专注APT攻击与防御

https://micropoor.blogspot.com/

本季是《高级持续渗透-第七季demo的成长》的延续。

https://micropoor.blogspot.com/2019/01/php-demo.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。

在第六季关于后门中，文章假设在不得知notepad++的源码，来引入无目标源码沟门构造。

在第七季关于后门中，文章让demo与上几季中对比，更贴近于实战。

而在第八季，继续优化更新demo，强调后门链在高级持续渗透中的作用。该系列仅做后门思路。

在上季中引用一个概念：“安全是一个链安全，攻击引入链攻击，后门引入链后门”，而”链”的本质是增加对手的时间成本，金钱成本，人力成本等。

第七季的文章结尾是这样写道：

而增改后门每一个功能，则需要更改demo的功能，或者增加几个功能的集合。那么它并不是一个标准的"链"后门。为了更好的强调“链”后门在高级持续渗透中的作用。第八季把demo打造成一个远控。以及可结合任意第三方渗透框架。

远控4四大要素：

可执行cmd命令

可远程管理目标机文件，文件夹等

可查看目标摄像头注册表和服务操作等等

而以上功能需要大量的代码以及大量的特征加入到该dll里，而此时，后门不在符合实战要

求。从而需要重新构建后门。思路如下：dll不实现任何后门功能，只做“后门中间件”。而以上功能则第四方来实现。第三方作为与后门建立连接关系。

Demo 环境：

Windows 2003 x64 Windows 7 x64 Debian

notepad++ 7.6.1，notepad++7.5.9 vs 2017

Windows 2003： ip 192.168.1.119

开放端口：

notepad++版本：

notepad++v7.6以下版本插件直接放入X:\Program Files (x86)\Notepad++\plugins目录下即可。

放置后门：

配置后门链：

配置下载服务器：

配置msf：

再次打开notepad++：

变化如下：

下载服务器：

msf服务器：

执行顺序为：

notepad++挂起dll后门

后门访问下载服务器读取shellcode

根据shellcode内容，加载内存

执行shellcode

Micropoor.rb核心代码如下：

而此时，无需在对dll的功能改变而更改目标服务器，只需更改下载服务器shellcode，以

messagebox为例：

msf生成shellcode如下：

替换下载服务器shellcode：

再次运行notepad++，弹出messagebox，而无msf payload功能。

后者的话：

在第八季中，只需配置一次目标服务器，便完成了对目标服务器的“后门”全部配置。以减小最小化接触目标服务器，来减少被发现。而以后得全部配置，则在下载服务器中。来调用第四方框架。并且目标服务器只落地一次文件，未来其他功能都将会直接加载到内存。大大的增加了管理人员的对抗成本。“后门链”的本质是增加对手的时间成本，金钱成本，人力成本等。而对于攻击者来说，下载，执行，后门分别在不同的IP。对于对抗安全软件，仅仅需要做“落地”的exe的加解密shellcode。

附：Micropoor.rb大小: 1830 字节

修改时间: 2019年1月4日, 15:46:44

MD5: D5647F7EB16C72B94E0C59D87F82F8C3

SHA1: BDCFB4A9B421ACE280472B7A8580B4D9AA97FC22 CRC32: ABAB591B

https://drive.google.com/open?id=1ER6Xzcw4mfc14ql4LK0vBBuqQCd23Apg

MicroNc.exe

注：强烈建议在虚拟中测试，因Micropoor已被安全软件加入特征，故报毒。

大小: 93696 字节

修改时间: 2019年1月4日, 15:50:41

MD5: 42D900BE401D2A76B68B3CA34D227DD2

SHA1: B94E2D9828009D80EEDDE3E795E9CB43C3DC2ECE CRC32: CA015C3E

https://drive.google.com/open?id=1ZKKPOdEcfirHb2oT1opxSKCZPSplZUSf

Micropoor