VajraEleph from South Asia - Cyber espionage against Pakistani military personnel revealed

QAX Virus Response Center *Qi Anxin Virus Response Center 2022-03-30 18:00*
Qi Anxin Virus Response Center

1. Summary of the event

In February 2022 , the mobile security team of Qi'anxin Virus Response Center noticed that since June 2021, an APT group mainly targets Pakistan the Tanzanian military has launched organized, planned and targeted military espionage intelligence activities. After just nine months of attacks, the group has affected dozens of Pakistani military personnel. This part of the victim The personnel are mainly Pakistani national border guards (FC) and special forces (SSG), especially the Balochistan border guards (FCBLN); in addition lso contains a small amount of FBI (FIA) and police. Another attack also affected a small number of Nepalese personnel, but domestic users in China were not affected by it.

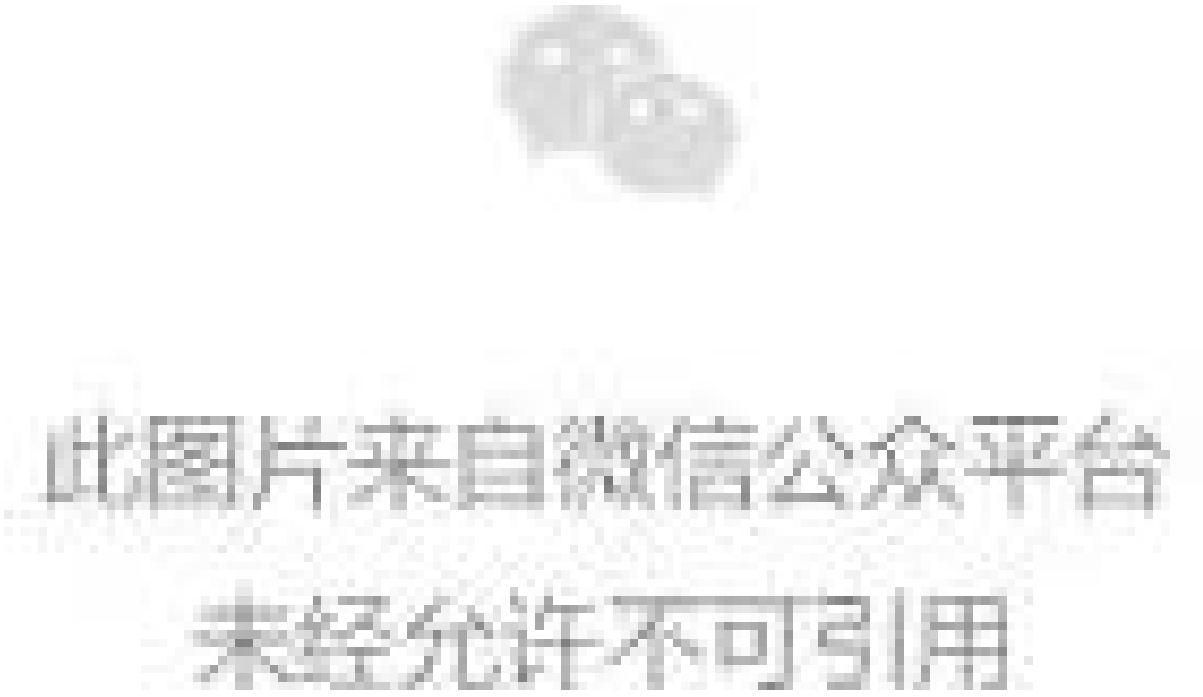

Figure 1.1 Distribution of affected countries

The organization usually uses public social platforms to find the target of concern , and combines pornographic words and other chats to induce the target users to install the specified bait chat attack application. Used for phishing attacks. Furthermore the attacker also published the malicious chat application on a well-known foreign app store platform, but the relevant links are now inaccessible.
As of the time of this report , all the attacks of this group that we have intercepted are carried out through the An d r oi d platform , and we have not found any via the Windows platform attack. A total of 8 malicious application download servers have been captured , and at least 5 different Android platform attack samples can be downloaded on the servers. All samples were dedicated chat software for Italian codes. We name all these captured malicious samples VajraSpy .
Comprehensive analysis of the attack activity characteristics, sample coding method, C2 server architecture and other clues shows that the organization has a regional power in South Asia. the background of the government, but also live with the region Other APT tissues that jumped, such as Sidewinder, Manling Flower Bitter, Belly Brainworm Donot, etc., were not significantly associated (only with Bellyworm Donot there is a small amount of similarity), with strong independence and independent

characteristics. Therefore we identified this organization as a new APT organization active in South Asia. We named it King Kong Elephant, English the document name is VajraEleph, and the organization number is APT-Q-43. King Kong Elephant is the 15th APT organization that Qi Anxin independently discovered and first disclosed.

2. Load delivery _

Through the Qi Anxin Virus Response Center mobile security team and the Qi Anxin threat intelligence platform (https ://ti.qianxin.com/) joint tracking analysis found that the earliest activities of the King Kong Elephant Organization can be traced back to June 2021. The following picture shows the earliest payload server information of the organization that we intercepted.

Figure 2.1 Screenshot of the earliest domain name payload server discovered (using NameSilo registrar domain name)

In the early attacks of this group, the "short link" of the download address of the attack payload is usually sent to the target through social software such as WhatsApp. Later, with the major social Taiwan banned related links, and the organization switched to delivering short links to target people in the form of pictures.

payload short chain address	**Corresponding to the actual download address**
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

Table 1 The discovered payload delivery short chains and their corresponding actual download addresses _

The load name servers used by this organization are all registered for less than a year and the registrars are mainly NameSilo and NameCheap. This is in line with another recent activity in South Asia the activity of the advanced attack group, the Brainworm, is similar.

Figure 2. 2 part of the domain name payload server who is the situation

3. Attack target

The King Kong Elephant Group has obvious intentions to steal military intelligence, mainly targeting Pakistani military personnel, affecting dozens of military personnel who have been involved in several units. Here is what we get from attacker C2 The photos and information of some victims' mobile phones were intercepted on the server.

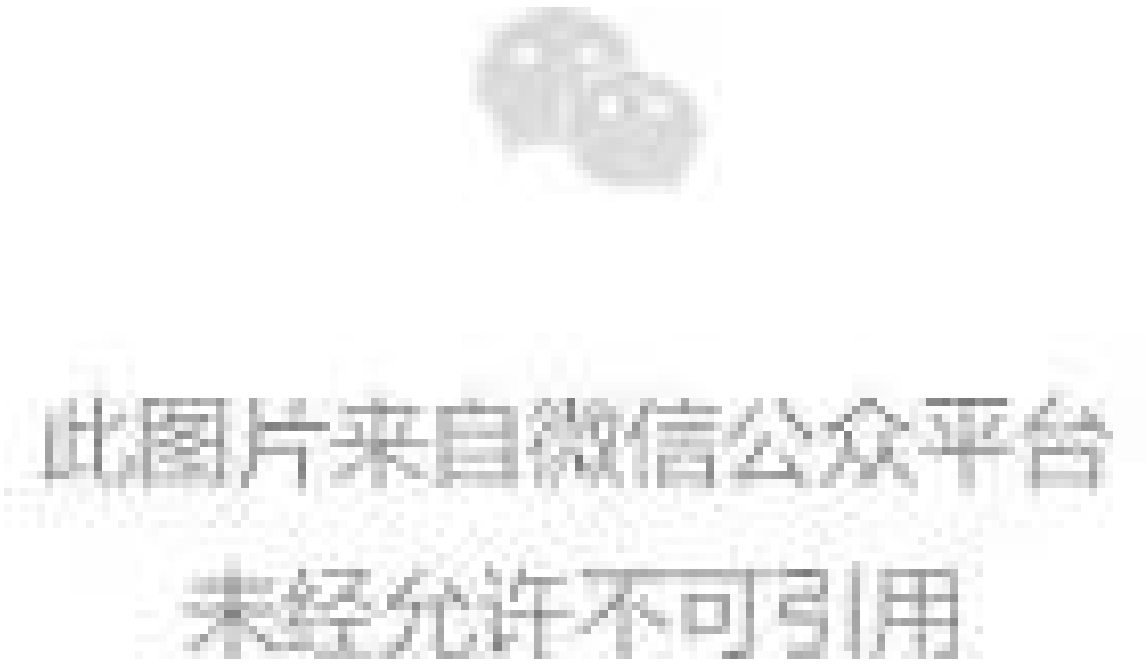

Figure 3.1 Stolen photos of Pakistan Frontier Guard (FC, FrontierCorps) personnel

Figure 3.2 Stolen photos of Pakistani Balochistan Border Guard (FC BLN , FC Balochistan) personnel

Figure 3.3 Information stolen from Balochistan border guards

Figure 3.4 Stolen photos of Pakistani special forces

Figure 3.5 Stolen photos of Pakistani police

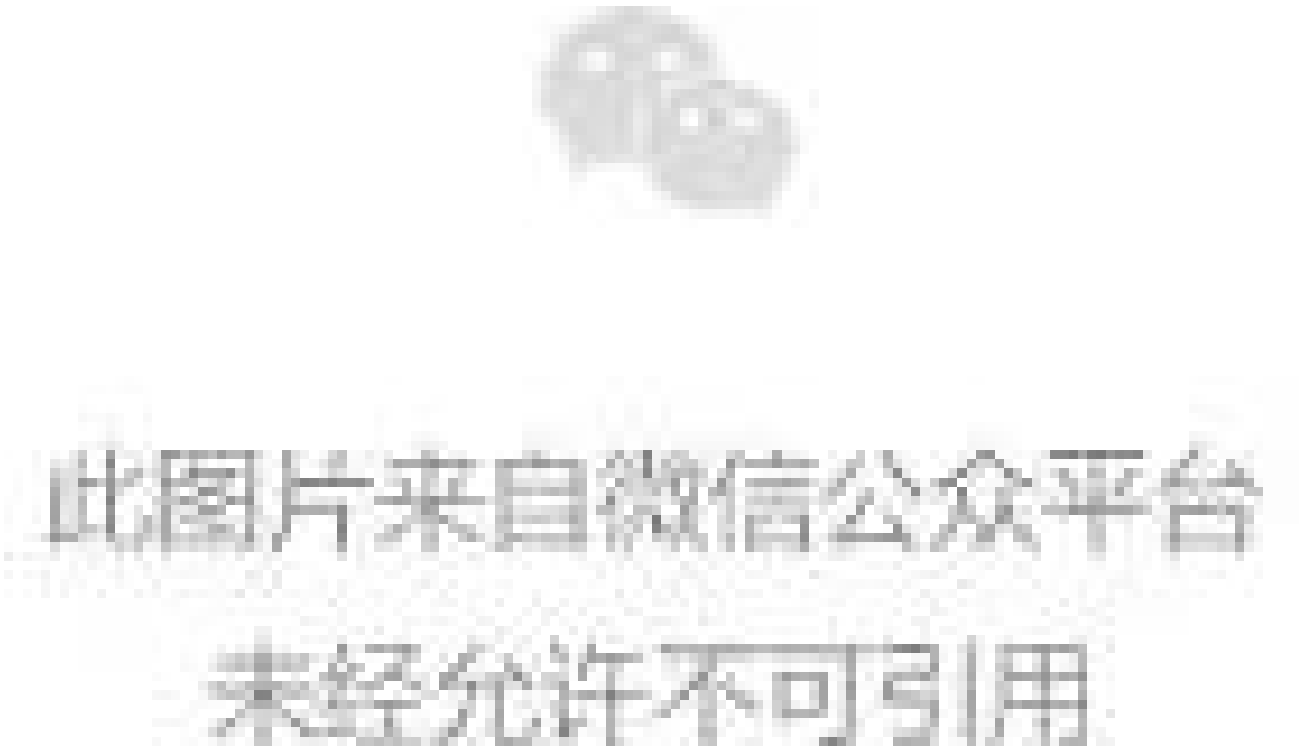

Figure 3.6 Information stolen from Pakistani police

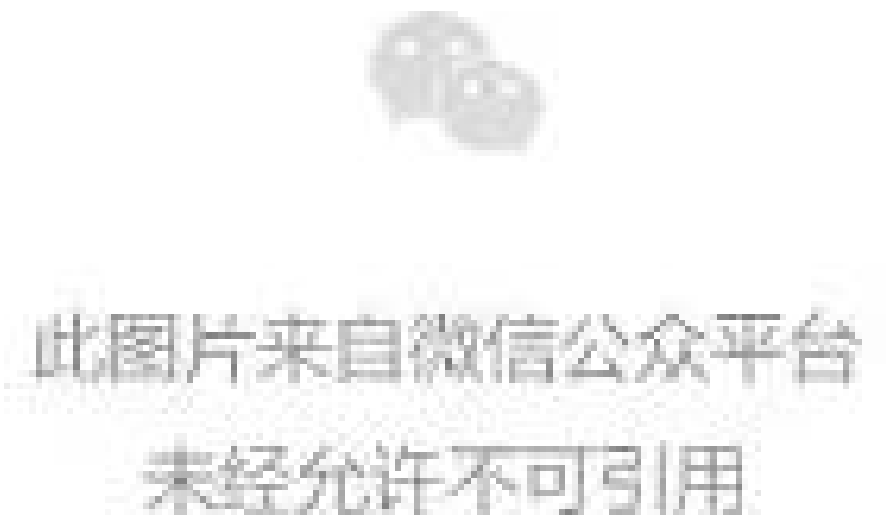

Figure 3.7 Pakistani Federal Bureau of Investigation (FIA, FederalInvestigationAgency) personnel were stolen photos piece

Figure 3.8 Stolen Information on the Chief of Staff of the Army

4. Technical Analysis _

Through analysis, it is found that the attack RAT invested by the King Kong Elephant Organization is currently targeting the Android platform. Analysis shows that the organization has a high degree of RAT customization and we Named VajraSpy. VajraSpy supports all the classic functions of espionage and stores the stolen data in a designated Google cloud storage space.

function	**Corresponding post - stealing data storage file name**
steal call logs	logs.json
steal address book	contacts.json
Steal SMS	sms.json

Steal 1 5 types of files in the specified directory of the SD card	file / filename
Steal notification bar information	noti/13-bit timestamp.json
Steal device information	device.json
Steal installed application information	appdetails.json
Stealing three versions of WhatsApp information	wa.json / wab.json / wabs.json

Table 2 VajraSpy RAT main stealing functions

Figure 4.1 15 types of files (text, pictures, audio) related code snippets stolen

5. Attacker portrait

1) The purpose of the attack

Attackers targeted Pakistani military , security and police personnel, including border guards (FC), special forces (SSG), Federal investigators Bureau (FIA) and Police and so on. Among them, the border guards are the main target. There are also a small number of activities targeting Nepalese military personnel. It can be seen from this that military personnel and military secrets are the the main purpose of the activity.

2) Attack method

Attackers are good at using social induced delivery and SMS induced delivery to attack, among which social induced delivery is the main method.

3) Network assets

The mobile phone numbers used by the attackers are all exclusive numbers of mobile service providers in a country in South Asia.

4) Native language features

The attackers used a large number of languages from a South Asian country in their attacks. The country has a longstanding military and geopolitical conflict with Pakistan.

5) Association with other APT organizations

The activity characteristics of the malicious sample download server are similar to those of the belly worm (Donot).

Some of the filenames used in the attack have certain similarities to the Bellyworm tissue.

To sum up, the King Kong Elephant Organization should be a senior executive with a government background in a South Asian country who mainly launched cyber attacks against Pakistani military personnel and military activities. attack group, is an active new APT organization in South Asia.

6. Summary and Recommendations

In traditional APT activities, the use of mobile social platforms is not common. This is because most of the sensitive and confidential information is stored on the computer and on the other hand, it is also caused by since attacks are launched through social platforms, it is easy to leave traces.

However, in the past two years, with the increasing popularity of mobile social platforms, we have found that many APT activities targeting developing countries will be more or less via mobile platforms, social platforms to proceed. For example, the Nuo Chong Lion Organization, the Blade Eagle Organization and the Diamond Elephant Organization disclosed this time all target the Android platform and network of social platforms attack activity. The analysis believes that the reasons for the increasing attention of APT activities on mobile platforms and social platforms mainly include the following aspects:

First of all, the level of network security construction and management in many developing countries is relatively backward, so that it is possible to gain access to smartphones only through attacks on smartphones. Large amounts of sensitive and confidential information.

Second, the popularity of smartphones is getting higher and higher. It is a low-cost, high-cost way to launch cyber attacks through social platforms against secret-related personnel with insufficient security awareness. Efficient attack.

Third, smartphones often have more unfixed security vulnerabilities, and the penetration rate of mobile security software is not high, which leads to the launch of network targeting mobile platforms. The technical threshold of attack is relatively lower.
Then, for government and enterprise institutions, especially the military, police and other secret or sensitive institutions, how should they do a good job in protection and try to avoid or reduce the targeting of immigrants as much as possible? Mobile platform, social platform, what is the impact of APT activities on yourself ? Here we give some practical suggestions as follows.

1) Work and life are separated, and sensitive information is not shared

Agencies should strive to avoid staff using personal smartphones for routine office activities. Conditional units can distribute work mobile phones or confidential mobile phones to staff. If the conditions are true It is not allowed. You can use enterprise - level secure mobile work platforms for internal communication and office work, such as Lanxin and cloud mobile phone security management systems.

2) Strengthen safety awareness education and strictly implement safety regulations

Relevant institutions should strengthen employee security awareness education, do not use personal mobile phones to shoot, store sensitive or confidential information, and do not share sensitive or confidential information through social platforms information; don’t click on strangers’ posts Unknown links come; reject the temptation of illegal information such as pornography and gambling. At the same time, relevant agencies should also formulate practical cybersecurity management standards and employee code of conduct, and carry out strict Supervision and review.

3) Update software system, use security software

Relevant institutions should require employees, whether it is an office mobile phone or a personal mobile phone, to update the operating system and core software in a timely manner to ensure that the smart phone starts to work. Always in the best safe condition. Same Install the necessary mobile phone security software at any time to reduce the damage of various Trojan horses and viruses as much as possible.

4) Establish threat intelligence capabilities to prevent APT attacks

Relevant institutions should work with professional security vendors to build efficient threat information collection, analysis and disposal capabilities, and timely detect, intercept and track various APT activities. Bring APT activities to the Impact and losses are minimized.
At present, a full line of products based on Qi'anxin's self - developed Owl engine and Qi'anxin Threat Intelligence Center 's threat intelligence data , including Qi'anxin's threat intelligence platform (TIP), Tianqing, Tianji, Sky Eye Advanced Threat Detection System, Qi An Xin N G SOC, Qi An Xin Situational Awareness, etc., have all supported the accurate detection of such attacks.

IOCs

Domain name / IP	**Purpose**
appplace.shop	payload server
appz.live	payload server
apzshare.club	payload server
appzshare.digital	payload server

appzshare.club	payload server
212.24.100.197	payload server

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