# 疑似APT-C-56（透明部落）针对恐怖主义的攻击活动分析

By 360烽火实验室

Archived: 2026-04-05 16:35:45 UTC

**APT-C-56**
**透明部落**

由于巴基斯坦国内自身独特的宗教、民族、历史等因素以及外部力量的干预与支持，巴基斯坦已成为世界上深受恐怖主义威胁的主要国家之一，其经济发展以及社会现代化转型深受恐怖主义的掣肘。恐怖主义不仅对巴基斯坦自身的国际形象与国内社会政治经济发展造成了严重威胁，也对南亚地区的和平与安全产生了深远影响。

近期，360烽火实验发现了一批疑似APT-C-56（透明部落）针对恐怖主义发起攻击的恶意样本，通过溯源关联分析发现，攻击活动至少开始于2018年6月，至今仍处于活跃状态。攻击中使用样本涉及Android和Widows平台。

## 一、攻击活动分析

攻击者分别使用了Android和Window 平台的远控工具，其中Android平台攻击样本使用了商业间谍软件SpyNote和SonicSpy，以及开源间谍软件AhMyth和Metasploit；Windows平台使用了开源远控工具AsyncRAT。

### 1.Android端样本分析

Android平台攻击样本主要伪装成恐怖主义相关样本以及工具类样本，如Explosive_course（爆炸物课程）、Abdul Rasheed（巴基斯坦伊斯兰原教旨主义者和圣战活动家）、Bolan Attack Video（俾路支解放军攻击视频），样本对应的图标如下所示：


图1 Android 样本图标

#### 1.1.SpyNote

SpyNote 是一款功能强大的商业间谍软件，具有强大的功能，以及管理平台。其主要功能为：

- 文件管理
- 短信管理
- 通话记录管理

- 联系人管理
- 位置管理
- 账号管理
- 键盘记录
- 手机设置
- 拨打电话
- 拍照、录音、录像
- 实时录音
- 实时录像
- 获取应用列表
- 执行shell命令
- 聊天功能

SpyNote控制端界面如下图所示：

图2 SpyNote控制端

### 1.2.SonicSpy

SonicSpy是一款疑似伊拉克开发者开发的间谍软件，支持73中不同的远控指令，其主要功能为：

- 静默录音
- 拍照
- 拨打电话
- 向攻击者指定的号码发送短信
- 获取联系人列表
- 获取通话记录
- 获取WIFI接入点信息

图3 SonicSpy包结构

### 1.3.AhMyth

AhMyth开发的一款开源的远控管理平台，其中该平台使用的远控工具主要有以下功能：

- GPS记录
- 麦克风录音
- 查看联络人
- 短信记录
- 发送短信
- 通话记录
- 查看已安装的应用
- 查看已获取的权限
- 实时剪贴板记录
- 实时通知记录
- 查看WiFi网络记录
- 文件浏览器和下载

图4 AhMyth 包结构

### 1.4.Metasploit

Metasploit是一款开源的渗透测试框架，它本身附带数百个已知软件漏洞的专业级漏洞攻击工具，可以针对多种平台进行安全检测，验证漏洞的缓解措施。Metasploit Android payload 则是Metasploit框架针对Android 系统的一个有效负载，可以针对Android设备的渗透工具。攻击者将Metasploit打包进正常的APK中进行攻击活动，其包结构如下图所示。

图5 插入Metasploit的包结构
该APK通过动态加载恶意模块实现隐私窃取功能，其主要功能有：

- 获取通话记录
- 获取联系人
- 获取短信
- 隐藏图标
- 获取位置
- 设置壁纸
- 获取已安装应用列表
- 启动应用

- 卸载应用（API的方式）
- 剪切板管理
- 文件管理
- 录音、录像、拍照
- 实时录音
- 实时录像
- 获取设备信息
- 获取网络信息
- 截图
- 检测ROOT权限

恶意模块源码结构如下图所示：

图6 Metasploit payload源码结构

## 2.Windows端样本分析

Windows 平台使用了开源的AsyncRAT，该远控工具主要功能如下：

- 屏幕查看和记录。
- 反病毒以及完整性管理
- SFTP上传和下载
- 聊天
- 动态DNS和多服务器支持
- 密码恢复
- jit编译
- 键盘记录
- 反分析
- 自启动

图7 AsyncRAT控制端界面

图8 左边为样本反编译代码，右边为AsyncRAT源码

图9样本配置选项

## 二、归属研判

## 1.伪装对象与攻击目标

在攻击样本中，部分样本伪装成Explosive_course（爆炸物课程），安装运行后，会打开一份炸药介绍及制作的文档，文档内容如下：

图10 文档内容

还有部分攻击样本伪装成Abdul Rasheed相关应用，Abdul Rashid Ghazi Shaheed 是巴基斯坦伊斯兰原教旨主义者和圣战活动家，出身于巴基斯坦旁遮普省边境地区，于 2007 年 7 月 10 日在“沉默行动”中丧生。他被认为是极端分子的沙希德（烈士），影响了巴基斯坦以及全球范围内的恐怖主义，例如活跃于叙利亚内战的逊尼派伊斯兰武装叛乱组织（Ansar al-Sham）将他命名为训练营。

近期使用的攻击样本伪装成了Bolan Attack Video（俾路支解放军攻击视频）相关应用，俾路支解放军（BLA）是巴基斯坦与阿富汗一个俾路支人的武装组织。2004年起，俾路支解放军武力对抗巴基斯坦政府，声称旨在为长年受压迫的俾路支人争取平权与民族自决。俾路支解放军大多在巴基斯坦的俾路支省活动，常对巴基斯坦军事武装力量发动攻击。俾路支解放军被巴基斯坦、英国、欧盟、美国等多个国家认定为恐怖组织。

结合以上几点，我们推测本次攻击的攻击目标为当地和周边的恐怖主义。

## 2.攻击组织

我们怀疑本次攻击的组织为APT-C-56（透明部落），主要依据以下几点判断：

1. 攻击者的PC设备位于巴基斯坦，这与APT-C-56（透明部落）所属地域相同；
2. 我们在设备还发现了APT-C-56（透明部落）组织使用的远控测试样本；
3. 此前有其他安全厂商揭露过APT-C-56（透明部落）曾使用过伪装成恐怖主义相关文档进行攻击，这与本次攻击样本的伪装类型相同。

因此，我们认定为本次攻击与APT-C-56（透明部落）高度相关。

**总结**

本次披露样本与之前披露样本属于同类型样本,但是样本与之前有所差异,是未被披露过的相关样本。该类型样本结构相对复杂,载荷更新也较快,需要引起足够的重视。

恐怖主义是全人类的敌人，是世界各国面临的共同挑战。多年来，巴基斯坦在打击恐怖主义方面作出了巨大的努力和牺牲，也取得了显著的成效。根据资料显示，自2015年以来，巴境内恐怖主义袭击事件和致死人数逐年减少；但是由于新冠肺炎疫情影响，巴境内恐怖主义活动显现出卷土重来之势，恐怖袭击事件开始出现增涨势头。今年巴基斯坦政府也加大了国内反恐力度，我们推测巴政府针对恐怖主义的网络攻击行动或许会更加频繁。

我们列出了一些通用的安全防范排查建议。

1. 确保安装了杀毒应用。
2. 仅从应用商店下载并安装软件。

3. 谨慎打开通过短信或邮件收到的任何链接。

4. 尽量不授权应用敏感权限。

5. 保持操作系统和应用程序处于最新状态。

6. 定期检查移动设备上安装的应用程序移动/Wi-Fi数据的使用情况。

7. 密切关注杀毒应用提示的警报信息，并采取必要的措施。

**附录 IOC**

## Android

f0321bd5a4b887811a352433879166f7

68cda60d457e2205e9cb613df2bd5f17

29914ab4a4ef57708a9f81e2d251526d

f2b16ef64ee0833f479bb68f65e66a0a

20e0dd26e1f438e1e481cc0ff6f16e25

a198a817f118a32dae1e7b285c36aba1

949119651c349f0fa49e28d20e912d5f

19c47f35dac1fe1e1250187715914eeb

dfa61290a1ef08b683098263673746e8

d0585f0efbd3cf3d365cf2d66852a3bd

7fa4f2d0df94f2579f28a38a582ffe9c

7534df0e3e0a0da62a80ad71a3f536f0

7f8692fa057136ff64ace384b857dc3b

4e025929a1e16261ff04d70976255810

5a3f683b2cb3947c05ed3790dd7cf39a

a5257b9d3a3f387f2537e107e6dba2a4

47e18f7ad48adce7542bb7396b5c1124

fe2b0502f6467d46f055fde0afeeac1f

93c651e2afd793ffdd0fcf884f995153

7a71cd056a83860643102764147aca5e

4720a201d0e8e7c6be7f15254dd41866

1bcab52932a721f05d0fc22b7e380a64

## Windows

7e12d2f8e8f6d83ab65dec16f77be9d0

## C&C

tandertx.ddns.net

tindertx.ddns.net

**参考**

https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp

https://github.com/AhMyth/AhMyth-Android-RAT

https://github.com/rapid7/metasploit-payloads

https://wikitltl.top/wiki/Abdul_Rashid_Ghazi

https://baike.baidu.com/item/%E4%BF%BE%E8%B7%AF%E6%94%AF%E8%A7%A3%E6%94%BE%E5%86%9B/7757691

https://www.163.com/dy/article/GTVGI5FJ0515R479.html

**360烽火实验室**

360烽火实验室致力于移动恶意软件分析、移动灰黑产研究、移动威胁预警、移动APT的发现与追踪等移动安全领域的深入研究。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不仅首发了多篇具备国际影响力的移动安全生态研究成果，并且成功狩猎了蔓灵花、拍拍熊等多个APT组织针对我国及境外重要目标的攻击活动。实验室在为360手机卫士、360手机助手、360加固保等公司产品提供核心安全数据的同时，也为科研单位、手机厂商、应用商店及上百家国内外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

---