一次模拟 APT 攻击计划来展望未来企业网络安全规划与建设

前言：

此次模拟 APT 攻击，前前后后大约持续 3 个月左右，信息搜集，踩点大致在 2 个月左右。正式开始于 3 月中旬敲定计划开始实施。通过此次的模拟，更清晰的对目前企业网络安全现状的规划与建设更具有行业针对性。更清晰清楚，针对不同行业的网络建设是不具备统一规划与建设方案的。

注：模拟 APT 计划：模拟一次虚拟任务，来真实攻击目标（非破坏，非窃取等）。

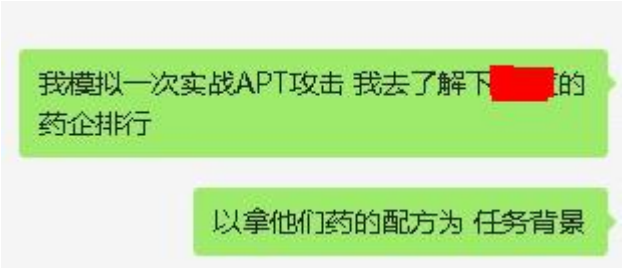
序言：

目前市场上的企业网络安全规划与建设大部分存在统一实施方案，或者是模板方案。而非针对特定行业，特定客户群体来制定针对方案。而不同行业，不同背景的企业安全规划方案也一定是不相同的。如传统行业（医药，食品，汽车）对待企业安全的建设是起跑阶段。如金融行业（证券，银行，保险）对待企业安全的建设是规划与实施阶段。如互联网行业（某度，某巴，某鹅）对待企业安全建设是自研或商业化阶段。为了更好的了解，所以制定了一次模拟计划，在计划中，更能清楚的看到，未来企业网络安全对待企业发展的重要性，以及特定行业特定规划方案，特定行业特定防御对象。由于此次计划时间过长，导致部分无截图。或者后补截图（可能是本地模拟的截图）

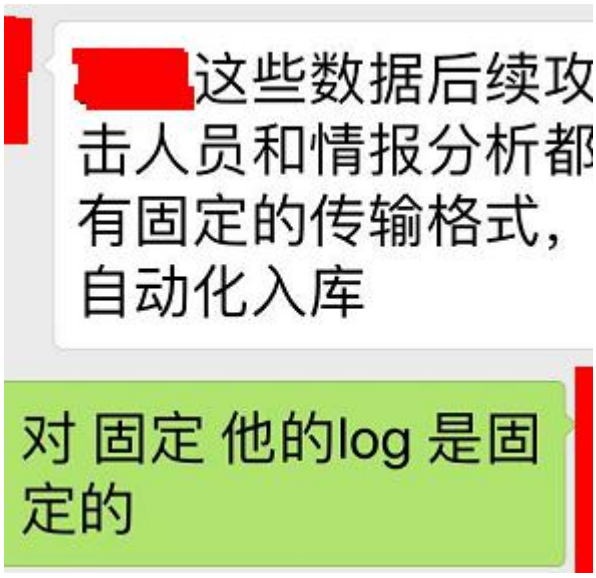
故事 1：
故事就这样开始了，针对传统行业，药企。起初定的计划是以配方为任务结点，也就是看到或者可以确定到具体存放位置就点到为止，但是随时目标的深入（为了避嫌），临时更改了计划，任务背景临时更改成，定向打击该企业的某人，那么整体 APT 攻击流程如下：
（由于第一阶段时间跨度较长，大部分截图丢失）

点 1------->面 2------->点 3------->面 4------->点 5------->总结

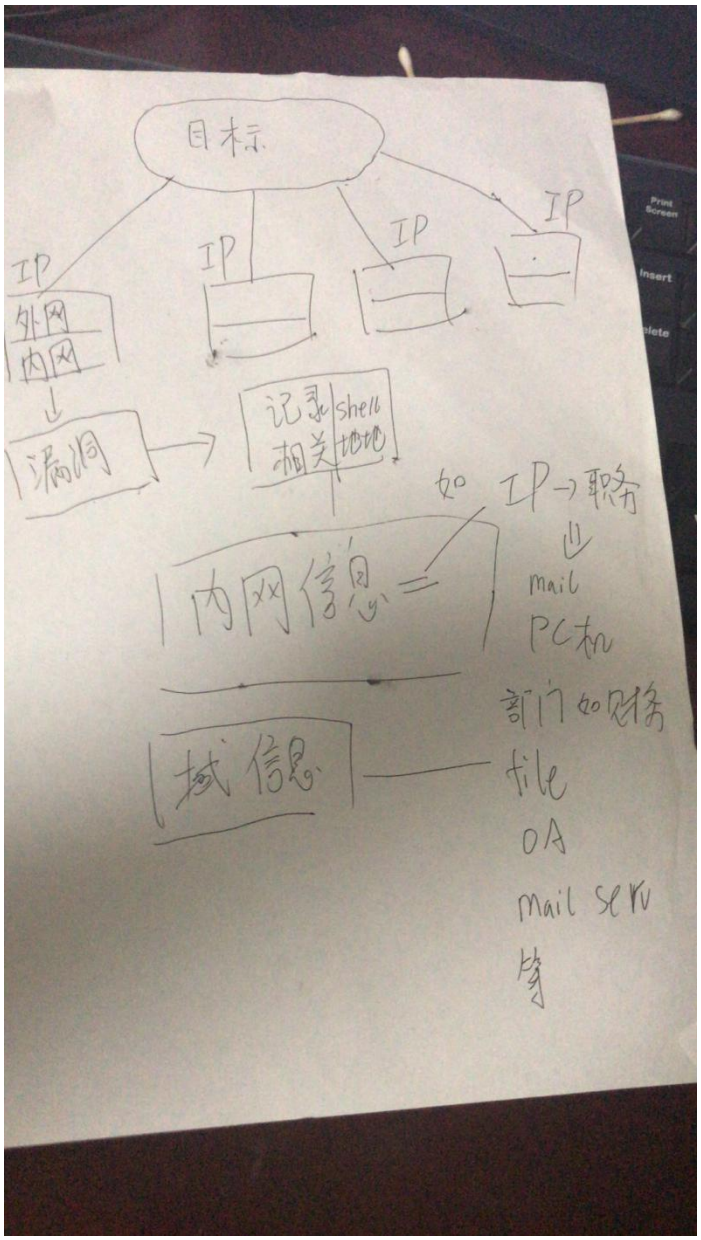
点 1：某个点漏洞
面 2：由点漏洞开始渗透面，该企业（传统行业医药，企业安全建设起跑阶段）
点 3：由面，该企业中的某人，定向打击
面 4：针对目标人物的行踪，定向打击某航空公司（重视企业安全建设，实施阶段）
点 5：最终了解了该人的全部资料与行程计划。



针对该国的药企排名信息搜集，定该国的 top1 为目标开始定向搜集，分为被动信息搜集，与主动信息搜集。其中主动信息搜集又分为，外部主动搜集与后期的内部主动信息搜集。并且把先期所有外围主动与被动信息搜集入库。与后期的内部信息搜集入库。形成完整的攻击方向链。



根据攻击方向链，制定攻击方向计划

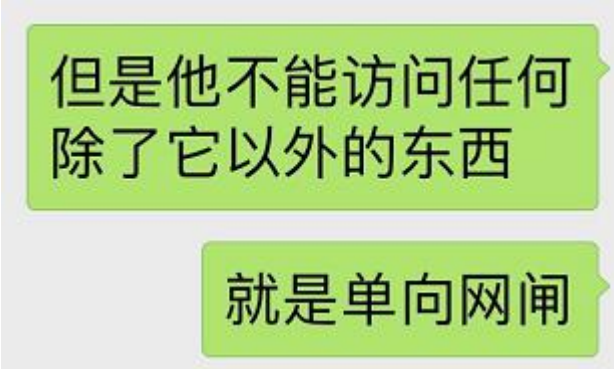


并且根据目前入库数据分析，很快得到了某台 DMZ 区域的 windows 主机权限。

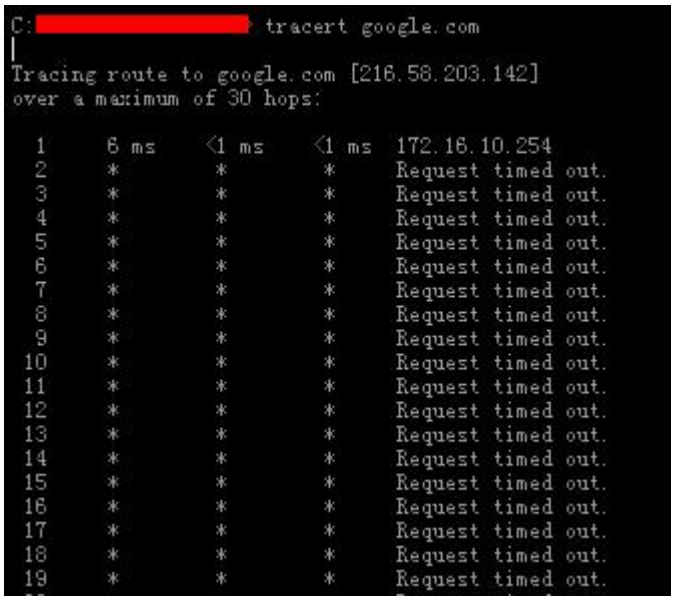
```
TCP    172.16.10.50:80
TCP    172.16.10.50:80
TCP    172.16.10.50:80
TCP    172.16.10.50:135
TCP    172.16.10.50:1102
TCP    172.16.10.50:1433
TCP    172.16.10.50:1433
TCP    172.16.10.50:1433
TCP    172.16.10.50:1433
TCP    172.16.10.50:1433
TCP    172.16.10.50:1433
TCP    172.16.10.50:1433
TCP    172.16.10.50:1433
TCP    172.16.10.50:1433
TCP    172.16.10.50:1862
TCP    172.16.10.50:1927
TCP    172.16.10.50:2210
TCP    172.16.10.50:2211
TCP    172.16.10.50:3389
```

上文已分析得出，该药企目标为传统行业，一般传统行业的安全网络设备较差，部分涉及到

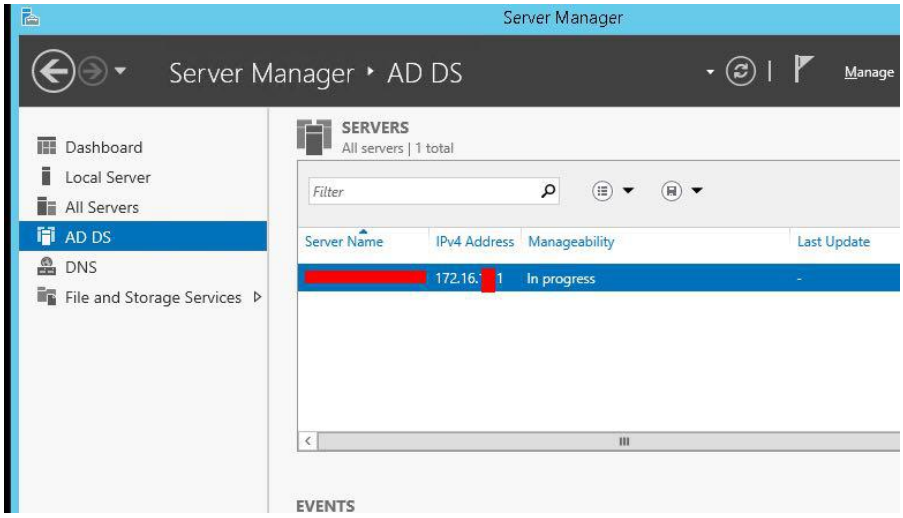
核心的数据库会有网闸，恰恰该目标某些设备具备网闸。



任何的本地访问都会到内网中的 254。



技术细节略过，在过网闸后，定向查找跨 B 段域控，在得到域控后，继续搜集信息入库分析并且完善攻击方向链，也就是需要分析出攻击方向，如财务，研发。避免 IT 等内部安全部门。



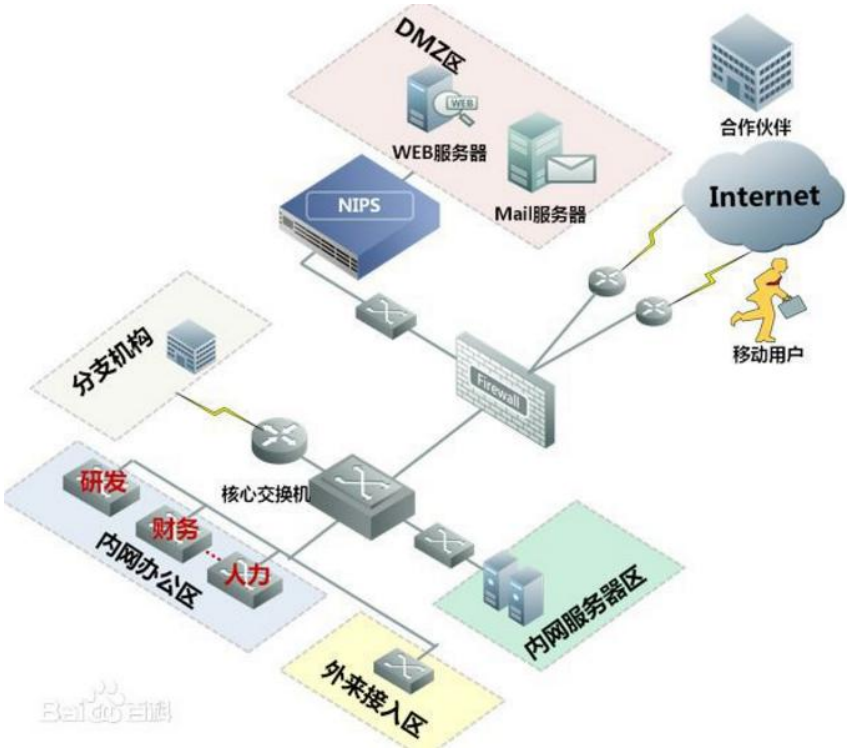
得到域控后，临时更改了以配方为主的计划方案。因为：

并且在 net group /domain 得到返回信息如下：

如果目前终止计划，那么此次仅仅是一次即时渗透，非 APT 定向攻击。临时更改计划，该企业中的某人 X，在 OA 得知，X 人，某天乘坐飞机到某地，具体业务并没有更为详细的说明。那么计划临时更改为，需要了解该人去某地的具体意图。

阶段性 1 总结：

目前大部分网络攻击主要分为：黑产黑客攻击，政治黑客攻击，商业黑客攻击，其他攻击。而针对传统企业（如医药，食品，汽车，传统国有企业，军工企业等）面临的攻击大部分来自商业黑客与政治黑客攻击。这 2 种类型的攻击，特点是时间换空间攻击，以最小化发现为主拉长时间抽的 APT 方式攻击。针对这种类型的企业，除了有效的安全产品外，而更多的是针对员工的安全意识培训。尤其是车企，并且部分车企的图纸，或者参与军工研发，甚至次年的发展规划，报表，都是黑客的主要攻击对象。由于部分车企采取多地甚至跨国联合办公，移动办公，移动用户，包括许多方面的合作伙伴。（如下图）导致了攻击点不仅仅在是针对企业面的攻击，更多的是以员工点方式的攻击。从而快速有效并且跳过部分防火墙，直接搜集敏感数据。



故事 2：

在故事 1 中得结尾得知 X 人要乘坐某航空到某地。具体做什么，从 OA 中无法得知。为了定向打击 X 人，开始针对对某航空公司的外围，主动/被动信息搜集，以及内部信息刺探。在航空行业中重视企业安全建设，实施阶段。其实并没有把这条规则入库到攻击链中，导致在入侵中发生了许多不必要的问题，如外网信息刺探的某 web 服务，部分有 sql 注入，但是一直把时间浪费在与 waf 的对抗中，而在这类行业中，都会部署着规则强大并且性能较好的 waf。大部分对外的网站中，没有明显漏洞。后期，把行业性质入库到攻击方向。重新定制计划，继续搜集信息，定向打击该航空员工。从而绕过安全设备。

那么整体攻击流程如下：

点 1------->点 2------->面 3------->点 4

点 1：搜集外围信息，主动/被动

点 2：针对爬虫信息入库，分析公司员工，职务人员。

面 3：根据该点员工，攻击该航空公司。

点 4：在航空数据中，查找药企 X 人的下一步的去向。

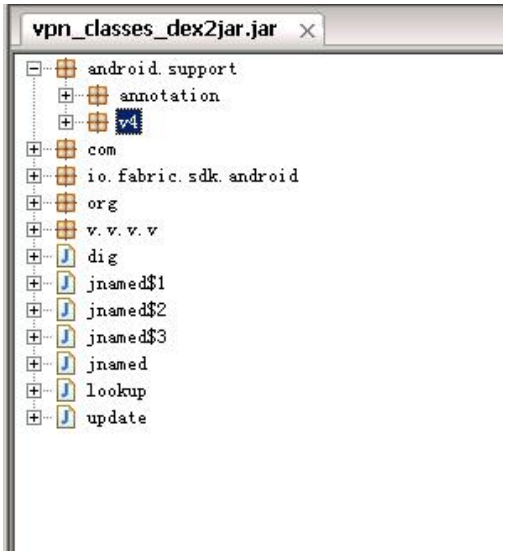
在外围信息搜集中得到某 json 接口返回，得到该公司全部员工代号，又在某接口返回得到无代号返回的全部员工邮箱账号。二者入库匹配，来获取 username，mail，职务。

（以下图片已经处理，无敏感，由于目标敏感，域内信息，以及数据库信息无图）

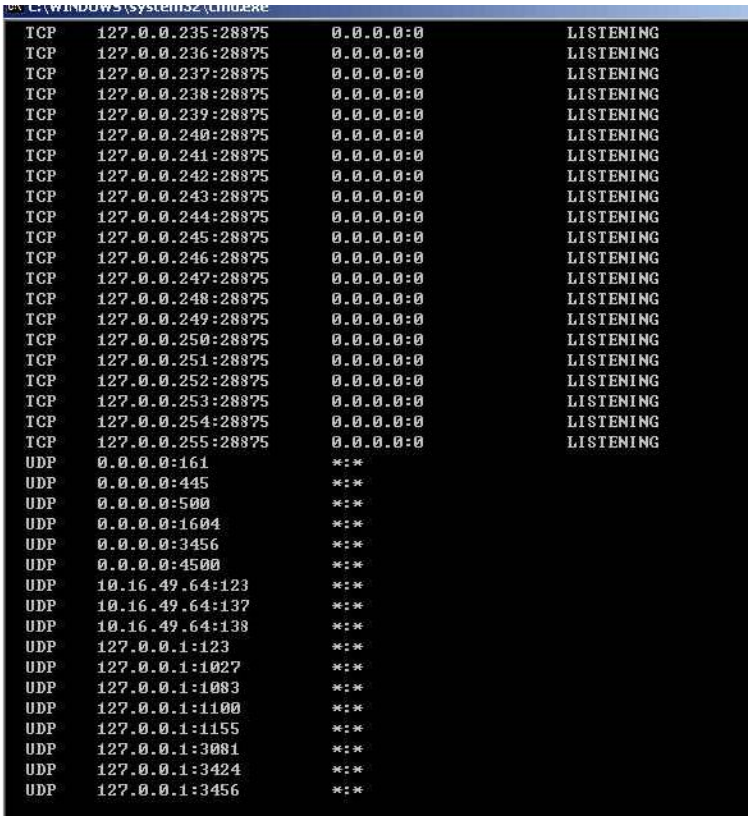
27-Dec-2013	名古屋分公
27-Dec-2013	名古屋分公
27-Dec-2013	名古屋分公
12-Aug-2014	名古屋分公
01-Oct-2014	名古屋分公
19-May-2015	名古屋分公
09-Apr-2016	名古屋分公
28-Jun-2016	名古屋分公
14-Mar-2018	名古屋分公
27-Dec-2013	名古屋分公
27-Dec-2013	名古屋分公
27-Dec-2013	日本貨運中
27-Dec-2013	名古屋分公
27-Dec-2013	東京分公司
27-Dec-2013	大阪分公司
27-Dec-2013	東京分公司

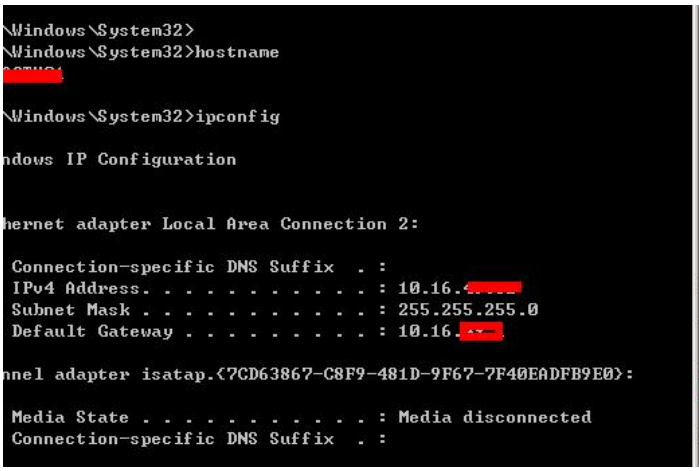
	澳洲分公司
	布里斯本分公司
	紐西蘭分公司
	紐西蘭分公司
	紐西蘭分公司
	紐西蘭分公司
	紐西蘭分公司
	紐西蘭分公司
	紐西蘭分公司
	韓國分公司釜山分公司
	韓國分公司釜山分公司
	韓國分公司釜山分公司
	韓國分公司釜山分公司
	韓國分公司釜山分公司
	印度分公司
	印度分公司
	印度分公司
	印度分公司
	印度分公司
	印度分公司
	印度分公司
	歐洲地區法國營業處
	歐洲地區法國營業處
	荷蘭分公司
	荷蘭分公司
	荷蘭分公司
	荷蘭分公司
	荷蘭分公司
	荷蘭分公司
	荷蘭分公司

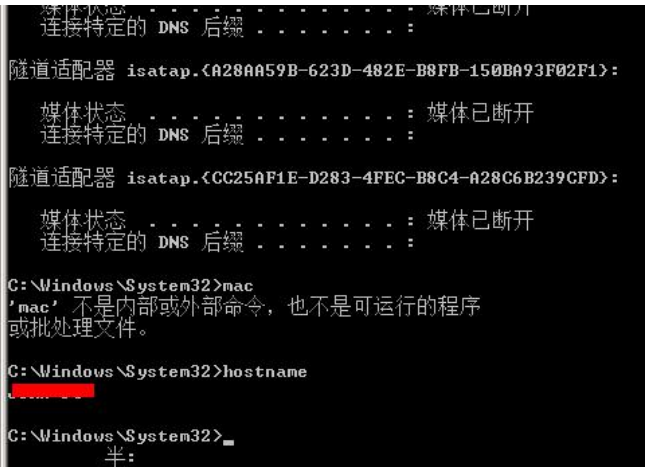
重新入库分析攻击链方向整理后，得到全部员工信息后开始匹配，打开某员工邮箱，并且在附件中得到 vpn.apk，逆向得到相关 api，导致可爆破。后在某处得到新版本 VPN.apk

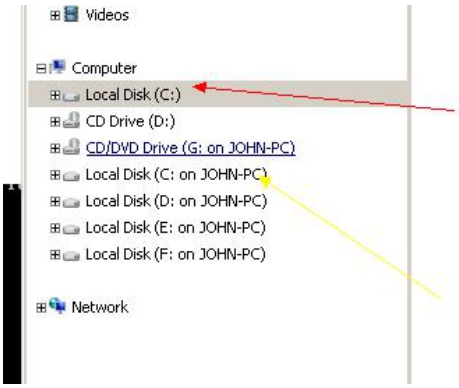


新版本的 vpn 有双因子劫持跳过。遂连，触发远程加载。得到内网，拓展域权限。
（以下图经过处理，无铭感，可能打乱顺序）


C:\Windows\system32\cmd.exe
TCP 127.0.0.235:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.236:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.237:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.238:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.239:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.240:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.241:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.242:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.243:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.244:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.245:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.246:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.247:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.248:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.249:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.250:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.251:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.252:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.253:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.254:28875 0.0.0.0:0 LISTENING
TCP 127.0.0.255:28875 0.0.0.0:0 LISTENING
UDP 0.0.0.0:161 *:*
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:1604 *:*
UDP 0.0.0.0:3456 *:*
UDP 0.0.0.0:4500 *:*
UDP 10.16.49.64:123 *:*
UDP 10.16.49.64:137 *:*
UDP 10.16.49.64:138 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1027 *:*
UDP 127.0.0.1:1083 *:*
UDP 127.0.0.1:1100 *:*
UDP 127.0.0.1:1155 *:*
UDP 127.0.0.1:3081 *:*
UDP 127.0.0.1:3424 *:*
UDP 127.0.0.1:3456 *:*


\Windows\System32>
\Windows\System32>hostname
[redacted]
\Windows\System32>ipconfig
ndows IP Configuration
hernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 10.16.[redacted]
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.16.[redacted]
nnel adapter isatap.{7CD63867-C8F9-481D-9F67-7F40EADFB9E0}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :


媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
隧道适配器 isatap.{A28AA59B-623D-482E-B8FB-150BA93F02F1}:
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
隧道适配器 isatap.{CC25AF1E-D283-4FEC-B8C4-A28C6B239CFD}:
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
C:\Windows\System32>mac
'mac' 不是内部或外部命令，也不是可运行的程序
或批处理文件。
C:\Windows\System32>hostname
[redacted]
C:\Windows\System32>
半:


Videos
Computer
Local Disk (C:)
CD Drive (D:)
CD/DVD Drive (G: on JOHN-PC)
Local Disk (C: on JOHN-PC)
Local Disk (D: on JOHN-PC)
Local Disk (E: on JOHN-PC)
Local Disk (F: on JOHN-PC)
Network

```
C:\Windows\System32>quser
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
 administrator         rdp-tcp#2           7  Active       5:59  2018/3/31 上午
10:40
```

```
C:\>arp -a

Interface: 10.16.49.[redacted] --- 0xb
  Internet Address      Physical Address      Type
  10.1[redacted].49.[redacted]           00-[redacted]-0c-07-ac-[redacted]     dynamic
  10.1[redacted].49.[redacted]           00-[redacted]-f7-16-8a-[redacted]     dynamic
  10.1[redacted].49.[redacted]           00-[redacted]-f7-16-e7-[redacted]     dynamic
  10.1[redacted].49.8             00-[redacted]-56-80-44-[redacted]     dynamic
  10.1[redacted].49.9             5c-[redacted]-fc-e9-84-[redacted]     dynamic
  10.1[redacted].49.0             00-[redacted]-5e-f5-8c-[redacted]     dynamic
  10.1[redacted].49.3             00-[redacted]-56-80-59-[redacted]     dynamic
  10.1[redacted].49.4             00-[redacted]-56-80-59-[redacted]     dynamic
  10.1[redacted].49.5             00-[redacted]-56-80-59-[redacted]     dynamic
  10.1[redacted].49.6             00-[redacted]-56-80-2e-[redacted]     dynamic
  10.1[redacted].49.0             00-[redacted]-56-95-44-[redacted]     dynamic
  10.1[redacted].49.1             00-[redacted]-5e-3d-2e-[redacted]     dynamic
  10.1[redacted].49.2             00-[redacted]-56-80-2b-[redacted]     dynamic
  10.1[redacted].49.6             00-[redacted]-56-80-11-[redacted]     dynamic
  10.1[redacted].49.8             00-[redacted]-56-80-59-[redacted]     dynamic
  10.1[redacted].49.9             00-[redacted]-56-80-01-[redacted]     dynamic
  10.1[redacted].49.5             00-[redacted]-56-80-00-[redacted]     dynamic
  10.1[redacted].49.8             00-[redacted]-56-80-75-[redacted]     dynamic
  10.1[redacted].49.9             00-[redacted]-56-80-59-[redacted]     dynamic
  10.1[redacted].49.0             00-[redacted]-56-80-71-[redacted]     dynamic
  10.1[redacted].49.0             5e-[redacted]-fc-b9-10-[redacted]     dynamic
  10.1[redacted].49.0             00-[redacted]-25-29-a3-[redacted]     dynamic
  10.1[redacted].49.0             00-[redacted]-56-a5-53-[redacted]     dynamic
  10.1[redacted].49.1             00-[redacted]-56-80-5f-[redacted]     dynamic
  10.1[redacted].49.2             00-[redacted]-56-80-2e-[redacted]     dynamic
  10.1[redacted].49.2             00-[redacted]-56-80-07-[redacted]     dynamic
  10.1[redacted].49.2             00-[redacted]-56-80-73-[redacted]     dynamic
  10.1[redacted].49.5             a2-[redacted]-00-3c-f6-[redacted]     dynamic
  10.1[redacted].49.5             d2-[redacted]-f4-47-85-[redacted]     dynamic
  10.1[redacted].49.6             be-[redacted]-1f-e8-e0-[redacted]     dynamic
  10.1[redacted].49.8             00-[redacted]-f6-0c-c3-[redacted]     dynamic
  10.1[redacted].49.8             ca-[redacted]-02-bb-a6-[redacted]     dynamic
  10.1[redacted].49.9             a6-[redacted]-8c-96-05-[redacted]     dynamic
  10.1[redacted].49.3             00-[redacted]-56-80-7a-[redacted]     dynamic
  10.1[redacted].49.5             ff-[redacted]-ff-ff-ff-[redacted]     static
  169.[redacted]54.6[redacted].9          0e-[redacted]-be-25-06-[redacted]     dynamic
  169.[redacted]54.9[redacted].1          d2-[redacted]-f4-47-85-[redacted]     dynamic
  169.[redacted]54.1[redacted]3.102       d2-[redacted]-f4-47-85-[redacted]     dynamic
  169.[redacted]54.1[redacted]0.25        5a-[redacted]-9e-6d-43-[redacted]     dynamic
  169.[redacted]54.2[redacted]8.159       0e-[redacted]-be-25-06-[redacted]     dynamic
  224.[redacted].0.2[redacted]            01-[redacted]-5e-00-00-[redacted]     static
  224.[redacted].0.2[redacted]2           01-[redacted]-5e-00-00-[redacted]     static
  239.[redacted]55.2[redacted]5.250       01-[redacted]-5e-7f-ff-[redacted]     static
```

在结尾处，发现 X 人是去度假去了。（捂脸，后飞至某国）

阶段性总结 2：

目前的航空行业，金融行业都是黑产黑客的高发地，以窃取数据为核心攻击。而此类行业中，所有数据库又具备数据的完整性。如身份证，姓名，电话，照片等。数据较为敏感。此类行业每年都会有信息安全建设的大量预算，这种类型的目标，往往打点极其困难，大部分的 waf 或监控流设备就拦截了非法信息，并且有专门的信息安全部门对内部进行安全测试与部分整改意见。而针对大型该行业企业，由于员工众多，导致部分信息不能及时共享与整

改。甚至会出现本公司的网络资产表覆盖不全面。以点溃面。

总结：由于信息化，自动化的办公，企业成本的考虑，传统的“以点打面”的点会越来越分散与难以集中管理，如跨国办公，移动办公等。那么可预知的攻击方式将会以人为突破口的事越来越多。安全的本质又不能仅仅靠预算与设备的投入而杜绝，尤其是在未来的大型甲方公司，都会有着自己的安全团队，那么如何把网络安全发展成未来甲方公司的企业文化，将会是一个漫长的过程。而近些年无论是国内还是国外的官方部门开始重视网络安全，但是效果不明显，同样这里借用某大佬的总结，同样部分也适用于企业：

1 领导不重视
2 岗位无编制
3 专业能力弱
4 攻防更新快
5 人才留不住

可见，不同的行业，企业安全规划建设是不同的并且不具备模板化建设，不具备安全设备堆建建设，如果在行中在按照地域划分也有着部分的不同特征，比如一些地方以国企（大量工控），重工业为支撑，一些沿海地区有着发达的金融业的企业安全建设。针对的主要攻击对象不同，针对的防护内容不同。来制定适合本企业的安全建设规划方案。但是有一点一定是相同的，把企业的网络安全发展成企业文化。