

溯源方法总结

笔记本： 应急

创建时间： 2022/9/22 5:29

- [1、入侵痕迹查找](#)
- [2、溯源方法](#)
- [3、小结](#)

1、入侵痕迹查找


如何确定自己被入侵那是很简单，如页面被篡改、勒索病毒数据被加密、挖矿木马导致服务器卡等现象，当确定遭受攻击时就要开展应急处置了，首先确定既然出现页面篡改等情况了意味着网站服务器已经被拿下，通过获取的权限对系统实施攻击，拿下服务器的权限方法有很多，先确定被害主机都有哪些应用，如果存在web应用就要考虑是常见web漏洞了，如果存在OA、致远等一些通用办公软件，就要考虑是不是为0day或nday，如果服务器上什么都没有那就考虑是不是爆破了，如果不是爆破就考虑是系统0day或n day了，就类似17年的永恒之蓝漏洞。当出现挖矿或勒索病毒除了服务器权限外也可能会出现内部人员下载了捆绑该类木马的软件，或收到了该类恶意文件的邮件等，也就是所谓的人为误操作，这次主要讨论第一种情况的入侵痕迹查找，常用方法如下：

1、netstat 查看异常连接，通常情况下挖矿木马或勒索病毒都会存在一个外部的连接地址，用来进行通信，该地址通常为国外地址，也可能是某个vps的地址，可通过关闭正常的一些互联网连接后重点分析剩下的链接信息，可利用脚本去分析判断ip归属地，分析是否为异常连接；

2、根据异常连接可获取pid进而获取异常程序存放位置；

3、通常情况下挖矿病毒会占用较高cpu，可用top等命令进行筛选，查找确定异常进程；


3、根据时间查找，可根据事件发生时间进行搜索，win下可使用dm:20221212 udd命令查找，linux下可使用find等命令，dm命令利用everything进行搜索

 dm:20211212 udd - Everything

文件(F) 编辑(E) 视图(V) 搜索(S) 书签(B) 工具(T) 帮助(H)

dm:20211212 udd|

名称

 CallingConvention.udd

4、针对web类攻击首先利用shell扫描工具等方法定位shell，然后对日志进行分析，中间件日志、防护设备等日志，根据关键字和时间进行攻击ip定位；

5、windows、ssh等登录日志也要进行排查，之前确实碰到过通过爆破3389登录服务器成功，然后植入勒索病毒进行加密的；

2、溯源方法

当然具体的排查方法还有很多，主要总结下溯源的一些方法：

ip定位：

通过情况下能根据日志或连接获取ip地址，接着就是顺藤摸瓜获取更多信息：

微步在线查看：

微步在线有一个很好用的功能，可以根据ip地址进行分析，判断改ip地址是否为恶意地址，是否被存在曾经被解析的域名，利用尝试对此ip地址进行溯源223.75.236.241，微步显示该ip地址为恶意地址，存在扫描等恶意行为

地区

Q 223.75.236.241

🔄

🔍 语法说明

2021-03-21

2022-02-11

微僵尸机

过期

相关情报

3 条可疑/恶意情报，其中 C 段IP 3个。

开源情报

1 条开源情报

安全博客

4家博客，提及7条相关内容，其中1条可疑（占比14%）。

🌐 网页结果 10

🔍 攻击画像 122

🔍 解析域名 15

🔍 资产测绘 0

🔍 数字证书 1

🔍 相关样本 0

🔍 相关URL 0

🔍 RDNS 0

当前解析 (7)

🔍 IP当前解析域名信息最大显示 1000 条数据。

高级查询：用户等级权限本月剩余 5 次。可前往用户中心首页查看“我的权限”或联系customers@threatbook.cn咨询。

🔍 高级查询

解析域名	域名发现时间	微步判定	微步标签	解析IP
ajwww.cn	2016-11-20	未知	暂无	9*.*.252
www.ajwww.cn	2016-11-28	未知	暂无	9*.*.252
gzajjc.com	2019-03-07	未知	暂无	223.75.236.241
www.gzajjc.com	2019-03-07	未知	暂无	223.75.236.241
b1111.vip	2016-05-22	未知	暂无	223.75.236.241
www.b1111.vip	2017-12-05	未知	暂无	223.75.236.241
b*.ccyiso.xyz	2021-02-25	未知	暂无	-

历史解析 (8)

解析域名显示的该ip地址曾被解析的域名有哪些

网页结果10攻击画像122解析域名15资产测绘6数字证书1相关样本1相关URL3RDNS1

当前解析 (7)

1 IP当前解析域名信息最大显示 1000 条数据。
高级查询：用户等级权限本月剩余 5 次，可前往用户中心首页查看“我的权限”或联系customers@threatbook.cn咨询。

高级查询

解析域名	域名发现时间	微步判定	微步标签	解析IP
ajwww.cn	2016-11-20	未知	暂无	9*.*.252
www.ajwww.cn	2016-11-28	未知	暂无	9*.*.252
gzajjc.com	2019-03-07	未知	暂无	223.75.236.241
www.gzajjc.com	2019-03-07	未知	暂无	223.75.236.241
b1111.vip	2016-05-22	未知	暂无	223.75.236.241
www.b1111.vip	2017-12-05	未知	暂无	223.75.236.241
b*.ccyiso.xyz	2021-02-25	未知	暂无	-

历史解析 (0)

知道了域名就可以查看域名相关信息，可以直接访问该域名，查看网站内容，对该域名进行反查等，查看域名相关注册信息，查看其中一个域名www.ajwww.cn的whois信息，可以获取域名注册人姓名、邮箱账号等相关信息

社区www.ajwww.cn语法说明

网页结果1域名解析14WHOIS6数字证书3子域名12相关样本1相关URL3网站分析4

当前注册信息

注册商

-

注册机构

-

邮箱

58*****@qq.com

地址

-

电话

-

注册时间

2019-04-09 03:56:07

过期时间

2023-04-09 03:56:07

更新时间

-

域名服务商

上海贝锐

域名服务器

ns1.oray.net

历史注册信息

已通过高级查询权限解锁数据，可前往用户中心首页查看权限剩余情况。

日期	重要信息更新	完整信息
2021-03-15	更新 非重要信息	完整 Whois 信息
2020-11-02	更新 非重要信息	完整 Whois 信息
2019-04-23	修改 注册商: 邮箱: fengsheng*****57	完整 Whois 信息
2018-09-29	更新 非重要信息	完整 Whois 信息
2018-09-07	更新 非重要信息	完整 Whois 信息
2018-07-14	更新 非重要信息	完整 Whois 信息
2017-09-08	修改 注册商: Information Privacy Protection Services Limited >> 周荣盛 邮箱: 65c7*****ns.com >> feng*****93.com	完整 Whois 信息
2016-12-10	修改 注册商: ***** Services Limited 邮箱: bz***** >> 65c753451*****	完整 Whois 信息
2015-12-26	更新 非重要信息	完整 Whois 信息

然后根据手机号等信息可具体在查找支付宝、微信，也能根据公开的社工库获取相关敏感信息。

ip定位：

所谓的ip定位就是根据ip地址去定位到大概的位置，可采用如下地址对常见的ip地址进行定位

https://www.ipuu.net/query/ip?

223.75.236.241

查询

我们每天提供多达3个IP地址/域名的免费查询，注册一个账户有权获得更高的每日限额，您今天仍有 1/3 IP 地址/域名的查询额度可用。

注册免费账户
立即注册 免费
1. 每天启用 100
2. 支持 IPv4 和
注：注册后充高
立即注册

公安版 商业版 区县级 城市级

此IP分布在以下一个区域

大洲	亚洲
国家/地区代码	CN
国家	中国
省份	湖北省
城市	武汉市
区（县）	洪山区
详细地址	-
经度	114.433896
纬度	30.543623
半径	27.5423KM



这个网站还有公安版，应该能查询更多详细的数据，但是收费

公安版 商业版 区县级 城市级

此IP分布在以下一个区域

× 高级查询功能

购买IPUU基础版/高级版 即可查询IP地址位置属性（公安版、商业版、区县级、城市级）、IP网络属性（应用场景、主机名称、运营商、所属机构）、IP风险信息（黑灰产、威胁情报）、IP业务属性（反查域名、端口&协议&组件、资产、操作系统、数字证书），域名，逆向IP查询，批量查询等高级查询全部特权>

推荐



高级版

14999元 / 年



基础版

5888元 / 年

立即开通

https://www.geolocation.com/zh_cn?

<https://www.ipip.net/ip.html>



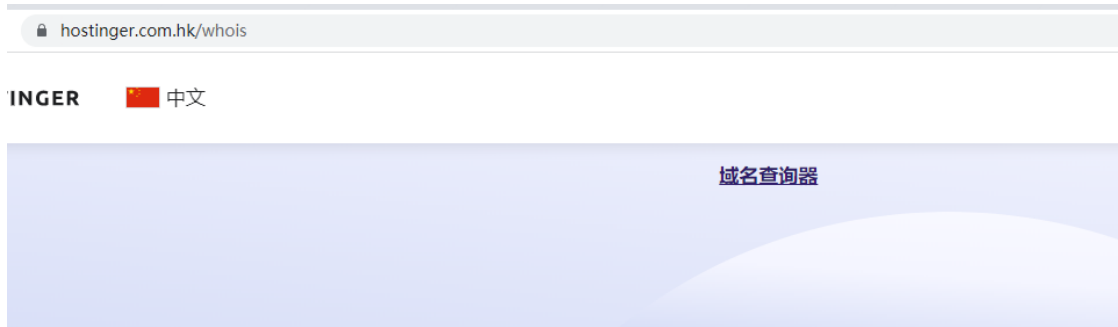
IP 相关数据信息

数据	地理位置信息(数据来源于企业版)		
当前IP	223.75.236.241	Ping	Trace 域名
地理位置	中国湖北武汉	产品详情	
行为位置	请登录后再查看		
定位范围	请登录后再查看		
定位经纬度			
运营商	chinamobile.com		
线路	移动		
应用场景	请登录后再查看	产品详情	
地区中心经纬度	30.572399,114.279121		

whois查询:

对网站域名进行whois查询, 查询域名服务商等相关信息

<https://www.hostinger.com.hk/whois>



ajwww.cn的WHOIS记录

Domain Name: ajwww.cn
ROID: 201904010001s11135941-cn
Domain Status: clientDeleteProhibited
Domain Status: clientTransferProhibited
Registrant: [REDACTED]
Registrant Contact Email: [REDACTED]@om
Sponsoring Registrar: 上海 [REDACTED]
Name Server: ns1.[REDACTED].net
Name Server: ns2.[REDACTED].net
Registration Time: 2019-04-09 03:56:07
Expiration Time: 2022-04-09 03:56:07
DNSSEC: unsigned

<https://domainr.com/ajwww.cn>

domainr.com/ajwww.cn?q=www

www.ajwww.cn

Home Documentation Sign Up

www.ajwww.在线
✓ Available

www.ajwww.us
✓ Available

www.ajwww.中国
✓ Available

www.ajwww.公司
✓ Available

www.ajwww.网络
✓ Available

www.ajwww.信息
✓ Available

www.ajwww.商城
✓ Available

www.ajwww.商标
✓ Available

www.ajwww.广东
✓ Available

www.ajwww.网店
✓ Available

ajwww.cn

Taken View Site

Make Offer

DomainAgents
Your offer presented, guaranteed

Whois

Domain Name:
ROID: 20190409s1000
Domain Status: clientDeleteProhibited
Domain Status: clientTransferProhibited
Registrant:
Registrant Contact Email:
Sponsoring Registrar: 上海兴锐信息科技股份有限公司
Name Server: ns1.oray.net
Name Server: ns2.oray.net
Registration Time: 2019-04-09 03:56:07
Expiration Time: 2023-04-09 03:56:07
DNSSEC: unsigned

Extension: .cn

http://whoissoft.com/



域名/IP地址: baidu.com 查询

全球域名WHOIS查询,支持220多种域名后缀,IDN(国际化域名)和IP地址

域名: baidu.com IP地址: 39.156.66.10/110.242.68.66/183.232.231.173
Google PageRank: 0

baidu.com 域名WHOIS查询结果:

Domain Name: BAIDU.COM
Registry Domain ID: 11181110_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-09-01T03:54:43Z
Creation Date: 1999-10-11T11:05:17Z
Registry Expiry Date: 2026-10-11T11:05:17Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.BAIDU.COM
Name Server: NS2.BAIDU.COM
Name Server: NS3.BAIDU.COM
Name Server: NS4.BAIDU.COM

邮箱账号查域名注册情况

http://whois.chinaz.com/reverse?ddlSearchMode=1

<div> <input type="text" value="6@qq.com"/> 查看分析 查询记录 </div> <div> <input type="checkbox"/> 自定义时间 </div>								
序号	域名	注册者	电话	注册商	DNS	注册时间	过期时间	更新
1	1810088.com	nenghe	*****456789	NamePal.com #8001 Inc	ns1.gname-dns.com ns2.gname-dns.com	2021-10-15	2022-10-15	
2	brcsigroup.com	nenghe	*****456789	DropCatch.com 1094 LLC		2020-12-11	2021-12-10	
3	akronpalm.com	nenghe	*****456789	Domainsnapper LLC	ns2.gname-dns.com ns1.gname-dns.com	2020-09-13	2021-09-13	
4	fannan-sat.com	mingliangli	*****90059	DropCatch.com 877 LLC		2020-08-20	2021-08-19	
5	zeroadoze.com	mingliangli	*****90059	DropCatch.com 1542 LLC		2020-08-17	2021-08-16	

常用的安全情报中心地址：

奇安信威胁情报中心 (qianxin.com)

RiskIQ Community Edition

VenusEye威胁情报中心

<https://ti.360.cn/>

常用id信息查询

百度信息收集：“id”（双引号为英文）

谷歌信息收集

src信息收集

微博搜索

微信ID收集：微信进行ID搜索

如果获得手机号（可直接搜索支付宝、社交账户等）

攻击者画像常见方式

攻击路径

攻击目的：拿到权限、窃取数据、获取利益、DDOS等

网络代理：代理IP、跳板机、C2服务器等

攻击手法：鱼叉式邮件钓鱼、Web渗透、水坑攻击、近源渗透、社会工程等

攻击者身份画像虚拟身份：ID、昵称、网名

真实身份：姓名、物理位置

联系方式：手机号、qq/微信、邮箱

组织情况：单位名称、职位信息

3、小结

攻击溯源主要看前期收集的信息是否全面，当然也可利用一些蜜罐进行反制，诱导攻击者进入蜜罐并进行相关软件下载，从而导致攻击者主机被控制，从而实现反控，达到意想不到的制敌效果。

