奇安信威胁情报中心

ti.qianxin.com/blog/articles/Blade-hawk-The-activities-of-targeted-the-Middle-East-and-West-Asia-are-exposed/

返回 TI 主页
RESEARCH

数 据 驱 动 安 全

概述

近期奇安信威胁情报中心移动安全团队注意到一波针对伊斯兰国、基地组织、库尔德族群和土库曼族群进行持续攻击控制的活动， 时间跨度从自2019年3月起至今，通过从多源信息的交叉比对我们推测攻击组织来自中东某国，将其命名为利刃鹰组织。

主要时间线如下：

图1.1 利刃鹰组织针对的特殊攻击目标部分攻击时间线

利刃鹰组织主要使用开源和商业攻击软件，平台涵盖Windows和Android，截止目前我们一共捕获到Android平台攻击样本43个，Windows平台攻击样本26个，涉及的C&C域名3个。

攻击目标

在对移动端的攻击样本分析过程中，我们发现到利刃鹰组织具有明显的攻击目标指向性，旨在对其目标实现监控及反监控，其攻击包含针对多个特色目标。

针对伊斯兰国及基地组织等

利刃鹰组织投递多个针对伊斯兰国及基地组织的移动端RAT，这些攻击样本涉及到伊斯兰国的主要新闻媒体Amaq及官方报纸Al-Naba；亲基地组织的宣传网站Minbar al-Tawhid wa'l-Jihad；伊斯兰的Tube视频应用等。

图2.1 针对伊斯兰国及基地组织的攻击样本应用图标

针对库尔德族群

其投递两种针对库尔德族群的移动端RAT，这些攻击样本涉及到库尔德斯坦的新闻杂志Darka Mazi及一款库尔德键盘应用。

图2.2 针对库尔德族群的攻击样本应用图标

针对土库曼族群

其投递一款针对土库曼人的移动端RAT，攻击样本涉及到伊拉克知名伊斯兰研究教授宣传网站应用，需要留意的是该网站采用的是土库曼语。特殊的地区人物和特殊的语言，结合地区的局势情况，这对锁定攻击者身份推测大有帮助。

图2.3 针对土库曼族群的攻击样本应用图标

图2.4 土库曼语的伊拉克知名伊斯兰研究教授宣传网站

疑似针对土耳其人

其投递一款伪装成流行的条形码扫描应用的移动端RAT，需要注意的是该样本留有特殊标识“Barcode Scanner Turkey”，疑似还针对土耳其人。

图2.5 疑似针对土耳其人的攻击样本应用图标

```
MainService.osux = new DataOutputStream(MainService.so.getOutputStream());
v1.this$0.rsex = new DataInputStream(MainService.so.getInputStream());
v1.this$0.sendip = ((String)v2);
v4_1 = v1.this$0;
v4_1.sendip = v1.this$0.resultipcount + "|Barcode Scanner Turkey|" + v1.this$0
        .resultip + "|" + v1.this$0.buildx + "|" + v1.this$0.mOdel + "|" + v1
        .this$0.prox + "|1.1.2|" + v1.this$0.apilev + "|8axxr32";
v4_2 = MainService.osux;
v4_2.writeBytes("#" + v1.this$0.sendip);
MainService.osux.flush();
v1.this$0.paster = 0;
v1.this$0.gfgfg = 0;
break;
}
catch(SocketException v0_1) {
    goto label_2048;
```

图2.6 攻击样本留下的特殊标识“Barcode Scanner Turkey”

疑似针对区域性的监控及反监控

其攻击样本还涉及到多种常见行业应用，包含电视应用、社交保护应用、保险应用、网络应用及游戏应用等，疑似来实现对其关注的区域进行范围监控；另还涉及到多款监控辅助应用，包含位置查看、电话号码定位、自动通话记录和屏幕录制等，疑似来实现反监控。

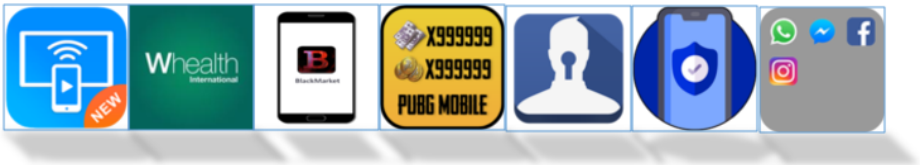

图2.7 疑似进行区域监控的涉及多种常见行业的攻击样本应用图标

图2.8 疑似实现反监控的攻击样本应用图标

载荷投递

基于奇安信威胁情报中心移动安全团队的内部分析系统和 奇安信威胁情报平台 关联系统等追踪分析，我们发现到利刃鹰组织攻击载荷主要存放在第三方存储网站上 (up4net.com)，再通过生成对应短链接，最后发布到钓鱼信息中进行载荷投递。如曾在社交平台Fackbook上进行的针对库尔德人的载荷投递过程可参见下图。

图3.1 在Facebook上发布钓鱼信息的方式

样本md5	样本钓鱼短链接url	样本实际完整下载url
7462d3be5f649b52794ca5a1f1d201f1	https://rb.gy/vfdfbc	https://up4net.com/uploads/up4net-Trace-Mobile-Number-v2-3.apk

图3.2 在Facebook上发布的载荷短链接及对应的样本关系

攻击样本分析

利刃鹰组织投入Windows和Android平台的攻击RAT，目前已被发现有五种商业RAT。其中Windows平台有四种（Bladabindi 、Remcos 、Loda 和Warzone），均是常见的RAT，故在此不再重复展开分析。Android平台有两种（SpyNote和Gaza007）。

SpyNote

SpyNote是一款流行的移动端商业RAT。其支持的功能多样，最新收费版售价可观，根据不同场景需求目前官方有三种价位($499、$4000和$6000)。其还带有免费版，另有早期版本源码被泄露，其多个破解版本和修改版本已在多个黑客网站上泛滥传播。

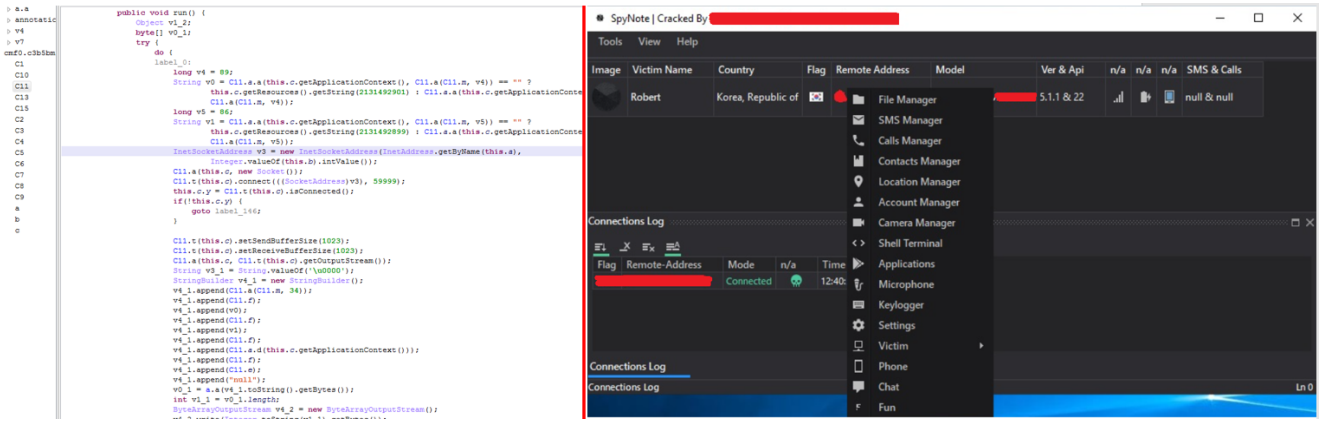

图4.1 SpyNote被控端代码结构(左)和控制端管理界面(右)

Gaza007

Gaza007是一款2019年诞生的移动端RAT。目前被发现最早于2019年3月出现，随后被多个攻击者投入使用，目前数量已有千级，我们通过其默认的签名信息进行命名为“Gaza007”。其类似于Spynote，功能也十分强大，现已支持近四十种远程指令，在初次登场后不久便迅速更新集成有专门钓鱼Fackbook的功能。根据其采用的证书签名信息及其主要投入的攻击区域来推测，其大概率是加沙黑客所制作的商业RAT。

指令	功能
Unistxcr	跳转到指定应用的详情页面
Dowsizetr	窃取/sdcard/DCIM/.dat/目录下指定文件其文件大小信息到C＆C服务器
DOWdeletx	删除/sdcard/DCIM/.dat/目录下指定文件
Xr7aou	窃取/sdcard/DCIM/.dat/目录下指定文件到C＆C服务器
Caspylistx	窃取/sdcard/DCIM/.dat/目录下所有文件列表名称信息
Spxcheck	检查是否成功开启或关闭窃取呼叫详细信息服务
S8p8y0	关闭窃取呼叫详细信息服务
Sxpxy1	开启窃取呼叫详细信息服务
screXmex	进行截屏并窃取
Batrxiops	监控电池状态
L4oclOCMAWS	监控受害者地理位置
FdelSRRT	删除盗取到的受害者Facebook凭证文件
Chkstzeaw	检查Facebook应用是否运行

指令	功能
IODBSSUEEZ	将已盗取到的受害者Facebook凭据文件发送到C＆C服务器
GUIFXB	启动钓鱼的Facebook登录界面
LUNAPXER	响应启动到另一个应用程序
Gapxplister	获取所有已安装应用程序的列表
DOTRall8xxe	对窃取信息目录下所有文件进行压缩到/DCIM/目录后再上传给C＆C服务器
Acouxacour	窃取受害者设备帐户信息
Fimxmiisx	进行拍照并窃取
Scxreexcv4	获取相机情况信息
micmokmi8x	进行录音并窃取
DTXXTEGE3	删除/sdcard/目录下指定文件
ODDSEe	启动指定的Activity
Yufsssp	窃取地理位置的经纬度
Getsssspo	窃取/sdcard/目录下指定文件其文件大小信息到C＆C服务器
DXCXIXM	窃取/sdcard/DCIM/目录下所有文件列表名称信息
f5iledowqqww	窃取/sdcard/目录下指定文件到C＆C服务器
SDgex8se	窃取/sdcard/目录下所有文件列表名称信息
PHOCAs7	响应拨打指定的电话号码
Gxextsxms	窃取收件箱短信信息列表
Msppossag	响应给指定的手机发送指定的短信消息
Getconstactx	窃取通讯录信息列表
Rinxgosa	播放铃声
Shetermix	响应执行指定的命令
bithsssp64	响应执行指定的脚本文件

指令	功能
Deldatall8	删除/sdcard/DCIM/.dat/目录下所有文件
M0xSSw9	响应弹出指定的Toast消息

表4.2 Gaza007功能指令表

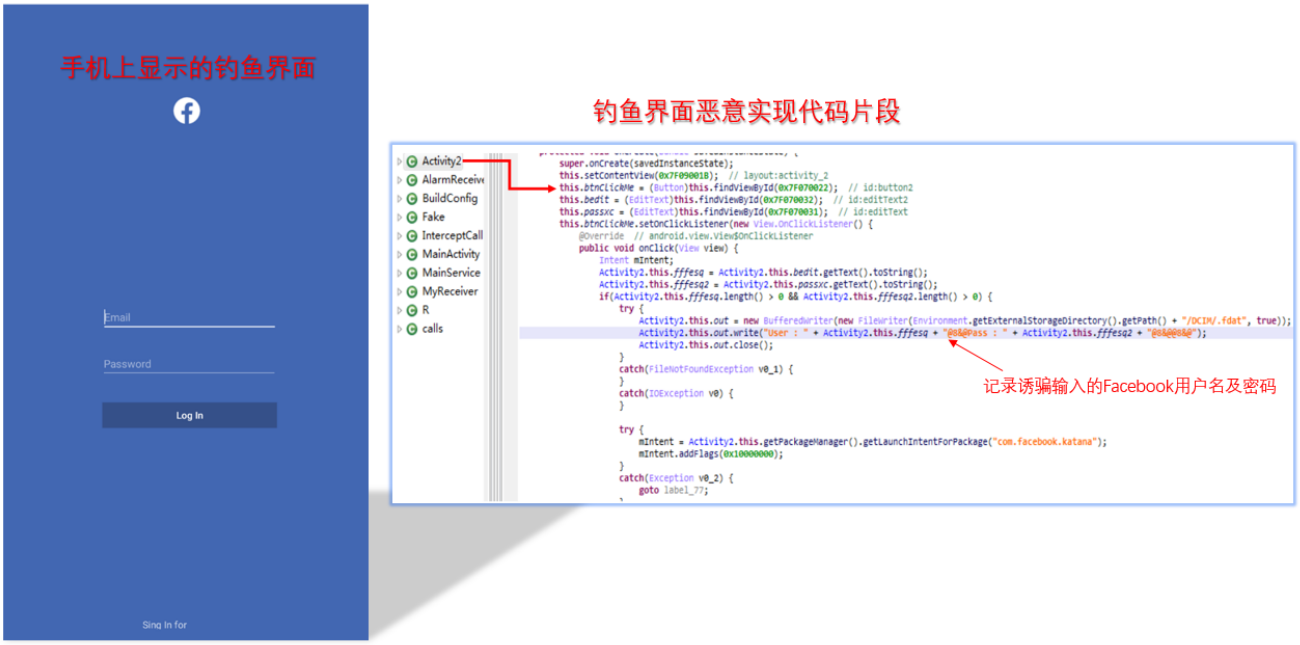

图4.3 Gaza007钓鱼Fackbook界面(左)及对应的实现代码片段(右)

攻击组织溯源分析

利刃鹰组织具有明显的针对特殊群体目标，显然不是普通的黑客组织的攻击需求，我们认为该组织疑似是来自中东某国国家背景下实行的监控活动。主要依据如下：

1. 熟悉某个地区的多种语言及背景，针对地区的库尔德族群、基地组织及土库曼族群，并对该区域疑似实行监控及反监控的攻击。
2. 结合中东某国的历史背景及地缘关系，攻击活动恰好符合其所需。
3. 三个C2的历史对应IP多次显示出位于中东某国，并有多次重叠，显然并不是一种巧合。

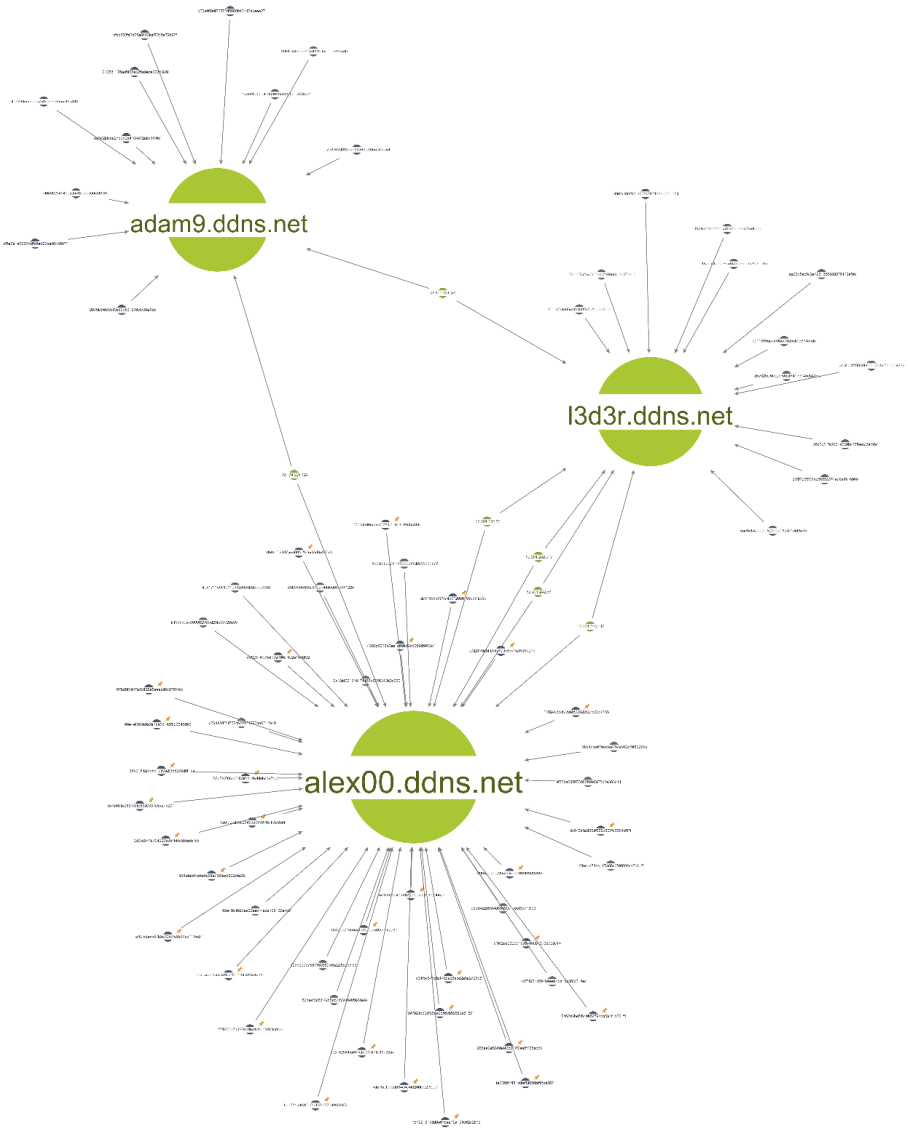

图5.1 选取的IOC关联图

总结

中东地区由于宗教种族和地缘政治关系，一直是多个APT组织的高度活跃地区。此次的利刃鹰组织也无疑又是其中的一个新代表。需注意的网络钓鱼可谓老生常谈，却仍是攻击者屡试不爽的惯用手法，最有效的武器。

应对这些攻击不仅需要安全厂商的各类安全产品的防护和到位的安全服务支持，更离不开企业对内部自身安全规程及企业内部员工安全防范意识的持续建设。针对普通用户如何避免遭受移动端上的攻击，奇安信威胁情报中心移动安全团队提供以下防护建议：

1. 在正规的应用商店下载应用。国内的用户可以在手机自带的应用商店下载，国外用户可以在Google Play下载。不要安装不可信来源的应用、不要随便点击不明URL或者扫描安全性未知的二维码。。
2. 移动设备及时在可信网络环境下进行安全更新，不要轻易使用外来的网络环境。

3. 对请求应用安装权限、激活设备管理器等权限的应用要特别谨慎，一般来说普通应用不会请求这些权限，特别是设备管理器，正常的应用机会没有这个需求。
4. 确保安装有手机安全软件，进行实时保护个人财产安全；如安装奇安信移动安全产品。

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信NGSOC等，都已经支持对此类攻击的精确检测。

附录A：IOC

APK 样本文件MD5

8967cf93287a93f747971689cf33e674

fe7266f1ff31c0faf8f650bfff8bd267

6034cad5ec2badd4ad3f009f33d2d86e

5e1e0e5247fd9b509ba25cfb8f2c442b

9b6c662447aea005a12fecf5d8e5734b

7d4991317dd0e67daa70a124c62d257c

271606d7a822610be10830fd13fc94cd

52d592f68dc64c8f881deddebdae7cb2

6f2cf52941fa837abd01fd71a16c32ae

e962674bc94fc7aff06e7fe2a1546f92

397921cd0df96ea2b46cb50352a61691

c31f5c84fb2a140ce26ebe2a5a2426b6

931efe504e5e6c58a738fea5802c6e38

bf9d2ea0329915b6498db7373e90dc14

253ea0a6889a8f2b217f0ae6f436ebc3

555ce971658adde6d5cec86edfbf2a8b

11024c3ccf7cbbf89c820327c90b7133

4303d5073d0ee1d69b19c5069d5613d4

2d0c8974b1942295c07f49c8f4a5b7c5

9a0f72cdc9a2846da937676e1efe8bf4

67b20f7d47a18128e8eaebd9c075f4b3

7462d3be5f649b52794ca5a1f1d201f1

bb7e661a983f491c63d0337c5da7b291

d52ecc2c3c57401e2170184b324d8a99

e9d2370a8ffb54ad7de6b77a1535e21b

5715d5d0ede440f22c3a468e3003a8bb

8c543bfa2f35df239b307fc3694bf9f1

7da70a17c9d804e4e4f6266f5e2f890d

38b018fbb4d5b1780a2f356238d0f1ea

dc97856c031fa4e0126b6786cd3fbe8c

bea771a408f3b3bfff4887704305187c

90e4ef393b9a2a4ba79148f9d0646d92

ef875da5b37b8e49f41e8844ec1135d7

2945b8f6e3310eb9b821276cfb30a188

1c499b3bb646868913e866190c4784a2

b20ad69df52872d5560bb3147abeea27

cf5e2a1a953248ffd6e192ca80485674

02b8767d6137cb3756fbc095c243cccf

bfdc838fa7c75a0113baf7215a72b97f

d6b36254646e2c5e0c969c56a3f876fe

010831176ad5f06a325a9ece278c386f

40678deceecee7c6cdb6e905a7f8c403

8a3d2bfcda27d2b2e4104812abd14f6d

C2服务器域名

l3d3r.ddns.net

alex00.ddns.net

adam9.ddns.net

PC样本文件MD5

4e81711c961011e6328043b8bdce9098

6bb4dce616edfe8754e962df9f89295b

45ecde74ee167a88c0f80009ea7c61f3

b1666d9ae06990298fbd23fa99728a56

12db000b7591360350f85a225e0dcfc3

d39da3d21f757c622171992aa9211b40

1c271931c694b9eeb4da1ca3f9d214ec

d9b58f64930a8d92b4446d8f66831225

4c9fbdbee78f7410b9e87d8c90d19578

68e4981bb2ea02eec44ada103129a4c0

95c94b2056f4059090c1c8ef65713f03

69baef3a6df42d6a5789948805b3fa88

9c18bf001316471165c9956313b2d230

8f37da085073082f99d3f25b2e303c44

a15fac323830b9a5e268af76acfe4232

ec11869aca4f08ad3fa5cbc58f94fbdc

d5e325cf6ce23f56c4841bb14beb40ee

aae6eb4a99d0f82977a187de1cf43a75

26c5b21fa2b01a0c9bc45fbead6ef36c

72ec17a2ac3b63d07269ddce9c7f38e0

639fc77077910cc6249da3b97258fa00

18acfe1a7038ca0c0229b0daf8060c6b

aa03d8ec5c2a4931386880275142ef9d

f800d75dd85d463f932c5d10b5b2fa0c

c45f2b6f032ac89553374ec9a4916966

30b1e448b5e7144024afafee0a8275db

附录B：奇安信威胁情报中心

奇安信威胁情报中心是北京奇安信科技有限公司（奇安信集团）旗下的威胁情报整合专业机构。该中心以业界领先的安全大数据资源为基础，基于奇安信长期积累的核心安全技术，依托亚太地区顶级的安全人才团队，通过强大的大数据能力，实现全网威胁情报的即时、全面、深入的整合与分析，为企业和机构提供安全管理与防护的网络威胁预警与情报。

奇安信威胁情报中心对外服务平台网址为 https://ti.qianxin.com/ 。服务平台以海量多维度网络空间安全数据为基础，为安全分析人员及各类企业用户提供基础数据的查询，攻击线索拓展，事件背景研判，攻击组织解析，研究报告下载等多种维度的威胁情报数据与威胁情报服务。

微信公众号：

奇安信威胁情报中心:　　奇安信病毒响应中心：

附录C：奇安信威胁情报中心移动安全团队

奇安信威胁情报中心移动安全团队一直致力移动安全领域及Android安全生态的研究。目前，奇安信的移动安全产品除了可以查杀常见的移动端病毒木马，也可以精准查杀时下流行的刷量、诈骗、博彩、违规、色情等黑产类软件。通过其内部分析系统可以有效支持对溯源分析等追踪。通过其高价值攻击发现流程已捕获到多起攻击事件，并在今年发布了多篇移动黑产报告，对外披露了三个APT组织活动，其中两个是首发的新APT组织（诺崇狮组织和此次的利刃鹰组织）。未来我们还会持续走在全球移动安全研究的前沿，第一时间追踪分析最新的移动安全事件、对国内移动相关的黑灰产攻击进行深入挖掘和跟踪，为维护移动端上的网络安全砥砺前行。

附录D：奇安信移动产品介绍

奇安信移动终端安全管理系统（天机）是面向公安、司法、政府、金融、运营商、能源、制造等行业客户，具有强终端管控和强终端安全特性的移动终端安全管理产品。产品基于奇安信在海量移动终端上的安全技术积淀与运营经验，从硬件、OS、应用、数据到链路等多层次的安全防护方案，确保企业数据和应用在移动终端的安全性。

奇安信移动态势感知系统是由奇安信态势感知事业部及其合作伙伴奇安信威胁情报中心移动团队合力推出的一个移动态势感知管理产品。不同于传统移动安全厂商着重于APP生产，发布环节，为客户提供APP加固、检测、分析等；移动态势感知面向具有监管责任的客户，更加着重于APP的下载，使用环节，摸清辖区范围内APP的使用情况，给客户提供APP违法检测、合规性分析、溯源等功能。

利刃鹰组织

分享到：