军刀狮组织（APT-C-38）攻击活动揭露

一、 概述

从 2015 年 7 月起至今，军刀狮组织（APT-C-38）在中东地区展开了有组织、有计划、针对性的不间断攻击。其攻击平台为 Windows 和 Android，截止目前 360 烽火实验室（360 Beaconlab）一共捕获了 Android 平台攻击样本 25 个，Windows 平台攻击样本 4 个，涉及的 C2 域名 16 个。

2018 年 5 月，Kaspersky 安全厂商发表报告《Who’s who in the Zoo》，首次批露该组织为一个未归属的专注于中东目标的间谍活动组织，并命名 ZooPark，涉及的攻击武器共包含四个迭代版本的 Android 端 RAT，载荷投递方式包括水坑和 Telegram 频道。

2019 年，360 烽火实验室捕获到军刀狮组织的最新攻击活动，除发现 Android 端攻击外还发现该组织带有 Windows 端攻击，其中 Android 端 RAT 仍属于第四代。我们结合 APT 攻击的地缘政治因素、攻击组织使用的语言以及该组织发起的历史攻击活动，分析后认为该组织是位于西亚的中东某国家背景的 APT 组织。**另在此感谢我们的兄弟团队----360 高级威胁应对团队**对本报告 Windows 端 RAT 内容的完成。

由于军刀狮组织的攻击目标有一个主要的特色目标是西亚中东某国的库尔德人，另 Windows 端 RAT 包含的 PDB 路径下出现多次的“Saber”，而亚洲狮为该中东国家的代表动物，结合该组织的一些其它特点以及 360 对 APT 组织的命名规则，我们将该组织命名为军刀狮（APT-C-38）。

图 1.1 军刀狮关键攻击活动时间事件点

二、 载荷投递和网络基础设施

军刀狮组织载荷投递的方式主要为水坑攻击和 Telegram 频道。需要注意的是该组织在 2018 年 5 月初被首次披漏后，攻击组织在当月月底使用了新一批的网络基础设施。

- **水坑攻击**

目前已发现有两家在中东地区流行的阿拉伯新闻报纸网站（科威特 Annahar 和埃及 Al-Nahar）曾被该组织用来水坑攻击。

图 2.1 埃及 Al-Nahar 网站

- Telegram 频道

除了上面两个针对指定中东地区阿拉伯国家的水坑攻击外，我们还发现到该组织在攻击其主要的攻击目标中东某国的库尔德人时多采用 Telegram 频道传播（如伊斯兰议会前对库尔德斯坦省选举攻击和库尔德斯坦省马里万萨南达季的抗议活动攻击等）。

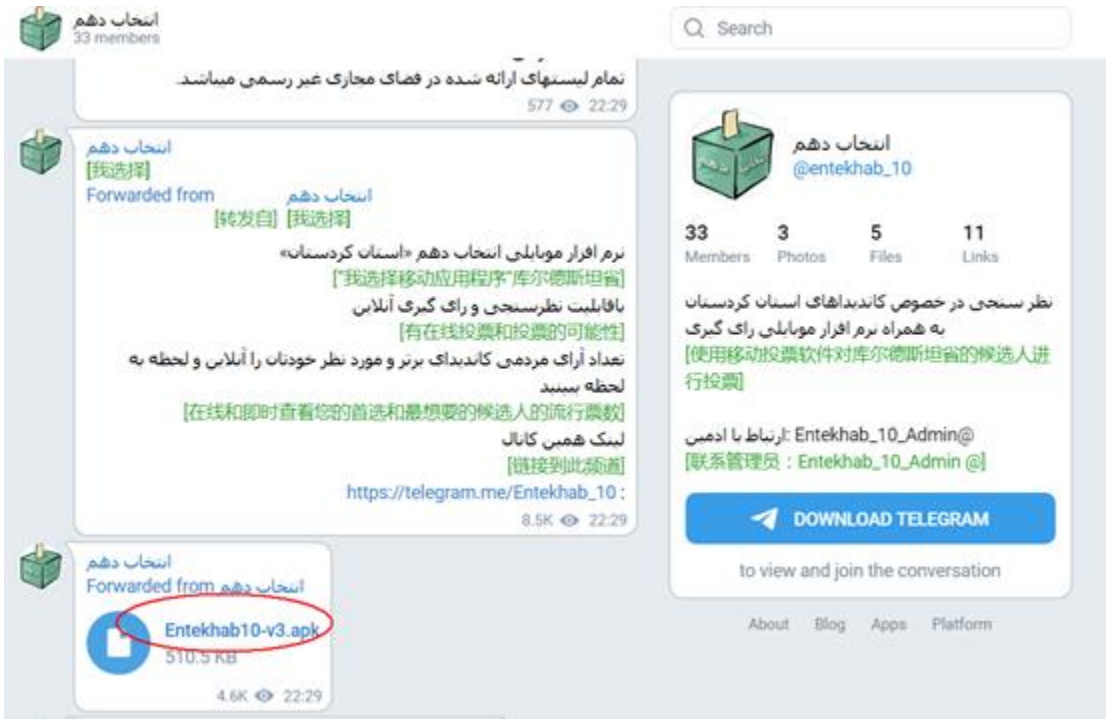

图 2.2 伊斯兰议会前对库尔德斯坦省选举攻击的 Telegram 频道

- 网络基础设施

至今军刀狮组织已经使用了多个网络基础设施。

表 1 军刀狮组织使用的网络基础设施

Server	Description	Registrant Country'City	Registrant Phone	Registrant Email	Registrant Postal Code
rhubarb2.com	C2 server	IR'Sanandaj	+98.93039382 51	pilton86@yahoo.com	6614478527
rhubarb3.com	C2 server	PrivacyProtect	PrivacyProtect	PrivacyProtect	PrivacyProtect
androidupdaters.com	Intermediate service（image）	IR'Tehran	+98.21885612 12	asgharkhof@gmail.com	9865214523
dlgmail.com	Intermediate service（image）	IR'Tehran	+98.21888882 99	silent.city2020@mail.com	1663976888
dlstubes.com	Intermediate servi	IR	+98.88775887 98	boldman.sam@mail.com	1558738817

Server	Description	Registrant Country'City	Registrant Phone	Registrant Email	Registrant Postal Code
	ce（image）				
googleupdators.com	Intermediate service（image）	IR	+98.88775887 98	boldman.sam@mail.com	1558738817
adobeactiveupdates.com	Intermediate service（image）	IR	+98.88775887 98	boldman.sam@mail.com	1558738817
adobeseupdater.com	Intermediate service（image）	IR'Tehran	+98.21778889 91	boldman.sam@mail.com	11155679
dlstube.com	Intermediate servi	IR'Tehran	+98.21226945 75	kimkallian@gmail.com	1771798635

Server	Description	Registrant Country'City	Registrant Phone	Registrant Email	Registrant Postal Code
	ce（image）				
adobeactiveupdate.com	Intermediate service（image）	IR' Tehran	+98.91061451 78	sirus_virus6688@yahoo.com	2417682380
5.61.27.154	null	null	null	null	null
5.61.27.157	null	null	null	null	null
5.61.27.173	null	null	null	null	null
91.109.23.175	null	null	null	null	null

需要注意的是其在 2018 年 5 月 23 日新申请了一批网络基础设施，最新的移动端攻击载荷于 2019 年 3 月部署在其中的一个服务器，这批中间服务器共有 4 个，有 3 个至今仍存活且解析后实对应同一 IP，这批服务器充当着 PC 端和移动端 RAT 的中间服务器角色。

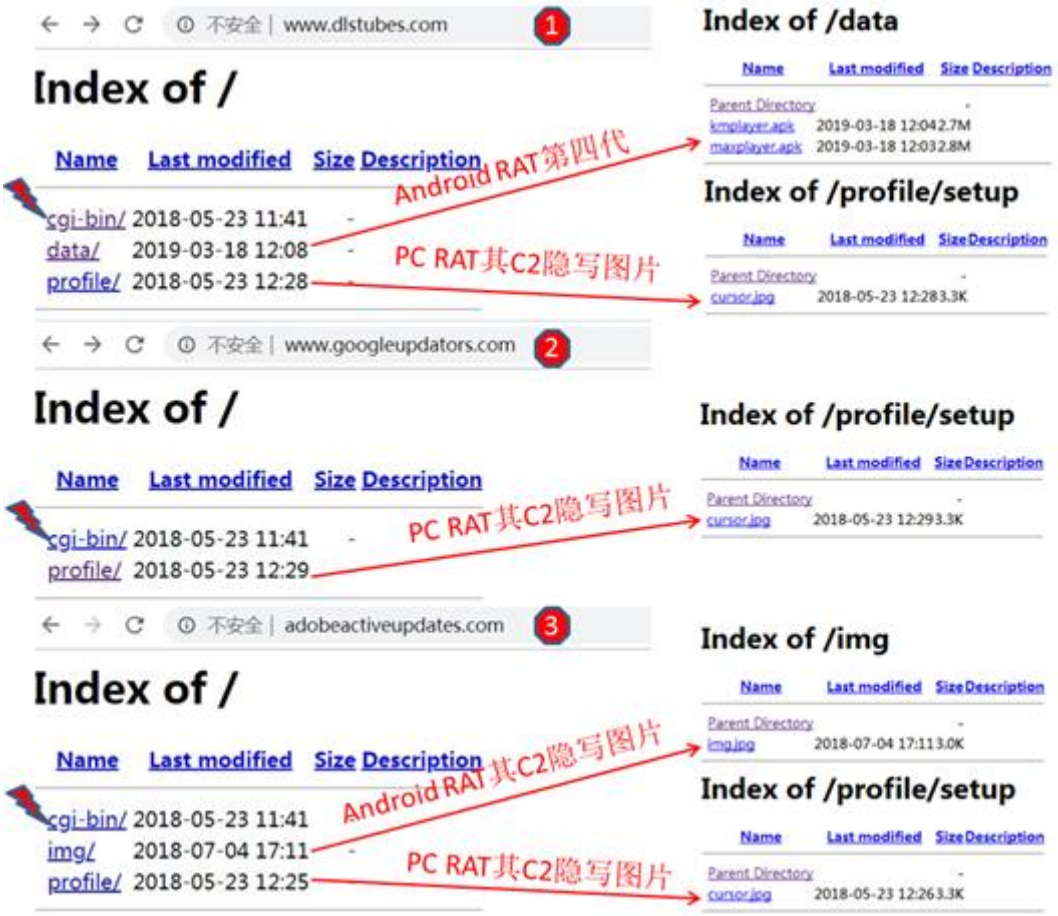

图 2.3 被披露后军刀狮组织当月新部署的一批网络基础设施

三、 诱导方式

军刀狮组织在这次行动中主要使用以下两种诱导方式：

- 含有正常 APP 功能的伪装

为更好的躲避被察觉到，除了对文件图标进行伪装外，还会在 RAT 启动时显示出正常的 APP 界面，目前四个迭代版本的 Android 端 RAT，运行后均会展示出正常界面，但在运行时或者接收到指定广播时，便开启在后台进行的间谍活动。

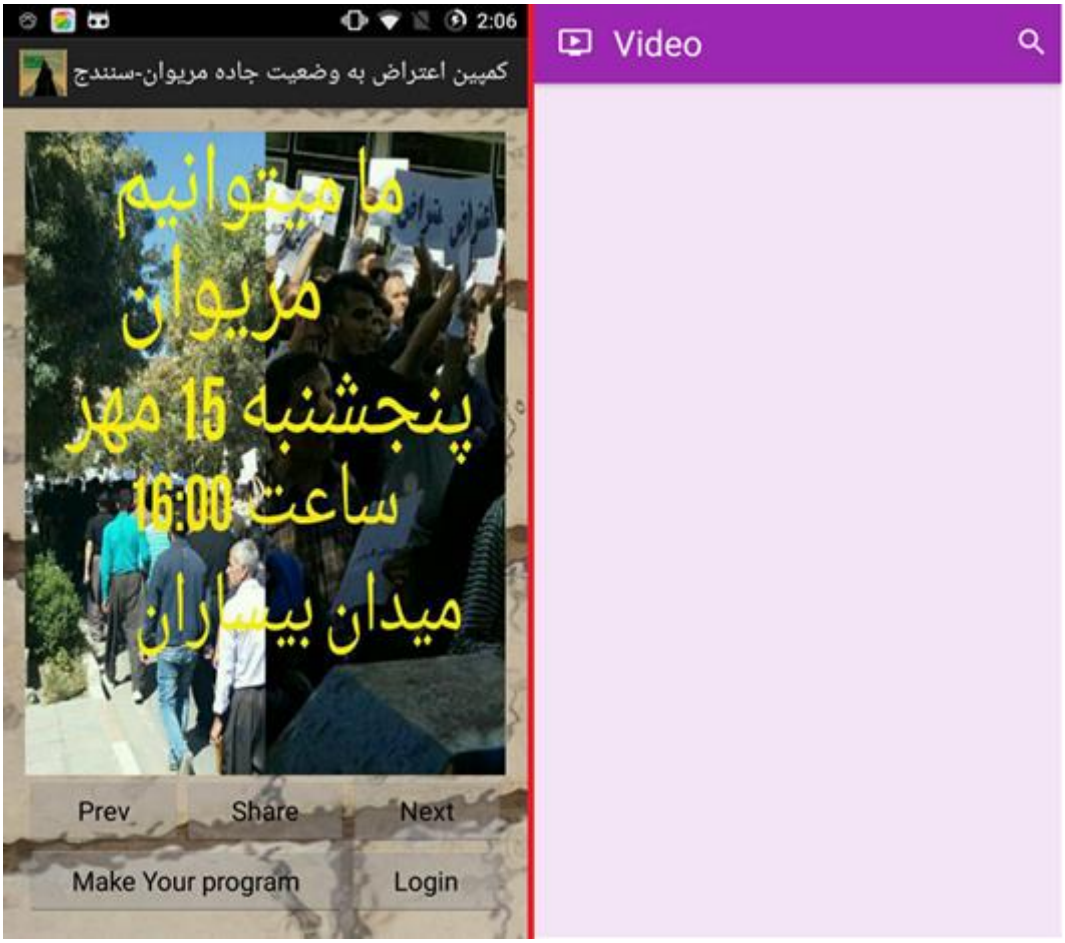

图 3.1 第二代和第四代的 Android 端 RAT 运行后展示举例

- 文件图标伪装

图 3.2 伪装的应用软件图标

四、 RAT 攻击样本分析

截至目前，军刀狮组织已使用到针对 Android 和 Windows 平台的不同 RAT，经过分析，我们认为最新的 Android 端 RAT 和 PC 端 RAT 应该购买自同一个商业开发组织，其中一名开发者昵称为“Apasec”。

- Android

Android 端共使用到四个迭代的 RAT，本报告中我们仅介绍最新攻击活动使用的第四代 RAT，我们命为 UnitMM，该 RAT 目前仅在军刀狮组织中出现，其它版本 RAT 的信息可参考本报告前面提到的 Kaspersky 安全厂商报告。

UnitMM 军刀狮组织的第四代 RAT。根据该 RAT 包含的类名和使用到的数据库名等，我们命名为 UnitMM。最新版本的 UnitMM 通过默认的数十个功能配置，进行控制窃取短信、通讯录、地理位置、浏览器书签和搜索历史记录、剪切板信息、外部指定的应用程序数据、捕捉照片/视频/音频等多种恶意行为。

此外 UnitMM 还能响应来自 C2 的指定指令进行交互。

表 2 C2 指令与功能对应表

指令	功能
2	更新恶意功能配置
4	执行 shell 命令
6	将指定的文件/文件夹压缩并保存到预设目录
8	将任务内容写入临时 zip 文件，从中提取所有内容并将其删除
10	将指定的文件/文件夹复制到指定的目录
12	将指定的文件/文件夹移动到指定的目录
14	重命名指定的文件/文件夹
16	删除指定的文件/文件夹
18	创建指定的目录
20	静默发送指定的内容短信到指定的号码
22	拨打指定号码电话

指令	功能
24	获取指定路径下的文件列表信息并将其保存到预设目录
26	更新中间服务器(C2 隐写图片)列表

- Windows

Windows 端目前发现到一种 RAT，我们命为 SpecialSaber，该 RAT 目前仅在军刀狮组织中出现，共有 4 个。

SpecialSaber 这是一个之前未被曝光的 RAT。根据最新版 PDB 路径下的目录名，我们命为 SpecialSaber。其具有检测杀软（包括 Bitdefender、Kaspersky、Avira、Avast、AVG、ClamWin、ESET、Norton、McAfee、Panda、Symantec），窃取多种浏览器信息、多种邮箱信息、用户帐户信息、磁盘文件信息等，并带有键盘记录及截屏等多种恶意行为。窃取后的各种信息后会以文件的形式保存在自身的工作目录中，文件名为随机生成的字符串，文件统一用指定的格式进行存储。

图 4.1 用统一格式存储的截图文件举例

表 3 部分文件类型数值与文件含义对应表

文件类型数值	对应的文件含义
1	屏幕截图，jpeg 格式
2	每个驱动器所有文件列表，包括目录、文件名、文件大小信息
3	键盘记录
4	FireFox、Chrome、IE、Opera、Safari、Thunderbird、Outlook 的账号密码信息
5	FireFox、Chrome、IE、Opera、Safari 浏览器的历史记录
6	FireFox、Chrome、IE、Opera、Safari 浏览器的书签信息
7	Yahoo Messenger 账号密码信息
8	用户帐户列表和每个帐户的详细信息
9	逻辑驱动器的大小，剩余空间和驱动器号
10	所有适配器的完整 TCP/IP 配置
14	Zip 压缩的文件
24	操作系统的详细配置信息，包括杀软信息、产品 ID 和硬件属性等

此外 SpecialSaber 还能响应来自 C2 的指定指令进行交互。

表 4 部分 C2 指令与功能对应表

指令	功能
3	创建指定的目录
4	重命名指定的文件/文件夹
6	文件下载
7	文件压缩加密 (Zip、AES)
10	获取 FireFox、Chrome、IE、Opera、Safari、Thunderbird、Outlook 的账号密码信息
11	获取 FireFox、Chrome、IE、Opera、Safari 浏览器的书签信息
12	获取 FireFox、Chrome、IE、Opera、Safari 浏览器的历史记录
14	获取卸载程序列表的名称
16	获取逻辑驱动器的大小，剩余空间和驱动器号
17	获取所有适配器的完整 TCP/IP 配置
18	获取用户帐户列表和每个帐户的详细信息
25	获取 Yahoo Messenger 账号密码信息

- 疑似购买自同一家商业开发公司

通过把 Android 端的 UnitMM RAT 和 Windows 端 SpecialSaber RAT 进行比较，我们看到两者在 C2 通信环节采用了相似的手法，且两者窃取的信息有特殊的共同性，我们认为两者应该来自同一个商业开发组织。

此外我们在一个 PDB 的路径中发现一个名为“Apasec”的开发者，我们发现这个名字曾多次出现在该组织移动端的 C2 panels 中，这个发现更加验证了我们的判断。

五、 受攻击地区分布情况

截至目前，360 烽火实验室发现此次军刀狮组织攻击活动影响到的国家共有 7 个，其中伊朗受影响最为严重，这和我们分析过程中发现到该国家的库尔德人受到几次的针对攻击活动不无关系。

图 5.1 受攻击的地区分布情况

六、 攻击者画像

基于攻击者几次特别的针对攻击、使用的语言以及 APT 攻击的地缘政治因素等，我们总结了该攻击组织以下的画像观点：

- 熟悉波斯语，阿拉伯语，其中波斯语使用最为频繁。
- 主要针对位于西亚的中东某国其某省的库尔德人，能实时甚至提前对其某些时刻的活动进行部署相应的攻击，此外也针对中东数个阿拉伯国家。
- APT 攻击大部分基于内部局势和地缘政治因素（本国或敌对国家）。
- 从受害者的背景以及攻击行动的持续时间来看，攻击者所关注的目标在政治和战略层面有重大意义，且持续时间较长。

综上所述，360 烽火实验室认为攻击者为来自位于西亚的中东某国家背景的 APT 组织。

七、 总结

近几年，我们看到 APT 攻击随着时代的发展，PC 端不再是独有的目标，越来越多的攻击组织同时会把移动端作为攻击的另一必备目标，甚至频繁投入于中东和亚太地区部分国家背景支持下的网络战争中。

APT 攻击发展迅速，尤其是移动端攻击的发展。我们看到前几年有些攻击组织能力还比较简陋，甚至一些安全厂商采用小猫等称呼进行命名表示对对应攻击组织攻击能力的低度尊重。但随着攻击获取到的价值效益，攻击组织加大投入力度，我们看到攻击越来越复杂，针对性和实效性越来越强，以前面的小猫为例进行形容的话，犹如年轻的小猫渐成成熟的狮子。此次军刀狮组织无疑又是 APT 攻击发展中的一个典型代表，另基于该组织的特殊背景及其隶属国家当下的时势我们认为该组织的攻击可能会有新一轮的变化。

附录 A：样本 MD5

	Android 攻击样本 MD5	Windows 攻击样本 MD5
2.	0745b0957aab92b6a09645e076b4f339	5b0431bbebdc48d2fa37882f7343b011
3.	1874aa71c9b13eec5b587e8ed6a71606	31edb7591bfeeb72e0652c17781640af
4.	191cc5d165472ae19e665821be71c282	58cc3935fbfdb2990304b99fbb919dad
5.	232bd3dde6914db0a3dbfc21ed178887	848193568a48f5742135667e9842890a
6.	2d91f7d1eb0d32ece0a8b1715a70b4cd	
7.	345c2325dd633099f29b6d7141a4703d	
8.	451ff729eaa1cf26943a812cd37eb4ac	
9.	4d8ddec9243bc6ac0419c561fe413cfc	
10.	519018ecfc50c0cf6cd0c88cc41b2a69	
11.	5ad36f6dd060e52771a8e4a1dd90c50c	
12.	5efddd7f0fc2125e78a2ca18b68464ec	
13.	699a7eedd244f402303bcffdee1f0ed1	
14.	6a388edbce88bb0331ae875ceeb2f319	
15.	73b0a3cae8510dd2efeca7d22f730706	
16.	7b530999847bbf43e7d6cbb76da684ae	
17.	7d7ad116e6a42d4e518378e2313e9392	
18.	a7d00c8629079f944b61c4dd5c77c8fb	
19.	a856f9de281cadad7142828dda3843b4	
20.	ac4402e04de0949d7beed975db84e594	
21.	b44b91b14f176fbf93d998141931a4aa	
22.	b714b092d2f28fcf78ef8d02b46dbf9c	
23.	c7e4d75caa8e07847e47eadce229c288	

24. cb67abd070ae188390fc040cbe60e677
25. e2f62b5acf3795a62e9d54e1301c4e7b
26. ec5a6f0e743f4b858aba9de96a33fb0c

附录 B：C&C

1. **rhubarb2**.com
2. **rhubarb3**.com
3. **androidupdaters**.com
4. **dlgmail**.com
5. **dlstubes**.com
6. **googleupdators**.com
7. **adobeactiveupdates**.com
8. **adobeseupdater**.com
9. **dlstube**.com
10. **adobeactiveupdate**.com
11. 5.61.27.154
12. 5.61.27.157
13. 5.61.27.173
14. 91.109.23.175
15. **solar64**.xp3.biz
16. **entekhab10**.xp3.biz

附录 C：PDB

1. C:\Users\apasec110\Desktop\Saber1\client\Saber1-Develop\Release\Saber1-Dev.pdb
2. C:\Users\apasec110\Desktop\Saber1\client\editing saber\Saber1-Develop-changed\Release\Saber1-Dev.pdb
3. C:\Users\M&M\Desktop\Saber1\Special-Saber1-Windows-Client-binder_backup(last stable socket communication)\Release\Saber1-Dev.pdb
4. C:\Users\M&M\Desktop\Saber1\Special-Saber1-Windows-Client-binder_backup\Release\Saber1-Dev.pdb

附录 D：参考链接

1. [1] https://en.wikipedia.org/wiki/Entekhab
2. [2] https://en.wikipedia.org/wiki/Islamic_Consultative_Assembly
3. [3] https://en.wikipedia.org/wiki/Annahar_(Kuwait)
4. [4] https://www.alnaharegypt.com/
5. [5] https://en.wikipedia.org/wiki/2017_Iraqi_Kurdistan_independence_referendum