Avecto

7 ways to crack Windows 7

Sami Laiho, Microsoft MVP and ethical hacker

In this short article, Sami explains seven different vulnerabilities in Windows 7 which demonstrate why the removal of admin rights is essential to optimizing security.

As an OS guy, I love cracking into Windows: this is the way I teach clients how to best protect and troubleshoot their operating system. I use my 'cracks' as learning examples on how Windows, its services and processes work. I don't use malware or anything that would be caught by antimalware software but simply manipulate Microsoft's own misconfigurations or flaws to get access to a system.

I have a plethora of examples of these 'cracks', but I will use this article to give you a run-down of the top 7 vulnerabilities you should address, whatever stage you are at in the migration process.

1) Logon screen processes

Back in Windows 2000, you could change you logon screensaver to cmd.exe and wait a few moments to get SYSTEM-account access to the machine. This has now been fixed to use LocalService account so it's not a problem anymore. Why they haven't done the same for processes like utilman.exe, displayswitch.exe and sethc.exe, I don't know. These processes can be replaced by cmd.exe to get access to the machine. How to prevent it? Use BitLocker and get rid of admin rights.

2) Image file execution options

There's a registry entry meant for debugging software called Image File Execution options. It can be used to play around with your colleague's computer by changing their Notepad.exe to always start calc.exe or their iexplore.exe to always start chrome.exe. It can also be used to crack the system by capturing processes like sethc.exe and changing them to run cmd.exe. Again, preventing this means using BitLocker and removing administrator rights.

3) Unsigned local Group Policies

Every Windows machine has a local group policy located at C:\Windows\System32\GroupPolicy. If it's not there, it will be after you run GPEDIT.MSC for the first time. This policy is not signed so you can build a policy on your machine and make it run a command that creates an admin account for you. After this, all you have to do is inject it on a computer that you want to break into. You can avoid this threat by stopping Local Group Policy Processing via Group Policy, using BitLocker and getting rid of admin rights.

Avecto

4) Scheduled task as bait

When you get admin access to a computer, nothing is more fun than creating a scheduled task that runs NET GROUP “Domain Admins” domain\sami /add /domain on every logon. Then you just call your help desk and ask them to RDP into your machine to “fix” it for some reason. If they use Domain Admin accounts so will you after this! How to prevent it? Get rid of admin rights and remember that users who have domain admin rights need at least three accounts to do their job: a normal user account, an account to administer desktops and servers and a domain admin account.

5) Disobeying Group Policy

Group Policy won’t apply if you can’t read it and it’s mostly just registry settings. So, if you deny your SYSTEM-account read permissions to HKLM\Software\Policies, your company’s policies won’t apply! Removing admin rights will prevent this one too.

6) Windows-folder weaknesses

Stuff like AppLocker can work when you don’t have too many rules. One of the most common ways of configuring Windows AppLocker is to allow software to run from C:\Windows. But how many admins realize that normal users can write to C:\Windows\debug\WIA , for example? How to prevent it? Use AppLocker exemptions to rule out the unsecure folders and get rid of admin rights.

7) Firewire

It’s not Windows’ fault that FireWire and ThunderBolt support Direct Memory Access that allows you to read BitLocker keys from the memory or tell the kernel that it should accept the next password typed in the logon screen. How to avoid this? Block Firewire/ThunderBolt with Device Restriction policies or Epox and, of course, get rid of admin rights.

Sami Laiho is a Senior Consultant and partner at Finland’s biggest training company, Sovelto, and a Senior Technical Fellow at his own company, Adminize.

He has been an MVP Windows ExpertITPro since 2011 and is part of Microsoft STEP group. Sami has been training and consulting upon OS Deployment, management, security and troubleshooting for the past 16 years.

About Avecto

Avecto is a leader in Privilege Elevation and Delegation Management. Since 2008, the company has enabled over 8 million users to successfully work without admin rights, enabling many of the world’s biggest brands to achieve the balance between overlocked and underlocked environments.

Avecto’s Defendpoint software has been deployed in the most highly regulated industries, enabling organizations to achieve compliance, gain operational efficiency and stop internal and external attacks.