Once you give away the farm, you can't take it back: Recovering from a rogue administrator

devblogs.microsoft.com/oldnewthing/20230228-00

February 28, 2023

Raymond Chen

A security vulnerability report arrived that went roughly like this:

- Create a new user "Attacker" with Administrator privileges.
- Log in as "Attacker".
- While logged in as "Attacker", browse to a folder that require Administrator privilege.
- When Explorer tells you that you don't have access, click "Continue" to gain access.
- Log out as "Attacker".
- Log in another administrator account.
- Change the account category of "Attacker" from "Administrator" to "Standard user".
- Log back in as "Attacker" and browse to those same folders.
- Notice that the Attacker has retained access to the folders, even though the Attacker is no longer an administrator.

This story is all accurate, but is there a security vulnerability?

Let's go through the usual questions.

Who is the attacker? The attacker is the user we called "Attacker".

Who is the victim? The victim is the other administrator who created the "Attacker" account and then later reduced the "Attacker" account's privileges to Standard User.

What has the attacker gained? The attacker gained persistent access to resources.

But wait, this all assumes that the attacker was able to log on as the Attacker account and exercise its Administrator powers. The attacker is an administrator on the system. You have already lost!

Once you let the attacker into your system with administrator privileges, they can do all sorts of things to establish persistent access. They can add themselves to the security descriptors of various resources. They can plant a backdoor that gives them an administrative command prompt. They can install malware that steals passwords.

In fact, they can even patch the "Remove a user from the Administrator group" user interface code so that it says "Yup, totally removed Attacker from the Administrator group" without actually doing it.

Once you give away the farm, you can't take it back. It's gone.

Note that the system did ask an administrator for permission to grant the Attacker account permanent access to the folder. The prompt from Explorer says, "You don't currently have permission to access this folder. Click Continue to permanently get access to this folder," and the Continue button requires administrator privileges. So it requires administrator privileges to gain persistent access to a folder. Fortunately, there's an administrator right there to grant that privilege: The Attacker!

Once you let a bad person become an administrator, you have lost the game. It is essential that you give administrator privileges only to people you trust.

The user interface to remove someone from the Administrator group does what it says on the tin: The user is removed from the Administrators group. But that is not sufficient to clean up behind a rogue administrator, because you haven't cleaned up all the backdoors the rogue administrator may have planted while they still had administrator privileges. And you may never be sure that you found them all. As the philosopher Ellen Ripley put it, "Nuke the entire site from orbit. It's the only way to be sure."