Университет ИТМО, факультет программной инженерии и компьютерной техники
Двухнедельная отчётная работа по «Информатике»: аннотация к статье
Дата прошедшей лекции: 27.09.2022 Номер прошедшей лекции: №2 Дата сдачи: 11.10.2022

Выполнил(а) Барсуков М. А., № группы *P3115*, оценка _____
Фамилия И.О. студента — не заполнять

Название статьи/главы книги/видеолекции
A better zip bomb

ФИО автора статьи (или e-mail)	**Дата публикации (не старше 2019 года)**	**Размер статьи (от 400 слов)**
David Fifield	"02" июля 2019 г.	11345

Прямая полная ссылка на источник или сокращённая ссылка (bit.ly, tr.im и т.п.)
https://www.bamsoftware.com/hacks/zipbomb/

Теги, ключевые слова или словосочетания
Сжатие данных, Zip-бомба, DEFLATE

Перечень фактов, упомянутых в статье
1. Созданная zip-бомба является нерекурсивной, но обеспечивает высокую степень сжатия.
2. Самый широко используемый алгоритм сжатия DEFLATE может достигнуть только степени сжатия 1032 к 1.
3. Обычно zip-бомбы используют рекурсивную декомпрессию, но большинство архиваторов не распаковывают zip-файлы рекурсивно.
4. Чтобы превысить предел 1032:1, можно использовать перекрытие файлов внутри zip-контейнера.
5. При создании zip-бомбы сложно одновременно увеличить степень сжатия и сохранить совместимость со стандартом ZIP.
6. Zip-файл состоит из нескольких частей, описанных в спецификации.
7. Zip – формат контейнера, а не алгоритм сжатия.
8. Формат ZIP очень неоднозначен, что создает много дыр в безопасности.
9. Разные архиваторы DEFLATE по-разному балансируют между скоростью и качеством сжатия.
10. Цитирование с перекрытием файлов позволяет разметить ядро и много раз его скопировать.
11. В формате Zip в архиве может быть не более 2^{16} - 1 файлов размером 2^{32} - 1 байт каждый, хоть это и зависит от реализации.
12. Алгоритм CRC-32 используется для подсчёта контрольной суммы несжатых данных файла.
13. Чтобы превзойти ограничения формата Zip, можно использовать Zip64, однако он не совместим.
14. bzip2 является 2-м по распространенности алгоритмом сжатия и позволяет использовать степень сжатия около 1.4 миллиона к 1, но в нем невозможно перекрывать файлы.

Позитивные следствия и/или достоинства описанной в статье технологии (минимум три пункта)
1. Многие антивирусные движки не способны определить такую zip-бомбу, из-за чего «падают». Это можно использовать для «протаскивания» вредоносного кода.
2. Такая zip-бомба в iOS 12 и 13 даже в «быстром просмотре» может вызвать ошибки, для устранения которых может потребоваться сброс до заводских настроек.
3. Создание zip-бомбы позволяет лучше понять спецификации zip-контейнеров и алгоритмов сжатия.
4. Надежная защита от этой zip-бомбы включает изолированную программную среду синтаксического анализатора, т.е не может быть представлена отдельным предварительным фильтром.

Негативные следствия и/или недостатки описанной в статье технологии (минимум три пункта)
1. Новые браузеры и архиваторы могут определить этот тип zip-бомбы.
2. Распаковка этой бомбы в сжатой файловой системе может быть относительно безопасной.
3. Тем не менее, логика обнаружения такого вида бомб довольна проста: достаточно найти перекрывающиеся файлы.

Ваши замечания, пожелания преподавателю *или* анекдот о программистах
Короткий старый анекдот: pkunzip.zip

(© absite.ru, от 2002 г.)