mp.weixin.qq.com /s/B0ElRhbqLzs-wGQh79fTww

来自南亚的金刚象组织VajraEleph ——针对巴基斯坦军方人员的网络间谍活动披露

QAX病毒响应中心 奇安信病毒响应中心
奇安信病毒响应中心

gh_416eb7efb780

奇安信病毒响应中心官方公众号

2022-03-30 18:00

收录于话题

一、 事件概要

2022年2月，奇安信病毒响应中心移动安全团队关注到自2021年6月起至今，一个来自南亚某国背景的APT组织主要针对巴基斯坦军方展开了有组织、有计划、针对性的军事间谍情报活动。经过短短9个月的攻击，该组织已影响数十名巴基斯坦军方人员。这部分受害人员主要为巴基斯坦国家的边防军（FC）和特种部队（SSG），尤其是俾路支省边防军（FC BLN）；此外还包含少量的联邦调查局（FIA）和警察（Police）。另攻击还影响了少量的尼泊尔人员，但我国国内用户不受其影响。

图1.1 受影响的国家分布情况图

该组织通常使用公开的社交平台找到关注的目标后，结合色情话术等聊天诱导目标用户安装指定的诱饵聊天攻击应用进行钓鱼攻击。此外，攻击者还曾在国外某知名应用商店平台发布该恶意聊天应用，但目前相关链接已无法访问。

截至本报告发布之时，我们已经截获的该组织所有攻击活动，都是通过Android平台进行的，尚未发现任何通过Windows平台进行的攻击。累计捕获恶意应用下载服务器8个，服务器上至少可以下载到5个不同的Android平台攻击样本。所有样本均为含有恶意代码的专用聊天软件。我们将所有这些捕获的恶意样本命名为VajraSpy。

综合攻击活动特征、样本编码方式、C2服务器架构方式等多方面线索分析显示，该组织具有南亚某地区性大国政府背景，但又与该地区活跃的其他APT组织，如响尾蛇SideWinder、蔓灵花Bitter、肚脑虫Donot等没有显著关联（仅与肚脑虫Donot存在少量相似性），具有很强的独立性和独立特征。因此，我们判定该组织为活跃在南亚地区的新APT组织。我们将其命名为金刚象，英文名为VajraEleph，组织编号APT-Q-43。金刚象是奇安信独立发现并率先披露的第15个APT组织。

二、 载荷投递

通过奇安信病毒响应中心移动安全团队与奇安信威胁情报平台（https://ti.qianxin.com/） 的联合追踪分析发现，金刚象组织最早的活动可以追溯到2021年6月。下图为我们截获的该组织最早的载荷服务器信息。

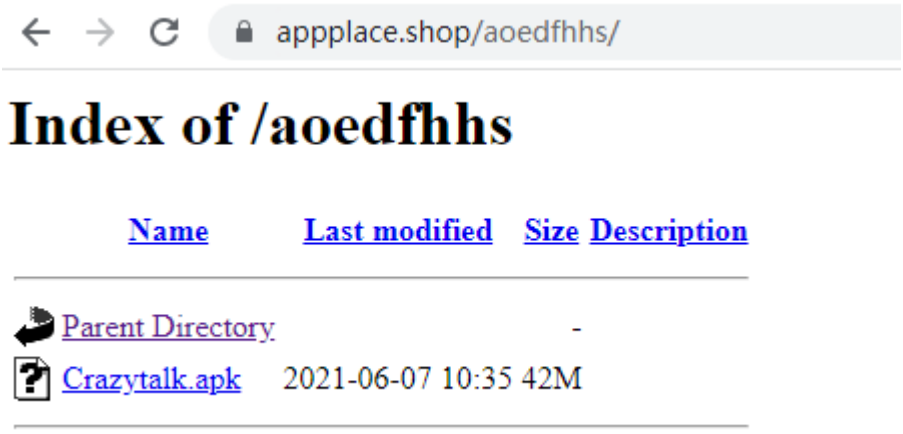


图2.1 发现的最早域名载荷服务器相关截图（采用NameSilo注册商域名）

该组织早期的攻击，通常会将攻击载荷下载地址的的“短链接”，通过WhatsApp等社交软件发送给攻击目标。后期，随着各大社交平台对相关链接进行封禁，该组织转为将短链接以图片方式向目标人进行投递。

载荷短链地址	**对应实际下载地址**
https://cutt.ly/qIrgCKo	https://appz.live/ichfghbtt/crazy.apk
https://bit.ly/3BrCxNU	https://appzshare.digital/coufgtdjvi/ZongChat(Beta).apk
https://bit.ly/39roCMd	https://apzshare.club/poahbcyskdh/cable.apk
https://rebrand.ly/Cable_v2	https://appzshare.club/poahbcyskdh/cable.apk

该组织采用的载荷域名服务器注册时间均不到一年，注册商主要是NameSilo和NameCheap。这与近期在南亚活跃的另一个高级攻击组织肚脑虫的活动相似。

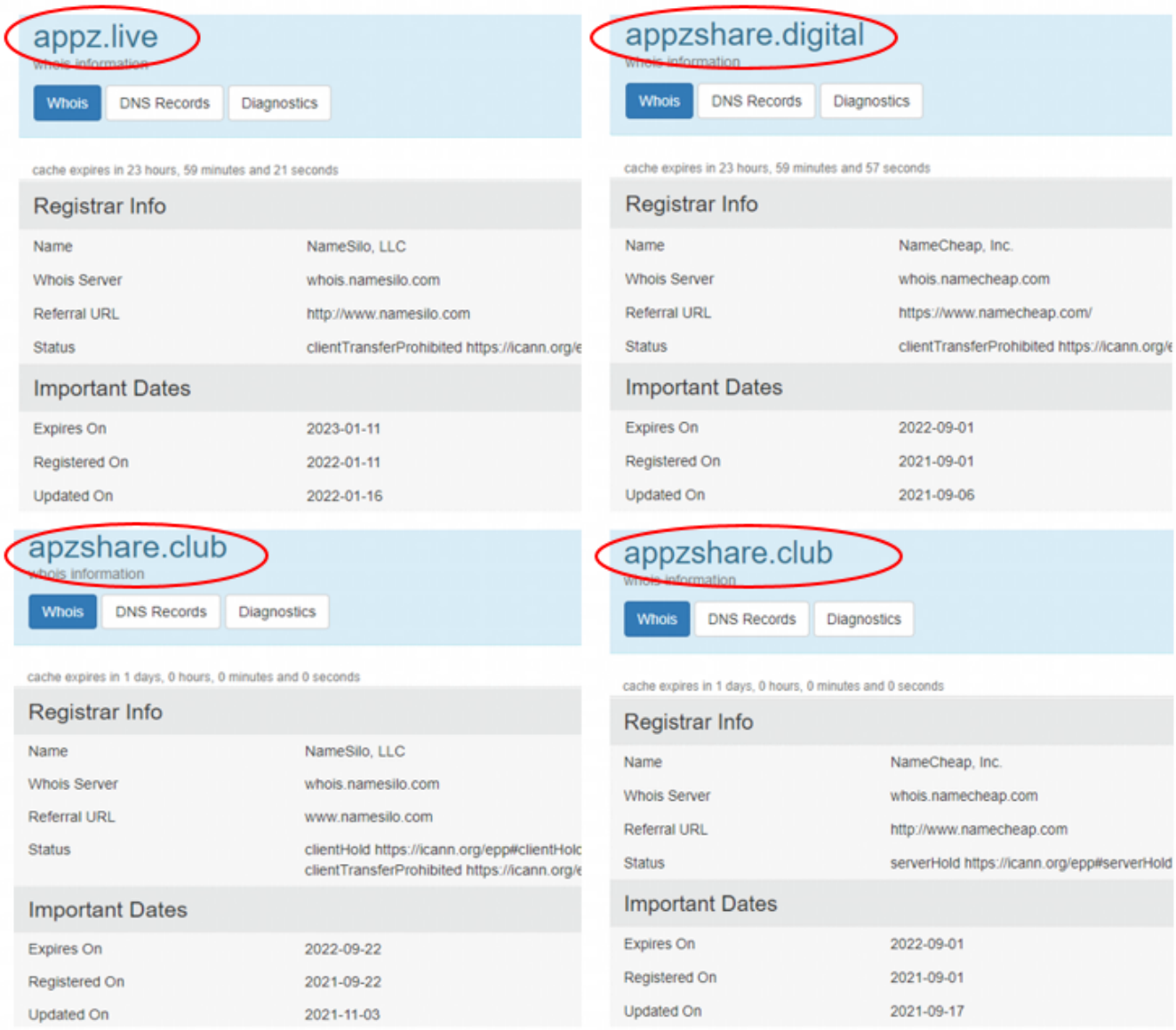


图2.2 部分域名载荷服务器whois情况

三、 攻击目标

金刚象组织具有明显的军事情报窃取意图，主要针对巴基斯坦军方人员，影响已涉及数种部队的数十名军方人员。以下是我们从攻击者C2服务器上截获的，部分受害者手机被窃取的照片和资料。

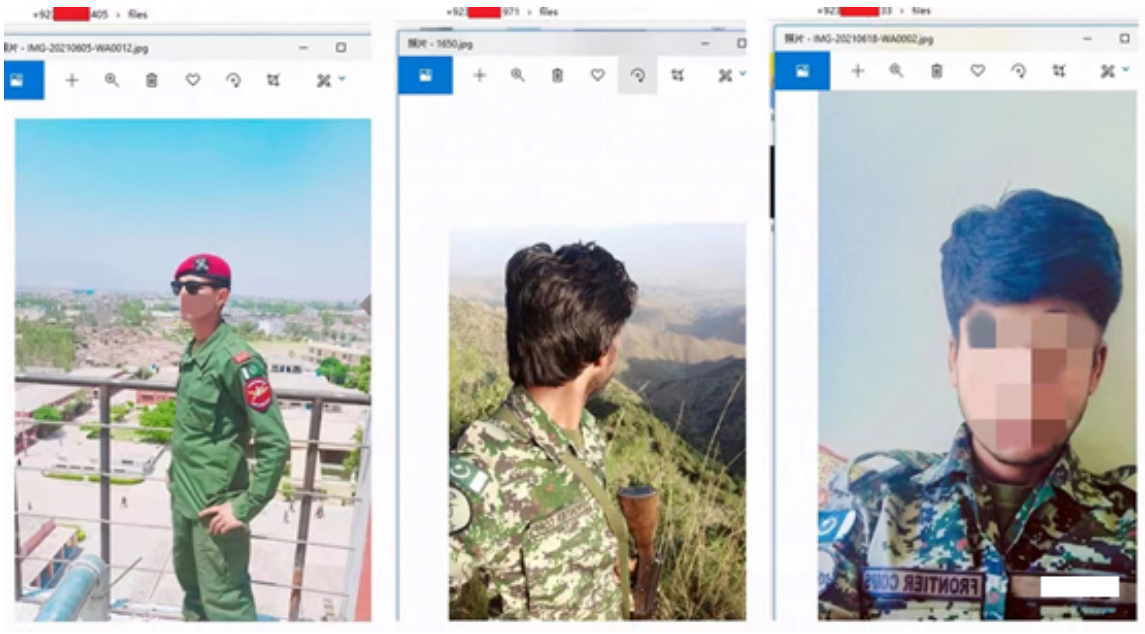


图3.1 巴基斯坦边防军（FC ，Frontier Corps）人员被窃照片

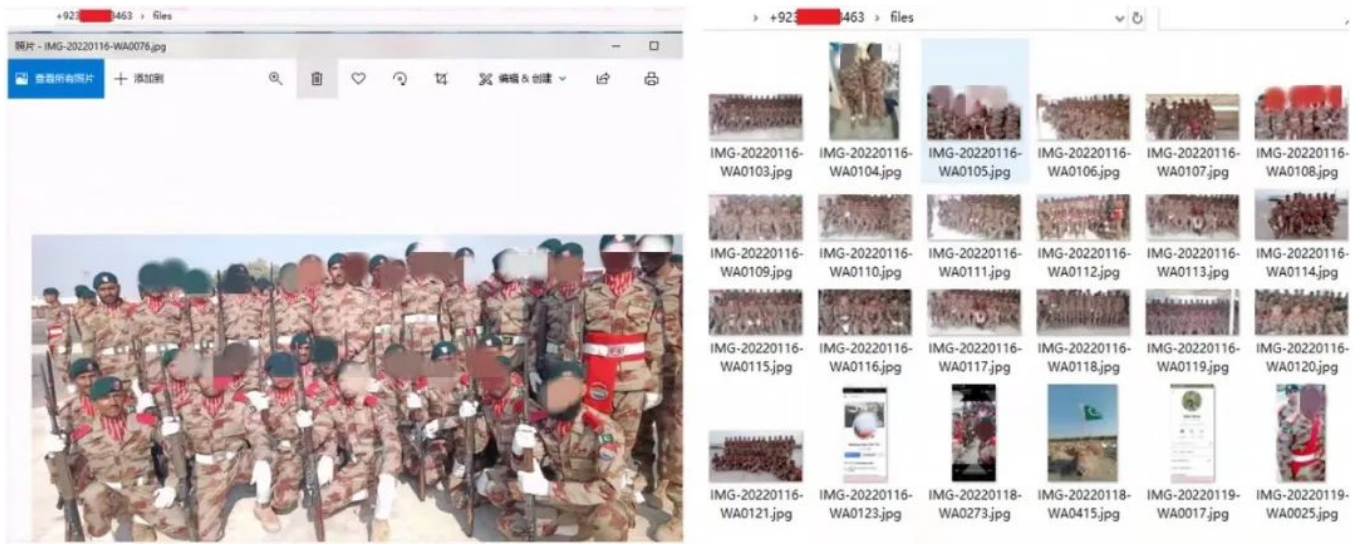


图3.2 巴基斯坦俾路支省边防军（ FC BLN ，FC Balochistan）人员被窃照片

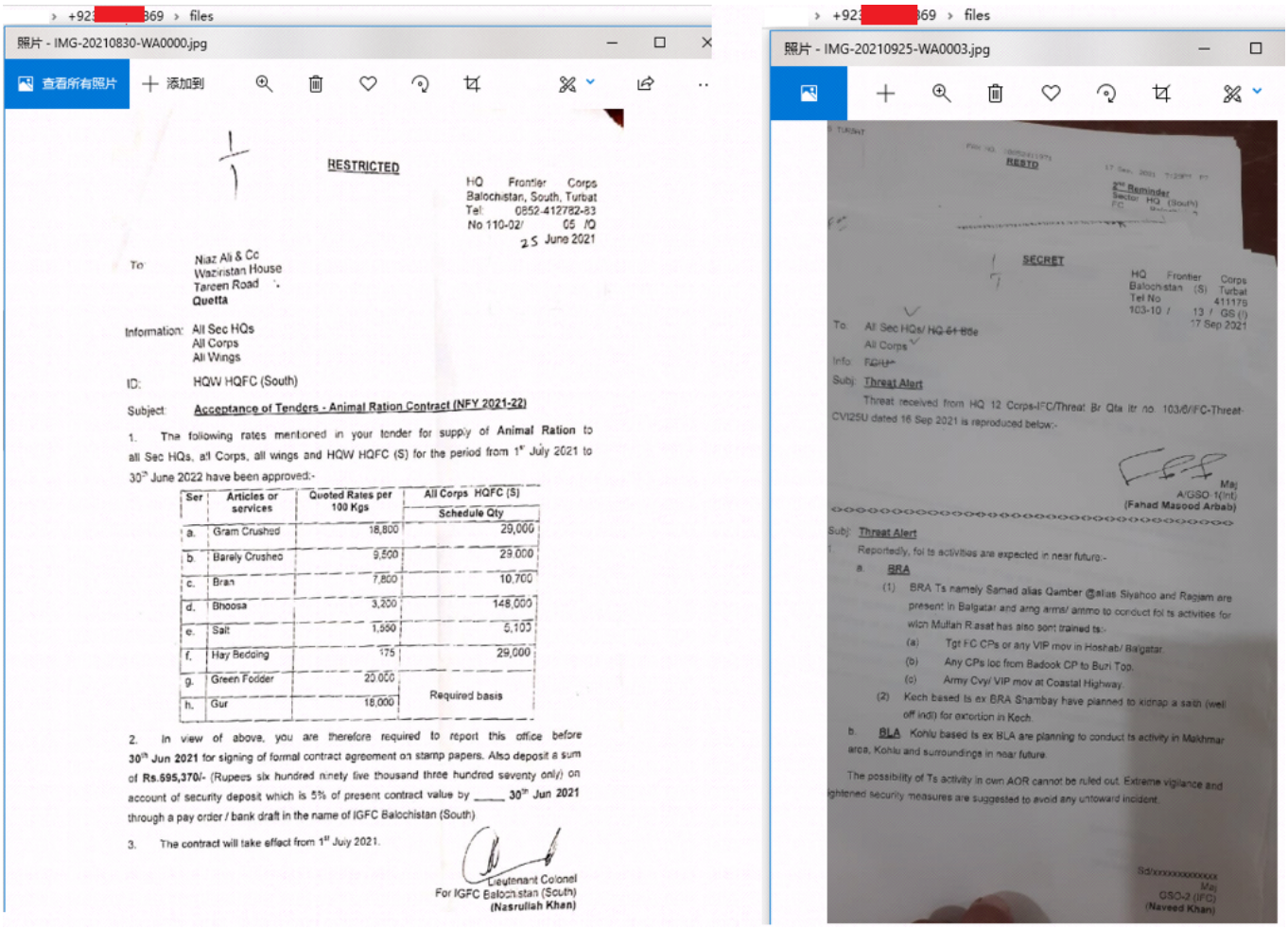


图3.3 俾路支省边防军人员被窃资料

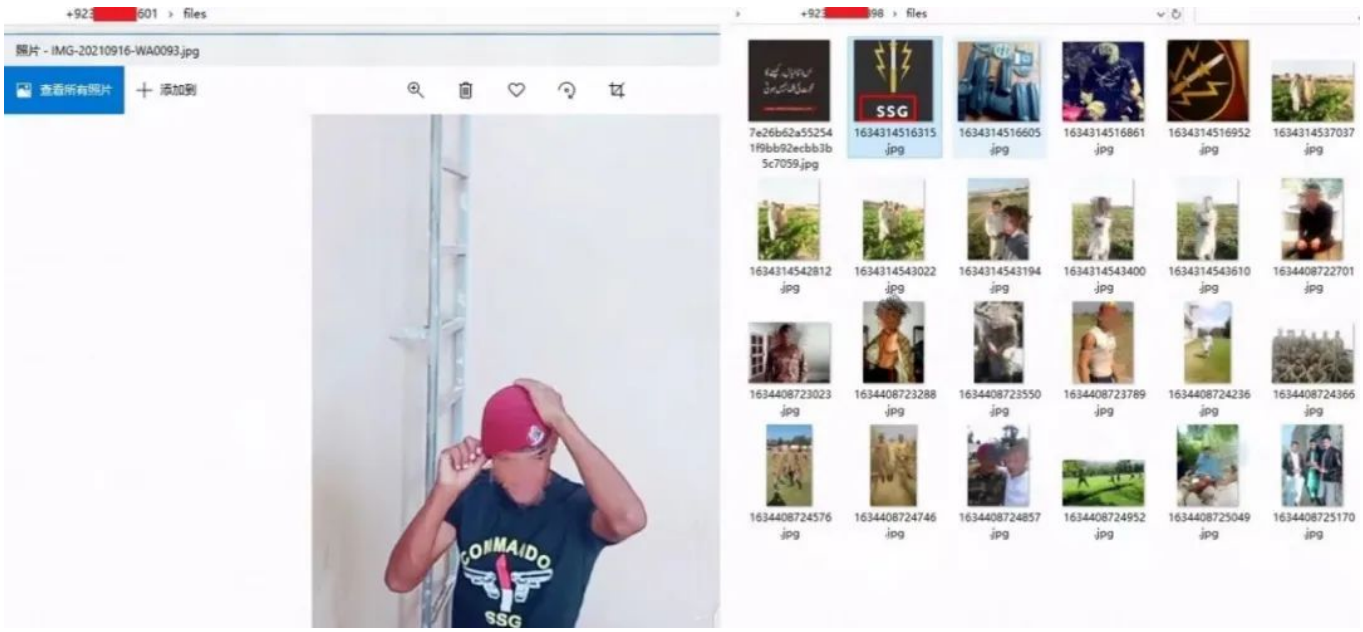


图3.4 巴基斯坦特种部队（SSG ，Special Service Group）人员被窃照片

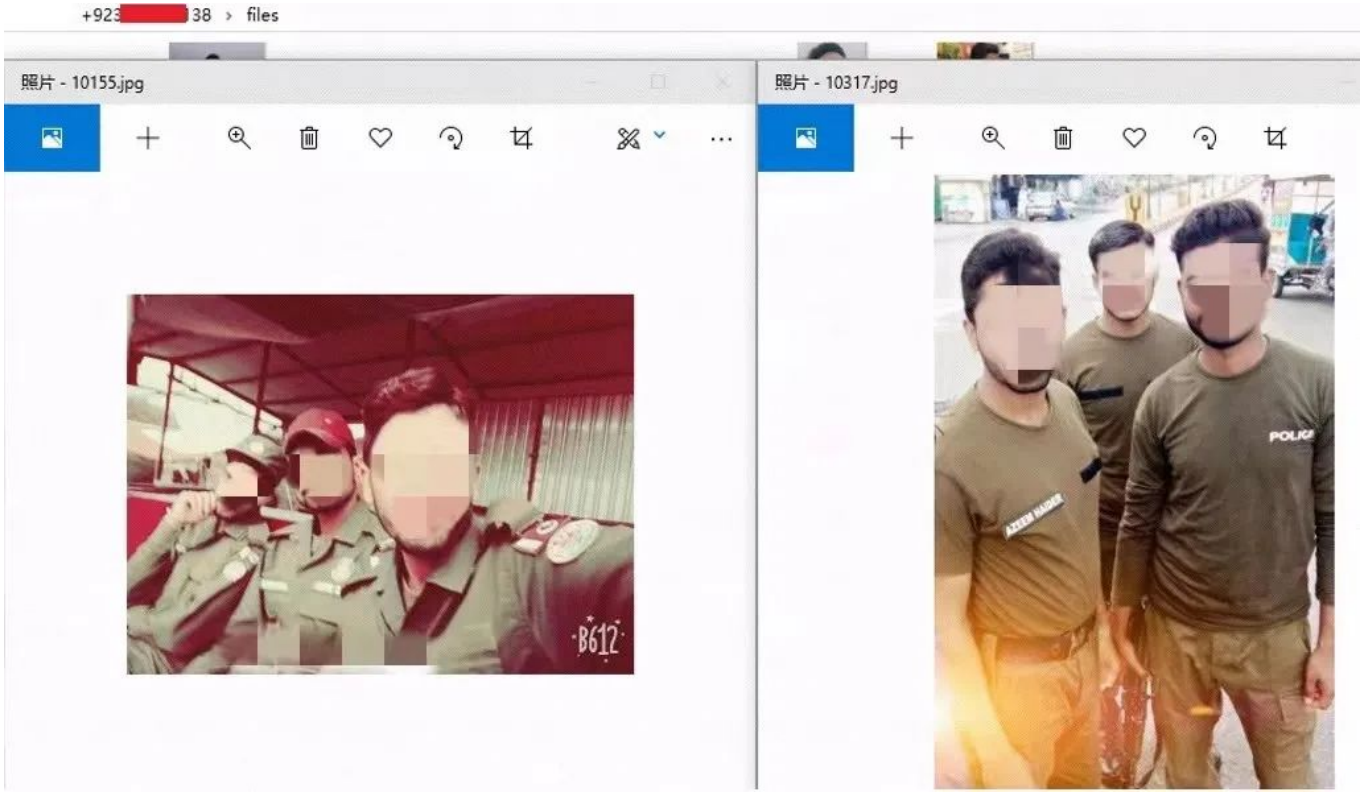
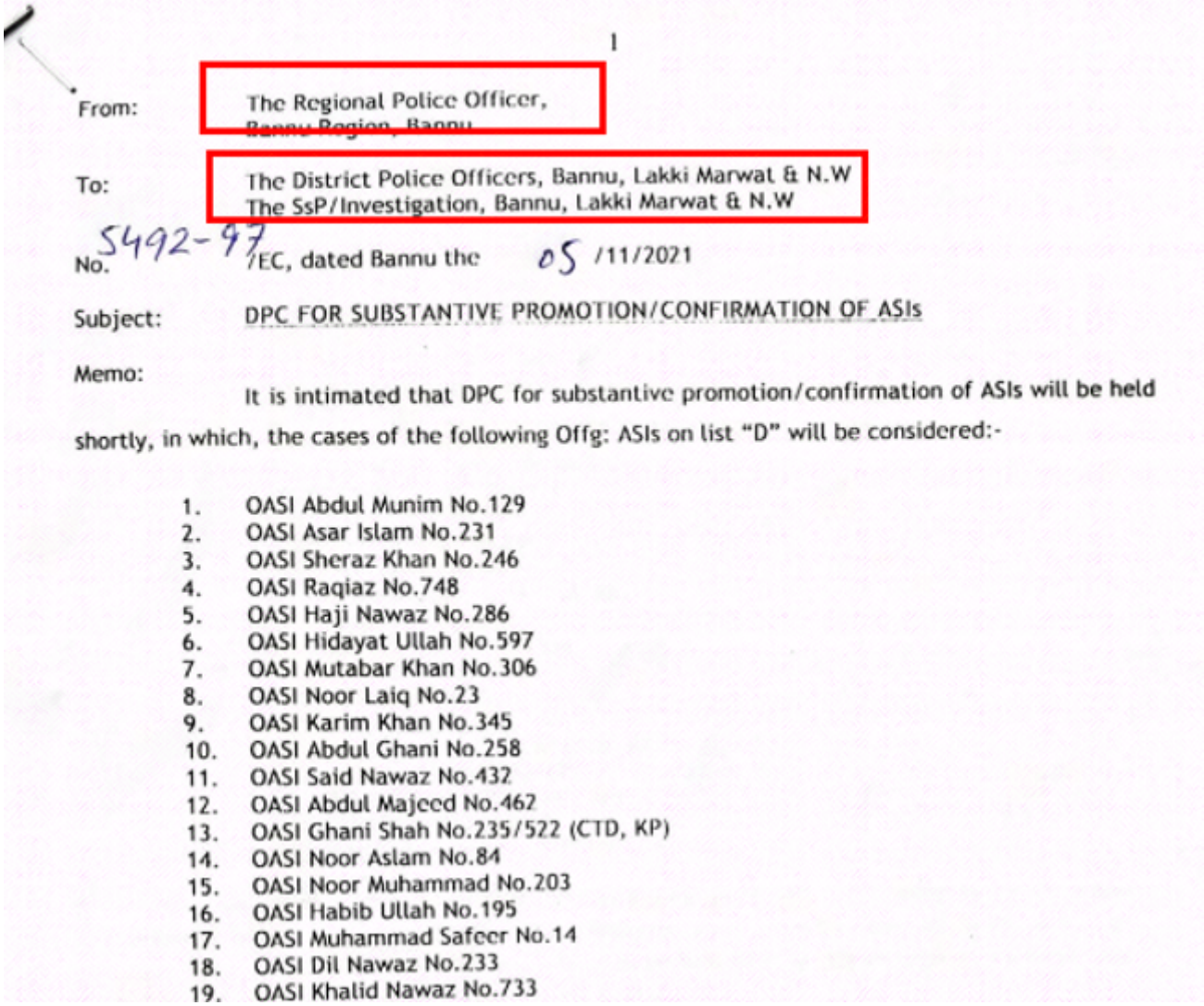


图3.5 巴基斯坦警察被窃照片



From: The Regional Police Officer, Bannu Region, Bannu

To: The District Police Officers, Bannu, Lakki Marwat & N.W
The SsP/Investigation, Bannu, Lakki Marwat & N.W

No. 5492-97 /EC, dated Bannu the 05 /11/2021

Subject: DPC FOR SUBSTANTIVE PROMOTION/CONFIRMATION OF ASIs

Memo:

It is intimated that DPC for substantive promotion/confirmation of ASIs will be held shortly, in which, the cases of the following Offg: ASIs on list "D" will be considered:-

1. OASI Abdul Munim No.129
2. OASI Asar Islam No.231
3. OASI Sheraz Khan No.246
4. OASI Raqiaz No.748
5. OASI Haji Nawaz No.286
6. OASI Hidayat Ullah No.597
7. OASI Mutabar Khan No.306
8. OASI Noor Laiq No.23
9. OASI Karim Khan No.345
10. OASI Abdul Ghani No.258
11. OASI Said Nawaz No.432
12. OASI Abdul Majeed No.462
13. OASI Ghani Shah No.235/522 (CTD, KP)
14. OASI Noor Aslam No.84
15. OASI Noor Muhammad No.203
16. OASI Habib Ullah No.195
17. OASI Muhammad Safeer No.14
18. OASI Dil Nawaz No.233
19. OASI Khalid Nawaz No.733

图3.6 巴基斯坦警察被窃资料

图3.7 巴基斯坦联邦调查局（FIA，Federal Investigation Agency）人员被窃照片

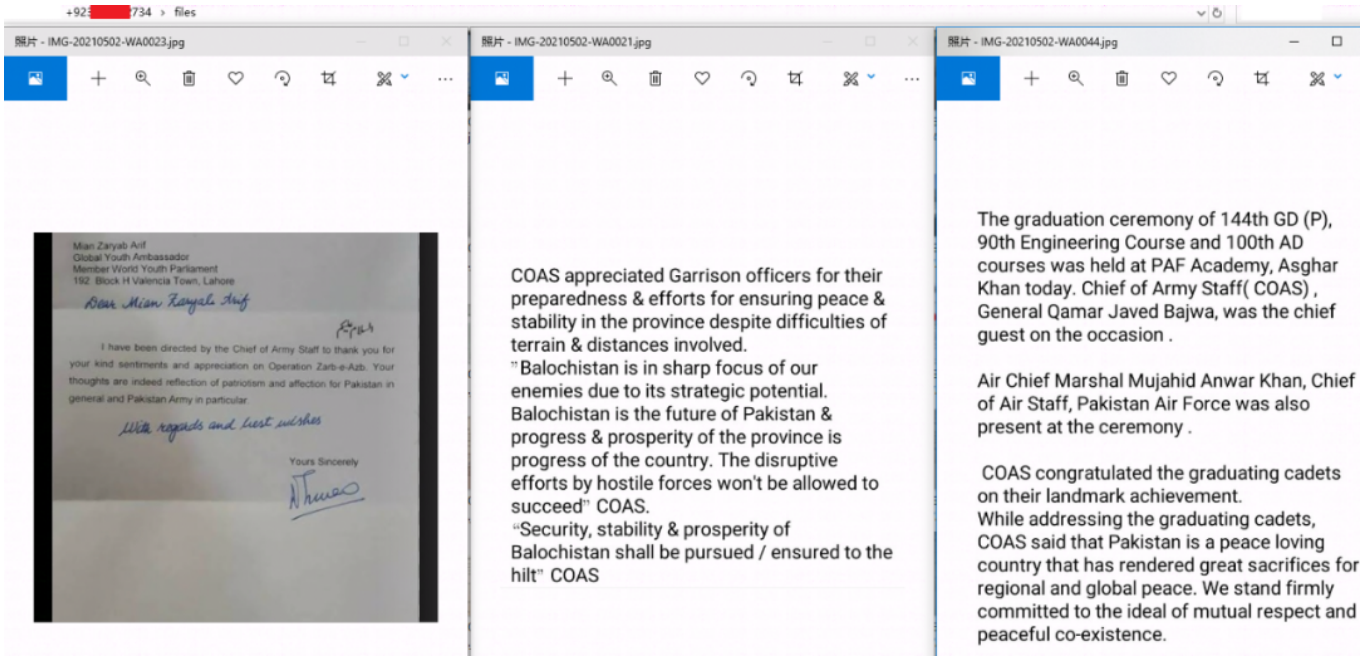


图3.8 关于陆军参谋长（COAS，Chief of Army Staff）的被窃资料

四、 技术分析

通过分析发现，目前金刚象组织投入的攻击RAT针对的都是Android平台。分析显示，该组织的RAT定制化程度较高，我们将其命名为VajraSpy。VajraSpy支持间谍活动的所有经典功能，并将窃取到的数据存储到指定的谷歌云存储空间中。

功能	**对应的窃取后数据存储文件名称**
窃取通话记录	logs.json
窃取通讯录	contacts.json
窃取短信	sms.json
窃取SD卡指定目录15种类型文件	files/文件名
窃取通知栏信息	noti/13位时间戳.json
窃取设备信息	device.json
窃取已安装的应用程序信息	appdetails.json
窃取三种版本的 WhatsApp 信息	wa.json/wab.json/wabs.json

```
else if(!v0.cloudFiles.contains(file.getName())) {
    int v13 = file.length() / 10000000L > 0L ? 2 : 1;
    if(file.getAbsolutePath().contains("/WhatsApp/")) {
        v14 = 1;
    }
    else if(file.getAbsolutePath().contains("/Download/")) {
        v14 = 2;
    }
    else {
        v14 = file.getAbsolutePath().contains("/Documents/") ? 3 : 4;
    }

    if(file.getName().endsWith(".pdf")) {
        v15 = 1;
    }
    else if(file.getName().endsWith(".doc")) {
        v15 = 2;
    }
    else if(file.getName().endsWith(".docx")) {
        v15 = 3;
    }
    else if(file.getName().endsWith(".txt")) {
        v15 = 4;
    }
    else if(file.getName().endsWith(".ppt")) {
        v15 = 5;
    }
    else if(file.getName().endsWith(".pptx")) {
        v15 = 6;
    }
    else if(file.getName().endsWith(".xls")) {
        v15 = 7;
    }
    else if(file.getName().endsWith(".xlsx")) {
        v15 = 8;
    }
    else if(file.getName().endsWith(".jpg")) {
        v15 = 9;
    }
    else if(file.getName().endsWith(".jpeg")) {
        v15 = 10;
    }
    else if(file.getName().endsWith(".png")) {
        v15 = 11;
    }
    else if(file.getName().endsWith(".mp3")) {
        v15 = 12;
    }
    else if(file.getName().endsWith(".0m4a")) {
        v15 = 13;
    }
    else if(file.getName().endsWith(".aac")) {
        v15 = 14;
    }
    else {
        v15 = file.getName().endsWith(".opus") ? 15 : 16;
    }

    if(v15 != 16) {
        inFiles.add(new FileInfo(file, ((int)v13), ((int)v14), ((int)v15), file.length()));
```

图4.1 窃取的15种类型文件（文本、图片、音频）相关代码片段

五、 攻击者画像

1）攻击目的

攻击者以巴基斯坦军方、安全及警务人员为主要攻击目标，包括边防军（FC）、特种部队（SSG）、联邦调查局（FIA）和警察（Police）等。其中，边防军是最主要的攻击目标。还有少量活动是针对尼泊尔军方

人员。由此可见，军事人员、军事机密，是该组织攻击活动的主要目的。

2）攻击方式

攻击者擅长采用社交诱导投递和短信诱导投递进行攻击，其中社交诱导投递是主要方式。
3）网络资产
攻击者使用的手机号码均为南亚某国移动服务商专属号码。
4）母语特征
攻击者在攻击活动中，大量使用南亚某国语言。而该国与巴基斯坦长期存在军事和地缘政治冲突。

5）与其他APT组织的关联

恶意样本下载服务器的活动特征与肚脑虫（Donot）具有一定的相似性。
攻击活动中使用的一些文件名与肚脑虫组织有一定相似性。
综上所述，金刚象组织应当是具有南亚某国政府背景，主要针对巴基斯坦军方人员和军事活动发动网络攻击的高级攻击组织，是一个活跃在南亚地区的新的APT组织。

六、 总结与建议

在传统的APT活动中，移动社交平台的使用并不常见。这一方面是由于绝大多数的敏感、机密信息都是存储在电脑端的，另一方面也是由于通过社交平台发动攻击，容易留下痕迹。
不过，近两年来，随着移动社交平台的日益普及，我们发现，很多针对发展中国家的APT活动，都会或多或少的通过移动平台、社交平台来进行。比如，我们先前披露过的诺崇狮组织、利刃鹰组织，以及本次披露的金刚象组织，都有针对Android平台和社交平台的网络攻击活动。分析认为，造成APT活动日益关注移动平台、社交平台的原因，主要有以下几个方面：
首先，很多发展中国家的网络安全建设水平、管理水平相对落后，导致仅仅通过针对智能手机的攻击，就有可能获得大量的敏感、机密信息。
第二，智能手机普及度越来越高，针对安全意识不足的涉密人员，通过社交平台发动网络攻击，是一种低成本，高效率的攻击方式。
第三，智能手机，往往存在更多未修复的安全漏洞，加之移动安全软件的普及率不高，导致针对移动平台发起网络攻击的技术门槛相对更低。
那么，对于政企机构，特别是军方、警方等涉密或敏感机构来说，应当怎样做好防护，尽可能的避免或减少针对移动平台、社交平台的APT活动给自身带来的影响呢？我们在此给予如下一些实用建议。

1）工作生活相分离，敏感信息不外传

相关机构应努力避免工作人员使用个人智能手机进行日常办公活动。有条件的单位，可以为工作人员配发工作手机或涉密手机。如果条件确实不允许，可以使用企业级安全移动工作平台进行内部的交流和办公，比如蓝信、云手机安全管理系统等。

2）加强安全意识教育，严格执行安全规范

相关机构应加强员工安全意识教育，不要使用个人手机拍摄、存储敏感或涉密信息，更不能通过社交平台分享敏感信息；不去点击陌生人发来的不明链接；拒绝色情、赌博等非法信息的诱惑。同时，相关机构还应制定切实可行的网络安全管理标准与员工行为规范，并进行严格的监督与审查。

3）更新软件系统，使用安全软件

相关机构应要求员工，不论是办公手机还是个人手机，都要做到及时更新操作系统与核心软件，以确保智能手机始终处于最佳安全状态。同时安装必要的手机安全软件，以尽可能的减少各类木马、病毒的侵害。

4）建立威胁情报能力，防范APT攻击

相关机构应与专业安全厂商一起，共建高效的威胁情收集、分析与处置能力，及时发现、拦截和追踪各类APT活动，将APT活动带来的影响和损失降到最低。
目前，基于奇安信自研的猫头鹰引擎和奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天机、天眼高级威胁检测系统、奇安信NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。

部分IOC

域名/IP	**用途**
appplace.shop	载荷服务器
appz.live	载荷服务器
apzshare.club	载荷服务器
appzshare.digital	载荷服务器
appzshare.club	载荷服务器
212.24.100.197	载荷服务器

Android MD5	**包名**
7a47d859d5ee71934018433e3ab7ed5b	com.cr.chat
0c980f475766f3a57f35d19f44b07666	com.crazy.talk

附录1 奇安信病毒响应中心

奇安信病毒响应中心是北京奇安信科技有限公司（奇安信集团）旗下的病毒鉴定及响应专业团队，背靠奇安信核心云平台，拥有每日千万级样本检测及处置能力、每日亿级安全数据关联分析能力。结合多年反病毒核心安全技术、运营经验，基于集团自主研发的QOWL和QDE（人工智能）引擎，形成跨平台木马病毒、漏洞的查杀与修复能力，并且具有强大的大数据分析以及实现全平台安全和防护预警能力。

奇安信病毒响应中心负责支撑奇安信全线安全产品的病毒检测，积极响应客户侧的安全反馈问题，可第一时间为客户排除疑难杂症。中心曾多次处置重大病毒事件、参与重大活动安全保障工作，受到客户的高度认可，提升了奇安信在业内的品牌影响力。

附录2 奇安信病毒响应中心移动安全团队

奇安信病毒响应中心移动安全团队一直致力移动安全领域及Android安全生态的研究。目前，奇安信的移动安全产品除了可以查杀常见的移动端病毒木马，也可以精准查杀时下流行的刷量、诈骗、博彩、违规、色情等黑产类软件。通过其内部分析系统可以有效支持对溯源分析等追踪。通过其高价值移动端攻击发现流程已捕获到多起攻击事件，并发布了多篇移动黑产报告，对外披露了多个APT组织活动，近两年已首发披露4个国家背景下的新APT组织（诺崇狮组织SilencerLion、利刃鹰组织BladeHawk、艾叶豹组织SnowLeopard和此次的金刚象组织VajraEleph）。未来我们还会持续走在全球移动安全研究的前沿，第一

时间追踪分析最新的移动安全事件、对国内移动相关的黑灰产攻击进行深入挖掘和跟踪，为维护移动端上的网络安全砥砺前行。

附录3 奇安信移动产品介绍

奇安信移动终端安全管理系统（天机）是面向公安、司法、政府、金融、运营商、能源、制造等行业客户，具有强终端管控和强终端安全特性的移动终端安全管理产品。产品基于奇安信在海量移动终端上的安全技术积淀与运营经验，从硬件、OS、应用、数据到链路等多层次的安全防护方案，确保企业数据和应用在移动终端的安全性。

奇安信移动态势感知系统是由奇安信安全监管BG态势感知第一事业部及其合作伙伴奇安信病毒响应中心移动团队合力推出的一个移动态势感知管理产品。不同于传统移动安全厂商着重于APP生产，发布环节，为客户提供APP加固、检测、分析等；移动态势感知面向具有监管责任的客户，更加着重于APP的下载，使用环节，摸清辖区范围内APP的使用情况，给客户提供APP违法检测、合规性分析、溯源等功能。