蔓灵花（APT-C-08）移动平台攻击活动揭露

2019 年 12 月 10 日

目　录

一、背景

蔓灵花（APT-C-08）APT 组织是一个长期针对中国、巴基斯坦等国家进行攻击活动的 APT 组织，主要攻击政府、电力和军工行业相关单位，以窃取敏感信息为主，具有强烈的政治背景，是目前活跃的针对境内目标进行攻击的境外 APT 组织之一。该组织最早在 2016 被国外安全公司进行了披露，并且命名为“BITTER”，同年 360 也跟进发布了分析报告，将该组织命名为“蔓灵花”。 迄今为止有数个国内外安全团队持续追踪并披露该组织 PC 端的最新攻击活动。

2019 年 8 月，360 烽火实验室在日常样本分析中发现一新型 Android 木马，根据其 CC 特点将其命名为 SlideRAT，深入分析后发现该家族木马属于蔓灵花组织。此后，我们对该家族样本进行持续监控，2019 年 11 初，我们发现 SlideRAT 攻击中国军工行业从事人员，11 月中旬，该家族样本开始攻击中国驻巴基斯坦人员。短短半个月内，蔓灵花组织在移动平台至少进行了两次的攻击活动，且受害者均为中国人，我们猜测随着年关将近，该时间段为该组织针对我国攻击的高发期。鉴于此我们决定通过已有情报和数据，将该家族在移动平台的攻击活动进行揭露。

二、概述

蔓灵花在移动平台的攻击活动最早可以追溯到 2014 年，2016 年首次曝光该组织在移动平台使用开源远程管理工具 AndroRAT 攻击巴基斯坦政府。其后有数篇关于该组织在 PC 端的攻击活动报告，而 Android 相关的报告几乎是一片空白。本报告将揭露该组织自 2016 年后在 Android 端的攻击活动。

(一) 主要发现

2016 年 6 月开始，蔓灵花组织开始使用定制木马 SlideRAT 针对中国和巴基斯坦展开了长期有组织、有计划的攻击活动。根据已有数据，我们发现该组织在攻击活动中常用的载荷投递方式包括水坑、钓鱼、短信、社交工具，受害者包括中国军工行业人员、中国党政干部、企业客服人员以及其他中国群众，也包括巴基斯坦和印度克什米尔区域群体。

(二) 攻击行动

通过对捕获到的所有 SlideRAT 家族样本证书初始时间和伪装对象进行梳理，该组织在移动平台的攻击活动线如图 1 所示 。

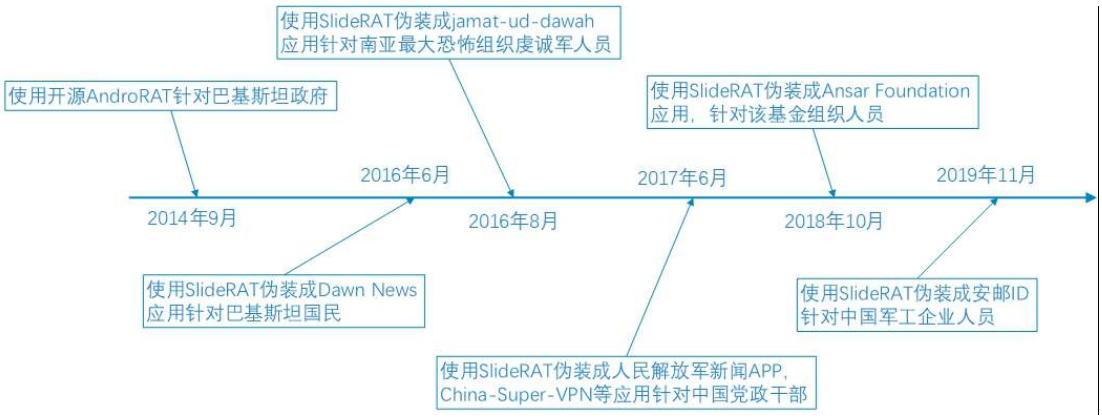

图 1 蔓灵花组织攻击时间线

- 2014 年 9 月开始使用 AndroRAT 攻击巴基斯坦政府。
- 2016 年 6 月开始使用 SlideRAT 伪装成 Dawn News 攻击巴基斯坦国民。
- 2016 年 8 月使用 SlideRAT 伪装成 jamat-ud-dawah 攻击南亚恐怖组织虔诚军人员。
- 2017 年 7 月使用 SlideRAT 伪装成人民解放军新闻 APP、China-Super-VPN 等应用针对中国政府。
- 2018 年 10 月使用 SlideRAT 伪装成 Ansar Foundation 应用攻击该基金组织人员。
- 2019 年 11 月使用 SlideRAT 伪装成安邮 ID 针对中国军工行业人员。

三、载荷投递

蔓灵花组织在移动平台载荷投递的方式主要为水坑攻击和钓鱼链接，其次还会通过短信和 WhatsApp 进行载荷投递。

(一) 水坑攻击

北京某科技有限公司是交通运输部“智能交通技术与设备”行业研发中心、北京市企业技术中心核心支撑单位。该公司官网在 2017 年 9 月被发现存在托管 SlideRAT 家族样本。巴基斯坦某公司从事工程机械、备件和土木工程项目交易，该公司官网在 2019 年 3 月被发现存在托管 SlideRAT 家族样本。

公司	链接
北京某科技有限公司	http://[redacted]/js/RESUME/China-Super-VPN.apk
巴基斯坦某公司	https://[redacted]/dawn/Dawn News Official.apk

图 2 水坑攻击网站

(二) 钓鱼

通过分析 SlideRAT 的来源，我们发现其仿冒了多个合法的网站进行钓鱼传播，主要冒充了 GooglePlay、安邮 ID、某旅游官网进行钓鱼传播。

说明	链接
伪装成GooglePlay官网	http://[redacted]/Image_Viewer.apk
伪装成安邮ID下载链接	https://[redacted]/安邮ID.apk
伪装成某旅游官网	http://[redacted]旅游app.apk

图 3 钓鱼网站相关信息

(三) 短信

除了以上的钓鱼链接，我们还发现 SlideRAT 通过冒充某旅游公司的短信进行传播，并且使用短链接进行伪装，下图为模拟短信传播界面。

图 4 模拟短信界面

(四) 社交工具

在部分受害者手机中，SlideRAT 样本出现在 WhatsApp 文档路径中，由此可以判断蔓灵花组织使用了 WhatsApp 社交工具进行载荷投递。

文件路径
/storage/emulated/0/WhatsApp/Media/WhatsApp Documents/IMG00623.jpeg.apk
/storage/emulated/0/WhatsApp/Media/WhatsApp Documents/Ramdan Mubarak.apk

图 5 WhatsApp 路径

(五) 图标伪装

SlideRAT 主要使用图像处理相关的图标进行伪装，其次还会根据攻击目标群体的特殊性，使用针对性的图标进行伪装，如伊斯兰教以及虔诚军相关图标，伪装的应用软件图标如下图所示。

图 6 伪装图标

四、样本分析

(一) RAT 演变

蔓灵花组织早期使用开源远程管理工具 AndroRAT 进行移动平台的攻击活动，2016 年 6 月后开始使用定制的 SlideRAT 持续攻击至今，两种 RAT 在代码结构和功能上存在较大差异，下图为 AndroRAT 和 SlideRAT 代码结构。

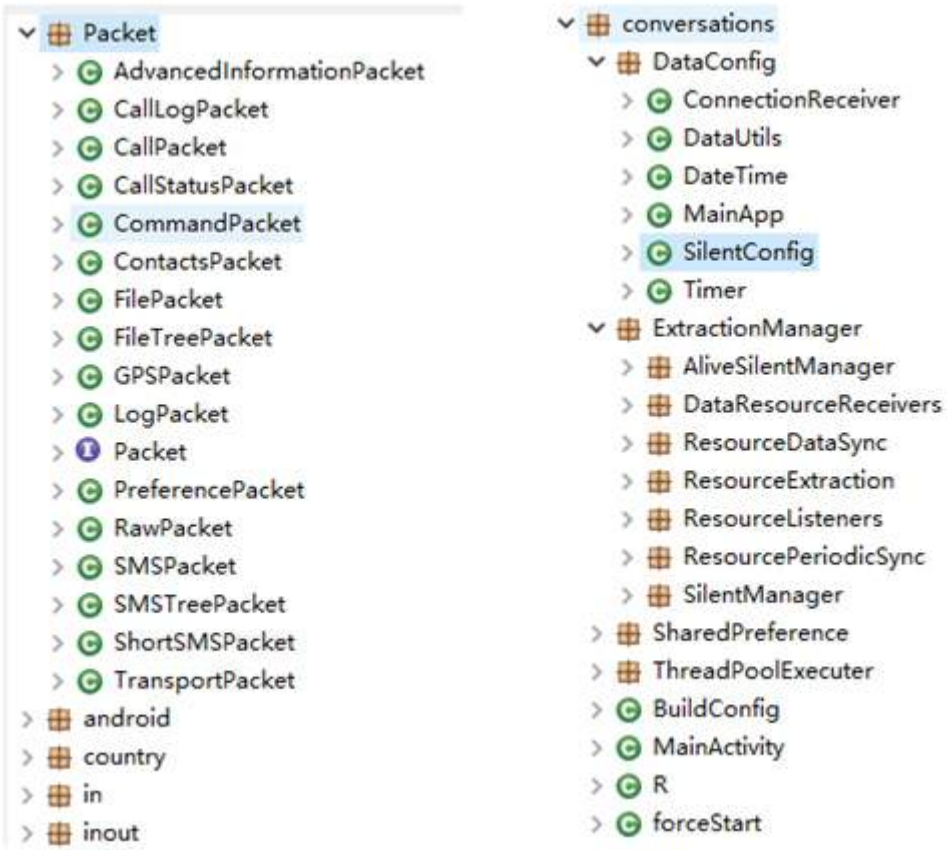

图 7 左图为 AndroRAT 结构，右图为 SlideRAT 结构

(二) 功能对比

AndroRAT 和 SlideRAT 两款 RAT 功能如下表所示，可以发现早期 AndroRAT 功能偏向远程控制，而后期使用的 SlideRAT 更偏向隐私的窃取。

功能	AndroRAT	SlideRAT
通话录音		√
上传文件		√
GPS/网络定位	√	√
获取通话记录	√	√
获取设备信息		√
获取账户信息		√
获取所有短信	√	√
获取联系人信息	√	√
实时获取手机状态	√	√
实时监控接收短信息	√	√
获取sdcrad文件列表		√
获取已安装应用列表		√
拍照	√	
响铃	√	
录音		√
录像	√	
发短信	√	
打电话	√	
手机震动	√	

图 8 功能对比

五、受害者人物画像

在蔓灵花组织所有移动平台攻击活动中，发现多名受害者，通过已有数据进行分析可以得到以下人物画像。

(一) 军工行业从业人员

安邮 ID 是某军工业邮件系统辅助登录工具，其首页有介绍安邮 ID 使用方法的相关文档，如下图所示。此受害者手机中发现了 SlideRAT 伪装成安邮 ID 的样本。

图 9 某军工业邮件系统首页新手指引

受害者的活动范围主要在沙特利雅得地区（如图 10），而某军工业沙特分公司位于利雅得（如图 11），并且受害者手机中装有较多航空相关和大量国内常用应用，我们推测受害者为经常出差沙特的某军工业人员。

图 10 活动范围

图 11 某军工业沙特分公司简介

(二) 党政干部

某干部网络学院由该省委组织部主办，省委党校承办，是集在线学习、信息发布、考试测评、培训管理、在线评估、资料查询、互动交流等功能于一体的综合性、开放式的干部网络学习平台(如图 12)。我们发现有受害者在 2017 年 9 月接收到蔓灵花组织伪装成某旅游公司的钓鱼短信，其 2016 年 7 开始参与该干部网络学院学习，我们推测其为该省党政干部。

图 12 某干部网络学院官网

(三) 赴巴基斯坦留学人员

伊斯兰堡联邦中级和中等教育委员会（FBISE）是“联邦教育和专业培训”部的自治机构。关于其相关介绍见下图，我们发现有受害者参与了 FBISE 的相关学习，据此推测其为准备赴巴基斯坦留学人员。

图 13 FBISE 介绍

(四) 企业客服人员

此次还发现中国某网络公司和某旅游公司相关工作人员的电脑也存在被蔓灵花组织攻击的痕迹，其 QQ 昵称包含自己的工作内容加姓名显示，疑似企业对外服务的客服人员。该网络公司主要业务涉及企业建站，IDC 数据中心，SMS 短信通等领域；该旅游公司是首批经国家旅游局批准为合法经营中国公民出国旅游的组团社。

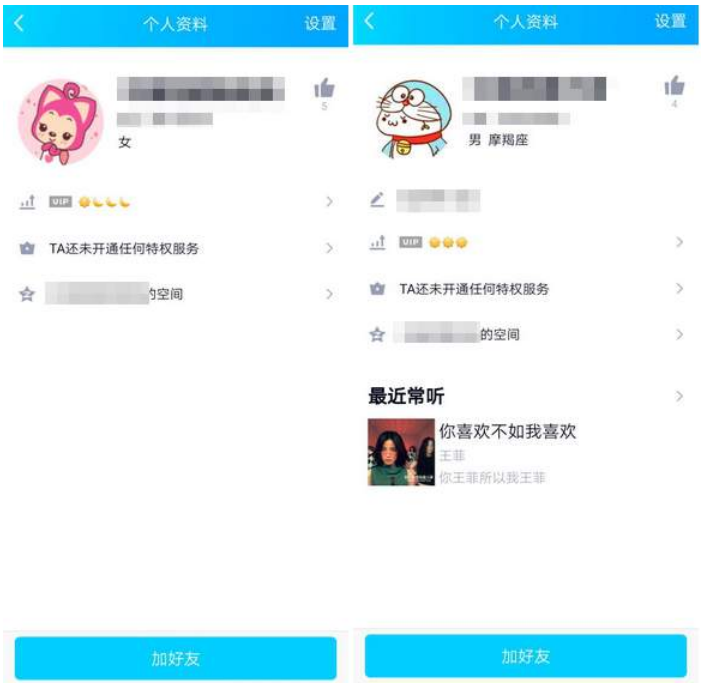

图 14 某网络公司受害者

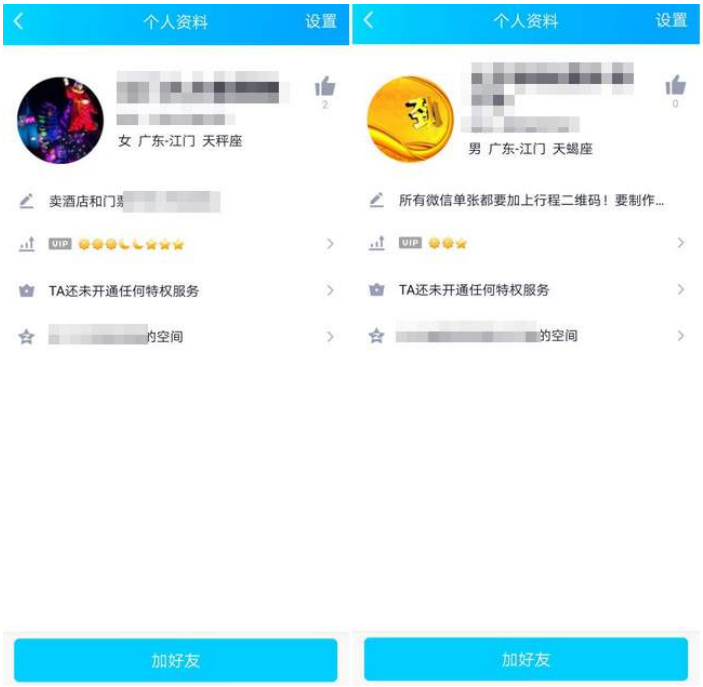

图 15 某旅游公司受害者

从时间上看，这些企业客服人员的被攻击时间要早于前面提到的党政干部被攻击的时间，而从企业性质来看，我们怀疑正是蔓灵花组织入侵了这两个企业后，利用其公司资源发送的钓鱼短信。

(五) 克什米尔区域群体

除中国受害者以外，我们还发现部分国外的受害者，其主要活动范围在印度和巴基斯坦

交界的克什米尔区域，如下图所示。

图 16 活动范围

六、溯源关联

根据已有公开情报可以知道在 2018 年 11 月至 2019 年 1 月之间，巴基斯坦的某公司网站托管了两个可执行恶意文件以及一个用于传递有效载荷的恶意文档，并最终将此归属于蔓灵花组织。本次揭露的 SlideRAT 在 2018 年 8 月也使用了该公司网站进行托管，基于此我们初步将 SlideRAT 归属于蔓灵花组织。而在针对 SlideRAT 家族 CC 进行分析中，我们发现其中关联了较多的 PC 样本，且与蔓灵花组织存在关联（如图 17），进一步证实 SlideRAT 归属于蔓灵花组织。

Scanned	Detections	Type	Name
2019-12-04	41 / 68	Win32 EXE	
2019-11-03	47 / 65	Win32 EXE	
2019-10-05	44 / 70	Win32 EXE	
2019-11-22	53 / 68	Win32 EXE	
2019-10-20	51 / 71	Win32 EXE	
2019-12-09	61 / 71	Win32 EXE	
2018-09-03	48 / 68	Win32 EXE	
2016-01-06	37 / 56	Win32 EXE	
2015-12-11	16 / 54	Win32 EXE	

Contained In Graphs

Description
BITTER_APT Campaign
Patchwork

图 17 VirusTotal 网站所展示的关联信息

七、总结

蔓灵花组织是一个长期活跃的 APT 组织，武器库十分强大，拥有对多平台进行攻击的能力，近年来，虽然该组织在 PC 端的攻击活动多次被安全厂商披露，但从未停止攻击，反而越发活跃，攻击目标也越发广泛。虽然本报告揭露了该组织在移动平台的攻击活动，但是该组织在移动平台的攻击活动不会因此而停止，甚至会随着攻击获取到的价值效益增加而加大移动平台的攻击活动。

此外，在此次揭露的持续两年多的多起攻击活动中，所有受害者所使用手机都是国产品牌。一方面，代表国产手机品牌市场占有率不断提升的同时，也在不断拓展海外市场。另一方面，也给手机品牌厂商敲响警钟，市场的不断拓展，必然会面临越来越多的安全问题，如何抵御攻击，则成为厂商应该深入思考的严峻问题。

参考

BITTER: a targeted attack against Pakistan : https://www.forcepoint.com/blog/x-labs/bitter-targeted-attack-against-pakistan
Multiple ArtraDownloader Variants Used by BITTER to Target Pakistan : https://unit42.paloaltonetworks.com/multiple-artradownloader-variants-used-by-bitter-to-target-pakistan/

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。