移动端跨越攻击预警：

新型APT攻击方式解析



****

2018年7月12日

随着信息技术的发展，移动存储介质由于其具有体积小、容量大的特点，作为信息交换的一种便捷介质，如今已经得到广泛应用，在个人、政府和企业中经常被使用。但也因此而来一直存在着持续的各种安全攻击问题，每当出现一种新型的移动存储介质，之后总会有一系列随之而来的攻击事件发生，举例历史两个“著名”的攻击事件：在中国，你应当听说过“熊猫烧香”病毒；在海外，你或者听说过微软重金悬赏的“Conficker”病毒。幸运的是微软2011年开始对Windows自动运行功能进行了限制，屏蔽了除光盘外的其它存储介质的自动运行功能，避免了利用自动运行功能来进行攻击的主要攻击方式。

移动端手机不仅仅是手机身份，很多时候它也经常同时成为移动存储介质身份(借助USB线连接或者网络进行实现)，一部分人甚至用它取代了其它移动存储介质，那么移动端手机会不会也已经开启了这种安全隐患？不幸的是，近期360烽火实验室在监测黄金鼠组织(APT-C-27)的攻击活动过程中，发现其新版本的移动端手机攻击样本首次具备了针对PC的RAT诱导跨越攻击，开启了移动端手机跨越攻击的“潘多拉魔盒”。

## 攻击样本的来源

此次新版移动端手机攻击样本的来源和360追日团队之前发布的报告[《黄金鼠组织--叙利亚地区的定向攻击活动》](https://ti.360.net/blog/articles/analysis-of-apt-c-27/)提到的来源类似，目前我们共发现到有两个相似名称的来源地址(见图1.1和图1.2)在进行迷惑传播，其中一个来源域名(chatsecurelite.us.to) 在之前的报告中出现过。而PC端RAT的攻击样本“hmzvbs”则直接嵌入在新版本的移动端手机攻击样本中。

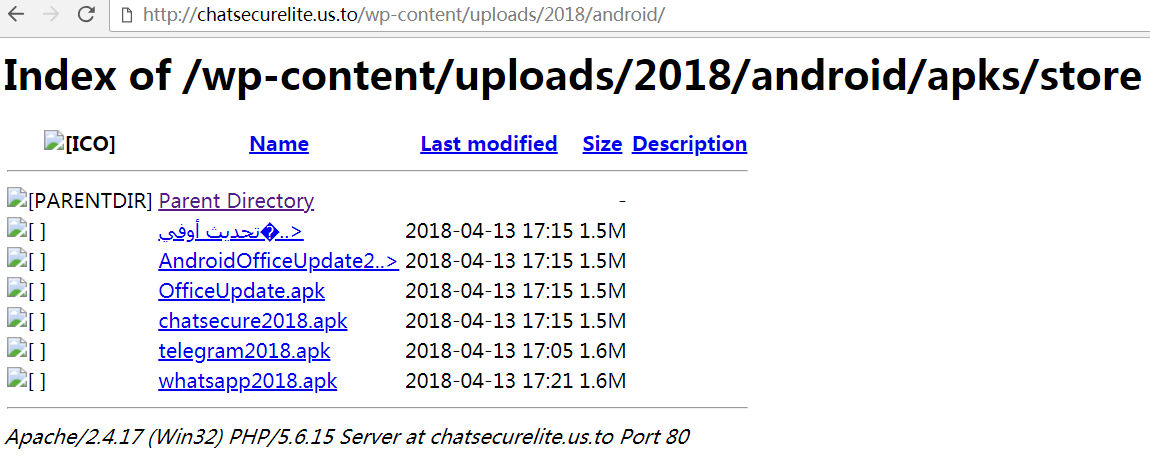


图1.1 来源地址一: chatsecurelite.us.to

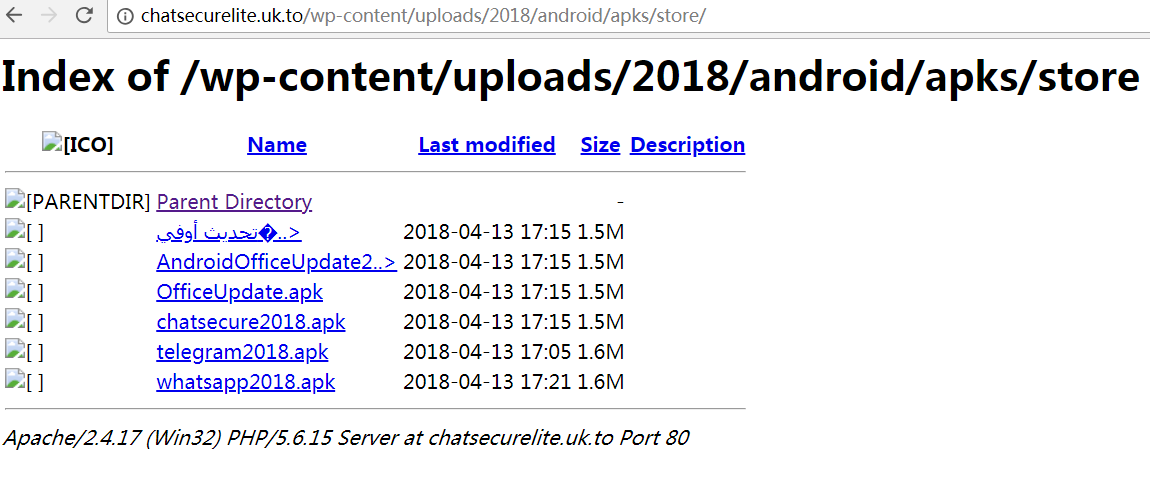


图1.2 来源地址二: chatsecurelite.uk.to

上述两个来源的域名名称相似，包含的内容相同，我们通过反查分析发现到两个域名实际是指向同一个ip，且关键的是该ip和该组织目前正在使用的C&C (82.137.255.57)正好一致。这意味着该组织使用的ip(82.137.255.57)至少在攻击中充当着钓鱼传播和远程控制两种用途。

## 攻击样本的分析

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，此次攻击新增移动存储介质诱导攻击方式，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”(见图2.1)。

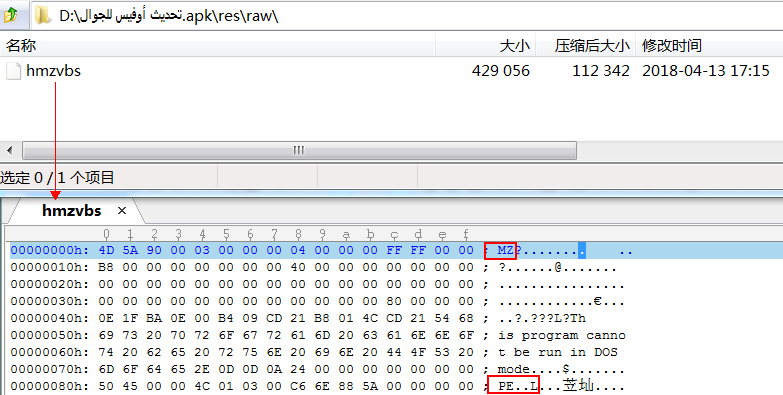


图2.1 携带的PE RAT攻击文件

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(见图2.2)。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)。

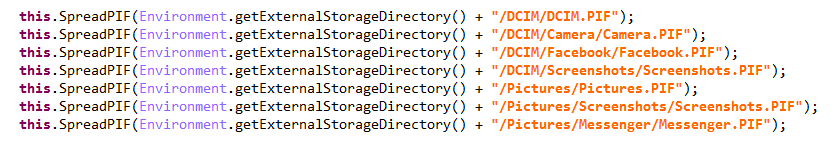


图2.2 跨越攻击前的特殊伪装准备

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2.3)，即运行起该PE RAT攻击文件，从而使PC遭受RAT攻击。



图2.3我们把正常目录和伪装后的攻击文件放一起进行对比虚拟图

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，对应的RAT功能分别和前文提到的360追日团队发布报告中分析的Android端RAT和PC端RAT功能基本保持一致，具体可查看之前分析报告的指令功能关系图表。

## 攻击危害及分布情况

黄金鼠组织(APT-C-27)攻击的目标是叙利亚及其周边的军事机构和政府机关。目标人群的办公、日常生活中通常都与手机和电脑紧密联系在一起。若手机和电脑一旦被成功攻破，就可能会造成不可预估危害和损失。

该组织长期对该地区实行多次的针对攻击，我们通过分析此次受攻击的地区主要分布在土耳其、约旦、叙利亚(见图3.1)同时此次出现的包含特殊含义的攻击者测试路径(见图3.2)，这在某种程度上更让我们相信该组织的攻击或已改变一场战争或者政治活动的走向。

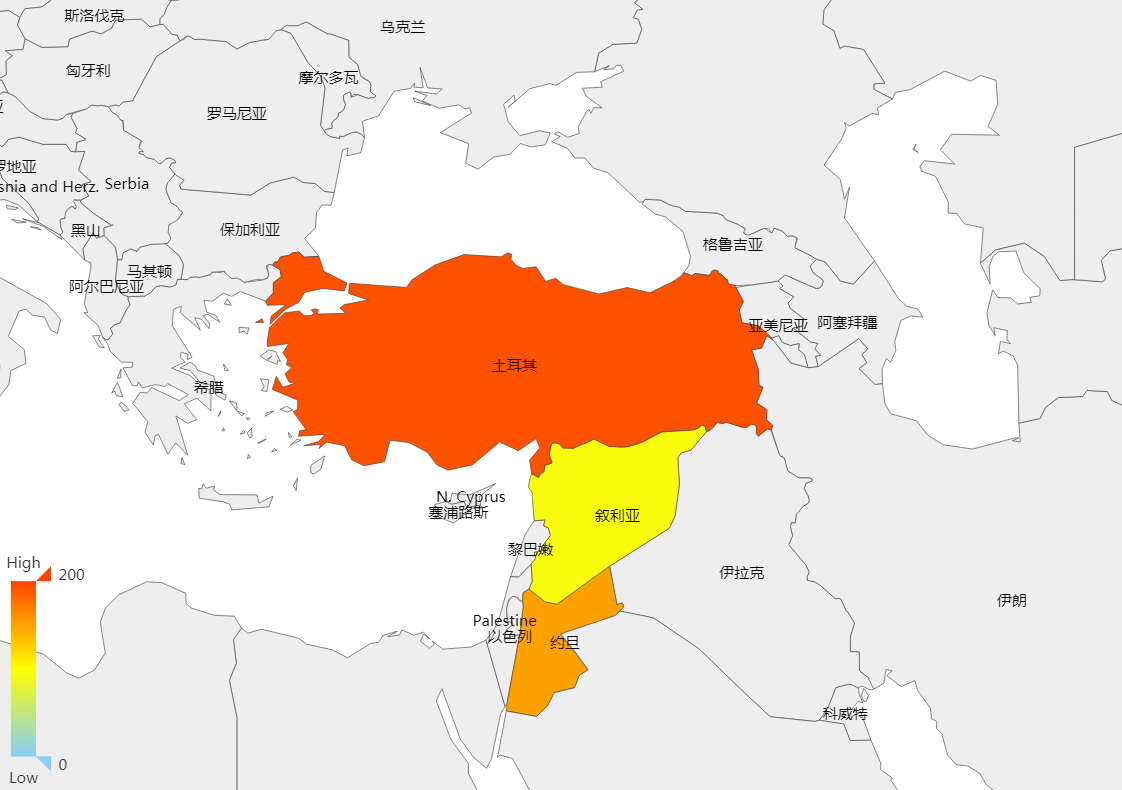


图3.1受攻击的主要地区分布统计情况(土耳其、约旦、叙利亚)

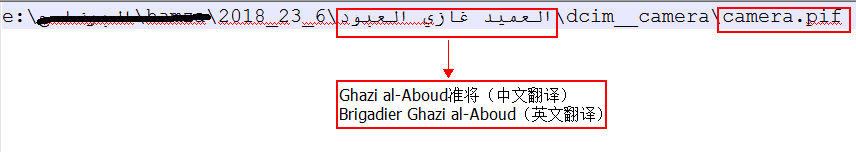


图3.2黄金鼠组织测试PC RAT时，采用的带阿拉伯语的特殊含义路径

## 攻击者---黄金鼠组织画像

我们根据此次攻击的情况信息，综合360追日团队之前公开的报告总结了下面黄金鼠组织(APT-C-27)的特点画像：

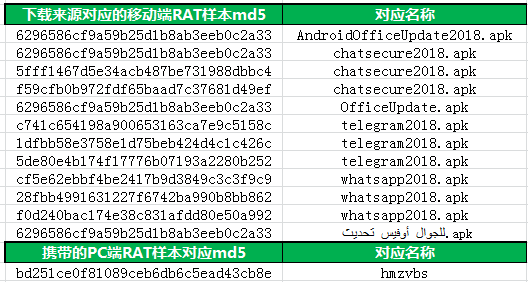
* 熟悉阿拉伯语，具有高度组织化、专业化的黑客组织；
* 长期针对叙利亚及其周边军事机构和政府展开有组织、有计划的持续性攻击；
* 擅长采用水坑攻击的钓鱼攻击，一般通过社交网站或者社交应用进行诱导传播。

## 预警及建议

在当下，智能手机已成为人们生活中不可分割的一部分，它影响到个人的隐私和财产安全，甚至影响着企业和国家安全，因此移动端的安全防护必不可少。移动端的安全防护，不仅要做好它作为手机身份的安全防护，同时也不要忽略它作为移动存储介质另一层身份的安全防护。此次新型跨越攻击，移动端手机真正被首次主动当作移动终端跨界攻击PC端中的跳板用来实行攻击。可以预见在不远的明天，可能会有加密勒索、蠕虫破坏等性的攻击方式出现，如同U盘移动传输介质历史出现过的攻击一样丰富；值得注意的是手机不像U盘那样，只靠USB来传播，单靠传统的USB屏蔽防护还不够，它还能直接利用网络来进行传播(如APP间的交互)，在此我们有以下几点安全提示：

* 企业做好自身的安全防护时，一定要加强内部人员的个人安全意识，很多时候攻击往往是从个人开始的；
* 做好网络隔离防护，如需要网络环境，在内部则不要轻易的直接打开、下载并运行第三方来源的链接内容(即使是熟人发送的信息)；
* 做好硬件隔离防护，可当作移动传输介质的手机、U盘等不要轻易直接连接办公PC进行使用；
* 使用可信的企业版软硬件安全防护产品做好实时防护，定期数据隔离备份等。

## 附录A：样本md5



## 附录B：C&C

82.137.255.57

## 附录C：参考链接

360追日团队《黄金鼠组织—叙利亚地区的定向攻击活动》报告链接：<https://ti.360.net/blog/articles/analysis-of-apt-c-27/>