意のコードを実行されたり、サービス運用妨害（DoS）攻撃が行われたりするなどの可能性があります。

AUS便りからの所感等

- glibcはLinux上で最も重要なライブラリであり、今回の脆弱性はDNSサーバに問合せを行う、ひいてはネットワーク通信を行う全てのプログラムに影響する恐れがあります。

- 回避策として、長大なDNSレスポンスパケット（UDP/TCP両方）の受信を拒否することが挙げられており、OS上でのiptablesの使用、あるいはファイアウォール・UTMで設定を行うことも考えられますが、副作用の発生や結局効果がない等の恐れもありますので、技術的に正確に理解できない限りは、速やかにパッチの適用を行うことを優先すべきでしょう。

●WordPress・Joomla!・Drupal･･･JPCERT/CCが改ざんされる傾向があるCMSのPHPファイルを指摘

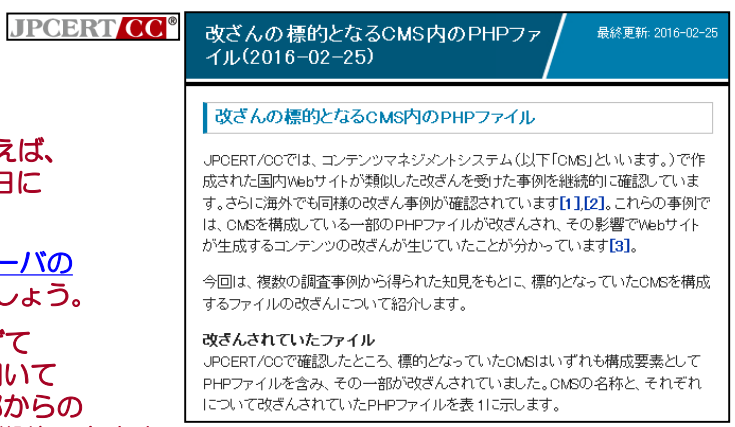
http://www.jpcert.or.jp/magazine/acreport-cms.html

このニュースをザックリ言うと･･･

- 2月25日（日本時間）、セキュリティ専門機関JPCERT/CCが「改ざんの標的となるCMS内のPHPファイル」と題した記事を発表しています。

- 記事では、特にPHPファイルが狙われ、改ざんされる傾向がある代表的なコンテンツ管理システム（CMS）として、「WordPress」「Joomla!」「Drupal」および「MODX」を挙げています。

- JPCERT/CCでは、該当するCMSを利用している場合、「不正コードが追加されていないかどうかを調査すること」「CMSとそのプラグインを常に最新のバージョンにアップグレードすること」「パスワードの管理を適切に行うこと」を推奨しています。


JPCERT CC®

改ざんの標的となるCMS内のPHPファイル(2016-02-25)

最終更新: 2016-02-25

改ざんの標的となるCMS内のPHPファイル

JPCERT/CCでは、コンテンツマネジメントシステム（以下「CMS」といいます。）で作成された国内Webサイトが類似した改ざんを受けた事例を継続的に確認しています。さらに海外でも同様の改ざん事例が確認されています[1],[2]。これらの事例では、CMSを構成している一部のPHPファイルが改ざんされ、その影響でWebサイトが生成するコンテンツの改ざんが生じていたことが分かっています[3]。

今回は、複数の調査事例から得られた知見をもとに、標的となっていたCMSを構成するファイルの改ざんについて紹介します。

改ざんされていたファイル

JPCERT/CCで確認したところ、標的となっていたCMSはいずれも構成要素としてPHPファイルを含み、その一部が改ざんされていました。CMSの名称と、それぞれについて改ざんされていたPHPファイルを表1に示します。

AUS便りからの所感等

- 挙げられているCMSは利用者が多く、一方でセキュリティパッチも度々リリースされており、例えば、WordPressは1月に、Drupalはつい先日の2月24日に最新バージョンがリリースされています。

- 攻撃の傾向を速やかに把握するためには、Webサーバのアクセスログを確認・分析することが一助となるでしょう。

- 社内ネットワークでWebサーバとCMSを立ち上げてコンテンツを公開しているケースでは、UTM等を用いてサーバをDMZ下に配置することにより、外部・内部からのPHPファイルを狙った攻撃を検知・遮断することが期待できます。