渗透的本质是信息搜集（第二季）

原创 Micropoor ChaMd5安全团队 2020-05-24

收录于话题
#Micropoor

1个

> 应当细心地观察，为的是理解。应当努力地理解，为的是行动。应当谨慎地行动，为的是再一次的观察。
>
> ----Micropoor

渗透的本质是信息搜集（第一季），第一季写于2018-03
https://micropoor.blogspot.com/2018/09/blog-post.html,本季作为第一季的补充。
注：本文所涉及的内容均为互联网公开内容，均来源于各个搜索引擎。

在第一季中，提到了信息搜集一定要“**多维度**”的搜集，“多维度”也正式本季的**核心思想**。以下将会从几方面论证信息搜集”多维度“的**重要性以及其思想**。
在大型网络攻防对抗中，”多维度“的信息搜集分为**4个方向**，既：

1. 一级资产
2. 二级资产
3. 上游资产
4. 下游资产

何为一级资产：
顾名思义，既目标的直接资产，也就是，直接面向对象。如常见的：
1. 目标子域名

2. 目标APP资产
3. 目标域名备案信息
4. 目标微博，公众号信息
5. 目标邮箱用户信息
6. 目标VPN用户信息
7. 目标GitHub泄露信息
8. 目标服务器/中间件/CMS框架信息
9. 目标所有存活网站Waf信息
10.目标网盘或第三方网盘敏感文件信息
11. 等等.....

以上为常见的“**目标直接资产**”，但一级资产信息搜集，一定要以“**直接面相对象**”的思想来散发思路，以“xxx”作为demo举例，论证“**直接面相对象**”的思想。

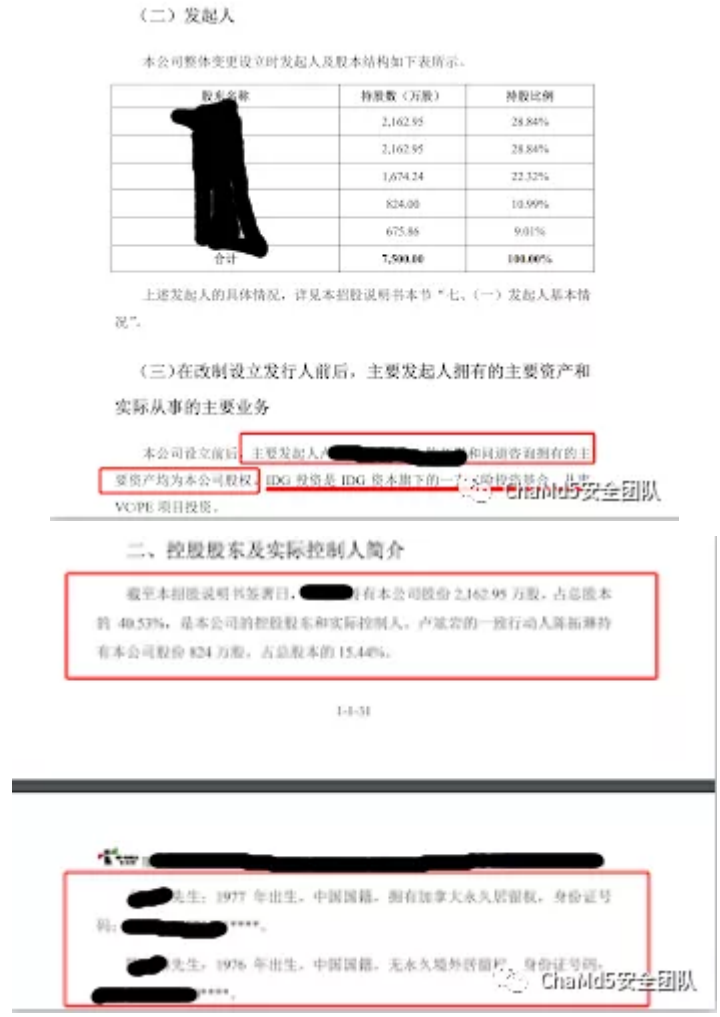
图片来源：Google搜索

在“xxx”招股书找明确的写到截至本招股说明书签署之日，公司及其控股子公司已办理备案正在使用的网站域名情况，也就是说这里的内容将会继续扩大目标的“一级资产信息”。而其中许多公司的招股书中，会有大量的资产域名。

图片来源：招股书

在招股书中，其中目标公司股权结构也非常清晰：

图片来源：招股书


（二）发起人

本公司整体变更设立时发起人及股本结构如下表所示：

股东名称	持股数（万股）	持股比例
[redacted]	2,162.95	28.84%
	2,162.95	28.84%
	1,674.24	22.32%
	824.00	10.99%
	675.86	9.01%
合计	7,500.00	100.00%

上述发起人的具体情况，详见本招股说明书本节“七、（一）发起人基本情况”。

（三）在改制设立发行人前后，主要发起人拥有的主要资产和实际从事的主要业务

本公司设立前后，主要发起人[redacted]和同道咨询拥有的主要资产均为本公司股权；IDG 投资是 IDG 资本旗下的一个风险投资基金，共有 VCPE 项目投资。

二、控股股东及实际控制人简介

截至本招股说明书签署日，[redacted]持有本公司股份 2,162.95 万股，占总股本的 40.53%，是本公司的控股股东和实际控制人。卢冠宏的一致行动人陈振辉持有本公司股份 824 万股，占总股本的 15.44%。

1-1-51

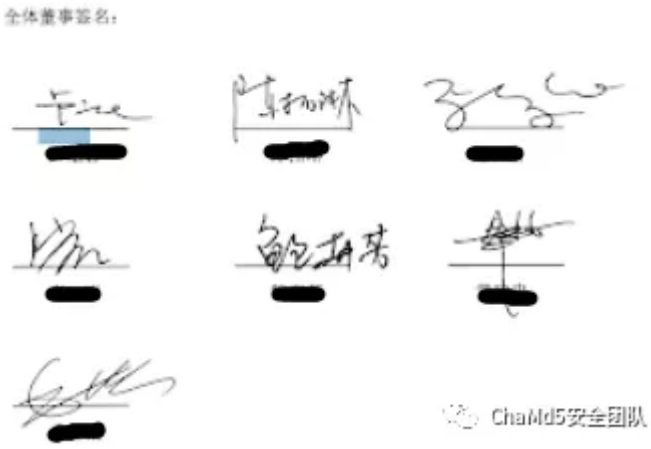
[redacted]先生：1977 年出生，中国国籍，拥有加拿大永久居留权，身份证号码：[redacted]****。

[redacted]先生，1976 年出生，中国国籍，无永久境外居留权，身份证号码：[redacted]****。

目标公司重要人员的其他重要信息也非常清晰：

例如手写签名：（用于后期钓鱼）

图片来源：招股书


全体董事签名：

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

例如注册商标：（用户了解更多的目标资产与品牌）

图片来源：招股书

（4）商标

截至2015年9月30日，公司及其控股子公司拥有的中国境内（不包含台湾及香港地区）商标情况如下：

序号	注册人	商标	证书号码	注册有效期限	核定服务项目
1	发行人	[redacted]	第[redacted]号	2010年12月28日至2020年12月27日	第16类
2	发行人		第[redacted]号	2011年01月14日至2021年01月13日	第28类
3	发行人		第[redacted]号	2010年07月07日至2020年07月06日	第35类

ChaMd5安全团队

1-1-185

序号	注册人	商标	证书号码	注册有效期限	核定服务项目
25	发行人	[redacted]	第[redacted]号	2010年02月28日至2020年02月27日	第28类
26	发行人		第[redacted]号	2010年05月21日至2020年05月20日	第41类
27	发行人		第[redacted]号	2013年03月28日至2023年03月27日	第42类
28	发行人		第[redacted]号	2010年02月14日至2020年02月13日	第16类
29	发行人		第[redacted]号	2011年02月21日至2021年02月20日	第28类
30	发行人		第[redacted]号	2011年06月28日至2021年06月27日	第28类
31	发行人		第[redacted]号	2011年12月21日至2021年12月20日	第41类
32	发行人		第[redacted]号	2011年10月21日至2021年10月20日	第9类
33	发行人		第[redacted]号	2011年10月28日至2021年10月27日	第16类
34	发行人		第[redacted]号	2011年10月21日至2021年10月20日	第18类
35	发行人		第[redacted]号	2011年10月21日至2021年10月20日	第25类
36	发行人		第[redacted]号	2011年10月21日至2021年10月20日	第28类
37	发行人		第[redacted]号	2012年08月14日至2022年08月13日	第41类
38	发行人		第[redacted]号	2012年06月[redacted]日至2022年06月06日	

ChaMd5安全团队

68	发行人	[redacted]	第[redacted]号	2011年01月07日至2021年01月06日	第16类
69	发行人		第[redacted]号	2010年12月14日至2020年12月13日	第28类
70	发行人		第[redacted]号	2010年03月14日至2020年03月13日	第9类
71	发行人		第[redacted]号	2010年02月14日至2020年02月13日	第16类
72	发行人		第[redacted]号	2010年04月28日至2020年04月27日	第28类
73	发行人		第[redacted]号	2010年03月21日至2020年05月20日	第38类
74	发行人		第[redacted]号	2010年10月21日至2020年10月20日	第41类
75	发行人		第[redacted]号	2013年05月14日至2023年05月13日	第9类
76	发行人		第[redacted]号	2013年05月07日至2023年[redacted]日	

ChaMd5安全团队

股权结构，需要**重点关注**，**非技术类人员**，例如：**销售**，**财务**，**后勤**等职务的人员。此类人员是目标的重要人员，而且此类人员相对其他技术类人员安全意识较弱，为“钓鱼”而铺垫。

简单的总结，既“一级资产”需要关注以下，这里主要分为2大类

1. 一级资产技术类，如子域名，C段等
2. 一级资产非技术类，如招股书的股权分析，目标公司的运营分析等。

注：如果目标是To B的公司，其很多核心人员为"非技术类"，这里需要根据目标公司的类型盈利方向等，制定出"适合"目标的特定方案。

一级资产总结：

以"**直接面向对象过程**"的**核心思想**，围绕目标进行"**多维度**"的信息搜集。

何为二级资产：

顾名思义，既围绕"一级资产"向下资产排查。如常见的：

1. 目标所有一级域名的C段
2. 目标所有存活资产的1-65535端口信息
3. 目标**历史非存活资产**，例：网络时光机
4. 目标所有主域名的向下第三方资源/资产排查
5. 目标关键人物（来源公司股权架构）的第三方信息，如mail，微信，百度网盘等
6. 第三方平台（要求特点：高频率互动），例如BOSS招聘，脉脉，领英。
7. 目标关键人物私有域名/APP
8. 目标关键人物GitHub泄露信息
9. 目标关键人物微博，公众号信息
10. 等等.....

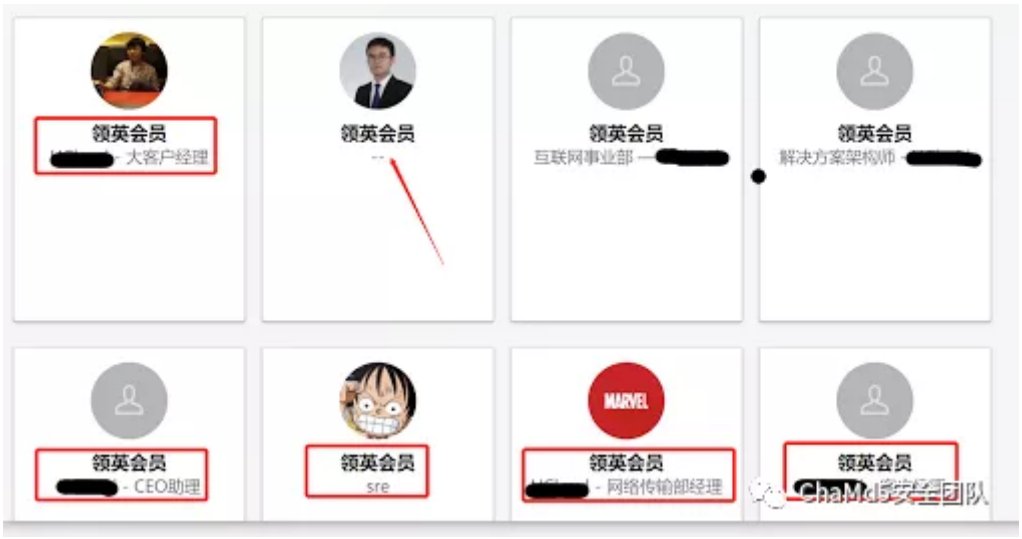
以上为常见的"二级资产"，二级资产一定要以"**化线为点**"思想来散发思路，也就是说，二级资产是基于一级资产的方向，"化线转点"，把"一级资产"分解到具体，也就是**量化到某个点**，如**某个端口**，**某个人**，**某个平台**，**某个邮箱**等。

以"xxx"作为demo举例，论证"化线为点"的二级资产搜集思想。（**相关图片已做处理，并全部基于互联网公开信息**）

"二级资产"的搜集其核心过程"化线为点"，把"一级资产"信息搜集的方向化解成可量化的"点"，也就是重点关注目标的某个人，某个物，某件事。

xxx 在领英1,756 位关注者，其中明确包含466位员工。

图片来源：领英



注：如果信息搜集的来源基于某一个指定平台，一定要考虑此平台的同类型竞争平台，然后再次完善信息搜集的补全。例如：某个信息搜集的来源是源于谷歌，那么也一定要尝试类似：Bing，Baidu等同类型的竞争平台。结合本思想应用于本Demo。

在领英会发现相关人员是无姓名，职务，邮箱等更具体的信息，此时考虑与**领英同类型竞争平台**，如下图，来源于脉脉，通过脉脉得知了真实姓名，职务，所在地等更为具体的信息。

图片来源：脉脉

图片来源：Google搜索

至此得到了目标Demo的姓名，邮箱，职务，手机，微信等等。（注：由于仅为Demo，并验证其思想，作证其方法论，故此处无涉及隐私图）

注：在二级资产信息搜集的过程中，尤其是在量化到某个组织“个人”时，部分精力倾斜到头像/照片为正装的目标人员，一般用于个人正装/照片当头像的人，其内心是自信，开朗并且大部分人为非技术人员，也就是安全意识相对较弱。相对较为近距离接触目标人物。在上例“领英”图片Demo中，会发现，随机出现的8人，有3人是非技术类，其中2人头像为“人像”照片，而此8人的技术类，无一使用正装”人像“为头像。

“二级资产”排查的过程中，秉承“向下”与“高交互”的核心思想，围绕“一级资产”展开行动。下例将继续佐证“向下”与“高交互”的核心思想进行行动。同以“xxx”作为demo举例

图片来源：Google搜索

上图行为满足：

1：以“一级资产”向下排查

2：量化到具体的某个人，某个事，某个物等。

3：该文案发布的平台符合“高交互”条件

上图行为不满足：

1：文案平台符合“向下”与“高交互，但可量化的的目标暂不符合“高交互”

按照以上思想继续补充下一步行动，既：可量化目标转化并且创造“高交互”条件，以此增加“二级资产“信息搜集维度。

至此，量化目标人物的相关更具体的信息多维度的并且有序的"向下"展开。（注：仅为demo，至此结束）

二级资产总结：

二级资产一定要以"**化线为点**"思想来发散思路，在搜集的过程中，务必要**清晰清楚的隔离开**"一级资产"，简单的概括：搜集一级资产，也就是线的过程中，务必且一定放弃"点"的信息，也就是能量化的信息。搜集二级资产，也就是点的过程中，务必且一定要放弃"线"的信息。**思想分离开，行动也一定要分离开。**

何为上游资产：

上游资产，是目标资产的上一个维度的信息搜集，既，降维搜集目标所有的资产其结果将会扩大"一级资产"并且联动了"二级资产"

上游/下游资产在大型网络攻防对抗中也是最容易忽略并且极为重要的一种手段，其根本原因是：上游/下游资产的信息搜集整理与排查是归类于：非技术并且涉及到了相关金融类知识领域。也就是攻防人员最容易忽略的一项。

"上游资产"的核心思想与"上游产业"极其相似，上游产业原指处在整个产业链的开始端，包括重要资源和原材料的采掘、供应业以及零部件制造和生产的行业，这一行业决定着其它行业的发展速度，具有基础性、原料性、联系性强的特点。在现代的产业链理论中，上游产业则是一个相对的概念。

同样，"上游资产"指"一级资产"的资产链开始端，"上游资产"与"下游资产"最大的区别在于"**产业结构分析**"与"**股权结构分析**"。以"xxx"作为demo举例。（注：所有信息取自

于互联网公开信息）

图片来源：天眼查

主要分析其参股公司：

A：业务分类

B：盈利分类

A：何为业务分类

既参股控股公司的主营业务是否与目标一致或一个方向。

例如：参股控股公司业务是餐饮类，而目标主营业务是IT类，那么就不符合“上游资产”

例如：参股控股公司是IT大类，而目标主页业务是IT大类其中某个分支，例如分支为网络安全为主营方向。这里就需要继续分析两者关联性。

B：何为盈利分类

既参股控股公司的盈利方式，是属于“非盈利”或“纯盈利”

例如：参股控股公司是某“非盈利”，而目标则是盈利公司，那么就不符合“上游资产”

例如：参股控股公司是某“纯盈利”机构，（如：XXX投资机构，XXX投资基金），那么就不符合“上游资产”

上游资产总结：

分析“上游资产”时，一定要把“业务分类”与“盈利分类”的思想模型考虑进去，否则”一级资产”会出现非常混乱的结构，从而影响”二级资产“。

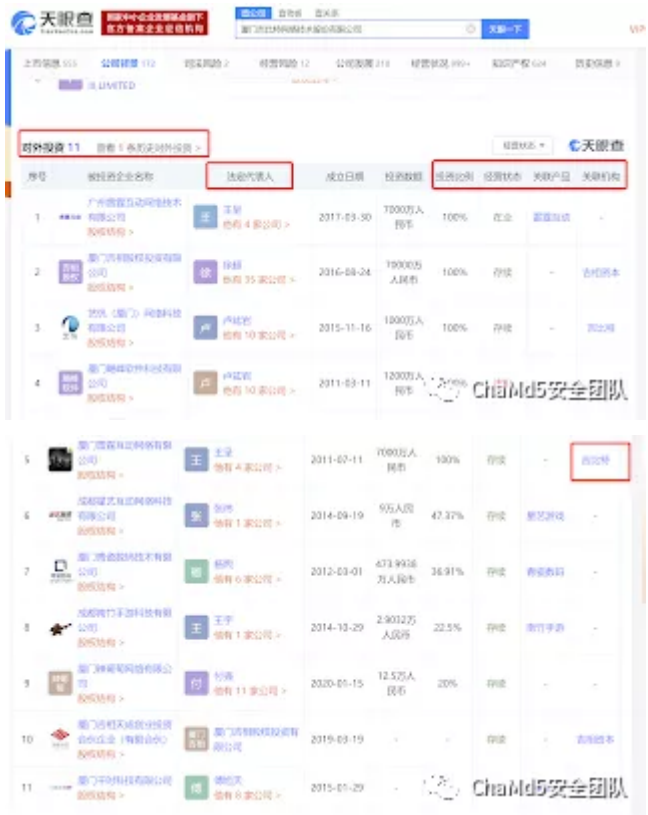
何为"下游资产"：

"下游资产"，是目标资产的下一个维度的信息搜集，既，"向下联动并关联"搜集目标所有的资产其结果将会扩大“一级资产”并且联动了“二级资产”范围。

“下游资产”的核心思想与“下游产业”极其相似，"下游产业"指处在整个产业链的末端，加工原材料和零部件，制造成品和从事生产，服务的行业。根据微笑曲线理论，上游往往是利润相对丰厚、竞争缓和的行业，原因是上游往往掌握着某种资源，比如矿产，或掌握核心技术，有较高的进入壁垒的行业。产业要形成竞争优势,就不能缺少世界一流的供应商,也不能缺少上下游产业的密切合作关系。

同样，"下游资产"是目标资产的延伸，既，"一级资产"与"二级资产"向下拓展延伸。在实际情况中，"下游资产"往往是大型目标的突破口，也是薄弱环节，同样它依然需要缜密的分析其两者的关联性。

图片来源：天眼查



排查与分析"下游资产"时，它又分为两类，既：

A：直接下游资产

B：间接下游资产

A：何为"直接下游资产"

"直接下游资产"的公司与目标直接参与参股控股，一般为80%——100%的投资比例，也就说为"下游资产"的大股东，或者完全控股子公司，其"下游资产"的产业为目标延

伸产业互补或者是相同。也需重点关注目标公司实控人的"其他公司"是否有资金往来，业务往来，间接往来关系。

B：何为"间接下游资产"

"间接下游资产"的公司非与目标间接参与参股控股，或者是小比例的投资比例，非大股东，或者非实际控股，非子公司，其"间接下游资产"的主营产业也不符合目标公司的延申产业或者非互补产业。

下游资产总结：

大型网络对抗需要考虑攻击方的"主要成本"，不同的环境，不同的背景，不同的方案，其"主要成本"不同，有的"主要成本"是时间成本，有的是"金钱成本"，有的是"安全成本"等等，根据所在团队，所在任务，所在背景，建立不同的模型，并且考虑精力倾向于“直接下游资产”或是“间接下游资产”，而在分析的过程中，也一定要考虑目标与"下游资产"的关联性，紧密性，业务性，关系性，来往性，资金性，人员流动性等等。

文末：

随着互联网发展，信息传递的成本，透明度等成本比都在大幅降低，随着金融市场的完善，各行各业将会涉及到了大量的“上游资产”与“下游资产”，企业的网络安全方护离不开信息的保护与数据安全的完整性，这是每个一甲方与乙方值得思考的一个问题。也是每一个安全从业者值得深思的一个问题。攻击者在整个信息搜集的模型中，一定要考虑到可量化的目标的特性，目标人物特性，目标行业特性等，而防御方的网络安全意义培训也一定要考虑职员岗位特性，公司行业特性，攻击者来源特性等。

最后，关于模型总结致每一位安全从业者：
中小型的网络攻防对抗，如果最终取胜，一定是赢在了技术上。
大型的网络攻防对抗，如果最终取胜，一定是赢在了战术上。