УДК

DOI

Валидность файла в форматах .exe и .pdf одновременно

Евгений К. Мазайшвили

Национальный исследовательский университет ИТМО

Санкт-Петербург, Россия, evgenij997@yandex.ru

File valid both in pdf and exe formats

Evgeny K. Mazayshvili

ITMO University

Saint-Petersburg, Russia, evgenij997@yandex.ru

Аннотация. В данной работе предлагается способ создания гибрида .pdf и .exe файла – один и тот же файл, переименованый в .exe – запустится как приложение, а переименованый в .pdf – откроется как документ. Данный способ позволяет обойти ограничение социальных сетей и мессенджеров, не позволяющих отправлять .exe приложение, путем отправки его в pdf. В pdf-документе может содержаться просьба переименовать его в .exe для запуска приложения.

Ключевые слова: pdf, exe, форматы файлов, объединение файлов, расширение файла

Annotation. This paper proposes a way to create a hybrid .pdf+.exe file. The same file, renamed to .exe, will run as an application, and renamed to .pdf, will open as a document. This method allows you to bypass the restrictions of social networks and messengers that do not allow you to send an .exe application, by sending application in pdf format. The content of pdf document may ask user to rename it to .exe in order to run the application.

Keywords: pdf, exe, file formats, file merging, file extension

Проблема невозможности отправки .exe файлов присутствует во множестве социальных сетей и мессенджеров. Это ограничение соблюдается из соображений

безопасности, чтобы получатель не мог просто так запустить потенциально вредоносный файл.

Для обхода этого ограничения было необходимо менять расширение приложения перед отправкой. Файл после этого переставал открываться, и нужно было объяснять получателю, что перед открытием его нужно переименовать. Было бы удобнее, если бы файл с новым расширением открывался и представлял собой инструкцию по открытию приложения. Чтобы человек, открыв такой файл, сразу видел строчку “переименуй меня в .exe”. Для этого требовалось создать файл, одновременно являющийся валидным .pdf и валидным .exe. Если поставить у такого файла расширение .pdf, он откроется как документ, если поставить расширение .exe – запустится как программа. Такой файл не нарушает безопасность, т.к. для запуска (потенциально вредоносной) программы, необходимо поменять расширение с .pdf на .exe.

Алгоритм создания такого файла основан на том, что в файлах exe для Windows байты с 2 по 60 представляют собой заголовок DOS [1]. При запуске приложения в DOS, этот заголовок читается и приводит к выполнению кода, который печатает сообщение об ошибке и прекращает выполнение программы. В современных системах Windows эта область никак не интерпретируется, и на это место можно записать заголовок pdf и начало pdf-объекта stream. Файл останется валидным .exe, но теперь при открытии файла в pdf-ридере он будет определяться как (невалидный) pdf-файл с одним незаконченным объектом stream. Чтобы сделать pdf-файл валидным, нужно дописать в конец файла окончание объекта stream и другие необходимые объекты, чтобы создать желаемое содержание pdf-документа. Файл не перестанет быть валидным .exe, т.к. любая информация, дописанная в конец .exe файла игнорируется.

Схема полученного таким образом файла изображена на рис.1.

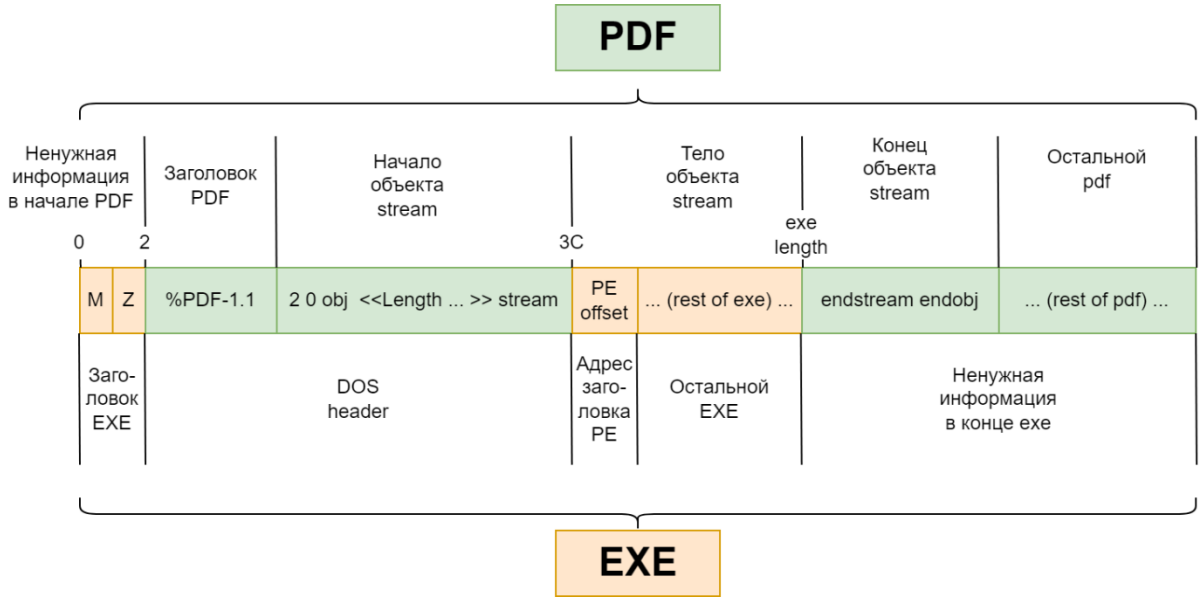

Рис.1. Схема файла, являющегося одновременно валидным .pdf и валидным .exe

Формально pdf не позволяет дописывать информацию в начало файла [2], поэтому файл на рис.1, имеющий перед pdf-заголовком 2 байта exe-заголовка, не считается строго удовлетворяющим спецификации. Однако, большинство pdf-ридеров считают документ с лишними байтами перед заголовком валидным, и без проблем открывают его.

Таким образом, получается файл, удовлетворяющий сразу двум спецификациям – .pdf и exe. Который можно открыть и как документ, и как приложение. Было создано программное обеспечение, объединяющее любой .exe файл с .pdf файлом [3].

Литература:

1. Sedory, Daniel B. (2004-10-12). "DOS Stub Program". The Starman's Realm. Self-published. Дата обращения: 11 февраля 2023.
2. Hardy, M.; Masinter, L.; Markovic, D.; Johnson, D.; Bailey, M. (March 2017). "The application/pdf Media Type". doi:10.17487/RFC8118. RFC 8118.
3. https://github.com/Evg-Mazay/PdfExeJoiner