奇安信威胁情报中心

ti.qianxin.com/blog/articles/who-is-the-next-silent-lamb-nuo-chong-lions-apt-organization-revealed

一. 概述

无论物理还是网络空间的对抗，中东从来都是高度活跃的区域，奇安信红雨滴团队也一直保持着关注。基于长期的分析整理，本文公开一波持续几年的定向攻击活动及背后的团伙，值得分享到安全社区以增进我们对地缘政治背景下的网络行动的理解。

自名为“Operation Restoring Hope” 的也门干预行动当天，也就是2015年4月22开始，截至2018年世界杯结束后的数月里，有一个网络攻击组织一直持续针对阿拉伯用户、什叶派及评论人士进行展开攻击，在攻击后我们发现不少被攻击的社交平台账号变成“沉默账号”，在目前已知的APT组织中均未发现和该组织有重叠，因此奇安信红雨滴把其归属为一个新的组织：诺崇狮组织。

有一句话这样形容Dota游戏里的一名角色人物----沉默术士(诺崇)：一切魔法，遭遇了他，都将归于寂静。其后半句用在该攻击组织上相当吻合，再加上该组织的震慑力和其中的配合如同狮群，故我们将其命名为诺崇狮组织。随着该组织所属相关领导者近期可能发生的变动，该组织有可能会再度活跃。

目前已经关联到的攻击活动时间线总结如下：

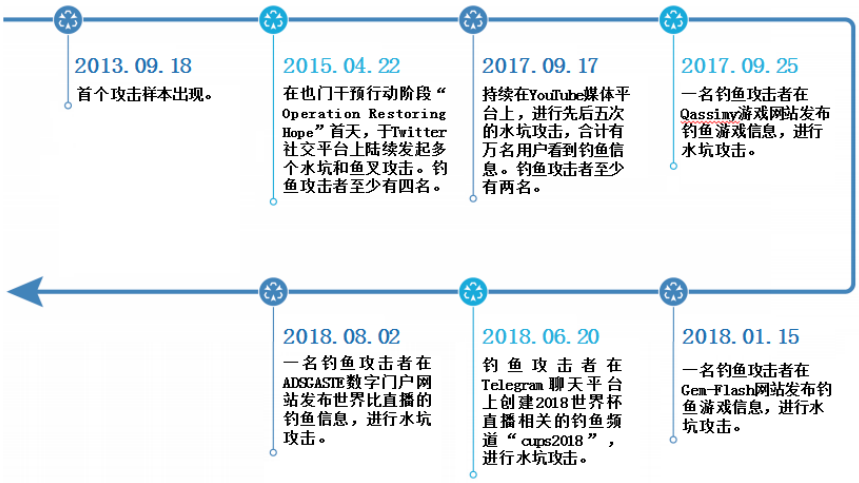

图1.1 诺崇狮组织在多个网站和社交平台上发起攻击的时间线

二. 背景介绍

诺崇狮组织掌握有一个由大量机器人及雇佣而来的成百上千名年轻人组成的虚拟团队，用于传播虚假信息和亲政府宣传进，长期以来其一直专注于监视攻击，使国内外的批评者保持沉默，其能够利用昂贵的间谍软件瞄准生活在世界另一端的持不同政见者。

Twitter是该组织的主战场，因为Twitter被当作广受欢迎的新闻发布平台。诺崇狮组织可能培养了两名Twitter员工，尝试访问持不同政见者和激进分子的私人信息，包括电话号码和IP。后Twitter在2015年11月11日，向几十个被其中一名前Twitter员工访问过帐户的所有者发出了安全通知：“作为

预防措施，我们提醒您，您的Twitter帐户是一小部分帐户之一，这些帐户可能是由国家赞助的参与者所针对的”。在2019年9月20日，Twitter又发出了一个新披露通知，宣布永久暂停了一个名为卡塔尼(Saud al-Qahtani)的Twitter账号。

类似的，该组织还会操纵YouTube和Facebook平台，于此就不再展开描述。

三. 载荷投递

诺崇狮组织在攻击活动展开期间，红雨滴团队捕获到其至少投入近十名攻击投递者在多个网站和社交平台上进行非定向的水坑传播式钓鱼攻击及定向目标的鱼叉攻击。

（一）. 水坑攻击

至今已发现有数名攻击者在配合发布钓鱼信息，发布地点涉及了三个网站与三个社交平台(视频平台YouTube、聊天平台Telegram和社交平台Twitter)。钓鱼消息使用的语言均为阿拉伯语，仅从YouTube平台进行评估，约有万名用户可能受到攻击影响。

1. 攻击者在Qassimy游戏网站进行发布虚假游戏信息，诱导用户转向钓鱼网站进行恶意载荷的下载。

图3.1 Qassimy游戏网站上的钓鱼信息

2. 在Gem-Flash网站进行发布虚假游戏信息，诱导用户进行恶意载荷的下载。攻击者(“wafa3”应该和Qassimy上发布的为同一个，此次钓鱼信息里还带有指向YouTube的一个引链。

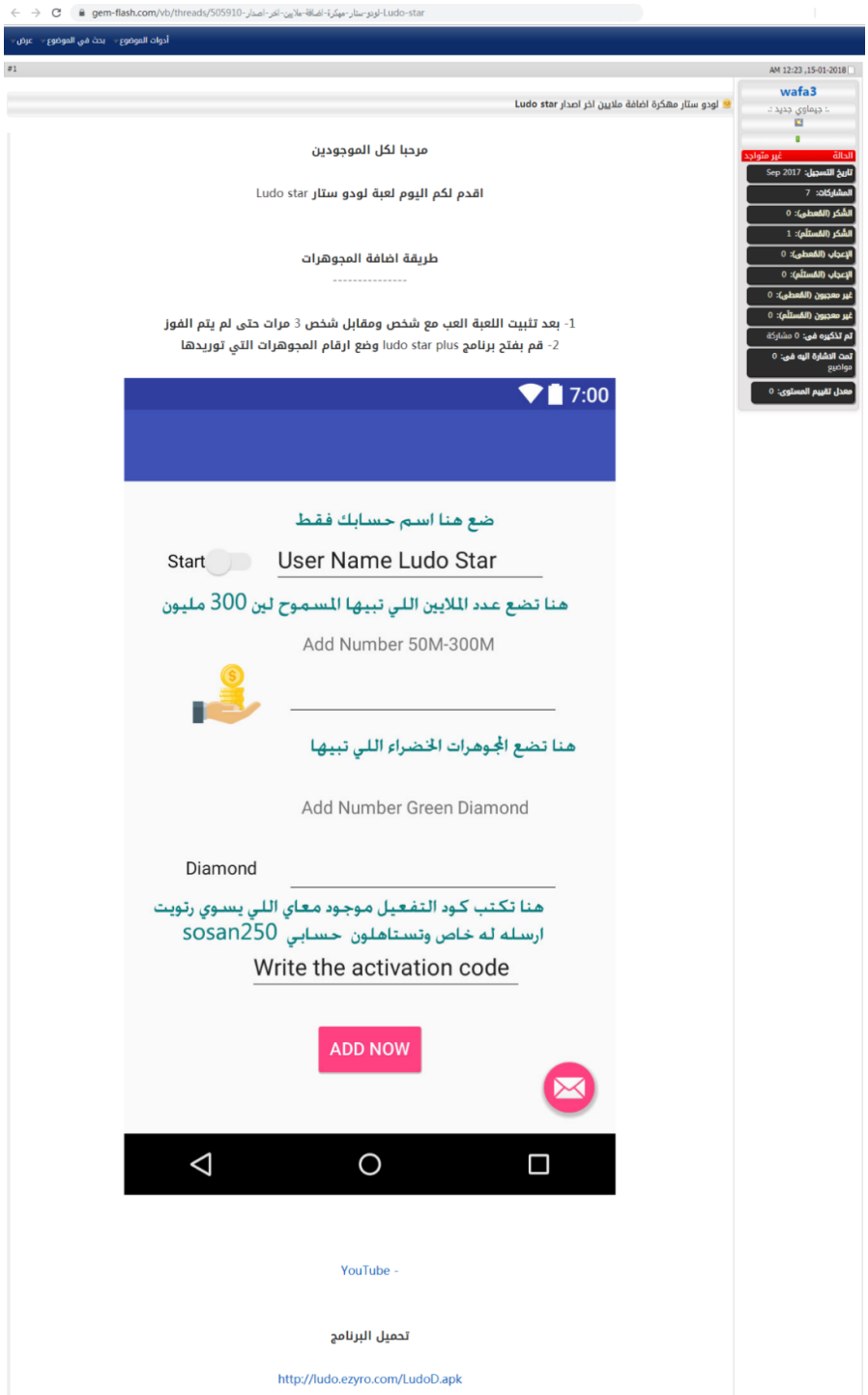

图3.2 Gem-Flash网站上的钓鱼信息

3. 世界杯期间，在ADSGASTE数字门户网站进行发布虚假的世界杯播放应用信息，诱导用户转向钓鱼网站进行恶意载荷的下载。

图3.3 ADSGASTE数字门户网站上的钓鱼信息

4. 在YouTube平台上，目前已发现到有两个钓鱼攻击者；其中名叫“Nothing”的攻击者，发布了四次钓鱼信息，按观看数进行评估，约有万名YouTube用户收到钓鱼信息。另外，值得注意的是该攻击者在YouTube上发布的其中一个钓鱼信息地址被上面Gem-Flash网站的名为“wafa3”的攻击者使用在其钓鱼信息中当做引链，类似的还可以经常看到该组织下不同钓鱼攻击者之间的相互配合。

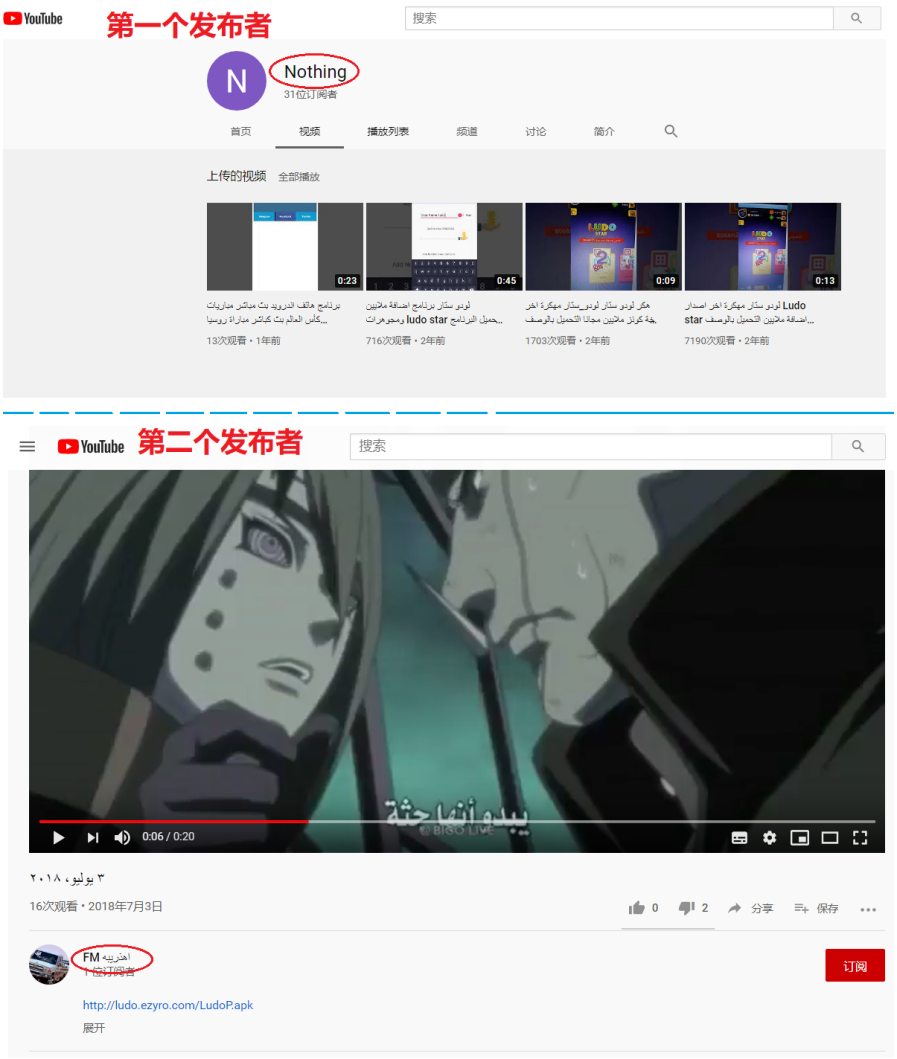

图3.4 两个攻击者在YouTube平台上发布的钓鱼信息

5. Telegram上伪装成2018世界杯直播的群频道。

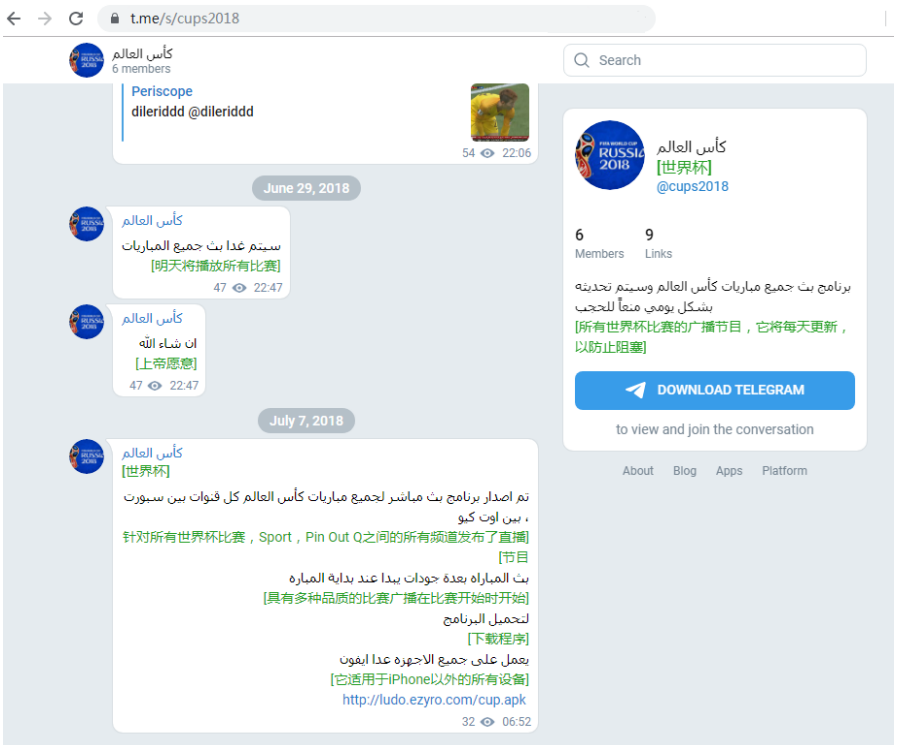

图3.5 Telegram上使用的伪装世界杯直播频道

注：此处友情提醒广大安全友军，载荷投递的链接有防盗保护，所以流程有没有抓取到呢?

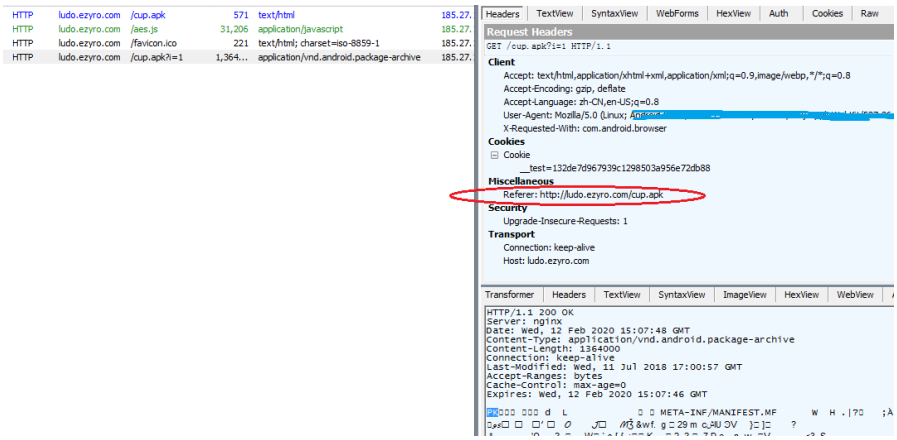

图3.6 Telegram上使用的伪装世界杯直播频道

6. 在Twitter平台上，已发现到该组织的四个攻击者发布了未定向的多条不同内容的钓鱼信息进行广泛传播。

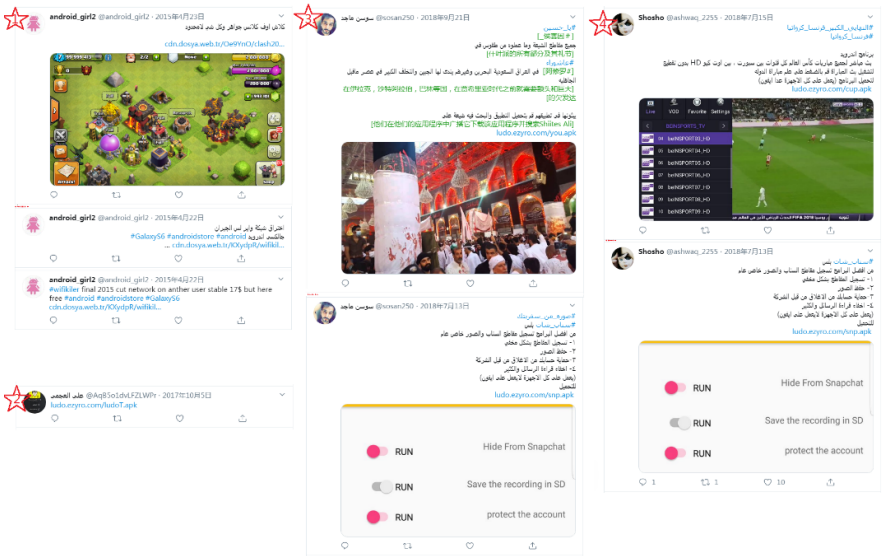

图3.7 四个攻击者在Twitter平台上发起的未定向钓鱼攻击片段

7. 此外还有一个钓鱼网站，目前看其主页面荒废了有一阵子，故在此略过。

（二）. 鱼叉攻击

在Twitter社交平台上，诺崇狮组织除了使用水坑攻击进行广泛传播外，还使用了数十次的定向鱼叉攻击。我们抽看了其中一些被该组织攻击的目标账号，有不少账号显示已被冻结或者在之后的很长时间里没有再更新过，成了永久的“沉默账号”。

图3.8 已发现到的Twitter平台上该组织最早攻击者发起的定向攻击片段

四. 攻击样本的诱导伪装形式

诺崇狮组织为避免攻击时被用户察觉到，对攻击样本采用了图标伪装和功能伪装两种形式。通过图标伪装攻击样本把图标换成正常应用的图标；通过功能伪装攻击样本除了带有在后台进行间谍活动的功能，还带有正常应用的功能支持在前端界面展现，让用户难于察觉。

（一）. 图标伪装

攻击样本伪装了几类软件的不同应用：游戏类应用(“Clash of Clans”和“Ludo”)、直播类应用(“Bigo live”和“world cup”注:红色的是大写的i字母，非字母L) 和一些工具类应用。

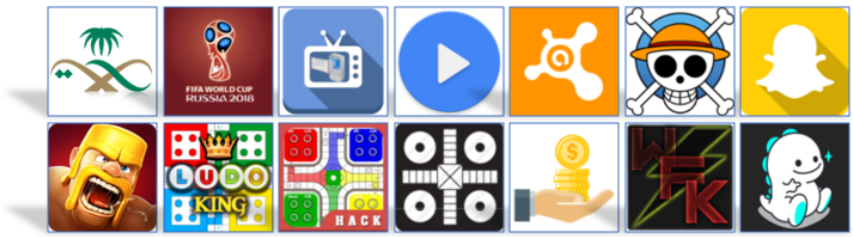

图4.1 恶意攻击样本采用的伪装图标

（二）. 带正常应用功能进行伪装

此次攻击样本进行带正常应用功能的伪装采用了两种伪装方式：一种是通过插包的方式，直接和正常应用整合在一起，整个过程只有一个应用；另一种是运行后，会释放出正常的应用包，诱导用户安装正常应用进行正常使用，而自身再进行隐藏图标，在后台进行间谍活动，整个过程实际有两个应用。

五. 攻击样本分析

至今，诺崇狮组织在其历史攻击活动里已使用了四种移动端的RAT，包括开源的RAT（AndroRat）和三种商业RAT（SandroRat、SpyNote及MobiHok）。这些RAT都是很成熟的间谍木马，用户手机一旦安装即刻能被攻击者完全控制。

（一）. Androrat

Androrat是一款开源在GitHub上的远程管理工具，包含有基本的远控功能，且可以根据自身能力扩展更丰富的监控功能，支持攻击者在PC上对受害用户手机进行远程操控。

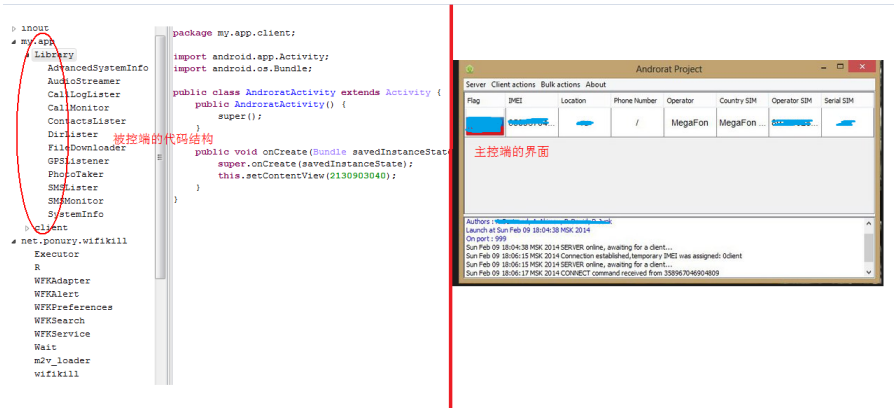

图5.1 Androrat被控端代码结构(左)和控制端管理界面(右)

（二）. DroidJack

Droidjack是一种非常流行的商业RAT，目前官方售价$210。其功能强大，支持在PC上对手机进行远程操控，使用很方便。

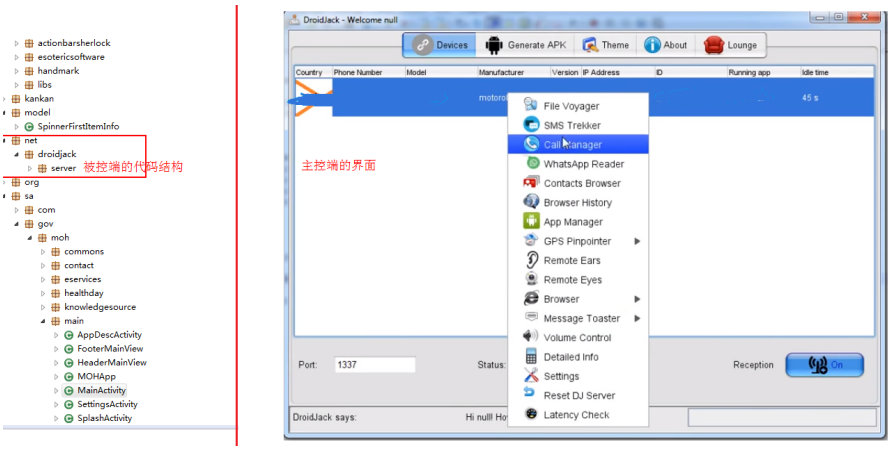

图5.2 Droidjack被控端代码结构(左)和控制端管理界面(右)

（三）. SpyNote

SpyNote类似Droidjack，也是一款流行的商业RAT。其支持的功能更丰富些，售价相对更贵，根据不同场景需求目前官方有两种价位($499和$4000)。

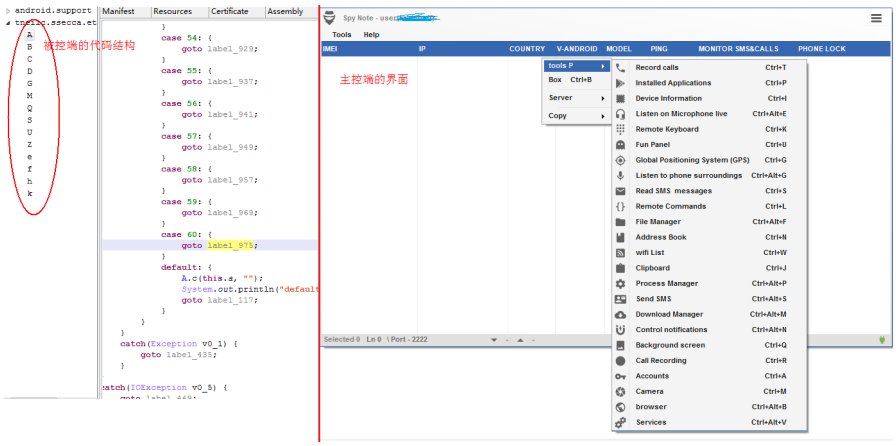

图5.3 SpyNote被控端代码结构(左)和控制端管理界面(右)

（四）. MobiHok

MobiHok价格不菲,有4种价位($700、$6500、$11000和$20000)，曾是阿拉伯地区流行的商业RAT，目前已被汉化引入，详情请参阅我们此前发布过的历史报告《阿拉伯木马成功汉化，多款APP惨遭模仿用于攻击》。

图5.4 MobiHok被控端代码结构(左)和控制端管理界面(右)

六. 攻击组织溯源分析

从整个攻击中，我们总结了诺崇狮组织以下特点：

1. 针对的目标包含：懂阿拉伯语的人、什叶派人等
2. 攻击活动时间活跃在：2015年4月22日（也门干预行动的“Operation Restoring Hope”当天）至2018年9月21日。
3. 攻击队伍较大，有大量的Twitter账号。
4. 根据两个攻击者间的交流目的是为了改变评论者，而攻击后的结果是被攻击者变成了“沉默账号”。

图6.1 Twitter平台上的两名攻击者间的一次交流

5. 其中一个攻击者第一条消息向账号“qahtan_tribe”发了个问候语，“qahtan_tribe”账号不久前还在使用卡塔尼的头像，结合该账号的信息及权力，看起来其甚至有着和Twitter一样地位的“权限”。

图6.2 Twitter平台上的一名攻击者的首条消息的问候

七. 总结

此次诺崇狮组织的攻击主要发生在公开的社交媒体平台。近几年，公开的社交媒体平台成为了某几个国家电子军的另一个战场，我们也看到多个社交媒体平台也都在致力应对，当然我们也知道这种威胁不是在短期能够解决避免的，这需要多方配合一起努力才能有效遏制。

如果你是公开的社交媒体平台的一名用户，请务必保持安全防范意识，安装上必要的官方来源安全防护软件，做好个人敏感隐私数据不在公开的社交媒体平台上或者甚至不公开，不轻易点击或者接收其他人发来的图片、视频及链接等!

而作为安全厂商，在这个万物互联的时代，如何根据不同的客户场景定制出对应的有效安全防护产品和策略，做到能及时查杀拦截及发现，做好保障住国家安全、用户生命财产安全及数据安全，是我们当下最首要需要攻克的命题，望一起坚定信念，不停探索，共同奋斗。

附录A：IOC

C2
samsung.apps.linkpc.net

MD5	AppName	CreateTime
ae6f0bd64ed0f2280c9d19a8108c3ae9	WiFiKill	2013-09-18 00:23
0b972efbaa5338d103f705b307a1d816	WiFiKill	2015-04-14 16:01
9f5626d244e29b546416cc9bba70bdbc	Clash of Clans	2015-04-22 09:40
58723a625eab5a3ba9e909e881cdb4e5	وزارة الصحة	2015-05-22 19:38
ced33d5b11980bdfa4f859a1dbcb2153	وزارة الصحة	2015-06-10 01:38
349e95ac3c12cf762c66ad264af552e7	healthfinal33	2015-06-10 03:40
17296ce181160cd963b0f32f747204e5	Ludo Stat	2017-09-14 03:39
ddf29d64a2c197f8a062c448ebf7ac19	ludo	2017-09-17 01:13
e48f99bb1720f64fe71ab091193e7bf8	Zudo	2017-09-18 04:02
62dcc4b974c156c684296dfff549d93d	zLudo	2017-09-19 06:55
d0213982edff32f2137ec946d1160fc3	yLudo	2017-09-20 02:48
1b7ce26fd5abd604c99ed0b0681455db	Avast	2017-09-22 07:40
ff34287974df6b7dc982c0d925eb9f76	Avast	2017-09-22 09:30
57926dd755016e11c98e9e9e43bb20c9	Avast	2017-09-25 16:53
ed8507053e3e02d3701bf9c94da2902d	Avast	2017-10-03 17:10
0b878cbc90814a4d5b09686b1cf61254	avast anti virus	2017-10-13 00:27
07ad82252e0f4971a7e2774480969bb5	Avas	2017-10-28 23:13
4f0f7186c88b92f701b5a64abce50486	Avast	2017-11-02 18:29
85bd302eb656bbad1339d5a6e93352e4	Avas	2017-11-02 20:01
2443e314d22251947f92c388479e7a34	Zavas	2017-11-03 01:09
e69a562296cd658192c3ad363bfc1d19	Zndroid	2017-11-10 01:39
12f433f958f9853c152ec1c9b27c6b28	Android	2017-11-10 04:20
bd2506b148cf8c56265405d4cfb2bfe0	zLudo	2017-11-11 10:04
d3062991398f87a229159f679741a8f9	Zone	2017-11-16 01:28
5220de45a564dc611d95be366092716b	App	2018-01-21 08:34
f83c777e447cbac0e774771c8b46695d	Bigo live	2018-02-01 00:33
5e4d10552edd2870ed0d1006deb398d1	world cup	2018-07-07 19:52

b7681f2e94920bf46ba23417d31c860b	world cup	2018-07-11 19:59
536da24fd43587477357e3bb92f0507e	Snapchat	2018-07-13 00:45
ea5c8f89d0b33ed70495c0b63cee06c6	uSnapChat	2018-07-17 00:51
b0bdb1e3ee0b7fd048ad982684227133	Player	2018-08-02 18:45
c883c5c8dac7e3b71898fdaa67fae3c9	avast anti virus	2018-08-06 18:25
f88569ba93c08ab1e27824c293493c7d	Player	2018-08-13 01:36

FileMd5	DownloadUrl
0b972efbaa5338d103f705b307a1d816	http://cdn.dosya.web.tr/KXydpR/wifikillfinal3_9.apk
9f5626d244e29b546416cc9bba70bdbc	http://cdn.dosya.web.tr/Oe9YnO/clash2015.apk
b7681f2e94920bf46ba23417d31c860b	http://ludo.ezyro.com/cup.apk
b0bd-b1e3ee0b7fd048ad982684227133	http://ludo.ezyro.com/FB.apk
f88569ba93c08ab1e27824c293493c7d	http://ludo.ezyro.com/you.apk
e69a562296cd658192c3ad363bfc1d19	http://ludo.ezyro.com/SMS.apk

附录B：参考信息

《纽约时报》：Saudis' Image Makers: A Troll Army and a Twitter Insider

《纽约时报》：Former Twitter Employees Charged With Spying for Saudi Arabia

《纽约时报》：Someone Tried to Hack My Phone. Technology Researchers Accused Saudi Arabia.

《华盛顿邮报》：Former Twitter employees charged with spying for Saudi Arabia by digging into the accounts of kingdom critics

公民实验室(CitizenLab)：Stopping the Press

New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator

《Vice》：How 'Mr. Hashtag' Helped Saudi Arabia Spy on Dissidents

《贝灵猫》：Lord Of The Flies: An Open-Source Investigation Into Saud Al-Qahtani

Twitter通告：New disclosures to our archive of state-backed information operations