It rather involved being on the other side of this airtight hatchway: Account vulnerable to Active Directory administrator

devblogs.microsoft.com/oldnewthing/20141217-00

December 17, 2014

Raymond Chen

A security vulnerability report came in that went something like this:

> **Disclosure of arbitrary data from any user**
>
> An attacker can obtain arbitrary data from any user by means of the following steps:
>
> 1. Obtain administrative access on the domain controller.
> 2. Stop the XYZZY service.
> 3. Edit the XYZZY.DAT file in a hex editor and changes the bytes starting at offset 0x4242 as follows:
> 4. …

There's no point continuing, because the first step assumes that you are on the other side of the airtight hatchway. If you have compromised the domain controller, then you control the domain. From there, all the remaining steps are just piling on style points and cranking up the degree of difficulty. A much less roundabout attack is as follows:

> 1. Obtain administrative access on the domain controller.
> 2. Deploy a logon script to all users that *does whatever you want*.
> 3. Wait for the user to log in next, and your script will DO ANYTHING YOU WANT.

No, wait, I can make it even easier.

> 1. Obtain administrative access on the domain controller.
> 2. Change the victim's password.
> 3. Log on as that user and DO ANYTHING YOU WANT.

You are the domain administrator. You already pwn the domain. That you can pwn a domain that you pwn is really not much of a surprise.

This is why it is important to choose your domain administrators carefully.

Raymond Chen

Follow