Misunderstanding the “Prevent access to registry editing tools” policy

devblogs.microsoft.com/oldnewthing/20241001-22

October 1, 2024

There is a group policy called “Prevent access to registry editing tools”. A customer found that even if they enabled the policy, malware was still able to call `RegSetValue` to modify values in the registry. The malware was able to modify the registry even though the policy blocked access to the registry! Is the policy broken?

Take a closer look at the policy name: “Prevent access to *registry editing tools*.” If you missed it, look at the policy description.

> This setting disables the Windows registry editor or Regedit.exe.
>
> If you enable this policy setting and the user tries to start Regedit.exe, a message appears explaining that a policy setting prevents the action.
>
> If you disable this policy setting or do not configure it, users can run Regedit.exe normally.
>
> To prevent users from using other administrative tools, use the “Run only specified Windows applications” policy setting.

What this policy does is prevent tools like `regedit.exe` and `reg.exe` from running. Those programs check the policy setting when they start up, and if the policy is set, then they display an error message and exit.

```
C:\> reg.exe query HKLM\Software\Microsoft\Windows
ERROR: Registry editing has been disabled by your administrator.

C:\> regini.exe
Error: Registry editing has been disabled by your administrator.
```

Registry Editor
ⓧ Registry editing has been disabled by your administrator.
OK

The policy has no effect on other programs. They are still allowed to access the registry, subject to the normal rules.

In other words, this is not “prevent access to the registry”. It’s “prevent access to registry editing tools.”

After all, if this policy prevented anybody from accessing the registry, then a lot of things would stop working. For one thing, Windows keeps some of its own configuration data in the registry, so blocking access to the registry would prevent Windows from knowing, say, which drivers to load.

Bonus chatter: Since the policy check is performed voluntarily from `reg.exe` and `regedit.exe`, a dedicated end user could look for other ways to perform registry modifications, such as PowerShell scripting or downloading their own alternate registry editing tool. This policy is intended to block casual users from messing up their own machines. It is not a security boundary.