Copyright Root Services, 2015

WinRAR Archiving and RTLO Vulnerability

Alexander Chopra[1]*, Michael Kaufman[2]

Abstract
This article provides an overview of vulnerabilities that exist within Windows as well as WinRAR's archiving. File names that exist within archives can be spoofed such that the user is unaware of the actual file that exists within the archive. In addition to spoofing the name of the file that exists within an archive, the Unicode character set has a vulnerability which allows an attacker to rename a file to effectively hide the file extension to the user. The process is detailed and preventive measures are suggested to prevent these issues in the future.

Keywords
Archiving Vulnerability — WinRAR Vulnerability — Right to Left Override — RTLO Unicode — ZIP Archive

[1] *Research and Development, Root Services, Rockville, Maryland, United States*
[2] *Research and Development, Root Services, Rockville, Maryland, United States*

Contents

	Introduction	1
1	Background	1
2	History	2
3	Nulling	2
4	Proof of Concept	2
5	Right to Left Override	2
6	Conclusion	3
	Acknowledgments	3
	References	3

Introduction

Archiving and compressing files takes up less storage space and allows the files to be transferred to others more quickly, due to reduced file size. Archiving and compressing is often utilized when sharing a group of files to another user or computer, rather than transferring the files individually, which has the possibility of taking a long time if there is a large number of files to be transferred. WinRAR, the built in compression utility in Windows, 7-Zip and others are commonly used to accomplish compression and archiving. This paper will take a look at a possible usage of WinRAR for exploitation that was seen in a previous version of WinRAR that may be harmful to those using it.

1. Background

WinRAR is a program that is an alternative to the built-in archiving features in Windows and other operating systems, providing faster and more options than the alternatives. WinRAR is a commonly used archiving and compression application that allows users to backup their data and reduce file size. By default, a user can create an archive from within Windows to compress files so they take up less space by right clicking on the file or folder and selecting "Send to" and clicking compressed (zipped) folder. When opening a compressed zip folder, Windows presents the user to extract the files to a particular location upon opening the zip archive.

WinRAR is commonly used because of the variety of file types that it is able to support. WinRAR supports the following file types: CAB, ARJ, LZH, TAR, GZ, TAR.GZ, BZ2, TAR.BZ2, ACE, UUE, JAR, ISO, 7Z, XZ, RAR5 and Z in addition to the commonly utilized ZIP and RAR file formats. It is commonly used as a result of the easy to use graphical user interface (GUI) as well as the easy to understand powerful compression features and options that it has built into the program. When compressing or decompressing large archives, WinRAR is commonly faster than the alternatives available as a result of optimized multi-core CPU threading assisting the process. WinRAR also allows users "better resistance to archive damage such as archive truncation and recovery record"[1]. With an extensive options, including easy application of AES encryption, creation of self-extracting files, split archives and more, WinRAR has claimed notability as one of the most used pieces of software in the world.

2. History

WinRAR debuted in 1993 as a command line only program and slowly evolved with consistent releases over the years to its current version. All versions of the software, other than the Android versions (which are currently free for all users), are distributed as shareware. Shareware is a term utilized with software commonly indicating that the software is available free of charge to the user in the form of an evaluation version and the user has the option to continue to use the software past the evaluation deadline for a set fee. WinRAR has been consistent with their pricing model of charging 29 US Dollars for a single license or offering multi-user licenses at a discounted rate for between 6 and 21 dollars per user (depending on the quantity).

WinRAR, being one of the most popular pieces of software in the world, is plagued with issues in regard to software piracy. In an interview conducted in the later part of 2013 the CEO of WinRAR, Burak Canboy, noted that piracy rates of WinRAR are very high, but because the program itself can be utilized for free even after the evaluation time has ended (if you are willing to put up with a nag dialog box every time the software is opened), there is little need for piracy[1]. It can become annoying for users who have not purchased a legitimate version of the software to continuously have to close dialog boxes notifying them that their evaluation period has ended and resort to pirating the software to bypass the struggle. As a result of the need in the public for a nag free version of the software, individuals have taken the task to null or crack versions of WinRAR such that they can be verified as licensed and not bothered with the dialog boxes prompting the user to purchase a full version.

3. Nulling

When users utilize nulled versions of the program, often the user does not update to the latest version on a regular basis for lack of a nulled release of the most recent version, resulting in the user using out of date software which could contain vulnerabilities. Commonly with WinRAR the process is done through a generation tool which creates a valid key file that is associated with the particular release of the software that the user can create on their own, bypassing the activation methods of WinRAR and allowing them to use the software for free. Fighting for Fun (FFF) team regularly release versions of nulled software that started in 2002. Most likely when looking for a nulled version of WinRAR, their version will be the one most readily available for download. The group was started in 2002 and have over 15,000 various nulled software releases across multiple operating systems. One of the most widely used versions of WinRAR is still version 4.2.0 (even though the current version as of February 2015 was 5.21) and was nulled by FFF (among others) for public consumption.

4. Proof of Concept

A file spoofing vulnerability exists in WinRAR versions before WinRAR 5.x that could allow an attacker to create and distribute and archive containing malicious material without the end receiver realizing what is inside of the archive even upon inspection. Through examination of the file headers of a standard zip file one can expect it to look like the following:

Offset	Bytes	Description
0	4	Local file header signature = 0x04034b50
4	2	Version needed to extract (minimum)
6	2	General purpose bit flag
8	2	Compression method
10	2	File last modification time
12	2	File last modification date
14	4	CRC-32
18	4	Compressed size
22	4	Uncompressed size
26	2	File name length (n)
28	2	Extra field length (m)
30	n	File name
30+n	m	Extra field

From this information one can see that the name of the file is stored at an offset of 30. For this example, let us assume that the user creates a new archive named testarchive.zip with a file-name called attack.exe inside of that archive and opens that zip file in a common hex editor such as wxHexEditor, Hexinator or HT Editor. The user will be able to navigate to the offset of 30 and see that the file-name of the file that is contained within testarchive.zip is presented to the user at this location as can be seen in Figure 1.

Looking further down, the user can see at the offset of 130 is the same name of the file (attack.exe) at a different location than where the file-name is supposed to go as seen in the expected file header shown in Figure 2. At this offset location is the file-name that is presented to the user from within the WinRAR GUI. For this example, the file name starting at offset 130 can be altered to display a differing file name as seen in Figure 3. Only after decompression will the user realize that the file that they are extracting from the archive is not momdad.jpg but rather attack.exe. The deployment of harmful code can be achieved through this method on to individual or corporate computers, allowing an attacker an entry point into a system.

5. Right to Left Override

Continuing with the example of an attacker utilizing this vulnerability within WinRAR another spoofing vulnerability can be used in conjunction with the spoofing of the file name within the archive to make it appear as if the file is different than what is expected. The vulnerability lies within Unicode in the right to left override (RTLO) Unicode character set. To execute this vulnerability, a would be attacker would only

need notepad or another text editing software to rename a file using copied text from it. An attacker could insert the text "mom(RTLO)gpj.exe" into a notepad file by right clicking at the point where RTLO is indicated and have the character inserted. The attacker could then copy the text from notepad and rename the attack.exe file by pasting. The resulting file name would appear to anyone looking at that file as momexe.jpg.

The file itself, after being spoofed using the RTLO vulnerability, will execute as if it was a normal file but it offers the threat of potentially misleading people into thinking that the file type is that of a jpg instead of an executable (or any other file type for that matter). The user will think that the risk involved with the file is null as a result of the extension and it has the possibility of bypassing anti-virus and other protection software as a result. One can even use this method with the name of the archive itself to make the archive appear as something else (possibly a self-extracting archive), tricking the user into extracting the payload onto their computer. Download managers and in-built browser download tools do not appear to flag RTLO file names as a potential vulnerability and allow them to be downloaded or uploaded without prevention.

6. Conclusion

In conclusion, the threat of spoofing vulnerabilities are very much still real within Windows as well as popular Windows software. Without properly taking the time to evaluate what is being loaded or extracted on your machine, it is possible for an attacker to take advantage of the oversight in delivering a payload in an easy to miss circumstance. The RTLO vulnerability that is found within Windows should be addressed as the usefulness of the feature in file-names is minimal while the potential threat is high. WinRAR should be taking preventative action against users who are utilizing older versions of the software to present them with a forced upgrade to ensure that users are not unnecessarily exposed.

Figures

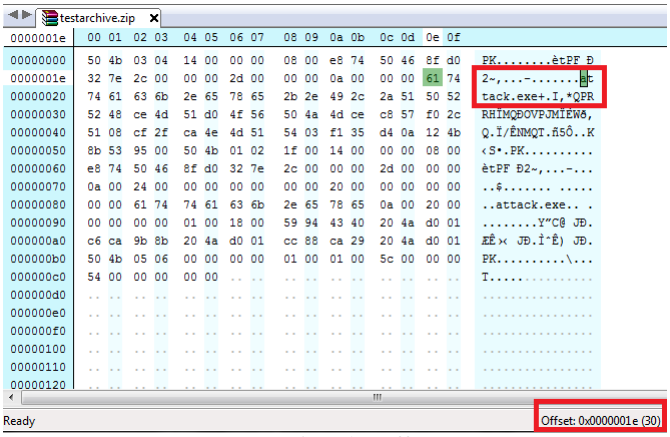

Figure 1. Noting the offset at 30

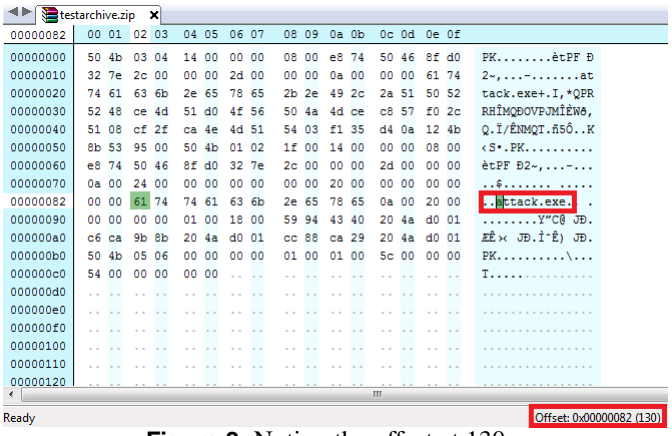

Figure 2. Noting the offset at 130

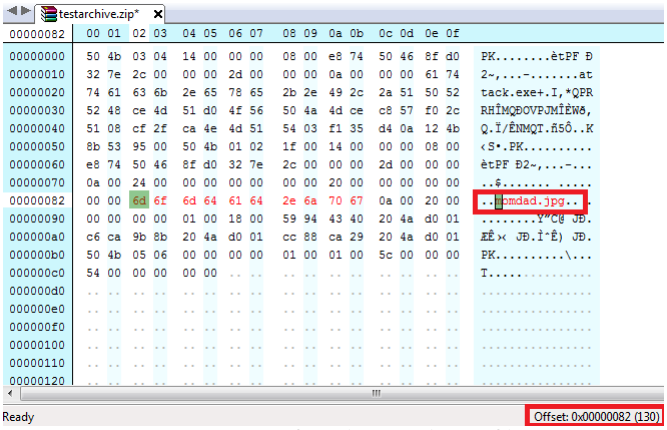

Figure 3. Spoofing the attack.exe file

Acknowledgments

WinRAR for providing older versions of their software for evaluation.

References

[1] Softsonic. Winrar 5.0: Interview with ceo burak canboy. *Softsonic Editorials*, 1, sep 2013. http://features.en.softonic.com/winrar-5-0-interview-with-ceo-burak-canboy.