Not even getting to the airtight hatchway: Planting files in world-writable directories

devblogs.microsoft.com/oldnewthing/20191113-00

November 13, 2019

Raymond Chen

A security vulnerability report came in declaring that the finder had discovered an elevation of privilege vulnerability. They explained that they identified a world-writable directory and that an attacker can exploit the directory by creating or deleting a file, or could perform arbitrary execution from that directory.

Their proof-of-concept copied a file into the world-writable directory and confirmed that it was there and could be read. They also copied an executable into the world-writable directory, and then executed it.

So, yeah, that's what happens when you have write permission in a directory. You can copy files into the directory, and that includes copying executables. But so what?

There had yet to be any demonstrated elevation of privilege. The user who copied the files into the directory is the same use that read them out or executed them.

Now, if the system automatically executed programs in that directory as some other user, say because the world-writable directory is on the default `PATH`, or because it's a directory like the global Startup Folder, then you'd have something. You placed an executable in a place that will execute as another user.

But so far, all you did was load a trap. You didn't do anything to *spring* the trap.

In order to spring the trap, you need to trick somebody into going into that world-writable directory and running your program. That requires the victim to take some significant nondefault actions, and you'll have to convince them to click on multiple things. At this point, what you have is a social engineering attack, not a security vulnerability.

After all, you don't have to look around for world-writable directories. You can always make your own!

```
mkdir %USERPROFILE%\trap
icacls %USERPROFILE%\trap /grant users:RW
```

Bingo, you just created a world-writable directory, just like the big boys.

Go ahead, copy your favorite malware into that directory. You haven't achieved any elevation of privilege. The files are there, but you still have to trick somebody into launching them, and that's where the real work begins.

Bonus chatter: This is a fertile ground for bogus security vulnerability reports. Most such reports claim elevation of privilege, but their "proof of concept" document doesn't show any actual elevation of privilege. Many of them don't even show any code execution! They title their report something like "Arbitrary file creation could potentially perform arbitrary execution," but nowhere in the report is any realization of this potential ever demonstrated.

Any program can be potentially executed. I plug in a USB drive with an executable on it. *Oh no, I have potential arbitrary execution!*

That's not the hard part. The hard part is getting it executed.

Raymond Chen

Follow