Use Group Policy to avoid ConFlicker in Windows

In this article, I will show you some methods to help you protect your computer to avoid being infected with a dangerous worm called ConFlicker.

Derek Melber

In this article, I will show you some methods to help you protect your computer to avoid being infected with a dangerous worm called ConFlicker .

Introduce

Windows security is always an easy task. Indeed, there are too many issues that need to be addressed in security, but are essentially the same as maintainers for the operating system and IT world. Each operating system has vulnerabilities and they can be attacked by a huge number of viruses and worms. In the case of ConFlicker, the story is the same. When the worm appeared again, the patch was released within an hour, but the number of infected computers continued to increase. Why is there a case? The following logic will show that your computers have not been patched properly! We use this article to introduce methods that can be used to help protect your computer against infection by deepening this ConFlicker, based on how it attacks the system.

Basic information about ConFlicker

ConFlicker has two variants since its first appearance in November 2008. The first variant is not as dangerous as the second, which must have been heard from the media. You can refer to the information about the Clicker provided by ms in the **MS08-067** security upgrade here. The next generation of ConFlicker was released in December 2008, this is a variant that can attack on a large scale and dangerous. You can read the following document for more information about this variant.

ConFlicker, in the latest variant, will attack the system at different points, they will try to embed themselves wherever possible with the hope that they will not be detected and difficult to remove when infected. This worm will attack parts of the computer below:

- Create hidden DLL files with different names in the Windows System folder
- Create hidden DLL files located in **% ProgramFiles% Internet Explorer folder** or **% ProgramFiles% Movie Maker**
- Create an entry in the Registry: **HKCUSoftwareMicrosoftWindowsCurrentVersionRun** .
- Load a service in the Registry under **HKLMSYSTEMCurrentControlSetServices** .
- Copy to the destination computers in the ADMIN $ system with the current credentials of the logged-in user.
- Hack the passwords of SAM users locally on the target computer using weak passwords.

- Create a task that has been programmed remotely on the destination computer (if the username and password are compromised).
- Copy to all mapped and removable drives.
- Creating an autorun.inf file on all drives will exploit the AutoPlay feature if enabled, thus launching deep on infected computers during autorun.
- Disable viewing of hidden files
- Adjust the TCP settings of the system to allow a large number of concurrent connections.
- Delete the Registry key for Windows Defender
- Reset system restore points
- Download files from other websites

As you can see, ConFlicker is a very dangerous worm that infects many different parts of the system, as well as folders, Registry and other areas of the system.

Get the patch

The best solution to fight ConFlicker is to obtain a patch from Microsoft here.

You will find that Windows Vista and Windows 2008 are only at the 'Important' level for this vulnerability, due to the protection and security of these two operating systems compared to previous operating systems.

The Group Policy settings protect against ConFlicker

First of all, if the user being attacked is not a member of the internal Administrators group, the worm will spend a lot of time in injecting it into the computer. So, to disable this situation, you can use Group Policy Preferences to remove user accounts from the local administrators group. This policy is located in the **User ConfigurationPreferencesControl Panel SettingsLocal Users and Groups** . You only need to configure the internal group policy for ' **Administrators** ', then select the option button ' **Remove the current user** ', as shown in Figure 1.

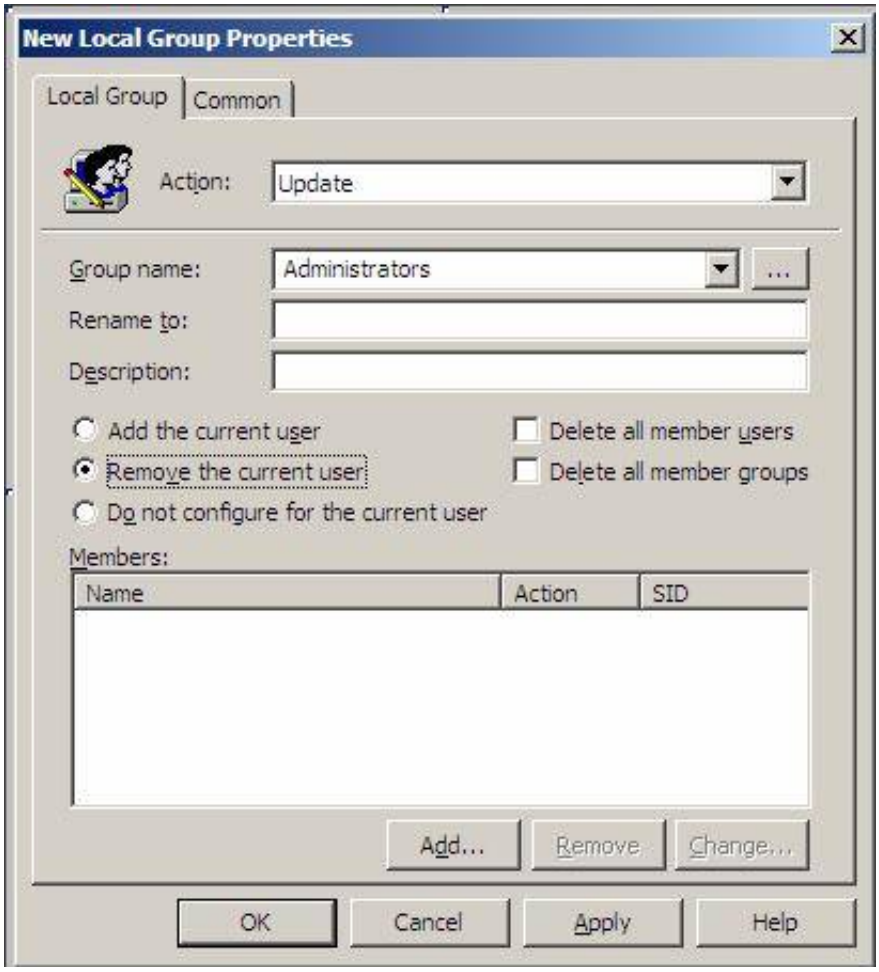

Figure 1: Remove the current user account from the internal Administrators group

Since this worm will attempt to list then attack the list of internal usernames on the target computer, you need to ensure that there are no user accounts in the local SAM for each client. This can be done using the policy shown in Figure 1, but also allows you to delete all users in the Administrators group, as shown in Figure 2.

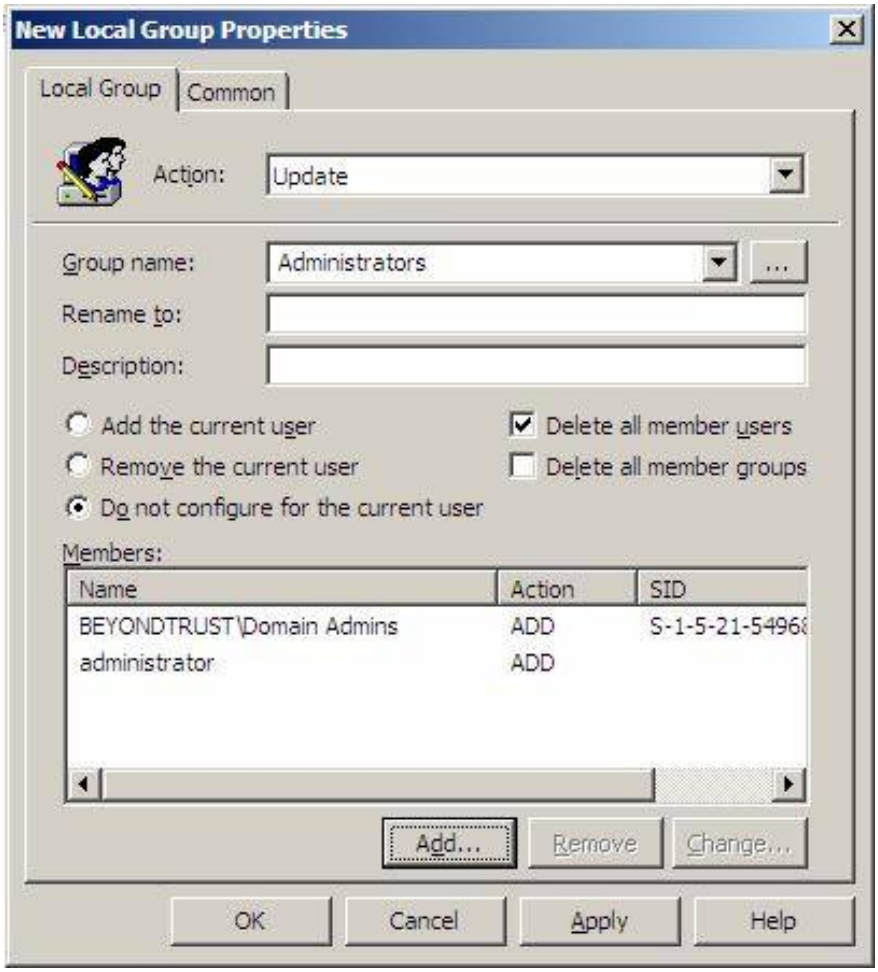

Figure 2: Remove all members from the internal Administrators group

Note:
In Figure 2, the Domain Admins group and the internal Administrator account can be forced into the local Administrator group, which is the best security solution here.

Although this next setting is not available in Windows XP or Server 2003, it is a great configuration for Windows Vista and Server 2008. Group Policy will control all User Account Control areas and then remind the application. pros for administrators and refusing to elevate rights (for standard users). This will prevent viruses, worms and other malicious software from performing tasks to change operating system files and the Registry. These actions should only be performed in the foreground section, when the user tries to perform one of the administrative tasks. ConFlicker will try to write and change a large number of protected files, folders and registry entries hidden behind. These UAC settings can be found in **Computer ConfigurationPoliciesWindows SettingsSecurity SettingsLocal PoliciesSecurity Options** . Figure 3 illustrates a complete list of settings that can be configured.

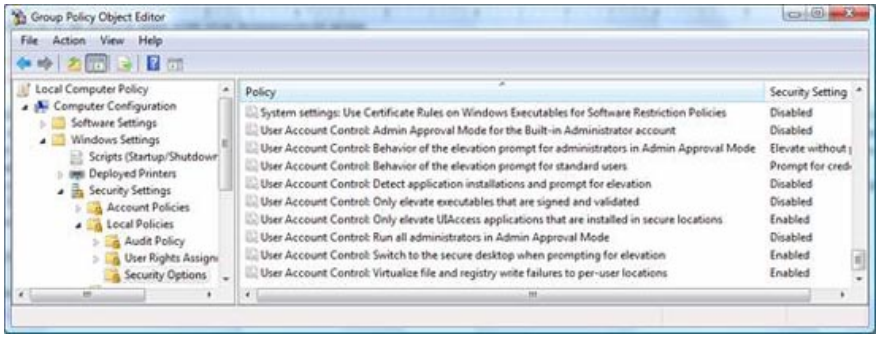

Figure 3: Access control of UAC settings on Windows Vista and Server 2008

The last set of Group Policy settings needs to be configured regarding user account passwords. Since ConFlicker will try to guess the passwords, we need to make sure that the Password Policies are set to get strong and long enough passwords. This can be done in the Default Domain Policy for Active Directory domains, but can also be configured in an internal GPO for standard computers. The settings for **Password Policies** are under **Computer Configuration, Windows SettingsSecurity SettingsLocal PoliciesAccount Policies** , as shown in Figure 4.

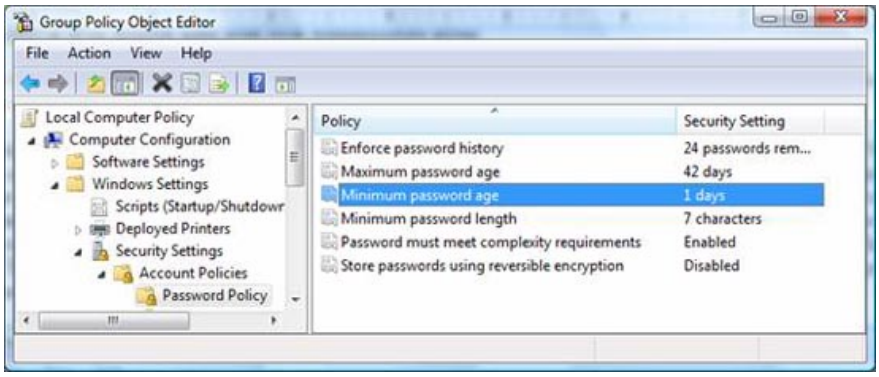

Figure 4: Password policies will limit the strength and weakness of a password

The last Group Policy setting can be configured as AutoPlay control. Because ConFlicker will write to external devices that can be controlled by AutoPlay, this worm can be initialized by lying in the file on external devices. However, if the AutoPlay feature is disabled, this action will not be allowed. To disable this AutoPlay function through Group Policy, go to **Computer Configuration Administrative TemplatesWindows Components** , as shown in Figure 5.

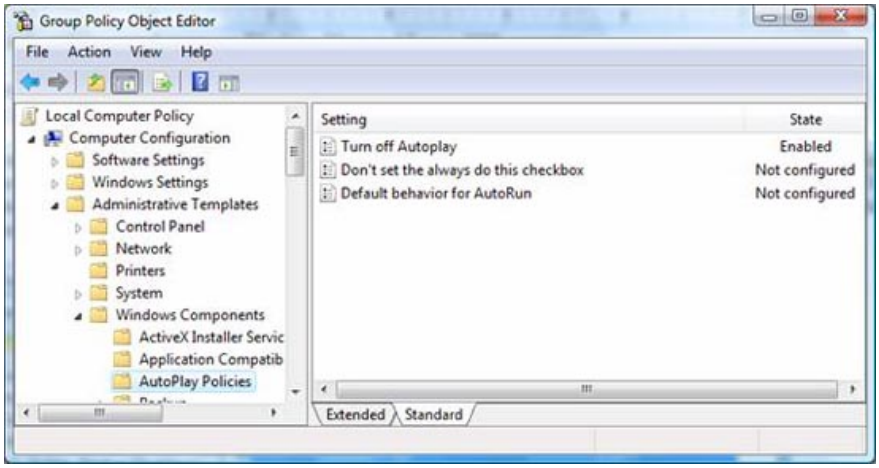

Figure 5: AutoPlay can be disabled via Group Policy

Conclude

ConFlicker is growing up is the lack of action in a timely manner. The patch is released and the ability to disable this worm is completely possible from the moment it is released. If administrators, companies and users take action to deny the penetration or further penetration of this worm, concerns will be relieved. However, until now, this worm continues to spread widely. That is why you need to take timely actions to stop its spread. The best action for this case is to configure Group Policy to restrict access to the system and improve the security of passwords on the system. Denying access of ConFlicker to the system can be done quite easily. Passwords are also protected quite easily and should be configured long enough and complex enough. When you perform these actions properly, your systems will be protected and this dangerous worm will not be able to penetrate the system.

Good luck!