

ZeroNet系列——通过Tor使ZeroNet匿名

发表于: 2016年04月18日 • 20 条评论 • 1,644 次浏览 • ZeroNet 安全 暗网 翻墙

最近在ZeroNet的GFW Talk与Telegram群组里很多朋友讨论有没有一个方便快捷的方式使ZeroNet自带的Tor工作...下面就是通过翻墙软件复活Tor使ZeroNet匿名

★需求群体

如果你准备在ZeroNet恶毒攻击党和政府或者做一些其他敏感的,会令公安不高兴的事情,则需要匿名性,如果不做敏感的事情而仅仅是看看,则不需要匿名性....

★复活Tor

◇使用翻墙软件

要复活Tor, 需要翻墙软件, 这个大家应该都会, 不会的话你也访问不到本站了:)

★配置ZeroNet

首先打开ZeroNet目录, 找到ZeroBundle\ZeroNet\tools\tor\torrc文件,使用记事本打开..

◇Socks代理

如果你使用的是SOCKS5类代理,如Shadowsocks,则添加一行

修改1080为你的翻墙端口

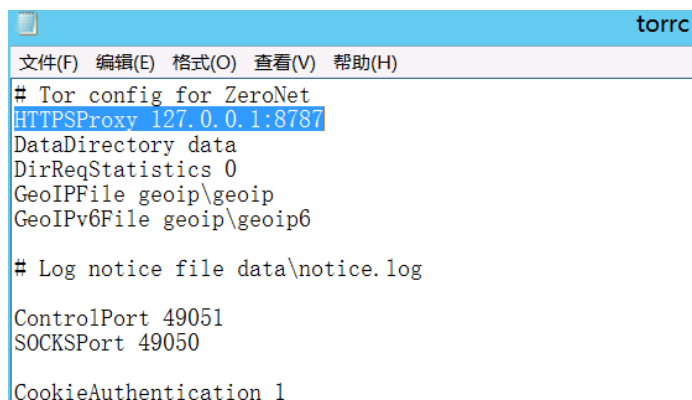
```
Socks5Proxy 127.0.0.1:1080
```

◇HTTPS代理

如果你使用的是HTTPS代理,如Lantern, 则在Lantern中设置代理全部流量,并添加一行

HTTPSProxy 127.0.0.1:8787

修改好之后应该如下图



```
# Tor config for ZeroNet
HTTPSProxy 127.0.0.1:8787
DataDirectory data
DirReqStatistics 0
GeoIPFile geoip\geoip
GeoIPv6File geoip\geoip6

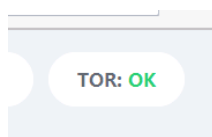
# Log notice file data\nnotice.log

ControlPort 49051
SOCKSPort 49050

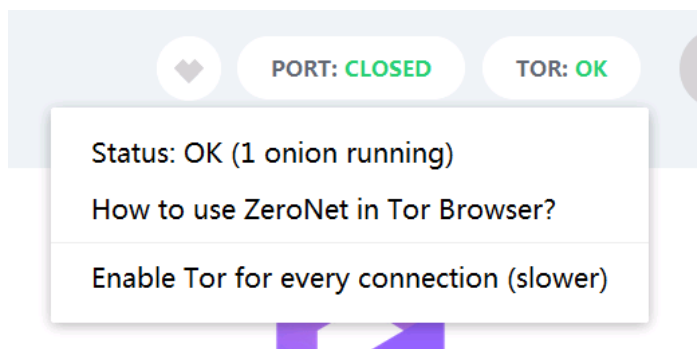
CookieAuthentication 1
```

保存文件,回到ZeroNet主目录,运行zernet.cmd

过一会儿(大约1分钟左右),会看到ZeroNet提示Tor的状态为OK

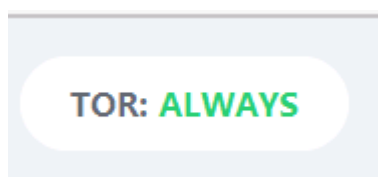


别急,还没完,等看到提示TOR: OK的 时候 点击Tor OK这个指示条



点击“Enable Tor for every connection (slower)” 之后重启Zernet

重启后,提示Tor: ALWAYS 就说明匿名化成功:)



★注意事项

1. 在Tor Always模式下,如果Tor无法开启,则无法使用ZeroNet,所以确保torrc文

件中设置的翻墙代理工作....

2. 如果不要点击陌生的链接,如果偏要点的话,请用Tor Browser, 如本系列[第一篇文章](#)中的Tor Browser设置方法..

转载请注明来自Xiaolan's Blog (<https://xiaolan.me>)

20 条评论



Anonymous • 2016年04月18日 • Reply

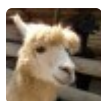
1在MSDN我告诉你里下载的win7原版系统是否可靠？是不是只要和官方给出的SHA1码比对一致就可靠了

2之前看过你的文章说公安有那种免杀木马的，那怎么确定我有没有中，如果有，重装系统能解决问题吗？如果不能，怎么彻底解决问题？

3我打算三虚拟机都用win7系统安全吗？看你们是都用linux，或者win 服务器系统，但都太难用，感觉这个学习成本太高，真的有必要去钻研吗？

4哪里能下到安全可靠的windows激活软件，我知道这类软件很多，自己也激活过很多次，但是因为要用的系统是用来发反动帖子的话需要绝对安全，网上的那些软件很多都报毒，能提供个你鉴定肯定安全的激活软件吗？

5你之前提到过有个漏洞浏览器跨站获取信息的，这个以及别的漏洞都修复了吗？我要上国内http网站用多重代理发帖，还有危险吗？



Xiaolan • 2016年04月18日 • Reply

1.itellyou.cn上的资源是国内订阅用户“雪龙郎”的ISO，校验SHA过后如果没问题的话是纯净的（我可没说是“安全的”哈，win10是场噩梦）

2.最好不要用windows，（如果装了win的话）可以的话比对一下你的系统文件和原始系统文件是否一样，如果你比较偏执的话（或称强迫症）最好还是重装一下吧：）

机子没有被人拿走或者没有装过国产（尤其是）安全软件的话一般没事。

3.举个栗子，whonix就是用debian搭起来的，而且，你用三虚拟机想要实现什么功能呢？如果仅仅是tor+某代理的话，我倒是建议你用whonix，更加安全一些。

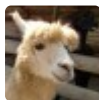
4.我不用windows...这个自行判断吧，或者利用你windows下的vmware的快照功能，不断循环最初始的安装状态。

5.noscript插件一直是你的好伙伴（自动防止xss,js,flash）



Anonymous • 2016年04月19日 • Reply

whonix的gateway没有前置代理Tor没法用，还是得用三虚拟机？



其实我不是Xiaolan：） • 2016年04月19日 • Reply

<https://www.cyberthink.me/whonix-gateway-config-china.html>

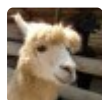


Anonymous • 2016年04月19日 • Reply

1win10怎么了？很危险吗？我现在虚拟机用的就是win10。换成win7好吗？我用下来还是win7最顺手

3就是希望安全发帖，可能要安装qq之类的国产软件。但是不知道那么慢的网速登陆qq会不会超时。

5用了这个插件，网页都不能正常显示了，如果只是浏览就不用那么麻烦了，有没有别的办法？



一个好心的仿Xiaolan • 2016年04月19日 • Reply

win10的安全【设计】很有问

题：[http://www.slate.com/articles/technology/bitwise/2015/08/](http://www.slate.com/articles/technology/bitwise/2015/08/windows_10_privacy_problems_here_s_how_bad_they_are_)

[/windows_10_privacy_problems_here_s_how_bad_they_are_](http://www.slate.com/articles/technology/bitwise/2015/08/windows_10_privacy_problems_here_s_how_bad_they_are_)
(Google一下可以找到很多相关的资料)

换成WIN7没问题的，记得打补丁。

(其实还是没想通你三个虚拟机都搞Windows的意义何在...)

所谓 安全发帖 的定义是什么？仅仅不暴露IP？还是什么都不留下？

比如，你装了QQ之类的（放在实际操作的虚拟机下），那么你的QQ号注册过程中是否有什么问题？（比如填写的你的真实信息，或者你在一个非代理环境下登陆过？），如果注册完全匿名的话，还要考虑QQ的软件是否有扫描的电脑上文件的问题。

登陆超时一般不会，QQ好像还没有把TOR节点拉入黑名单，好像。

其实，主要是这样（我之前没理解对...），如果你是放在网关之后的，浏览器基本不成太大问题

(不会暴露直接IP)，因为有网关挡在前面。

但一般我还是建议你加上她。

以下是官网的一段话：

The NoScript Firefox extension provides extra protection for Firefox, Seamonkey and other mozilla-based browsers: this free, open source add-on allows JavaScript, Java, Flash and other plugins to be executed only by trusted web sites of your choice (e.g. your online bank).

NoScript also provides the most powerful anti-XSS and anti-Clickjacking protection ever available in a browser.

NoScript's unique whitelist based pre-emptive script blocking approach prevents exploitation of security vulnerabilities (known and even not known yet!) with no loss of functionality...

You can enable JavaScript, Java and plugin execution for sites you trust with a simple left-click on the NoScript status bar icon (look at the picture), or using the contextual menu, for easier operation in popup statusbar-less windows.



Anonymous • 2016年04月20日 • Reply

你是xiaolan本人吗？都用windows是因为我不会用Linux,学习新的东西要付出不少时间，尽量减少学习成本吧。

我是担心网速不够登陆qq超时。

顺便问一句，你们用的翻墙软件 and 我们的都一样吗？怎么我感觉网速这么慢呢，看编程随想的博文那么多图片，多重代理下还要上传图片，不知道得花多久时间，我自己加载完一篇文章都要不少时间，这么慢的网速怎么登陆qq呢？

Anonymous • 2016年04月20日 • Reply



noscript这个插件以前用过，要防止漏洞的话要不要开启全局禁止脚本？之前开启过网页大部分内容无法显示，这样子还有什么用？你贴的英文翻译了也不是很懂，总之要不要开全局禁止脚本，如果要开那等于没用，那样网页不能正常显示



Anonymous • 2016年04月28日 • Reply

怎么不继续回了？漏洞的话装在虚拟机里就算中了也不会暴露ip吧？中木马还原快照可以复原吗？



Anonymous • 2016年04月19日 • Reply

这篇文章是把前置代理的翻墙软件放在宿主机了，这样并不安全吧



Anonymous • 2016年04月21日 • Reply

4我试了一下，就算在刚装完win7后保存快照，过几天恢复快照，剩余天数还是会减少。怎么解决？

ZeroNet系列——通过Tor使ZeroNet匿名 – 细节的力量 • 2016年04月20日 • Reply

[...] 原文: <https://xiaolan.me/zernet-2.html> [...]



Anonymous • 2016年04月23日 • Reply

有没有人肉这只共匪的

https://twitter.com/china_bj_tm



Ruo Wei • 2016年04月24日 • Reply

按上述配置Torrc文件，启动ZeroNet后，Tor一直显示在waiting状态，请问这是是什么原因呢？就是使用了Tor Browser，也是一样的情况。目前Torrc文件内容如下：

```
# Tor config for ZeroNet
Socks5Proxy 127.0.0.1:1080
DataDirectory data
DirReqStatistics 0
```

GeoIPFile geoip\geoip

GeoIPv6File geoip\geoip6

Log notice file data\nnotice.log

ControlPort 9151

SOCKSPort 9150

CookieAuthentication 0

操作系统是win10，Zernet也是最新的version 0.3.7(rev1254)，麻烦请博主指点一下，不胜感谢！



xiaolan.em • 2016年04月25日 • Reply

Socks5Proxy 127.0.0.1:1080

前置代理设置错了。

参考这里 <http://127.0.0.1:43110>

[/1NCezLP8aXjABVreBB1CKGPub2tKTtyhWU/?Page:map3](http://127.0.0.1:43110/1NCezLP8aXjABVreBB1CKGPub2tKTtyhWU/?Page:map3)



Ruo Wei • 2016年04月26日 • Reply

按博主的指点，根据链接文档说明，编写添加了myTBB命令文件，运行命令后ZeroNet界面中Tor状态果然显示出了绿色的connected状态。虽然不知具体原理何在，还是非常感谢博主的指点！



Ruo Wei • 2016年04月26日 • Reply

记错了，应该是绿色的OK状态。



xiaolan.em 我不是博主 • 2016年04月28日 • Reply

原理

1. 软件启动参数，相当于可选项。比如：[卖东西.exe - 苹果5袋]

1.1zernet 以及大部分软件都自带了一些可选项

1.2zernet刚好自带了 设置tor 代理的IP端口的可选项

2.cmd 批处理是一种脚本，可以用来启动软件，顺便加上参数



Anonymous • 2016年04月28日 • Reply

<https://petitions.whitehouse.gov/petition/investigate-background-regional-ceo-twitter-chen-kui-who-related-ministry-state-security-china>

能不能做个程序自动批量签名，看现在签名数量好少，要达到10万才能去调查陈葵的背景。



Anonymous • 2016年05月01日 • Reply

最近看别人提到了虚拟机剪贴板共享的隐患。那我把危险虚拟机的启用复制粘贴的勾去掉，只保留拖拽功能，是不是就行了？除了这个漏洞还有什么别的不起眼的危险漏洞

Leave a Reply

Your email address will not be published.

Comment

Name

Email

Website

Post Comment