It rather involved being on the other side of this airtight hatchway: Attacking a domain administrator from the local administrator

devblogs.microsoft.com/oldnewthing/20240213-00

February 13, 2024

Raymond Chen

A security vulnerability report arrived that claimed to have found a way to elevate from a local administrator to domain administrator.

Okay, this sounds interesting, because gaining local administrator privileges lets you pwn the local computer, but that doesn't extend to other computers on the domain. Let's see how the attack works.

The report explains that as local administrator, you can assert SeTcbPrivilege in order to do complicated things that ultimately extract network credentials of a domain administrator who has signed into the computer.

Okay, wait a second. You didn't actually gain domain administrator credentials on your own. You stole them from a domain administrator who signed into the system. You had help!

If you can assume that a domain administrator is signed in, then you don't need to do all those complicated things to extract the domain administrator's network credentials. You can just install a keylogger to steal the domain administrator's network credentials. Or even simpler: Just put a program of your choosing in the system Startup group.[1] That program runs with the identity of the domain administrator and can do anything the domain administrator can.

What you really demonstrated is that if a domain administrator signs into a system, they are giving that system access to their domain account. And if they sign into a malicious system, then oops, that malicious system can do anything it wants with their domain account.

It's like saying, "If I give my passport to a fake police officer, then the fake police officer can steal my passport!" Well yes. So don't give your passport to fake police officers. And don't sign into untrusted computer systems. After all, the computer system might be running a completely fake operating system that is just pretending to be Windows!

[1] This variant was also filed as a security vulnerability report six months later.