专注APT攻击与防御

https://micropoor.blogspot.com/

本季是作《php安全新闻早八点-高级持续渗透-第一季关于后门》的补充。

https://micropoor.blogspot.com/2017/12/php.html

在第一季关于后门中，文章提到重新编译notepad++，来引入有目标源码后门构造。

本季继续以notepad++作为demo，而本季引入无目标源码构造notepad++ backdoor。

针对服务器，或者个人PC，安装着大量的notepad++，尤其是在实战中的办公域，或

者运维机等，而这些机器的权限把控尤为重要。

该系列仅做后门思路。

Demo 环境：

Windows 2003 x64 Windows 7 x64 notepad++ 7.6.1 vs 2017

遵守第一季的原则，demo未做任何对抗安全软件，并且demo并不符合实战要求。仅提出思路。由于demo并未做任何免杀处理。导致反病毒软件报毒。如有测试，建议在虚拟机中进行测试。

Windows 2003： ip 192.168.1.119

开放端口：

notepad++版本：

导入dll插件：

notepad++ v7.6.x以上版本提示，后重新打开notepad++，来触发payload。

开放端口变化如下：

msf连接：

后者的话：

demo借助了notepad++的证书，在通过notepad++来调用自身。本季的demo并不符合实战要求。在实战中，当目标人启动notepad++时，或者抓取密码发送到指定邮箱，或者在做一次调起第四方后门等，这是每一位信息安全从业人员应该考虑的问题。

关于后门，无论是第一季还是最六季，都侧面的强调了shellcode的分离免杀，后

门”多链”的调用触发。同样，攻击分离，加大防御者的查杀成本，溯源成本，以及时间成

本。给攻击者争取最宝贵的时间。

PS：

关于mimikatz的分离免杀参考上一季《体系的本质是知识点串联》，

https://micropoor.blogspot.com/2018/12/blog-post.html。

本demo 不支持notepad++ v7.6版本。因为此问题为notepad++官方bug。7.6.1更新如下：

为此调试整整一天。才发现为官方bug。

Demo for dll：

由于demo并未做任何免杀处理。导致反病毒软件报毒。如有测试，建议在虚拟机中进

行测试。demo仅做开放443端口。等待主机连接。

HTMLTags\_x32.dll

大小: 73728 字节文件版本: 1.4.1.0

修改时间: 2018年12月31日, 18:51:20

MD5: FDF30DD5494B7F8C61420C6245E79BFE

SHA1: D23B21C83A9588CDBAD81E42B130AFE3EDB53EBB CRC32: D06C6BD1

https://drive.google.com/open?id=1\_sFKMWi6Zuy1\_v82Ro1wZR8OrqKr7GD4

HTMLTags\_x64.dll

大小: 88064 字节文件版本: 1.4.1.0

修改时间: 2018年12月31日, 18:51:09

MD5: D7355FF1E9D158B6F917BD63159F4D86

SHA1: 9E6BC1501375FFBC05A8E20B99DC032C43996EA3 CRC32: 606E5280

https://drive.google.com/open?id=1JwmW8KrxYoQ1Dk\_VNtnDs0MxM6tuqCs\_

Micropoor