#### 军刀狮

**别称:**

ZooPark

**可能操作来源:**

位于西亚的中东国家

**目标:**

位于西亚中东某国的库尔德人

* 阿尔及利亚
* 埃及
* 土耳其
* 伊拉克
* 伊朗
* 阿富汗
* 科威特

**(CFR) 事件类型:**

间谍行为

**组织简介:**

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。

军刀狮组织的关键攻击事件包括：

* 2015年11月到2016年伊朗议会选举前夕，创建了伊朗Entekhab媒体的Telegram频道，针对其中库尔德斯坦省得选举进行攻击；
* 2016年8月对多家流行的阿拉伯新闻媒体网站进行水坑攻击（科威特、埃及）；
* 2016年10月6日到当月底，对伊朗库尔德人在库尔德斯坦省马里万萨南达季的抗议活动进行攻击；
* 2016年11月到次月底，针对库尔德人的“HDP Is Not Alone”活动进行攻击；
* 2017年9月23日，提前针对两天后25日的库尔德斯坦独立公投进行攻击；
* 2018年5月，伪装APP进行攻击（DrpFirewall、VPN Easy、DeleteTelegram）；
* 2019年，PC端和Android端都启动了新一轮攻击，包括伪造Android端的两款流行的播放器（KMPlayer、Max Player）。

军刀狮组织攻击平台为Windows和Android。其载荷投递的方式主要为水坑攻击和Telegram频道。其诱导方式主要为：伪造含有正常功能的APP和通过设置文件图标来伪装。其在Android和Windows平台使用了不同的RAT：其中Android端共使用到四个迭代的RAT，第四代RAT被命为UnitMM，该RAT目前仅在军刀狮组织中出现；Windows端目前发现到一种RAT，被命为SpecialSaber，该RAT目前也仅在军刀狮组织中出现。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，猜测两者应该来自同一个商业开发组织。

**参考链接:**

* https://blogs.360.cn/post/analysis-of-APT-C-38.html