# Protecting Against WinRAR Vulnerabilities

February 27, 2019

A 19 year old, yet major, vulnerability was recently found by Check Point Research in the popular web application, WinRAR, that could potentially put over 500 million users at risk. The exploit works by simply extracting an archive from an innocent looking ACE file which could lead to a remote code execution.

Following the discovery, it was not long at all before the Check Point Research team, as well as a researcher from NCC Group, spotted malware sample leveraging this vulnerability in the wild. In this case, the malware is an ace archive containing a JS file that is, in turn, written to startup. It will download and run an executable when initiated. The downloaded executable is a .NET RAT called Orcus.

Fortunately, Check Point customers were already protected against this type of attack before the publication of this WinRAR vulnerability was made last week. By taking a closer look at how Check Point SandBlast Agent works we can get a better understanding of both the attack and protection against it.

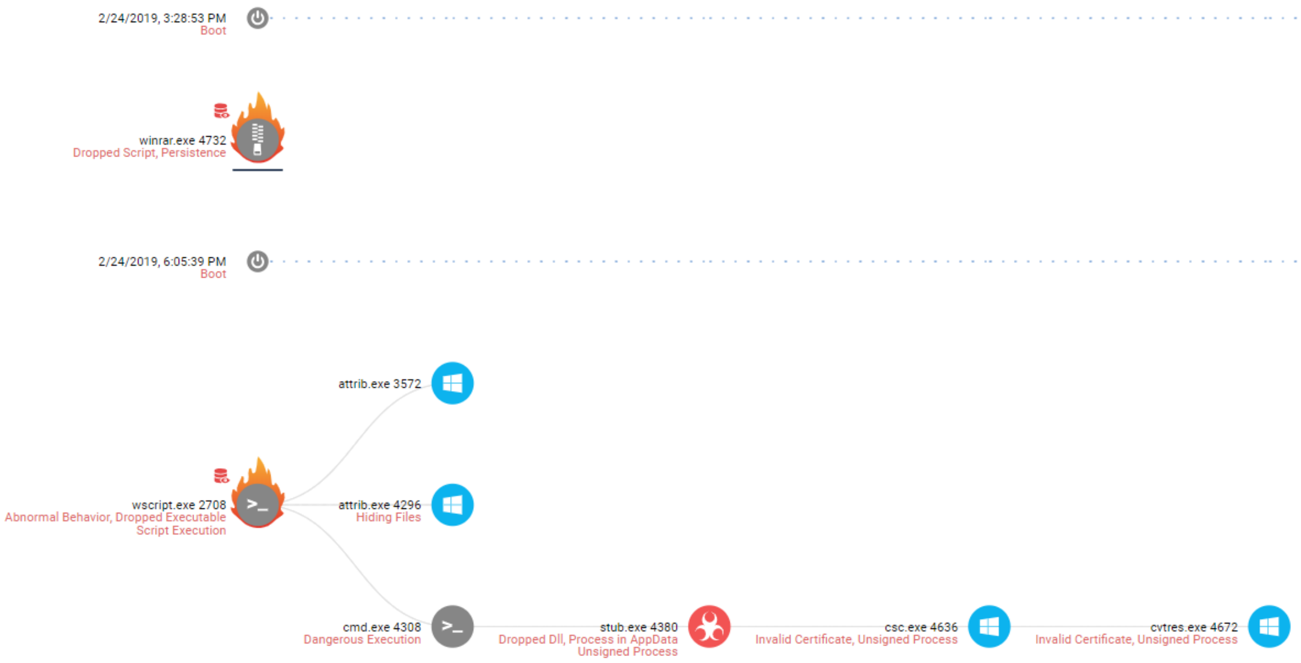
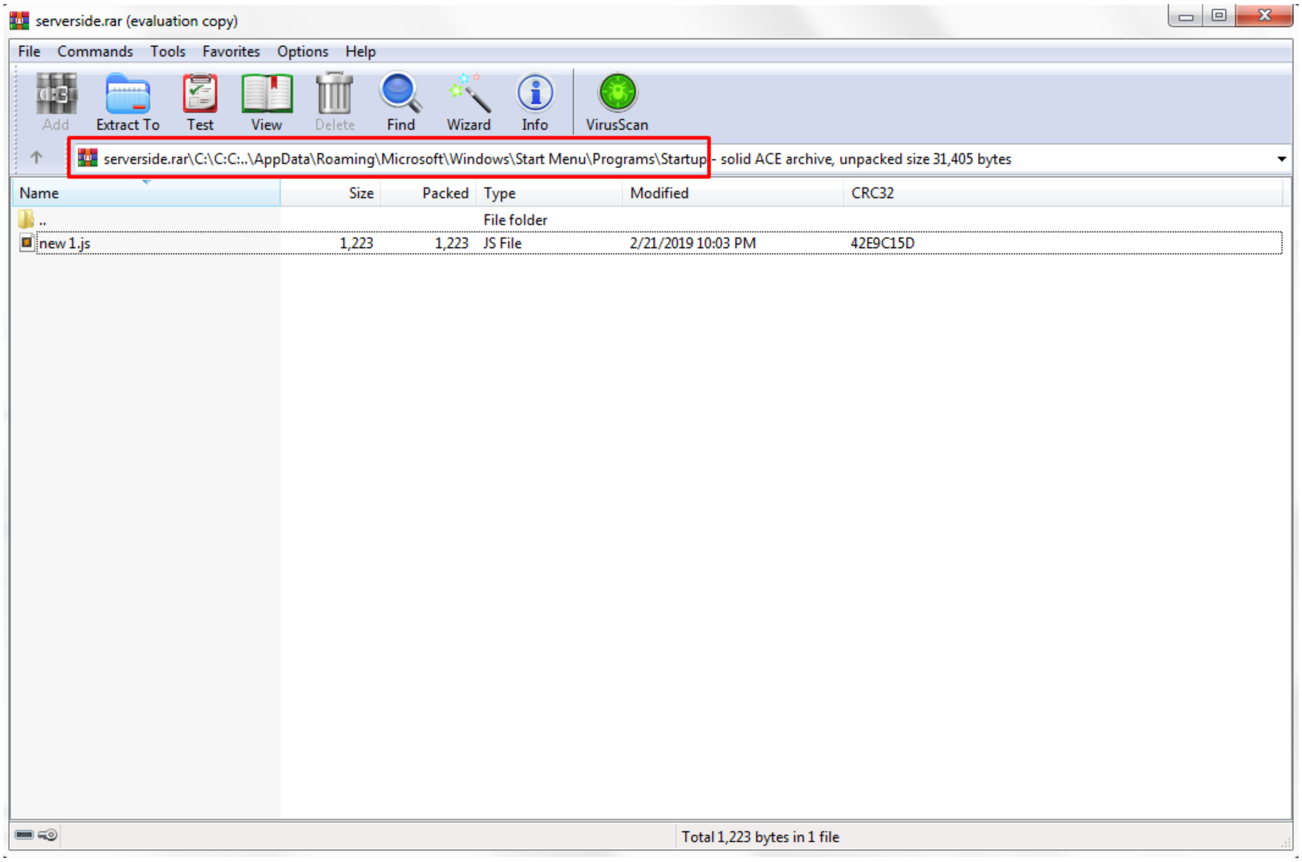


**Figure 1:** Forensics Report from Sand Blast Agent (in detect only mode to showcase the whole attack) highlighting the script drop and execution upon reboot. (Click here for the full report).

The attack begins by the user extracting an archive using WinRAR believing he is extracting a rbxm file which is a 3D model for Roblox, a popular online gaming platform. In addition to the 3D model, there is a hidden JS file with custom path to user’s startup folder as highlighted below.


serverside.rar (evaluation copy)
File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
Find
Wizard
Info
VirusScan

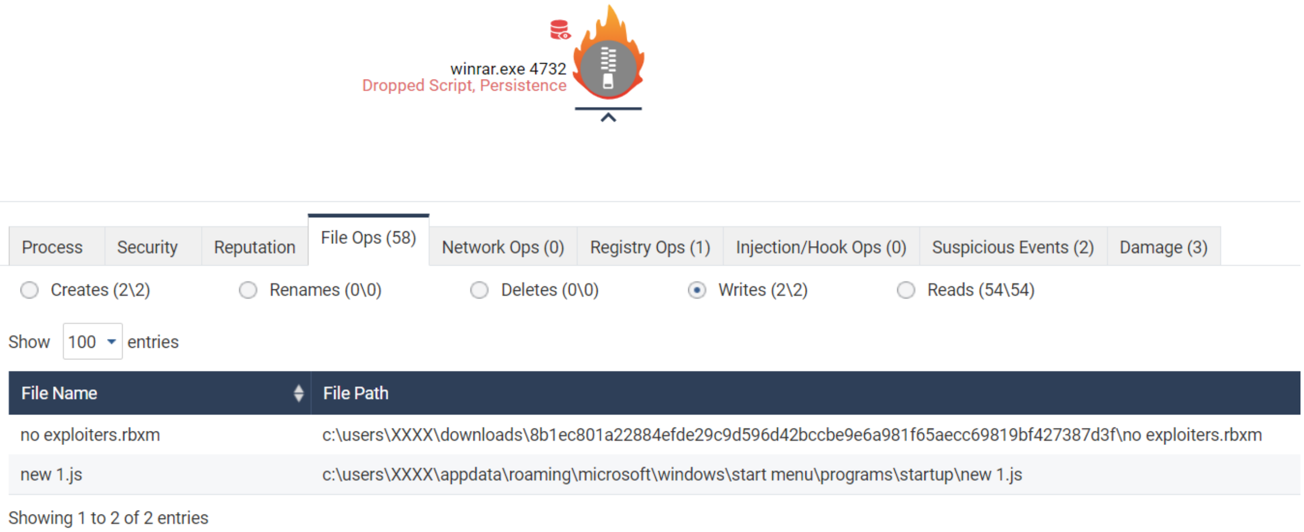
serverside.rar\C:\C:C:..\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup - solid ACE archive, unpacked size 31,405 bytes

| Name | Size | Packed | Type | Modified | CRC32 |
|---|---|---|---|---|---|
| .. | | | File folder | | |
| new 1.js | 1,223 | 1,223 | JS File | 2/21/2019 10:03 PM | 42E9C15D |

Total 1,223 bytes in 1 file

**Figure 2:** WinRAR archive containing JS file.

Meanwhile, we can see from the Sand Blast Agent Forensics report that the JS payload file is actually extracted to the user's start-up folder where it will then be launched once the user reboots the machine or simply logs off and logs back on.



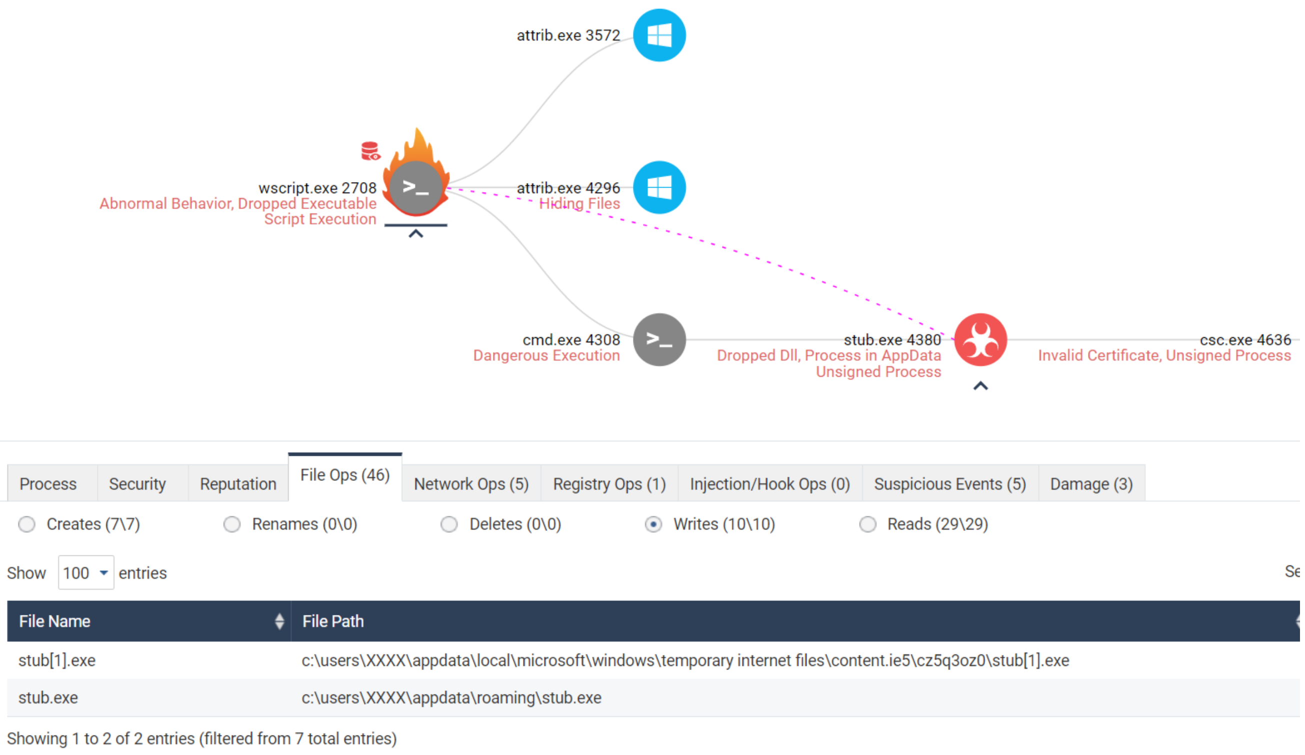
○ Creates (2\2) ○ Renames (0\0) ○ Deletes (0\0) ● Writes (2\2) ○ Reads (54\54)

Show 100 entries

| File Name | File Path |
|---|---|
| no exploiters.rbxm | c:\users\XXXX\downloads\8b1ec801a22884efde29c9d596d42bccbe9e6a981f65aecc69819bf427387d3f\no exploiters.rbxm |
| new 1.js | c:\users\XXXX\appdata\roaming\microsoft\windows\start menu\programs\startup\new 1.js |

Showing 1 to 2 of 2 entries

**Figure 3:** WinRAR process writing JS file to startup folder.



○ Creates (7\7) ○ Renames (0\0) ○ Deletes (0\0) ● Writes (10\10) ○ Reads (29\29)

Show 100 entries

| File Name | File Path |
|---|---|
| stub[1].exe | c:\users\XXXX\appdata\local\microsoft\windows\temporary internet files\content.ie5\cz5q3oz0\stub[1].exe |
| stub.exe | c:\users\XXXX\appdata\roaming\stub.exe |

Showing 1 to 2 of 2 entries (filtered from 7 total entries)

**Figure 4:** Execution of JS file, download and launch of the Orcus RAT.

SandBlast Agent is able to catch such activity through the SandBlast Agent Behavioral Guard protection name Gen.Win.WrarExp.A.

By performing Advanced Behavioral Analysis along with threat extraction and sandboxing techniques remotely on public or private cloud servers, SandBlast Agent is able to use a low-overhead, non-intrusive approach to protect users against modern malware techniques.

The exploitation of vulnerabilities in such commonly used applications like WinRAR highlights once again how easily users can be exposed to malware when downloading files. By doing so, they can inadvertently put an enterprise's entire IT network at risk of infection.

When suspicious events do occur, it is essential that organizations have immediate access to the information required to fully understand and triage attacks to quickly identify source and scope, and to determine the best path of resolution.

Check Point SandBlast Agent is a progressive new solution that extends advanced threat prevention to endpoint devices to defend against zero-day and targeted threats. With the capture and automatic analysis of complete forensics data, SandBlast Agent provides actionable attack insight and context to enable rapid remediation in the event of a breach.

For more information, please request a demo of Sand Blast Agent.

**Check Point customers are protected IPS protections:**
RARLAB WinRAR ACE Format Input Validation Remote Code Execution (CVE-2018-20250)

IOCs:
Sample: 8b1ec801a22884efde29c9d596d42bccbe9e6a981f65aecc69819bf427387d3f
https://www.virustotal.com/gui/file/8b1ec801a22884efde29c9d596d42bccbe9e6a981f65aecc69819bf427387d3f/detection

Downloaded RAT:
3a15f711370a667b41067f63ce181624451f542ca023825983446425d388fb70
https://www.virustotal.com/gui/file/3a15f711370a667b41067f63ce181624451f542ca023825983446425d388fb70/detection

C2 Server: galrov.warzonedns.com
Port: 1604