— AUS（アルテミス・ユーザ・サポート）便り 2019/07/22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。

●46MBが4.5PBに膨れ上がる危険なZIP爆弾に注意

https://news.mynavi.jp/article/20190717-860624/
https://gigazine.net/news/20190705-zip-bomb/
https://internet.watch.impress.co.jp/docs/yajiuma/1196892.html

このニュースをザックリ言うと・・・

- 7月2日（現地時間）、プログラマーのDavid Fifield氏により、ZIPファイルを展開（解凍）することで極めて大容量のファイルが生成される「ZIP爆弾」の新種について発表がありました。

- 発表では、同氏が作成した3つのZIP爆弾の例として、「①42KBのファイルが5.5GBに」「②10MBのファイルが281TBに」「③46MBのファイルが4.5PB(4,507TB)に」膨れ上がるものが示されており、例えば②の場合はわずか10MBから281TBへというように2800万倍に膨らみます。

- これまでにも存在した、大量のZIPファイルを何重にも入れ子にして圧縮する、いわゆる「再帰型」のZIP爆弾と異なり、今回のものは特殊な方法により一度だけの圧縮で生成される「非再帰型」とされ、現時点で各種アンチウイルスは対応していないとのことです。

AUS便りからの所感等

- 再帰型のZIP爆弾は巨大なファイルの出力まで複数段階のZIPファイルの展開が必要なことや、登場から年月が経ったこともあって、各種アンチウイルスでは既に対応されています。

- 非再帰型についても今後同様に対応されるものと思われますが、一度の展開だけで極端に大容量のファイルが出力されることにより、再帰型のように「ある段階以上に入れ子になったZIPファイルは無条件で削除」といった対応ができないことから、これまでと異なるアプローチでの対応が必要になるとみられます。

- ともあれ、ファイルのスキャンだけで、アンチウイルスソフトやUTMにディスク・メモリ等のリソースを浪費させるよう仕向けられる恐れがあり、これを悪用したメールが大量にばら撒かれるまでに如何に早く対応されるかが注目されるでしょう。

マイナビニュース


46MBが4.5PBに膨れ上がる危険なZIP爆弾に注意

後藤大地　2019/07/17 09:29

Fossbytesは7月13日(米国時間)、「This Dangerous 'Zip Bomb' Can Explode 46MB File Into 4.5 Petabytes」が、「Zip Bomb (ZIP爆弾)」と呼ばれる高圧縮ファイル爆弾に新たな方法が発見されたと伝えた。この方法を使うと、46MBのZIPファイルを展開することで4.5PBのサイズに膨張させることが可能とされており、注意が必要。

記事はDavid Fifield氏が公開した次のドキュメントがベースになっている。

説明によれば、ZIPコンテナ内部でファイルを重ね合わせることで高い圧縮率を実現したという。従来は再帰的な方法を使うことで高圧縮を実現していたが、今回発見された方法は再帰的な方法は使っておらず、1回の解凍で完全に展開されると説明がある。この方法を使うことでZIP形式の限界まで広げることが可能で、10MBのZIPファイルが281TBまで展開されるという。

64ビット拡張を使った場合はさらにファイルサイズを拡張することが可能で、46MBを4.5PBまで拡張できるとしている。また、報告されている方法は一般的な圧縮アルゴリズムDEFLATEのみを使用しているため、ほとんどのZIPパーサと互換性があるという。

この手法はまだ報告されてから日が浅いうえ、従来の再帰的手法に依存していないため、既存のセキュリティソフトウェアでは検出が困難な可能性があるとされている。Fossbytesは、疑わしいファイルはダウンロードして展開するといった操作をしないようにアドバイスしている。

GIGAZINE


2019年07月06日 20時00分　セキュリティ
「非再帰的ZIP爆弾」は10MBのファイルが281TBに膨らむ

by Tomas Sobek

数十KBのZIPファイルに見えて解凍すると膨大なファイル容量を食う「ZIP爆弾(高圧縮ファイル爆弾)」は、ZIPファイルの中にZIPファイルを格納し、内側のZIPファイルの中にさらにZIPファイルが……という入れ子構造を用いることで圧縮アルゴリズムの限界をうまく回避していますが、それゆえに多くのアンチウイルスソフトで対策されています。この弱点を乗り越えた「非再帰的ZIP爆弾」は、展開後のサイズこそ高効率で作られた再帰的ZIP爆弾にかなわないものの、わずか10MBから281TBへ2800万倍に膨らみます。

A better zip bomb
https://www.bamsoftware.com/hacks/zipbomb/
A better zip bomb
David Fifield
2019-07-02 updated 2019-07-03
Summary　This article shows how to construct a non-recursive zip bomb that achieves a high compression ratio by overlapping files inside the zip container. "Non-recursive" means that it does not rely on a decompressor's recursively unpacking zip files nested within zip files: it expands fully after a single round of decompression. The output size increases quadratically in the input size, reaching a compression ratio of over 28 million (10 MB → 281 TB) at the limits of the ZIP format. Even greater expansion is possible using 64-bit extensions. The construction uses only the most common compression algorithm, DEFLATE, and is compatible with most zip parsers.
42.zip　42 kB → 5.5 GB
10kb.zip　10 MB → 281 TB
4mb.zip　46 MB → 4.5 PB (Zip64, less compatible)
Source code:
git clone https://www.bamsoftware.com/git/zipbomb.git
zipbomb-20190702.zip
Data and source for figures:
git clone https://www.bamsoftware.com/git/zipbomb-paper.git

ZIPの圧縮で一般的に用いられているアルゴリズムは「Deflate(デフレート)」と呼ばれるもので、圧縮・展開速度の速さが特徴的です。圧縮率が最高で1032:1(約0.096%)という点はZIP爆弾を作る際の「足かせ」となっており、この制限を回避するため、ZIP爆弾ではZIPファイル内にZIPファイルを格納する入れ子構造を利用して、入れ子1つごとに1032倍にできるだけ近い圧縮率を得ることで、巨大ファイルを極小に見せています。

INTERNET Watch


解凍ツールでは事前検知不可能、46MBが4.5PBへと膨れ上がるZIP爆弾がネット上で公開中

tks24　2019年7月19日 06:00

ツイート　リスト　いいね！137　シェア　B! 30　Pocket　32

もとは数十MB程度のサイズながら、解凍するとペタバイト（PB）を超えるサイズにまで膨れ上がる圧縮ファイルがネット上で公開され、話題になっている。

これはDavid Fifield氏が「A better zip bomb（より効率的なZIP爆弾）」としてソースコードとともに公開しているもので、それによると42KBのファイルが解凍後は5.5GBへ、46MBのファイルが4.5PBへと爆発的に膨れ上がることが特徴。これまでも似た手口の通称「ZIP爆弾」が考案されたことはあったが、それらは圧縮ファイルの中にさらに圧縮ファイルを入れるという入れ子構造が共通しており、多くの解凍ツールでは無効化されていた。今回考案されたファイルはこうした入れ子構造を用いておらず、それだけに各解凍ツールでも新たに対応を強いられるとみられる。リンク先のページではソースコードとともに圧縮ファイルの実物も公開されているので、技術的に興味がある人は、5.5GBを超える空き容量をドライブ上に確保した上で、42KBのファイルを解凍してみるとよいだろう（言うまでもないが、自己責任で）。

- A better zip bomb
  https://www.bamsoftware.com/hacks/zipbomb/

●Mirai関連パケット減少、一方で別ポート宛パケット増加も…JPCERT/CC、警察庁発表

http://www.npa.go.jp/cyberpolice/important/2019/201907191.html

このニュースをザックリ言うと･･･

- 7月16日（日本時間）にJPCERT/CCより、同19日に警察庁より、それぞれが実施しているインターネット定点観測のレポートが発表されました。

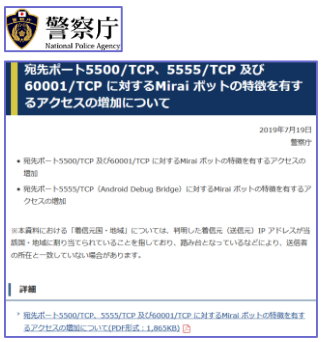
- JPCERT/CCの発表では、2019年4月～6月に国内で観測されたパケットの宛先ポートで最も多かったのはTCPポート23番(Telnet)で、その多くはIoTマルウェア「Mirai」に感染した機器から送信されていたものとされていましたが、「NOTICE」プロジェクトでの対策実施呼び掛けにより減少傾向にあるとのことです。

- 一方、警察庁の発表では、6月中旬～下旬に、TCPポート5500番、5555番および60001番に対するパケットが急増しており、パケットの特徴からMirai型ボットによると推測しています。

AUS便りからの所感等

- 警察庁の発表におけるポート5500番・60001番宛パケットの内容は、外部サーバから不正なプログラムのダウンロードを試みるHTTPリクエストとされ、その発信元は前者が海外製デジタルビデオレコーダ等、後者が主に国内製のWi-Fiストレージ製品とされています。

- 警察庁では家庭用ルータやIoT機器の利用者に対し「製造元のウェブサイト等で周知される脆弱性情報に注意を払いファームウェアのアップデートや設定変更等が必要な場合は速やかに実施する(自動アップデート機能がある場合は有効にする)」「IoT機器は直接インターネットに接続せずルータ等を使用する」「アクセス可能なポートやアクセス元IPアドレスを制限する」「ユーザ名およびパスワードは初期設定のままで使用せず必ず変更する」等を推奨していますので、根本的な対策の上にUTMの活用等を組み合わせることを検討するのが良いでしょう。


警察庁
National Police Agency

宛先ポート5500/TCP、5555/TCP 及び60001/TCP に対するMirai ボットの特徴を有するアクセスの増加について

2019年7月19日
警察庁

- 宛先ポート5500/TCP 及び60001/TCP に対するMirai ボットの特徴を有するアクセスの増加
- 宛先ポート5555/TCP（Android Debug Bridge）に対するMirai ボットの特徴を有するアクセスの増加

※本資料における「着信元国・地域」については、特明した着信元（送信元）IP アドレスが当該国・地域に割り当てられていることを限しており、踏み台となっているなどにより、送信者の所在と一致していない場合があります。

詳細

宛先ポート5500/TCP、5555/TCP 及び60001/TCP に対するMirai ボットの特徴を有するアクセスの増加について(PDF形式：1,865KB)

●BITPointがハッキング被害、30億円相当の仮想通貨が不正流出

https://www.itmedia.co.jp/news/articles/1907/12/news100.html

このニュースをザックリ言うと･･･

- 7月12日（日本時間）、リミックスポイント社より、同社子会社のビットポイントジャパン社（以下BPJ）が運営する仮想通貨交換所「BITPoint」が不正アクセスを受け、管理していた仮想通貨のうち約35億円相当が流出したと発表されました（その後の発表では約30億2,800万円とされています）。

- 被害を受けた仮想通貨は「Bitcoin」「Bitcoin Cash」「Ethereum」「Litecoin」「Ripple」で、同11日夜に送金エラーが検出されたことにより、流出が発覚したとのことです。

- 国内の仮想通貨交換所における流出事件としては、2018年のCoincheck（約580億円相当）、Zaif（約67億円相当）に次ぐものとされています。

AUS便りからの所感等

- 前述した国内仮想通貨交換所の例、あるいは今年5月の海外大手交換所Binance（被害額約45億円相当）の例とは、オンラインで保管する「ホットウォレット」が狙われ流出したこと、また専用デバイス等オフラインで保管する「コールドウォレット」は安全であったことが共通しています。

- 一方で、16日にBPJ社が行った記者会見では、仮想通貨の秘密鍵を分散管理する「マルチシグネチャ」を導入し、秘密鍵自身にも暗号化を施しているなど、安全性を意識した対策が行われていたように見受けられていました。

- ともあれ、CoincheckやZaif、Binanceの例と同様、流出の経緯の詳細が明らかになるとともに、他サービスを含めどういう対策が行われていくか、例えば全ての仮想通貨管理がコールドウォレットで行われる方向に至るのか等、今後の動向が注目されます。


ITmedia NEWS

ビットポイントから35億円相当の仮想通貨が流出

[ITmedia]

仮想通貨交換業者のビットポイントジャパン（BPJ）は7月12日、約35億円相当の仮想通貨が流出したと明らかにした。BPJは同日午前、緊急メンテナンスのため全サービスを停止していた。

流出したのは、BPJがホットウォレットで管理していた仮想通貨。流出の経緯や詳細は調査中だが、この手法で管理していたのはリップル・ビットコイン・ビットコインキャッシュ・イーサリアム・ライトコインの5銘柄という。コールドウォレットで管理している仮想通貨と法定通貨の流出は確認されていない。

顧客からの預かり分は約25億円相当、BPJ2の保有分は約10億円相当。BPJは資産が流出した顧客に対し、補填などの対応を行う方針だ。

11日夜にBPJの仮想通貨取引システムで送金エラーが検出され、調査の結果、不正流出が判明した。当初はリップルの流出のみ確認していたが、12日未明にその他の銘柄の流出も発覚。対応策として、全サービスの停止に至ったとしている。

ビットポイントは2016年3月設立。17年9月に金融庁の審査を通過し、仮想通貨交換業者として登録された。18年8月には、サッカーの本田圭佑選手をイメージキャラクターに起用するなど話題を呼んだ。

だが、マネーロンダリング対策が不十分などとして、18年6月に金融庁から資金決済法に基づく業務改善命令を受け、その後約1年間にわたって改善策の実施状況を報告。19年6月に報告義務を解除されていた。同年3月には電力小売などを手掛けるリミックスポイントの完全子会社となっている。

親会社のリミックスポイントは「関係者の皆さまにご迷惑をおかけいたしますこと、深くおわび申し上げます」と謝罪。「今後は原因究明と再発防止策の実施を行い、信用回復に努めてまいります」としている。連結業績に与える影響は精査中で、分かり次第開示する。