OWASP 中国 Open Worldwide Application Security Project

OWASP 中国 | 北京分会 Open Worldwide Application Security Project

网安加社区

探真科技 TensorSecurity

开源网安 SECZONE GROUP

BrainAu 脑动极光 BRAINAU

红队评估中的对抗策略与实战技巧

陈殷

2024 OWASP中国安全技术论坛

全球视野下的网络安全趋势

目录

CONTENTS

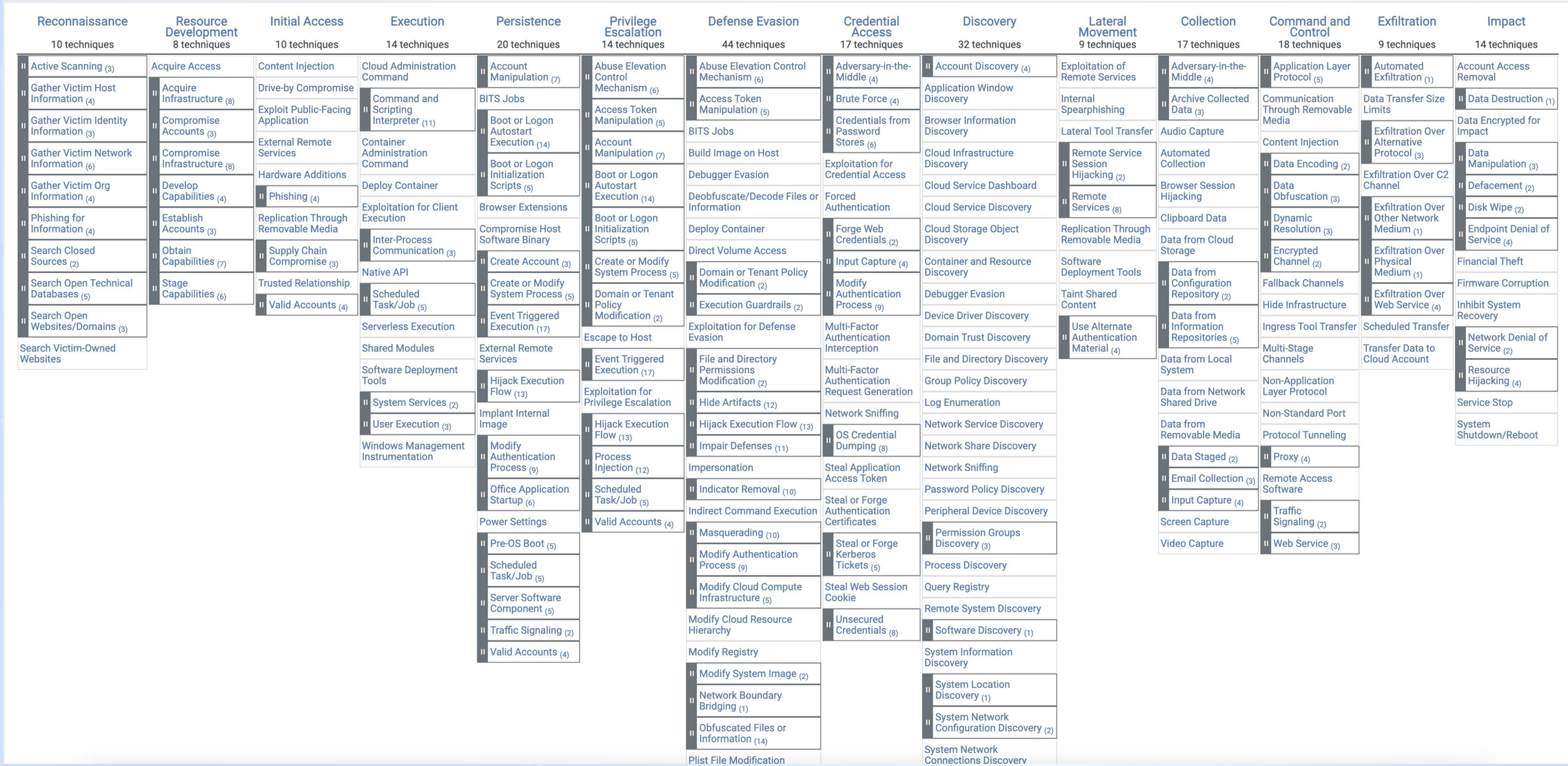
01

红队评估生命周期介绍

MITRE | ATT&CK®

ATT&CK全称为Adversarial Tactics, Techniques, and Common Knowledge（对抗性战术、技术和公共知识库）。它提供了一个基于真实世界观察的对抗技术知识库，专注于攻击者在操作过程中如何与系统交互，反映了攻击者攻击生命周期的各个阶段以及不同平台使用的各种技术。

ATT&CK框架基于攻击者的视角，描述了网络攻击中的战术、技术和过程（TTPs），并被广泛用于网络安全领域，以帮助防御者分析攻击者行为，构建威胁情报，进行对手仿真和红队行动，以及评估与工程决策。



ATT&CK Matrix for Enterprise | 参考来源：https://attack.mitre.org

红队评估概述

红队评估是一种模拟攻击者的安全评估方法，以攻击者视角对网络、基础设施、业务系统等进行模拟攻击，持续暴露防控薄弱点并协助改进，以提升企业安全的防御、监测和应急处置的整体安全水平。

在时间上

红队的一个生命周期为数周或更久，比较灵活且无固定时间限制；
渗透测试为几天一周左右，需要指定目标范围和测试时间。

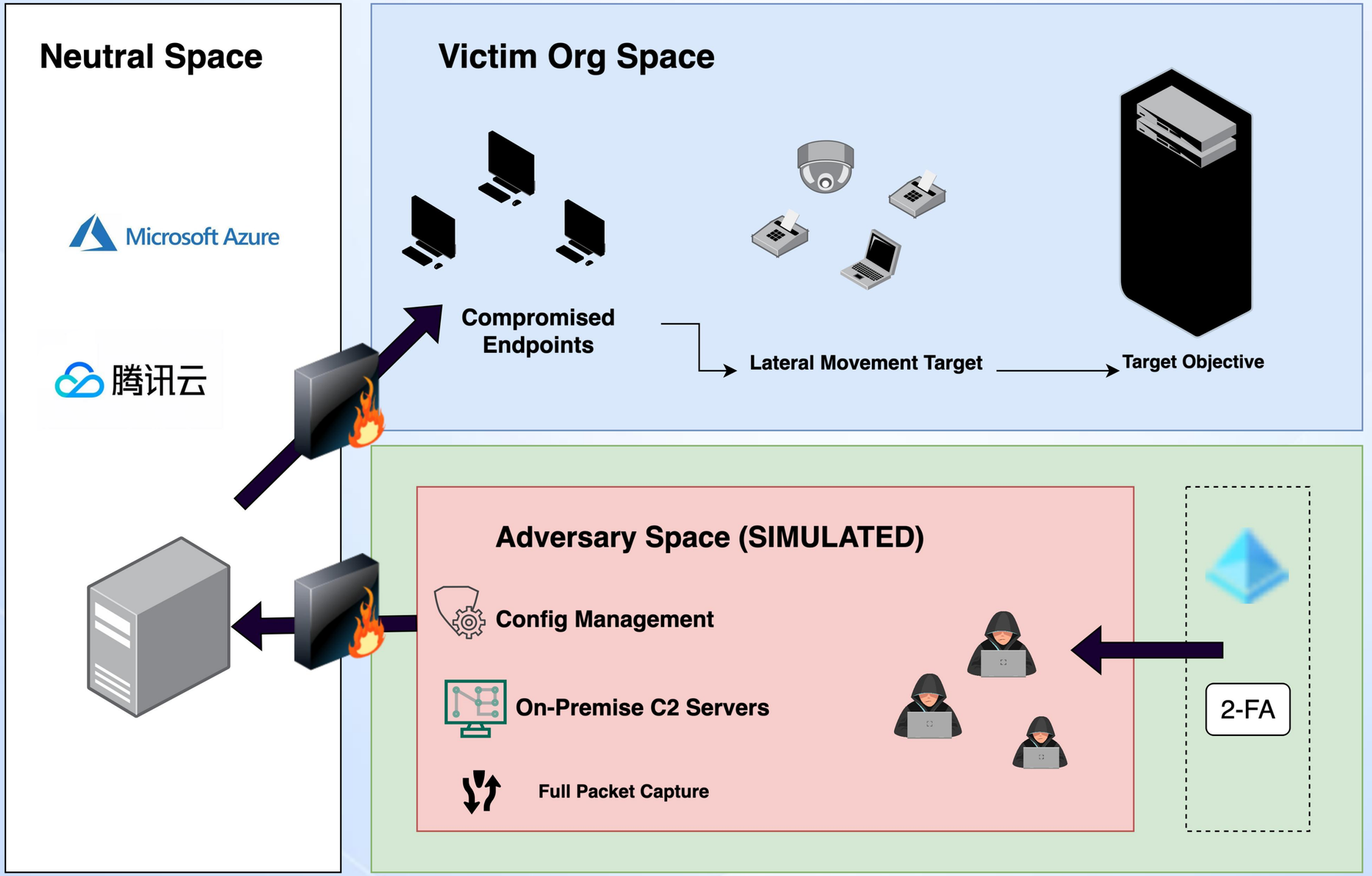
在深度上

红队可以进行深入的后渗透，社会工程学等等贴近真实攻击的手法；
国内的渗透测试还是以发现漏洞为主，一般情况下不进行后渗透等操作。

在实施过程上

红队注重测试的隐蔽性，尽可能的绕过现有的防御系统，拿到目标权限；
渗透测试一般会提前告知防御团队且设置白名单无需隐藏测试行为，有限的时间内尽可能地发现更多漏洞。

A simple model that works for consulting or internal corporate Red Teams.



02

关键战术和技术技巧分享

资源开发

@TA0042

建立可以用来支持行动的基础设施，包括基础设施、帐户等。

自动化脚本编排实现自动化测试/流程化处理

武器自动化或自主化，信息收集、邮件钓鱼、木马免杀的自动化，以及C2、Webshell自主管理工具。

流量加密：wireguard + 混淆协议/或者其他的vpn协议

服务器登录限制：ip限制 + 公钥限制

防火墙策略：敏感服务和端口，只由统一的跳板服务器接入

巡检：定期的安全检查和渗透测试

基础设施的匿名性（redteam服务器和域名等信息资产）

红队工具的匿名性（减少TTP被追踪的可能性）

网络通讯的匿名性（代理，VPN，物联卡等）

网络身份的匿名性（邮箱，社交账号，虚拟身份等）

多级加密代理协议伪装方案

部分场景下的需求：
1、加密传输（众所周知，明文传输等于没挂代理）
2、多级代理（众所周知，一层代理约等于没挂代理）

常用的SOCKS5协议虽然支持代理，但其传输过程是明文的，而TLS代理虽然提供了加密，但在速度上存在不足。因此我们选择使用WireGuard协议进行数据传输。

WireGuard协议在两端都实现了加密，并且基于UDP协议，既满足了加密的需求，也保证了传输速度。然而，WireGuard协议本身存在两个问题：

1. 不支持级联：WireGuard协议本身并不支持级联，这限制了其在多级代理场景中的应用。
2. 易被识别：WireGuard协议的特征较为明显，容易被识别和封锁。

PS：级联指的是将多个代理服务器串联起来使用

多级加密代理协议伪装方案

级联解决：通过在中转服务器（例如A服务器）上使用iptables进行端口转发，可以实现多级代理的级联功能。这样流量可以在不同的代理服务器之间无缝传递，而不需要WireGuard协议本身支持级联。

流量伪装：使用swgp-go工具将WireGuard流量伪装成普通的UDP流量。swgp-go是一个简单的WireGuard代理，可以减少WireGuard流量的开销，并且能够伪装流量，使其不易被识别和封锁。

C2隐藏通信三板斧

Domain Fronting：通过大型可信CDN或云服务提供商隐藏用户访问的目标服务器。

Domain Hiding：通过各种技术手段隐藏或混淆域名信息（适用国外）。

Domain Borrowing：使用合法且广泛信任的域名作为掩盖，使审查系统难以区分合法与非法流量。

《借助码云，仿冒微软，回连某电视台网站的RT样本分析》
https://mp.weixin.qq.com/s/XP7Dy0A21udrEcDJ9MJJkQ

侦察

@TA0043

收集可用于规划未来行动的信息，包括受害者组织、基础设施或员工/人员的详细信息等。

针对大范围的项目的资产发现

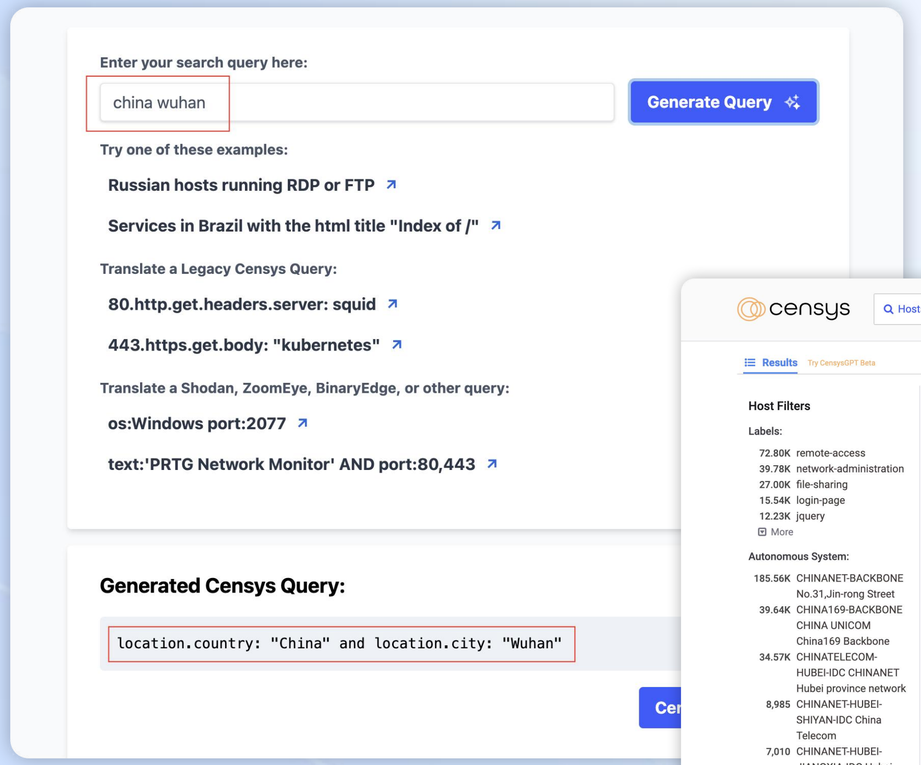

```
PS C:\Users\Administrator\Desktop\ceye> .\CEyes.exe -cloud -sc -s 'city="Changsha"'
[+]now fofa dork is: [ city=Changsha ]
[+]ipc:116.162.189.0/24  count: 150
[+]ipc:116.162.185.0/24  count: 147
[+]ipc:116.162.188.0/24  count: 145
[+]ipc:222.246.138.0/24  count: 132
[+]ipc:116.162.178.0/24  count: 121
[+]ipc:175.6.86.0/24     count: 121
[+]ipc:116.162.180.0/24  count: 112
[+]ipc:110.53.72.0/24    count: 109
[+]ipc:222.246.139.0/24  count: 95
[+]ipc:116.162.201.0/24  count: 94
[+]ipc:111.22.131.0/24   count: 86
[+]ipc:175.6.52.0/24     count: 78
[+]ipc:42.48.86.0/24     count: 56
[+]ipc:116.162.187.0/24  count: 50
[+]ipc:175.6.49.0/24     count: 45
[+]ipc:116.162.19.0/24   count: 44
[+]ipc:116.162.15.0/24   count: 39
[+]ipc:119.39.120.0/24   count: 38
```

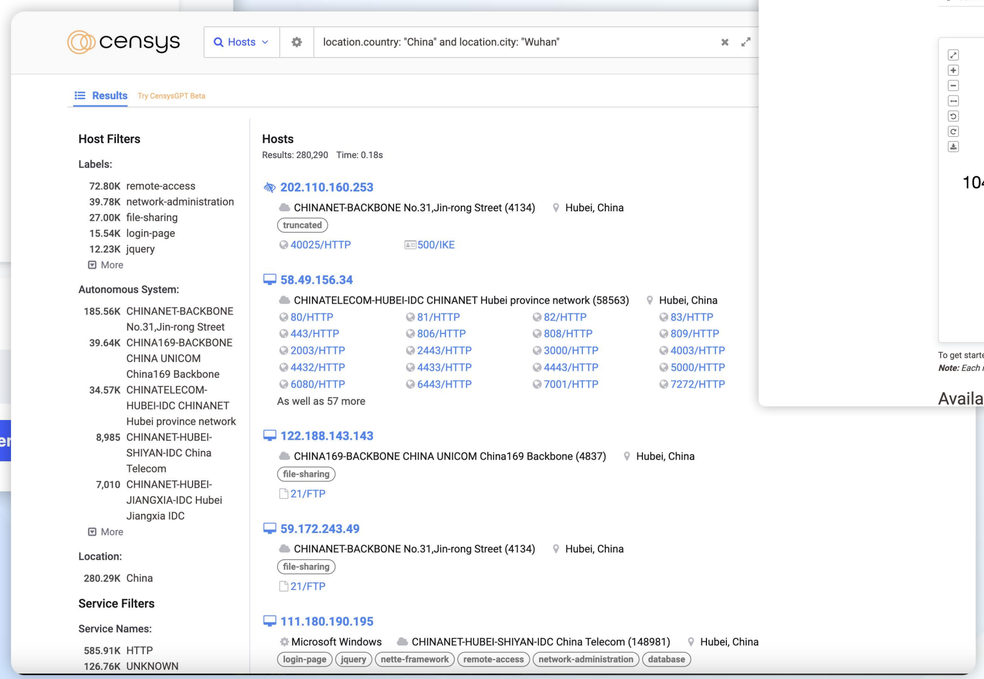
项目地址：https://github.com/SiJiDo/Ceyes

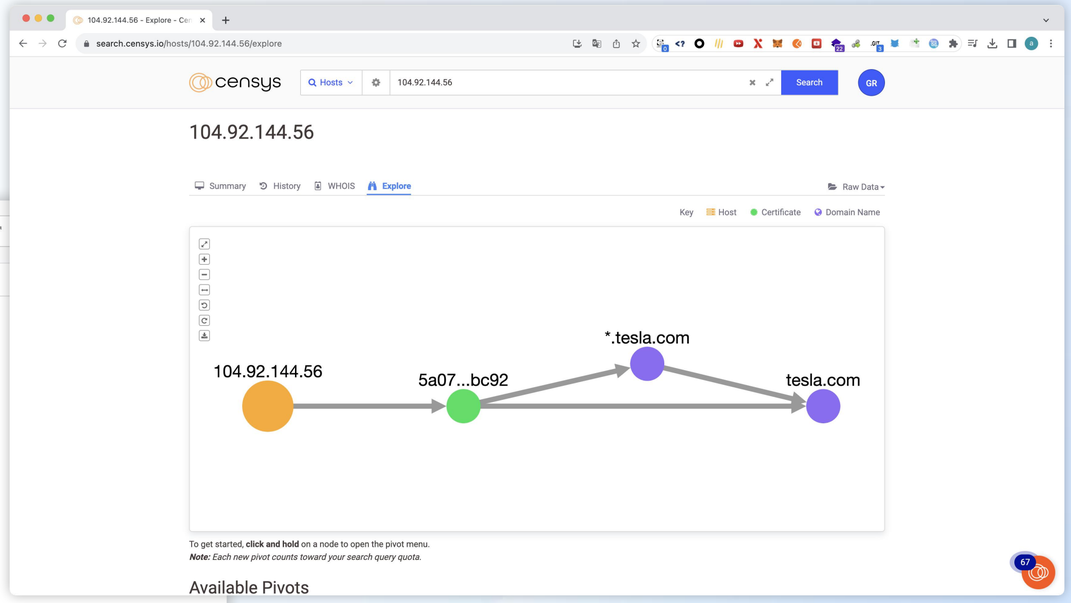
利用第三方引擎发现更多隐藏资产

(host="xxx.com" || domain="xxx.com"|| icon_hash="xxx" || cert="xxx.com" || cname_domain="xxx.com" || header="xxx.com") && country="CN" && region!="HK" && region!="TW" && is_domain=true

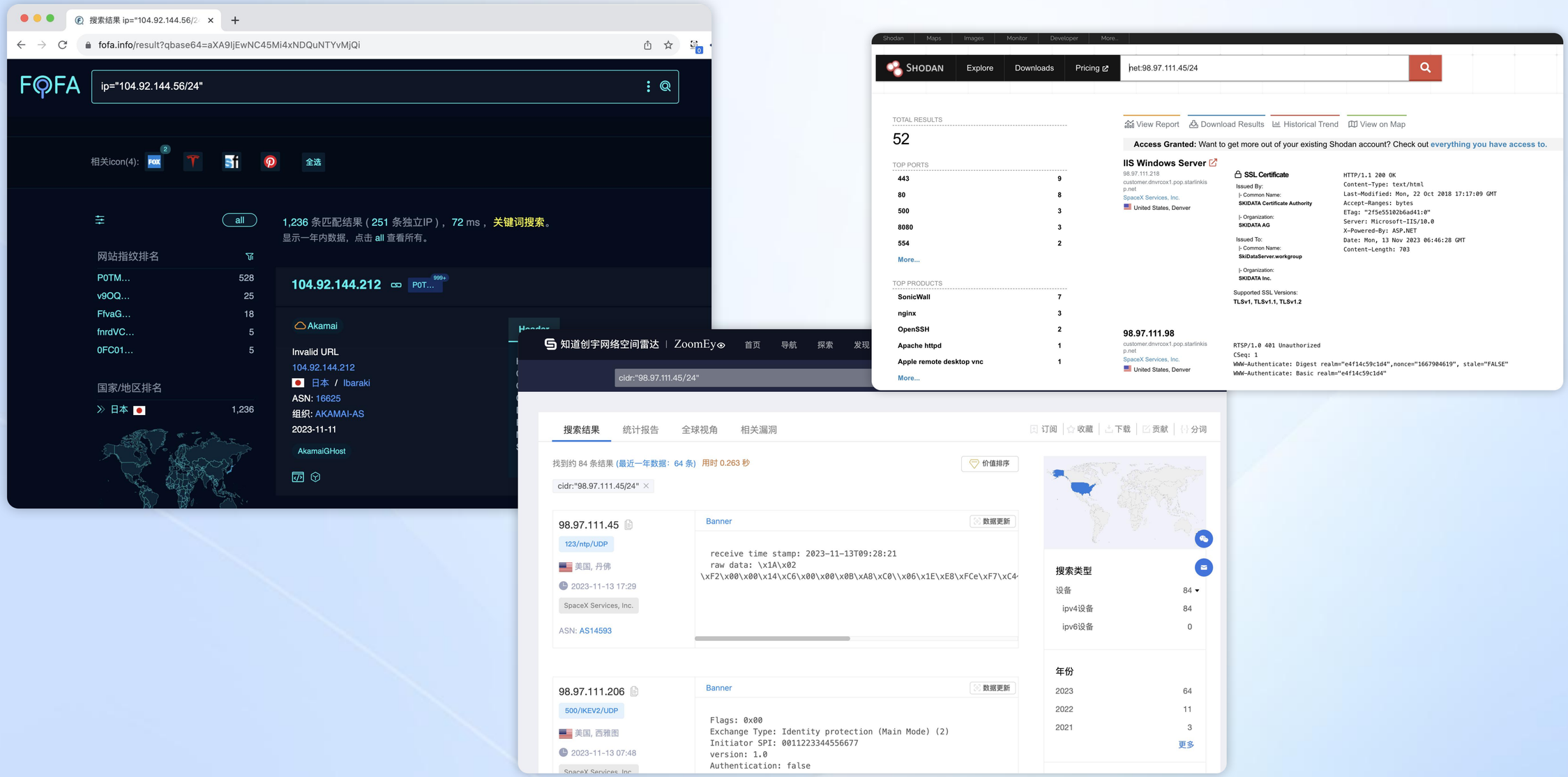
巧用censys GPT自动编排语句/发现域名对应关系



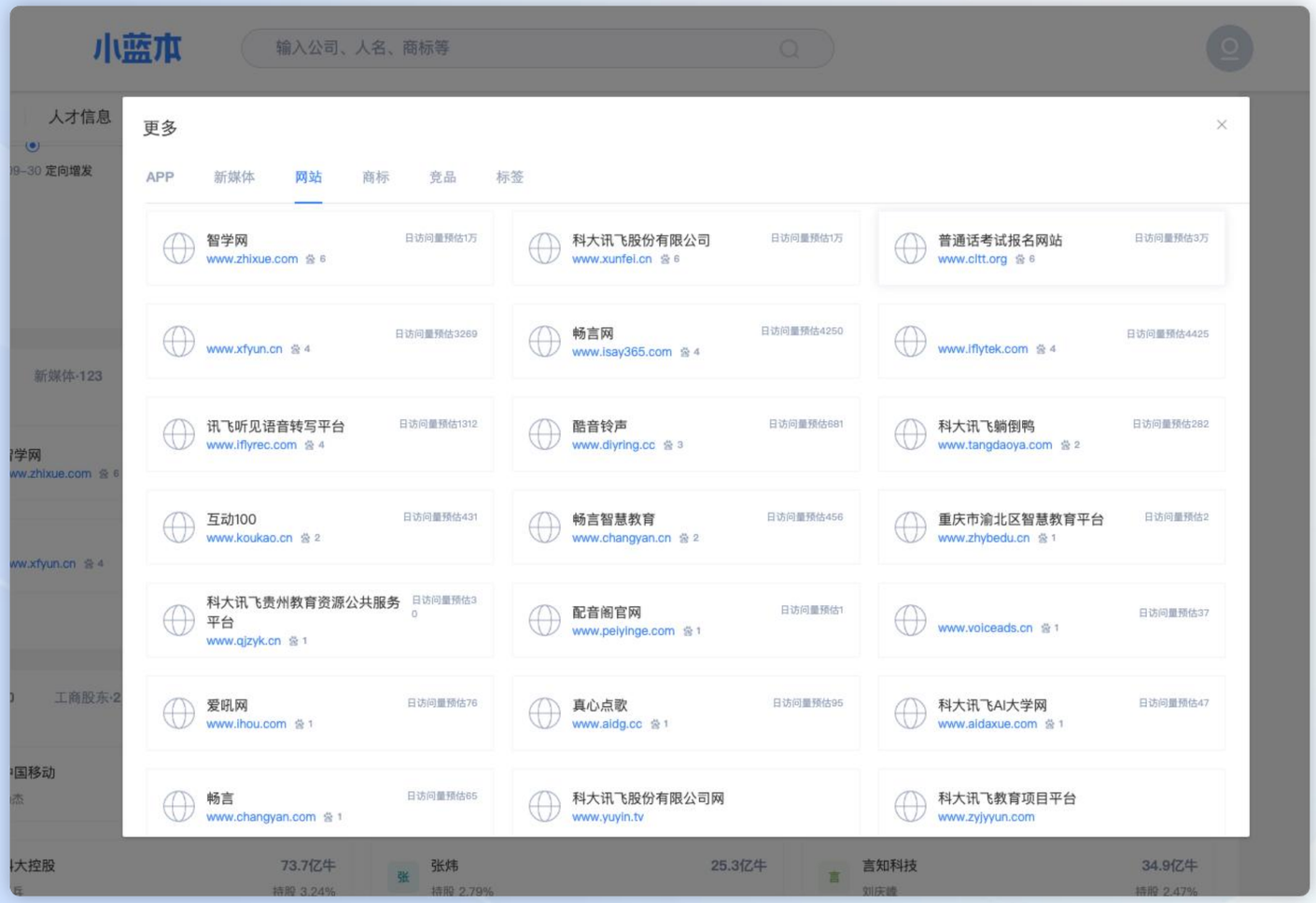




利用第三方引擎探测C段资产情况

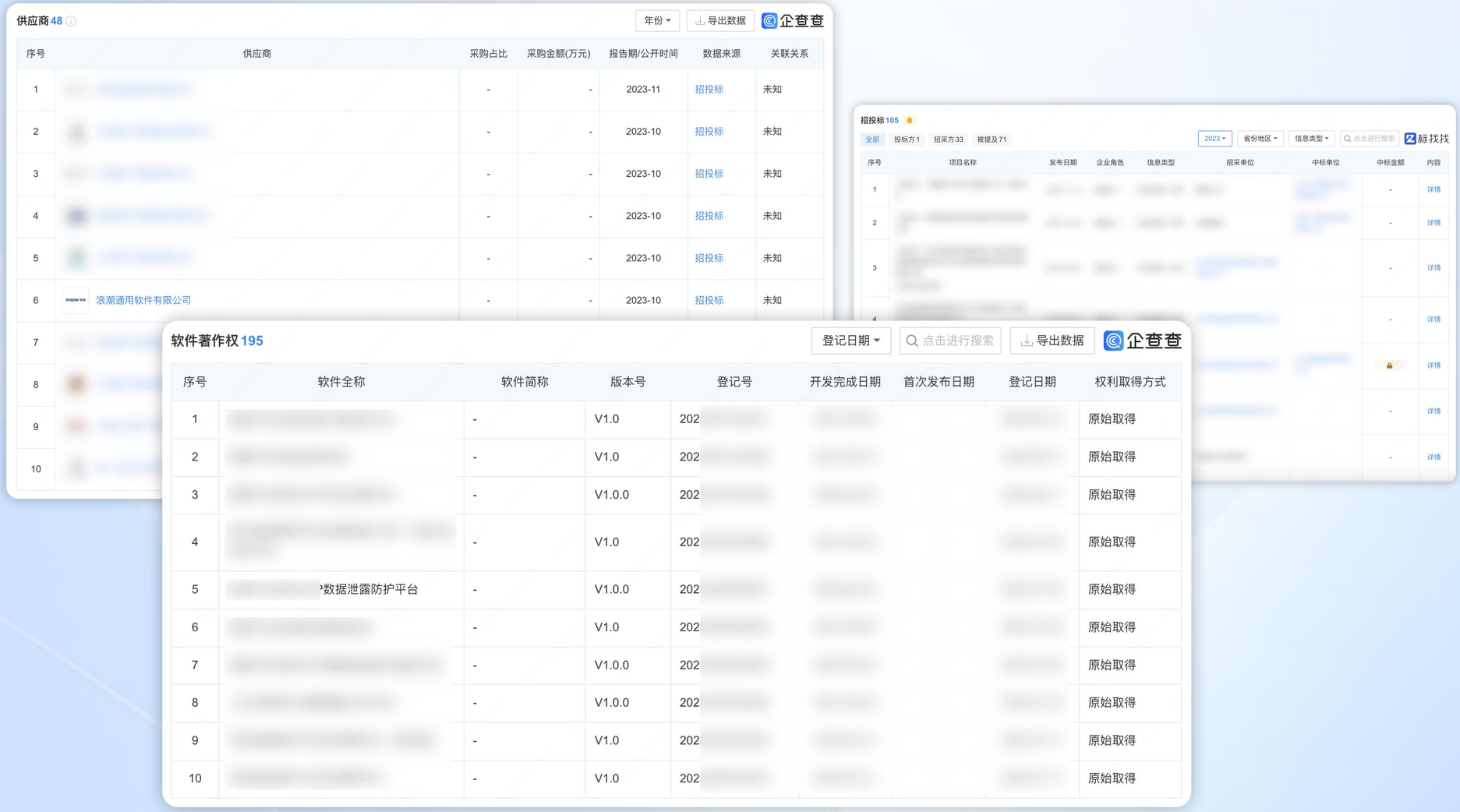


利用第三方服务平台获取应用信息



	A	B
1	component-website-item href	website-item-name
2	http://www.zhixue.com/	智学网
3	http://www.xunfei.cn/	科大讯飞股份有限公司
4	http://www.cltt.org/	普通话考试报名网站
5	http://www.xfyun.cn/	
6	http://www.isay365.com/	畅言网
7	http://www.iflytek.com/	
8	http://www.iflyrec.com/	讯飞听见语音转写平台
9	http://www.diyring.cc/	酷音铃声
10	http://www.tangdaoya.com/	科大讯飞躺倒鸭
11	http://www.koukao.cn/	互动100
12	http://www.changyan.cn/	畅言智慧教育
13	http://www.zhybedu.cn/	重庆市渝北区智慧教育平台
14	http://www.qjzyk.cn/	科大讯飞贵州教育资源公共服务平台
15	http://www.peiyinge.com/	配音阁官网
16	http://www.voiceads.cn/	
17	http://www.ihou.com/	爱吼网
18	http://www.aidg.cc/	真心点歌
19	http://www.aidaxue.com/	科大讯飞AI大学网
20	http://www.changyan.com/	畅言
21	http://www.yuyin.tv/	科大讯飞股份有限公司网
22	http://www.zyjyyun.com/	科大讯飞教育项目平台
23	http://www.xfyousheng.com/	科大讯飞有声平台
24	http://www.xftrans.cn/	科大讯飞翻译业务
25	http://www.kuyinyun.com/	讯飞酷音云
26	http://www.kuyin123.com/	酷音123
27	http://www.openspeech.cn/	
28	http://www.tingshuo51.com/	听说网
29	http://www.gyxx365.com/	科大讯飞通用语言学习平台
30	http://www.jicaibao.com/	联商在线
31	http://www.iyuji.cn/	科大讯飞语记项目
32	http://www.aifuwus.com/	科大讯飞开放平台业务网站
33	http://www.adsring.cn/	讯飞广告彩铃
34	http://www.91qycl.com/	小雨点彩铃
35	http://www.zhixue.cn/	科大讯飞智学业务网
36	http://www.xn--pssz37edimznm.xn--fiqs8s/	科大讯飞中文网站
37	http://www.xn--pssz37edimznm.com/	科大讯飞教育畅言服务
38	http://www.xn--czr85lg3d2o6e.com/	联商在线
39	http://www.xunfeitrans.com/	科大讯飞晓译翻译官网
40	http://www.xunfeidubao.com/	科大讯飞小飞读报
41	http://www.xunfeia.com/	讯飞小微企业产品创新
42	http://www.xn--pssz37edimznm.xn--fiqs8s/	安徽科大讯飞信息科技股份有限公司
43	http://www.xn--pssz37edimznm.com/	安徽科大讯飞信息科技股份有限公司
44	http://www.xfzyzl.com/	家庭医生
45	http://www.xfycjy.com/	讯飞远程教育网
46	http://www.xftransa.com/	讯飞小微企业产品创新
47	http://www.xfliusheng.com/	科大讯飞留声网
48	http://www.xfinfr.com/	讯飞移动互联
49	http://www.xf-yun.com/	

商业信息到攻击资源的转换



供应商 48

年份 | 导出数据 | 企查查

序号	供应商	采购占比	采购金额(万元)	报告期/公开时间	数据来源	关联关系
1	[redacted]	-	-	2023-11	招投标	未知
2	[redacted]	-	-	2023-10	招投标	未知
3	[redacted]	-	-	2023-10	招投标	未知
4	[redacted]	-	-	2023-10	招投标	未知
5	[redacted]	-	-	2023-10	招投标	未知
6	浪潮通用软件有限公司	-	-	2023-10	招投标	未知
7	[redacted]					
8	[redacted]					
9	[redacted]					
10	[redacted]					

招投标 105

全部 | 投标方 1 | 招采方 33 | 被提及 71 | 2023 | 省份地区 | 信息类型 | 点击进行搜索 | 标找找

序号	项目名称	发布日期	企业角色	信息类型	招采单位	中标单位	中标金额	内容
1	[redacted]						-	详情
2	[redacted]						-	详情
3	[redacted]						-	详情
4	[redacted]						-	详情
	[redacted]							详情
	[redacted]						-	详情
	[redacted]						-	详情

软件著作权 195

登记日期 | 点击进行搜索 | 导出数据 | 企查查

序号	软件全称	软件简称	版本号	登记号	开发完成日期	首次发布日期	登记日期	权利取得方式
1	[redacted]	-	V1.0	202				原始取得
2	[redacted]	-	V1.0	202				原始取得
3	[redacted]	-	V1.0.0	202				原始取得
4	[redacted]	-	V1.0	202				原始取得
5	[redacted]数据泄露防护平台	-	V1.0.0	202				原始取得
6	[redacted]	-	V1.0	202				原始取得
7	[redacted]	-	V1.0.0	202				原始取得
8	[redacted]	-	V1.0.0	202				原始取得
9	[redacted]	-	V1.0	202				原始取得
10	[redacted]	-	V1.0	202				原始取得

商业信息到攻击资源的转换

主要人员 发生变更时提醒我

最新公示 24　工商登记 11

序号	姓名	
1	[redacted]阳	TA有57家企业 >
2	[redacted]福	TA有32家企业 >
3	[redacted]奇	
4	[redacted]琳	
5	[redacted]生	
6	[redacted]	
7	[redacted]平	
8	[redacted]全	TA有45家企业 >
9	[redacted]波	TA有5家企业 >
10	[redacted]平	TA有1家企业 >

```
➜ cat uname.txt
张伟
王芳
李娜
刘强
陈静
杨勇
赵敏
周磊
吴秀英
黄军
```

```
➜ cat output.txt
zhangwei
Zhangwei
zhangw
zw
zwei
wangfang
Wangfang
wangf
wf
wfang
linuo
Linuo
lin
ln
lnuo
```

Index of /download/dict/

somd5.com/download/...

Index of /download/dict/

../		
SoMD5-Monthly-statistics/	16-Jul-2020 14:47	-
crack-software/	16-Jul-2020 14:47	-
china-all-hanzi.zip	16-Jul-2020 14:47	52K
china-gb3500.zip	16-Jul-2020 14:47	10K
china-xingshi.zip	16-Jul-2020 14:47	3006
domain_suffix.zip	16-Jul-2020 14:47	26K
english.zip	16-Jul-2020 14:47	51K
mobile.zip	16-Jul-2020 14:47	724K
name-pinyin-quanpin.zip	16-Jul-2020 14:47	6M
name-pinyin-shouzimu.zip	16-Jul-2020 14:47	34K
top1w.zip	16-Jul-2020 14:47	40K
username-num-top1000.zip	16-Jul-2020 14:47	3156
xingming.zip	16-Jul-2020 14:47	128K
yyyymmdd-1960-2020.zip	16-Jul-2020 14:47	40K

用户名字典生成工具 V0.21(汉字姓名转拼音) by:ABC_123

中文用户名转英文拼音　帮助

\/DICTIONARY/userdictTool/uname.txt　选择汉字姓名字典　生成拼音格式字典

用户名规则:

☑ wangxizhi　☑ Wangxizhi　☐ wang_xizhi　☐ wang.xizhi　选中所有

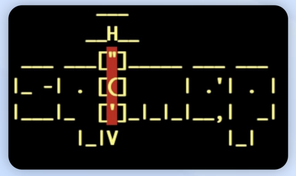
☑ wangxz　☑ wxz　☑ wxizhi　☐ wang.xz　取消选中

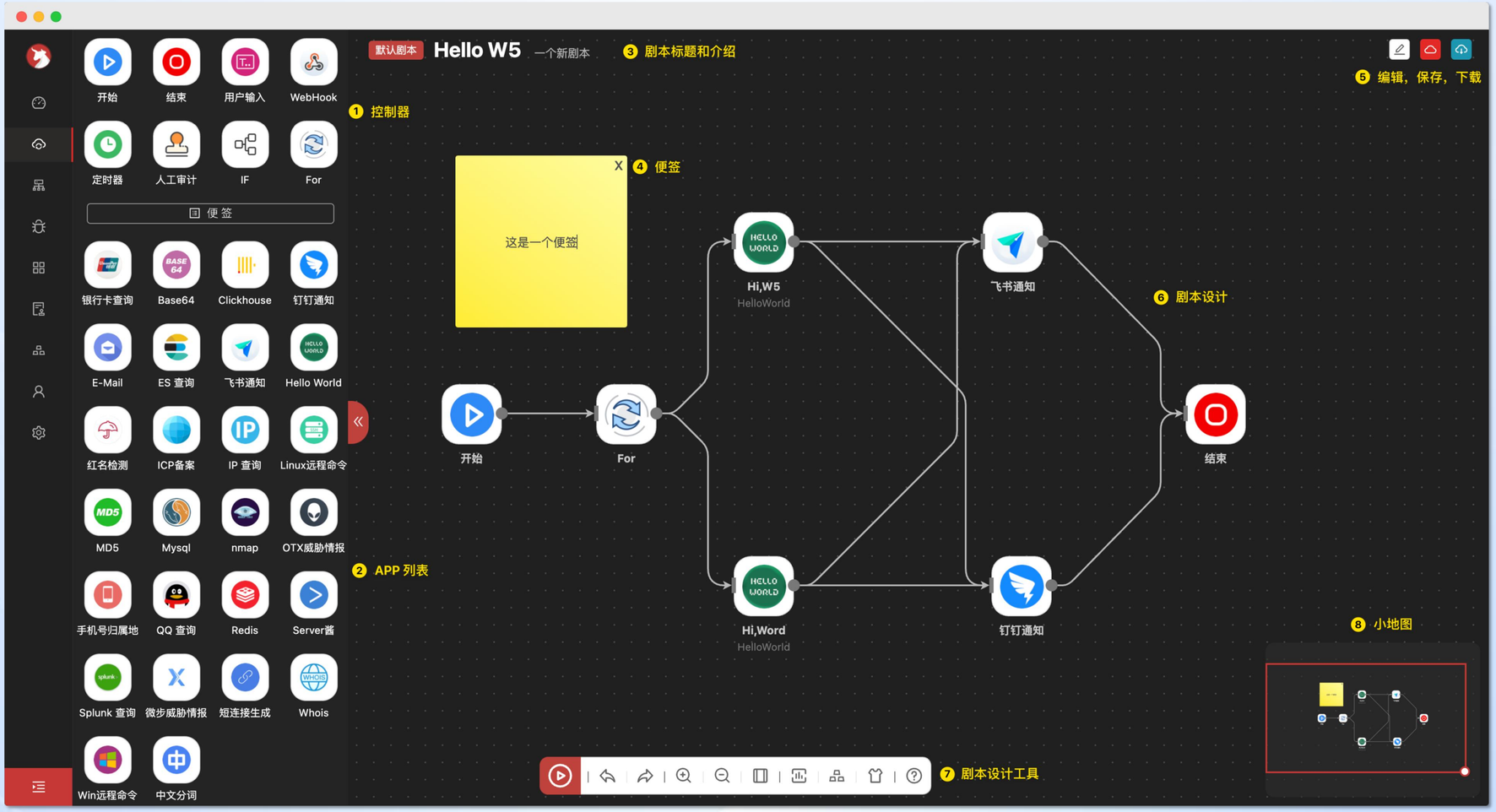
☐ xizhi.wang　☐ xz.wang　☑ wangxiz

信息输出窗口:

程序开始工作:
识别中文汉字姓名字典编码为:UTF-8
中文汉字姓名字典读入完毕，总行数为:10
拼音字典生成完毕，开始写出文本文件
写出文本文件成功!文件名为程序所在目录下的output.txt文件，编码格式为GB2312

自动化脚本编排实现自动化测试/流程化处理

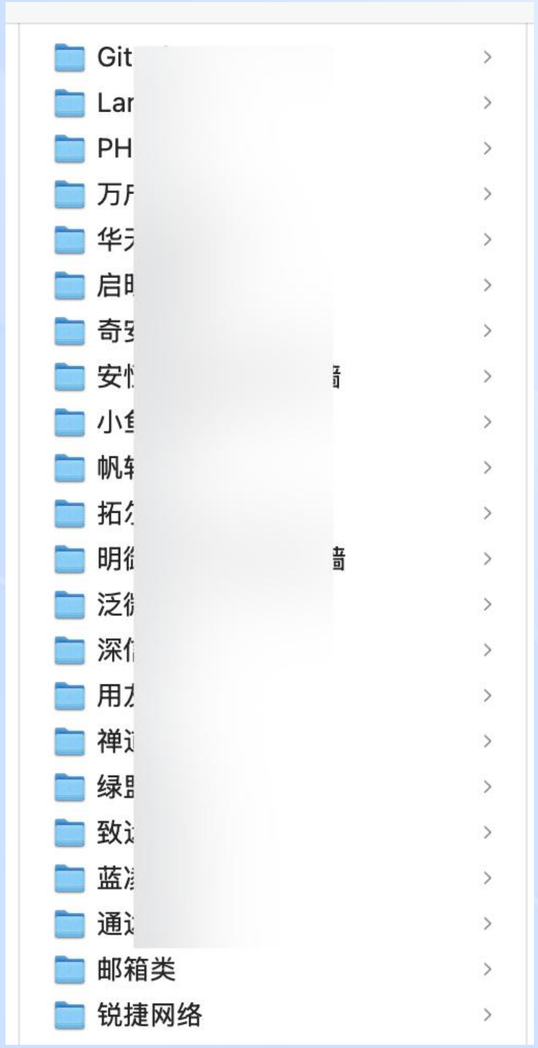




初始化访问

@TA0001

快速突破边界之硬实力



禅道 Landray 蓝凌 HIKVISION 致远互联 SEEYON.com

TDXK 通达信科 泛微 weaver 万户软件 WANHUSOFT 用友 yonyou

1day：

改良或原生的exp，并形成体系化的测试系统。

0day：

小的框架、cms、OA按需挖掘。针对常见见网络设备漏洞（VPN，邮箱），常用库（fastjson），常用中间件（weblogic）进行主动挖掘。

快速突破边界方法论

近源攻击

OWASP top 10

SANS top 25

0/1/nday漏洞

钓鱼攻击

佯攻?!

性价比较高的漏洞

- 文件上传
- SQL注入
- 代码执行 / 命令执行
- 中间件、组件与设备漏洞

关注边缘和业务线较长的资产

由于复杂的网络结构和长业务线，安全措施无法有效覆盖到远端节点，各级分支的安全系数差异大，攻击者可以从分支机构发起攻击。

小程序生态下的资产与漏洞发现

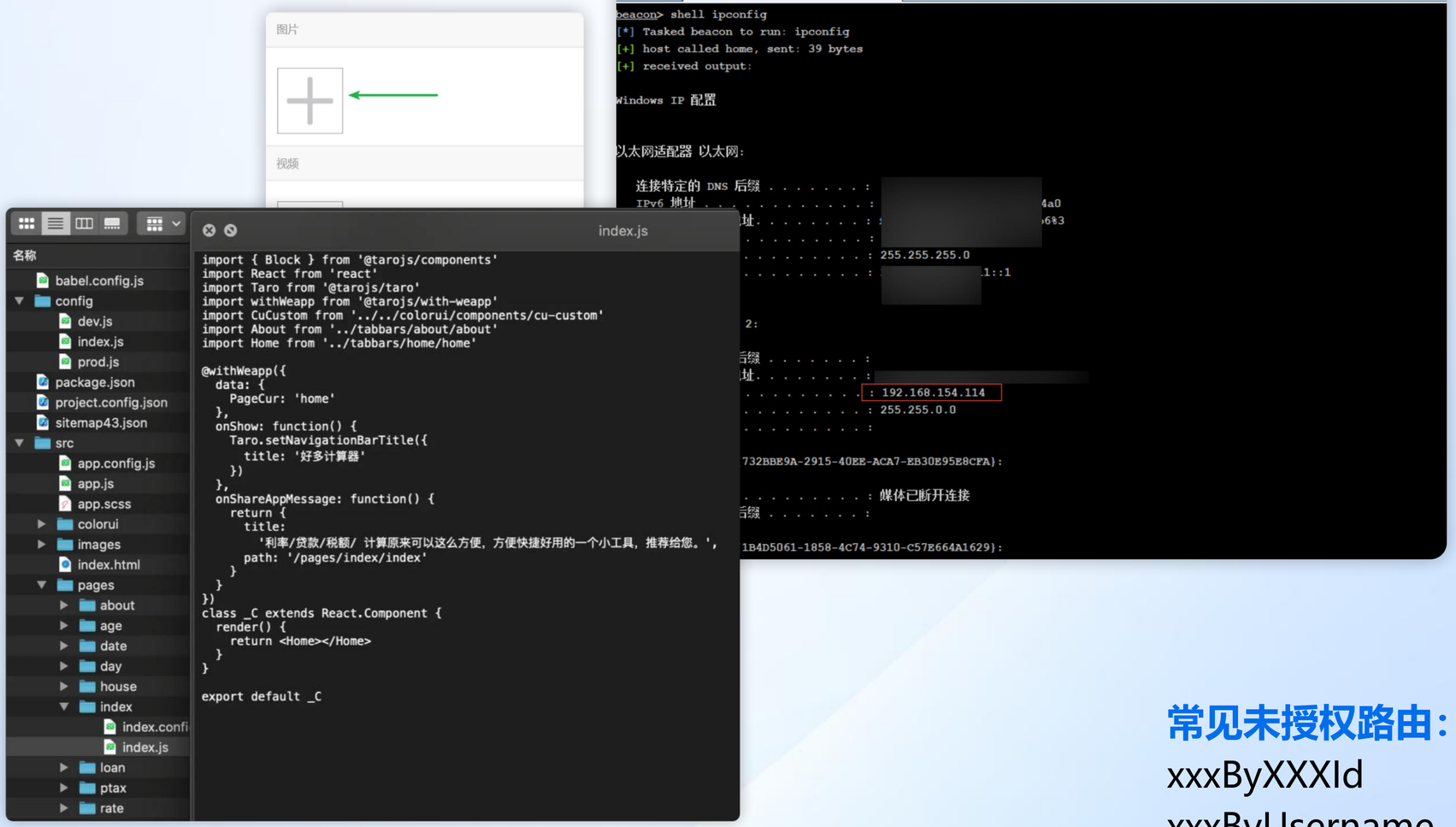
- 腾讯系：微信、QQ
- 阿里系：支付宝、淘宝

逻辑漏洞　文件上传

横纵越权　SQL注入

noMFA_login　SSRF

信息泄露　xxx.....




```
ATA:", end.deatil.value),"superior" === end.detail.value.username & "[redacted]sx!!" === end.detail.value.passwo
```

常见未授权路由：

xxxByXXXId

xxxByUsername

xxxbyphone

...

项目地址：https://github.com/ezshine/wxapkg-convertor/releases

利用时间机器发现资产/批量漏洞发现


```
➜ echo "https://tesla.com" | ./waybackurls | ./httpx -silent -timeout 2 -sc -mc 200,302 -title -threads 100
https://ir.tesla.com/events [302] []
https://service.tesla.com/docs/ModelY/ServiceManual/en-us/ [200] []
https://ir.tesla.com/news-releases/news-release-details/tesla-q3-2018-vehicle-production-and-deliveries [302] []
https://ir.tesla.com/news-releases/news-release-details/eric-branderiz-join-tesla-vice-president-corporate-controller [302] []
https://service.tesla.com/docs/BodyRepair/Body_Repair_Procedures/Model_Y_SP/HTML/en-us/GUID-F8F6D8A1-45E9-4E90-900C-87CA735B6B92.…3/5Area [200] []
https://service.tesla.com/docs/Public/diy/index-model-x-2015.html [200] [2015-2020 Model X Do It Yourself Guide]
https://ir.tesla.com/news-releases/news-release-details/tesla-q4-2018-vehicle-production-deliveries-also-announcing-2000 [302] []
https://service.tesla.com/docs/BodyRepair/Body_Repair_Procedures/Model_Y_SP/HTML/en-us/GUID-A6270F06-9BE3-4F54-9E79-C459671E1487.html [200] []
https://service.tesla.com/docs/BodyRepair/Body_Repair_Procedures/Model_Y_SP/HTML/en-us/GUID-F8F6D8A1-45E9-4E90-900C-87CA735B6B92.…1/5Cast [200] []
https://cx-api-apac.tesla.com/ [200] []
https://accounts.tesla.com/_next/static/chunks/pages/oauth2/callback-e42c7bcd74ec88b7.js [200] []
https://accounts.tesla.com/_next/static/chunks/polyfills-c67a75d1b6f99dc8.js [200] []
https://accounts.tesla.com/_next/static/chunks/framework-3671d8951bf44e4e.js [200] []
https://accounts.tesla.com/favicon.ico [200] []
https://accounts.tesla.com/_next/static/ERLs9sgiHr3P6YniJLl7v/_buildManifest.js [200] []
https://accounts.tesla.com/_next/static/chunks/2256-f2617942242c99c4.js [200] []
https://accounts.tesla.com/oauth2/callback?code=NA_3682dc9339a3d93fc8afd2d305781c58bc9fa389 [200] [Account Settings | Tesla]
https://accounts.tesla.com/oauth2/auth-login?redirect_url_path=https%3A%2F%2Fauth.tesla.com%2Foauth2%2Fv1%2Fauthorize%3Fresponse_type%3Dcode%26client_id%3Daccounts%26redirect_uri%3Dhttps%3A%2F%2Faccounts.tesla.com%2Foauth2%2Fcallback%26scope%3Doffline_access%2Buser%2Bprofile%2Bou_code%2Bemail%26locale%3Den-US&callback_url_path=https%3A%2F%2Faccounts.tesla.com%2F%2Faccount-settings%2Fpersonal-information [200] [Account Settings | Tesla]
https://auth.tesla.com/fqZZV/FS/8x/UF6p/2jJNrzk/iJ1QzS6cXGS5/dDswFj8m/Uwg/hTWFVLz0 [200] []
https://auth.tesla.com/_assets/modules/user-email-change/user-email-change.2980f438.js [200] []
https://auth.tesla.com/oauth2/v1/authorize?client_id=accounts&redirect_uri=https%3A%2F%2Faccounts.tesla.com%2Foauth2%2Fcallback&response_type=code&scope=offline_access+user+profile+ou_code+email [200] [Tesla SSO - Sign In]
https://auth.tesla.com/oauth2/v1/authorize?client_id=teslaservice-prd&response_type=code&redirect_uri=https://service.tesla.com/auth/callback&scope=openid%20email%20profile%20employee%20offline_access&state=4241e38d-6366-8d94-7c9f-f4d06c485e70&locale=en-US [200] [Tesla SSO - Sign In]
https://auth.tesla.com/oauth2/v1/authorize?post_enrollment_redirect_uri&login_hint&locale=en-US&audience=https%3A%2F%2Fmfa.tesla.com%2F&redirect_uri=https%3A%2F%2Fmfa.tesla.com%2Flogin%2Fcallback&client_id=mfaportal&response_type=code&scope=openid+email&code_challenge=ugelFOcJzVQ7_S_OJvViWcuFVjpQGVYxfGY8GN3Y710&code_challenge_method=S256&state=e9Kdy3b3CmILxQ9bQzGDFycDwaH0WrIu&prompt=login [302] []
https://auth.tesla.com/oauth2/v1/authorize?client_id=teslaservice-prd&response_type=code&redirect_uri=https://service.tesla.com/auth/callback&scope=openid%20email%20profile%20employee%20offline_access&state=6efc4183-a15b-103b-3950-955e059e5734&locale=en-US [200] [Tesla SSO - Sign In]
https://cyberbeer.tesla.com/app-ads.txt [302] []
https://developer.tesla.com/docs/images/navbar-cad8cdcb.png [200] []
https://developer.tesla.com/docs/fonts/slate-e55b8307.svg?-syv14m [200] []
https://developer.tesla.com/oauth2/auth-login?redirect_url_path=https%3A%2F%2Fauth.tesla.com%2Foauth2%2Fv1%2Fauthorize%3Fresponse_type%3Dcode%26client_id%3D37771985b5df-4688-8e19-24b05c3a6e05%26redirect_uri%3Dhttps%253A%252F%252Fdeveloper.tesla.com%252Foauth2%252Fcallback%26scope%3Doffline_access%2Buser%2Bprofile%2Bou_code%2Bemail%26prompt%3Dlogin%26locale%3Den-US&callback_url_path=https%3A%2F%2Fdeveloper.tesla.com%2Fen_US%2Fcore%2Fthemes%2Fstable%2Fimages%2Fcore%2Ficons%2F73b355%2Fcheck.svg [200] [Tesla | Developer]
https://developer.tesla.com/oauth2/auth-login?redirect_url_path=https%3A%2F%2Fauth.tesla.com%2Foauth2%2Fv1%2Fauthorize%3Fresponse_type%3Dcode%26client_id%3D37771985b5df-4688-8e19-24b05c3a6e05%26redirect_uri%3Dhttps%253A%252F%252Fdeveloper.tesla.com%252Foauth2%252Fcallback%26scope%3Doffline_access%2Buser%2Bprofile%2Bou_code%2Bemail%26prompt%3Dlogin%26locale%3Den-US&callback_url_path=https%3A%2F%2Fdeveloper.tesla.com%2Fen_US%2Frobots.txt [200] [Tesla | Developer]
```

echo "https://tesla.com" | ./waybackurls | ./httpx -silent -timeout 2 -sc -mc 200,302 -title -threads 100 | ./gf redirect | ./anew

钓鱼邮件烹饪正确基操

钓鱼邮件目的

- 获取相关凭证
- 获取机器权限（附件木马、二维码 >> APK）
- 获取邮箱权限

……

伪造发件人（网关、域名、代发、SPF等）

正文内容伪造（真实性 >> eml二次制作）

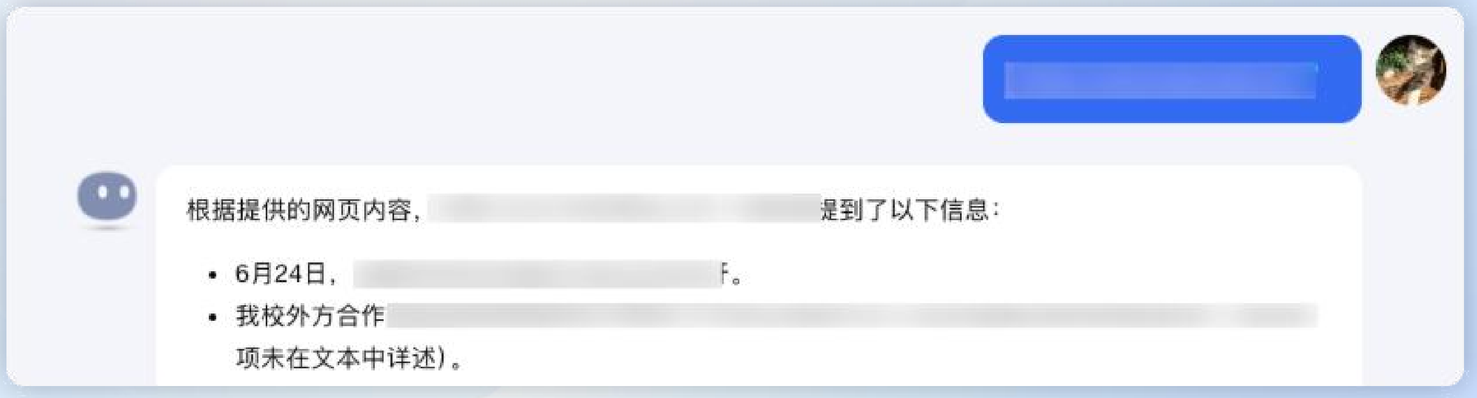
附件特征规避（加密和免杀）

利用对方系统的软件漏洞（各类RCE ）

利用0day漏洞

……

第三方内容



即时通讯钓鱼攻击KP

信任条件

人设包装

账户匿名

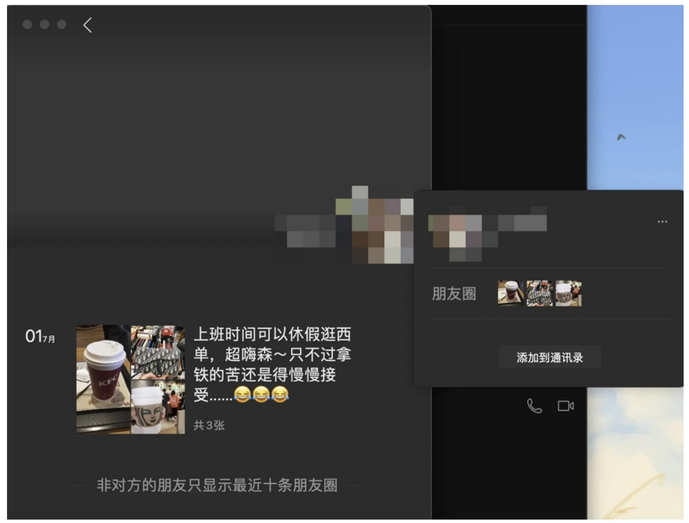
一些高级蓝队的玩法

……

Scanned	Detections	Type	Name
2024-04-02	33 / 70	Win32 EXE	LocaspaceViewer-Install-amd64-v3.23.21-Setup.exe
2024-04-01	34 / 71	Win32 EXE	Everything.exe
2024-06-05	40 / 72	Win32 EXE	360sdrun.exe

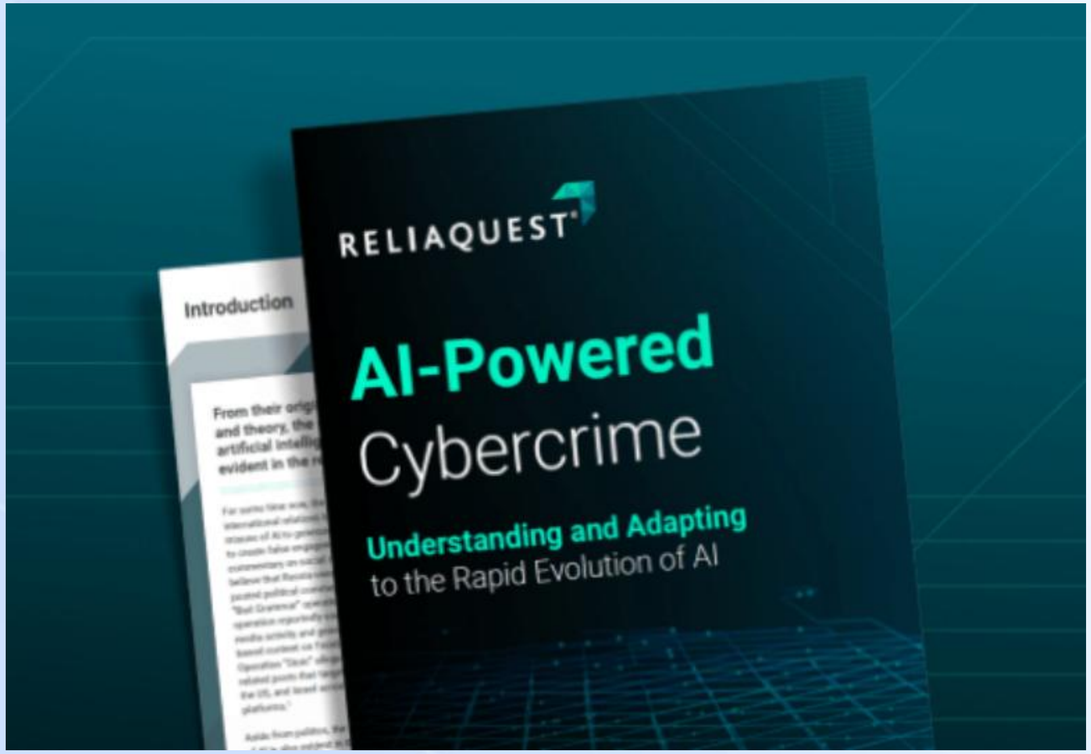
根据发件人的 163 邮箱地址进行关联分析，以及多个手机号线索溯源分析，攻击者疑似养了一批美女名媛微信号，还应关注微信社工攻击：

Page 5



报告来自：微步社区

AI驱动下的钓鱼攻击



AI-Powered Cybercrime report, ReliaQuest Team

网络钓鱼

•LLM模型允许威胁行为者用多种语言编写没有拼写或语法错误的钓鱼邮件，扩大其行动范围。

•AI增强的网络钓鱼不会引入新技术，但能显著增强、加快和扩展网络犯罪活动。

社会工程学中的深度伪造

•深度伪造视频通话实施的2500万美元抢劫。

•使用WhatsApp和视频会议平台进行的各种模仿尝试。

脚本生成

• “Scattered Spider”等组织使用“Llama 2 70B”生成恶意活动脚本，下载用户凭据。

•FlowGPT平台上，用户请求并接收来自ChaosGPT的漏洞脚本，显示出网络犯罪分子对生成恶意脚本和漏洞代码的测试。

红队触雷操作经典情景

1. 在服务器公钥中添加了自己的真实邮箱
2. 在目标的服务中进行了实名注册
3. 未授权下载源码和数据并存储 > 利益相关者数据
4. 反转角色的社会工程学交互场景
5. 安全控制失衡导致系统瘫痪

防御规避

@TA0005

突破终端第一道防线

静态扫描进化： 特征码扫描 → 骨架扫描 → 云查杀

文件名查杀：家里蹲大学-王海-个人简历.exe >> 中文名.简历

直接杀1：各种壳

直接杀2：压缩包内只存在exe

anti anti-virus

静态绕过

使用强加密/压缩： XOR, AES DES, 商用算法...

混淆加密：LLVM OLLVM ...

隐藏导入导出表： 动态调用Win API(GetModuleHandle())

减少文件熵： 分离加载, IPv4等资产

保护壳： VM, 自写, 商用

模拟正常软件： 签名、文件名、图标、属性信息、资源等

动态绕过

沙箱和虚拟化隔离进程

注册内核回调

ETW日志检测

堆栈跟踪检测

进程链检测(黑加黑)

利用AMSI接口

沙箱/虚拟对抗

延迟执行

检测无法虚拟化的设备

检测系统开机时间

检测物理内存是否大于4G

检测文件名是否修改

检测进程信息

- Vmtoolsd.exe
- Vmwaretrat.exe
- Vmwareuserexe
- Vmacthlp.exe
- vboxservice.exe
- vboxtray.exe

凭证收集

@TA0009

定向应用凭证获取

浏览器Dump工具

浏览器Dump工具用于从浏览器中提取信息，包括浏览历史、缓存、Cookies、书签等。如Chrome、Firefox、Safari、Edge等

IM工具Dump和监听

即时通讯(IM)工具的Dump和监听工具用于提取和监控即时通讯软件中的聊天记录、联系人信息等。如：WeChat、钉钉、Telegram等

邮件客户端Dump

邮件客户端Dump工具用于从邮件客户端软件中提取邮件数据，包括邮件正文、附件、发件人和收件人信息等。

终端和数据库管理工具Dump

终端工具如Xshell、Finalshell等，用于远程连接服务器和执行命令，也有相应的监控和数据提取工具。

03

典型红队评估案例分享

近源渗透那些事er

Plunder
Bug

无线安全评估

植入与远程控制

wifi-coconut

GL-XE300路由器

- 支持FRP
- WIFI/有线

omg-plug

bash-bunny

usb-rubber-ducky

screen-crab