2021 年 06 月 23 日
デジタルアーツ株式会社

PRESS RELEASE

PPAP のパスワードは 1 秒未満で解読可能

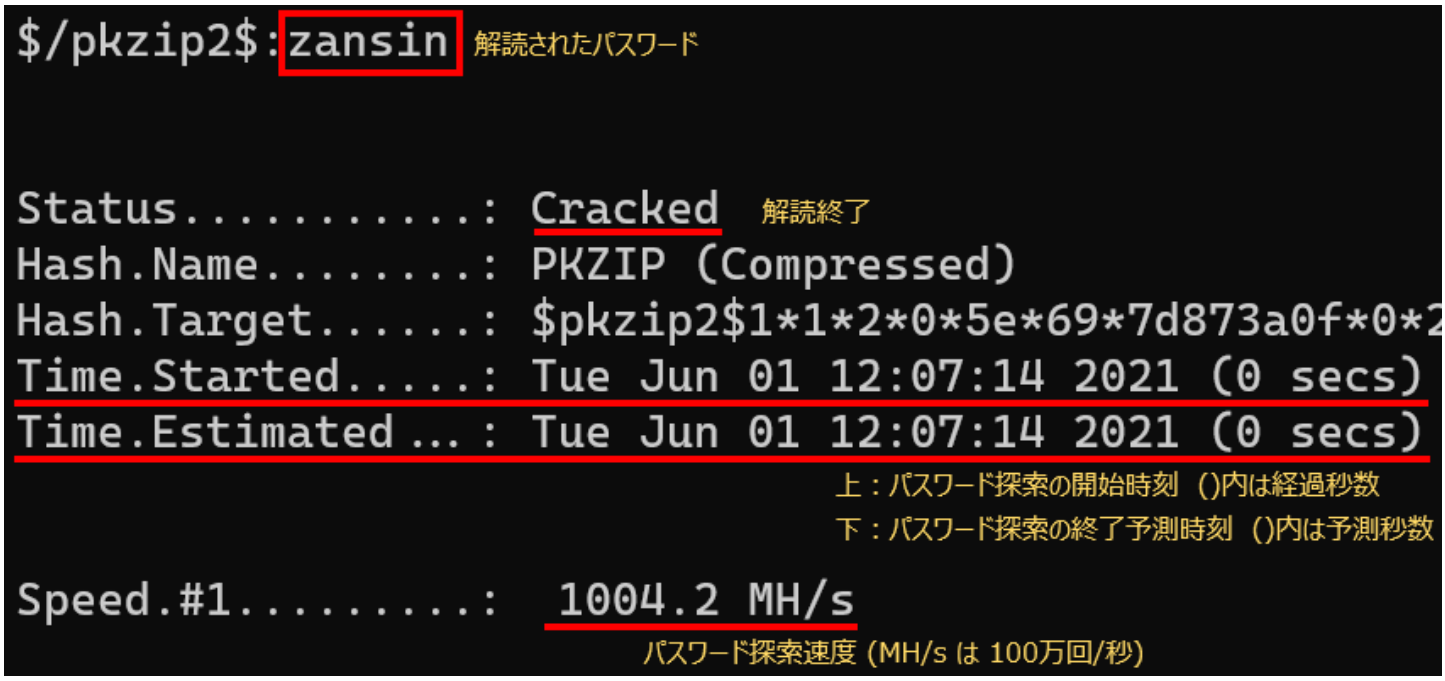
簡単なパスワードは一般のパソコンでも解読可、ファイルのパスワード運用は限界

情報セキュリティメーカーのデジタルアーツ株式会社（本社：東京都千代田区、代表取締役社長：道具　登志夫、以下 デジタルアーツ、証券コード 2326）は、PPAP（パスワード付き ZIP でのファイル運用）などで使われる ZIP ファイルのパスワードに関する分析レポートを公開したことを発表いたします。

メールで ZIP 暗号化ファイルを送信し、後からパスワードをメールで別送する方法（PPAP）は、多くの日本企業・団体で採用されています。昨今さまざまなインシデントリスクが指摘されていますが、今回はパスワードのリスクについて分析します。パスワードは主に「PIN コード」、「ログインパスワード」、「暗号キー」の 3 種類あります。スマートフォンのロック解除や銀行のキャッシュカードで使われる「PIN コード」、ウェブサービスのログインに使われる ID とセットで入力する「ログインパスワード」です。このうち、「PIN コード」と「ログインパスワード」は入力回数に制限がかけられるパスワードですが、ZIP ファイルの暗号化などに使われる「暗号キー」はパスワード入力を何度でも試すことができるという特徴があります。

パスワード入力を何度でも試すことができる ZIP ファイルのパスワードを解読する

ZIP ファイルのパスワードはどれくらいの時間で解読できるか、一般購入可能なパソコン、オープンソースで誰でも入手できるパスワード回復のソフトウェアを利用して試してみたところ、サンプルで設定した「zansin」という英語小文字 6 ケタのパスワードは 1 秒未満で解読することができました。



英小文字で 6 ケタの組み合わせは約 3.1 億（26 の 6 乗）通りですが、本テストではパスワード探索する速度は約 10 億回/秒を記録しています。ほかにも数字のみ 12 ケタと若干多めのケタ数であってもわずか 2 分 51 秒で解読が可能でした。「日付や日時の数字を ZIP ファイルのパスワード」として設定・運用している組織が少なからずあるのではないでしょうか。

本テスト結果の通り、簡単な ZIP ファイルのパスワードは一般のパソコンでも短時間で解読できました（※1）

パスワード文字列	ケタ数	文字列組み合わせ	解読時間（※2）
zansin	6 ケタ	英小文字	1 秒未満
zansinzz	8 ケタ	英小文字	20 秒
zansin01	8 ケタ	英小文字＋数字	2 分 13 秒
Zansin01	8 ケタ	英小文字＋英大文字＋数字	2 日 6 時間（注：最長見込み）
Zans!n01	8 ケタ	英小文字＋英大文字＋数字＋記号（※3）	55 日 13 時間（注：最長見込み）
20210601	8 ケタ	数字	1 秒未満
202106012045	12 ケタ	数字	2 分 51 秒

（※1）解読マシンは一般購入可能なパソコンで実施。OS:Windows10 Pro, CPU:Core i5-10210U（4 コア 8 スレッド）, RAM:32GB, SSD:500GB, GPU:GTX1070 8GB RAM。「GPU」とは、主にグラフィックを処理する際に用いられるプロセッサーのことです。パスワード解読のような処理においては、GPU を使うことで CPU の何倍ものスピードで処理が可能になります。大抵のゲーミングパソコンと呼ばれるパソコンにはグラフィックボード（グラフィックカード）があり、GPU が組み込まれています。ZIP ファイルの暗号化には、国内利用者が多いと思われるフリーの圧縮・解凍ソフトウェア Lhaplus の標準設定を用いて、同一テキストファイルをパスワードだけ変えて作成し、解読用ソフトウェアは、オープンソースで誰でも入手可能なパスワード回復ツールを用いました。

（※2）各パスワードの「文字列組み合わせ」での総当たり方式で解読。ケタの少ない方から順に解読していき、かかった時間を合算して記載しています。一部は解読終了までの最長の見込み時間を記載。

（※3）「記号」には 33 種を想定。≪space≫!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~

パスワードの運用には限界がある。PPAP の代替となるファイル送信方法の検討が必要

PPAP のインシデントリスクは、受信時と送信時の両方にあります。受信時のリスクは、ZIP 暗号化ファイルを悪用した Emotet や IcedID などの攻撃が、アンチウイルスソフトなどをかいくぐり、マルウェア感染などの被害に遭ってしまう場合です。そして送信時のリスクは、誤送信や転送された場合にファイルが漏洩してしまう場合です。また、パスワード自体も単純な文字列に設定したり、使い回したりするなど運用によっては脆弱なパスワードになりやすくなってしまっている点も改めて理解しておいた方が良いでしょう。

こうしたことからデジタルアーツでは従来 PPAP のインシデントリスクに警鐘を鳴らしてきました。PPAP に代わるファイル送信運用として、メールセキュリティ製品「m-FILTER」Ver.5 と「FinalCode@Cloud」の「脱 ZIP 暗号化運用」をご提供しており、自治体様などにも中心にご利用いただいております。

・「ZIP 暗号化」運用（PPAP）は効果がないのか？Emotet や IcedID などの外部攻撃対策にはデジタルアーツの『脱 ZIP 暗号化』運用

・「m-FILTER」と「FinalCode」の『脱 ZIP 暗号化』を北海道庁が採用

ZIP ファイル解読の解析情報レポートはこちら

以下、弊社コーポレートサイト上にて公開しております。

セキュリティレポート「有名ドラマで使われた『zansin』なパスワードも 1 秒解読 ZIP ファイルのパスワード」

デジタルアーツ株式会社　概要

Web、メール、ファイルなどのセキュリティソフトウェアの提供を核に事業展開する情報セキュリティメーカーです。
1995 年の創業以来、「より便利な、より快適な、より安全なインターネットライフに貢献していく」を企業理念とし、有害情報の閲覧を制限する Web フィルタリングソフトを開発、以来企業・公共・家庭向けに情報セキュリティ製品を提供しております。

東京都千代田区大手町 1-5-1 大手町ファーストスクエア　ウエストタワー14F
URL: https://www.daj.jp/

＜本リリースに関するお問い合わせ＞
デジタルアーツ株式会社　広報担当　山田
※新型コロナウイルス感染症拡大に伴う在宅勤務実施中のため、お電話でのお問い合わせは以下とさせていただきます
TEL　：090-1555-7254　/ E-mail : press@daj.co.jp

より便利な、より快適な、より安全なインターネットライフに貢献していく