肚脑虫组织（APT-C-35）针对巴基斯坦的攻击活动

一、背景

肚脑虫组织（APT-C-35），又称 Donot，是一个针对克什米尔地区相关国家的政府机构等领域进行网络间谍活动，以窃取敏感信息为主的攻击组织。该组织具备针对 Windows 与 Android 双平台的攻击能力。该组织的攻击活动最早可追溯到 2016 年，近年来该组织活动频繁不断被数个国内外安全团队持续追踪和披露。

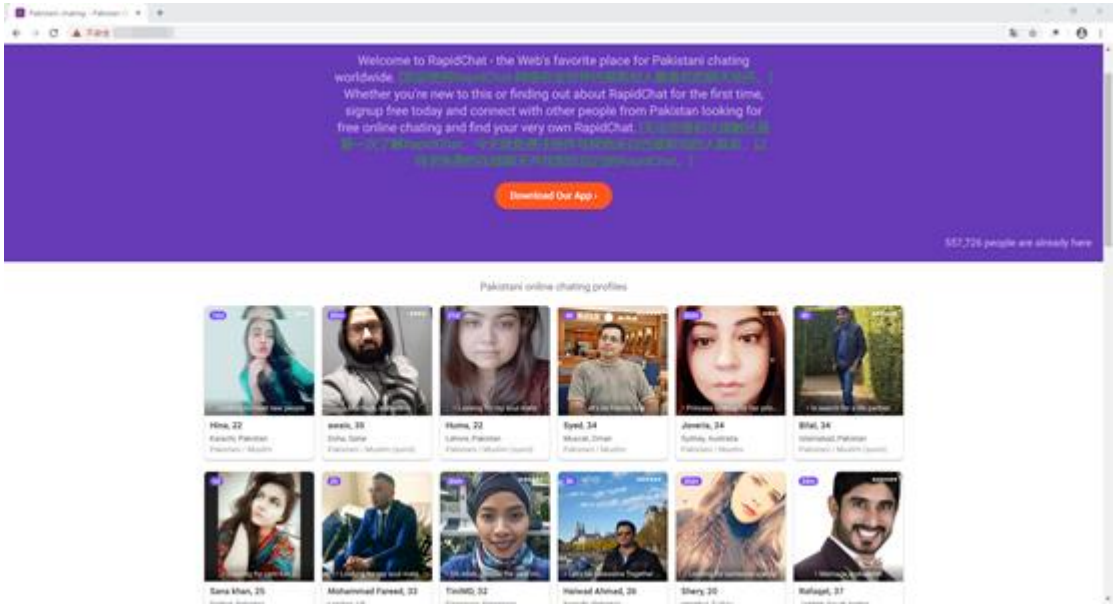
近期，360 烽火实验室再次监测到肚脑虫组织针对巴基斯坦的移动端攻击活动。根据我们监测数据，此次攻击活动疑似开始于 2020 年 1 月，该组织将攻击样本伪装成在线聊天工具 RapidChat，利用钓鱼网站和社交软件发起网络攻击。

二、载荷投递

（一）攻击方式

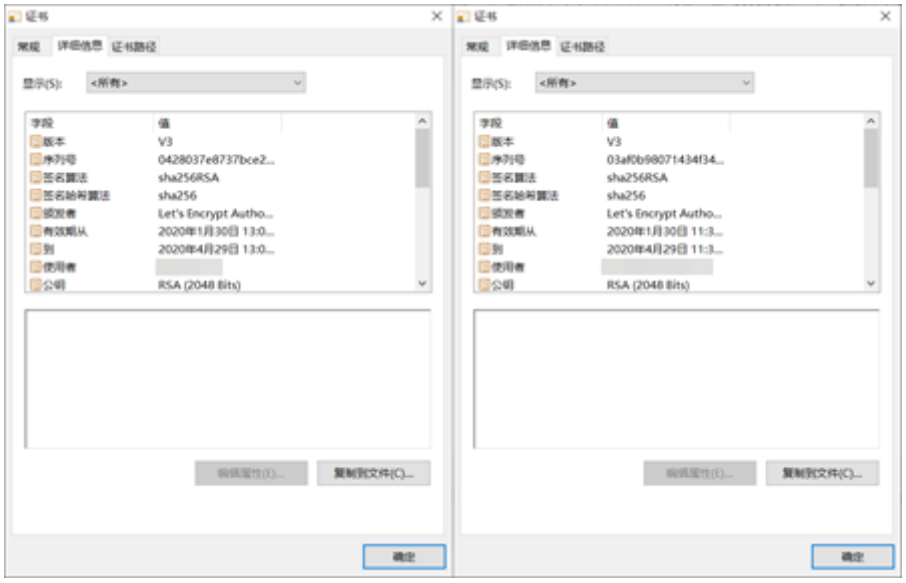
肚脑虫组织在此次攻击活动中使用的载荷投递方式为钓鱼攻击和社交软件。此次攻击活动中，攻击者搭建了一个名为 RapidChat 在线聊天功能的钓鱼网站，该网站首页介绍称其为全世界巴基斯坦人最喜欢的聊天场所，伪造了多名分布在世界各地巴基斯坦虚假人物。攻击者声称累计已经有超过 55 万人使用网站提供的聊天服务，网站还提供了相

应的聊天 APP 软件下载。通过该链接下载的 APP 软件实际为攻击样本，如下图所示。



该钓鱼网站采用了 HTTPS 协议，通过对网站证书分析，该网站证书由证书颁发机构 Let's Encrypt 颁发，有效期从 2019 年 12 月 30 日到 2020 年 3 月 29 日。目前该网站证书已经属于失效状态。

我们根据此钓鱼网站信息推测此次攻击活动可能开始于 2020 年 1 月，攻击目标为巴基斯坦人。 通过进一步关联，我们找到了肚脑虫组织的其他网络资产，其网站证书均由证书颁发机构 Let's Encrypt 颁发，并且有效期只有 4 个月。由此推测，肚脑虫组织每次攻击活动持续时间不长，并且会持续不断的更换钓鱼网站。



除了钓鱼网站，我们还在部分受害者手机中，发现该攻击样本出现在 WhatsApp 文档路径中，由此可以判断肚脑虫组织还可能使用了 WhatsApp 等社交软件进行载荷投递。

文件路径
/storage/emulated/0/WhatsApp/Media/WhatsApp Documents/rapidchat.apk

（二）诱饵文件

此次攻击活动中，攻击者对攻击样本进行了多种维度的欺骗保护，首先从文件名方面，攻击样本伪装成 RapidChat.apk，我们在

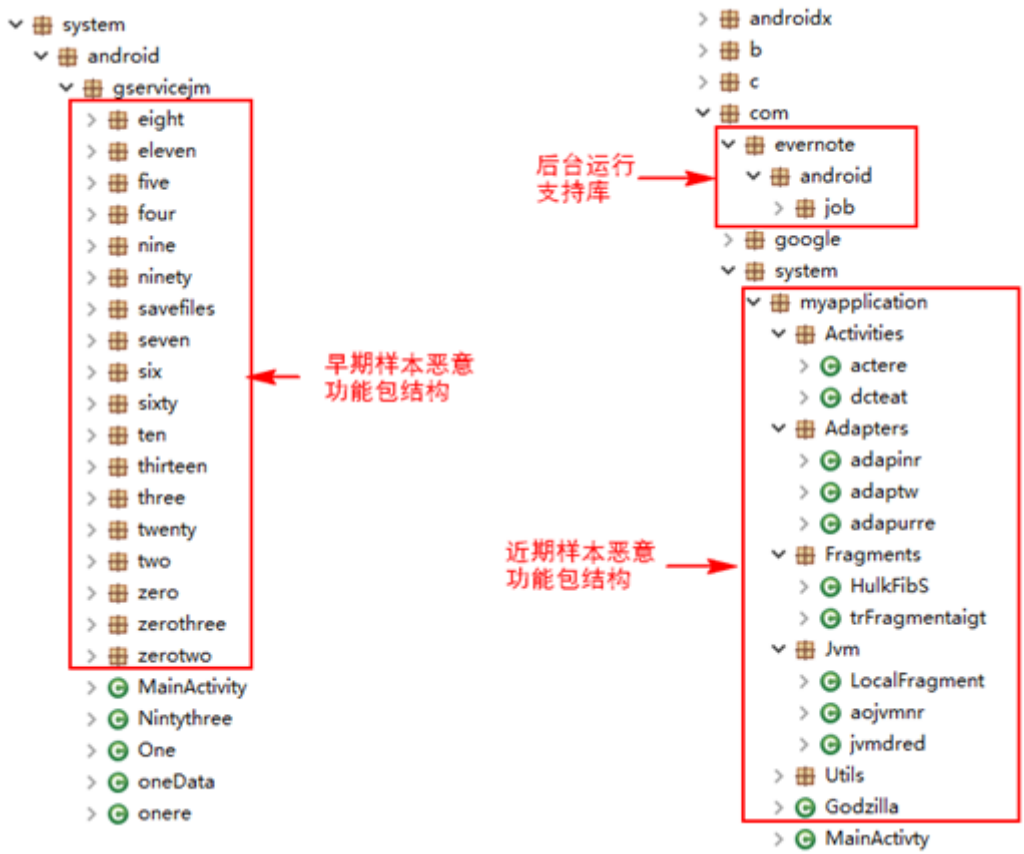
GooglePlay 上找到了相同名称软件，其具有钓鱼网站上所描述的相似功能。

其次，图标和包名分别伪装成系统软件和国内某主流社交应用软件。

图标	名称	包名
	RapidChat.apk	com.tencent.mobilemm

三、功能分析

肚脑虫组织此次攻击活动使用的攻击样本与我们早期揭露的攻击样本包结构相比，此次攻击样本不再使用数字英文进行命名，并且添加了后台延时运行的相关包，以支持其在高版本 Android 系统上实现后台运行。



除了以上区别外，此次攻击样本与早期攻击样本的恶意功能和云端执行命令完全一致，可以执行云端下发的命令进行录音、上传联系人、通话记录、短信等恶意行为，相关命令和功能如下表。

指令	功能
Call	获取通话记录信息
CT	获取联系人信息
SMS	获取短信信息
Key	获取APP输入内容信息
Tree	获取SD卡文件列表信息
AC	获取Account信息
Net	wifi、设备厂商、运营商等信息
CR	设置通话录音
LR	设置特定时间段录音
FS	文件上传开关
GP	获取地理位置信息
PK	获取已安装应用列表信息
BW	获取chrome书签信息
CE	获取日历事件信息
Wapp	获取whatsapp聊天信息

四、总结

近年来，多起利用网络社交媒体进行钓鱼攻击的 APT 攻击活动被揭露，相较于其他方式进行网络攻击活动，社交媒体主要利用人的安全意识较弱。安全防护就如木桶效应一样，一只木桶能盛多少水，并不取决于最长的那块木板，而是取决于最短的那块木板。在做好系统防护的同时也需要提升相关人员的安全意识，补齐所有的短板，整个系统才会更不容易被攻破。