Reporting on what you could do once you get to the other side of the airtight hatchway

devblogs.microsoft.com/oldnewthing/20200518-00

May 18, 2020

Raymond Chen

A security vulnerability report arrived that reported that a program was vulnerable to a DLL planting attack if the rogue DLL were planted in the `system32` directory.

This is not a vulnerability because writing to the `system32` directory requires administrator privileges. An exploit which requires administrator privileges is not really an exploit since there is no elevation of privilege. You got from administrator to… administrator.

The finder justified the report by saying, “Obtaining administrator rights is trivial. Nearly all malware will gain administrator privilege as one of their first steps.”

Whether or not obtaining administrator rights is trivial, defending against a compromised administrator is pointless. The attacker has already achieved their goal. There’s nothing the program can do to defend against it, the administrator could go in and disable any defenses that the program could create.

For example, the administrator could just go ahead and do whatever bad thing they want, without ever running the compromised program. In other words, using the compromised program as part of the attack is just adding style points. It doesn’t give you anything you don’t already have. All you’re doing is bringing an irrelevant component into the story, and then blaming that component for something it had no control over.

Raymond Chen

Follow