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

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

Original QAX Virus Response Centre Qi Anxin Virus Response Center *2022-03-30 12:00*

1. Summary of the event

In February 2022 , the mobile security team of Qi'anxin Virus Response Center noticed that since June 2021 , an A _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ P& T organization mainly targets PakistanThe 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 victimThe personnel are mainly Pakistani national border guards (FC) and special forces (SSG) , especially the Balochistan border guards (FCBLN) ; in addition _ _ _ _ Also contains a small amount of FBI (FIA) and police (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 V a j r a Sp y . _ _ _ _

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 regionOther APT tissues that jumped , such as Sidewinder Sidewinder , Manling Flower Bitter , Belly Brainworm Donot , etc. , were not significantly associated _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ (Only with bellyworm D o no o t _ _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 V a j r a E l e ph , and the organization number is A P T - Q - 4 3 . 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 (h t t p s : / / t i . q i a n x i n . c o m /) joint tracking analysis found that , the earliest activities of the King Kong Elephant Organization can be traced back to June 2021 . The picture below shows the earliest payload server information of the organization that we intercepted .

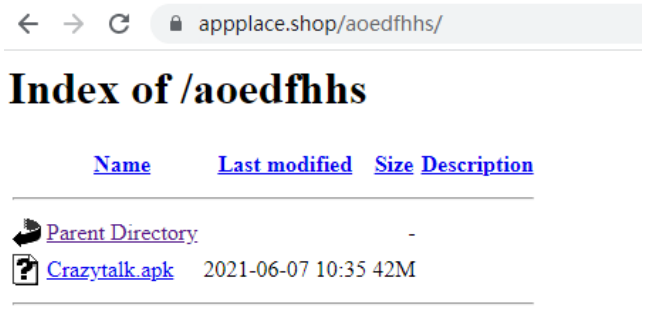


Figure 2.1 Screenshot of the earliest domain name payload server discovered (using Name Sil o registrar domain name) _ _ _ _ _ _

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 socialTaiwan 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 Discovered short chains of payload delivery 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 Name Sil o and Name Cheap . _ _ _ _ _ _ _ This is in line with another recent activity in South AsiaThe activity of the advanced attack group , the brainworm , is similar .

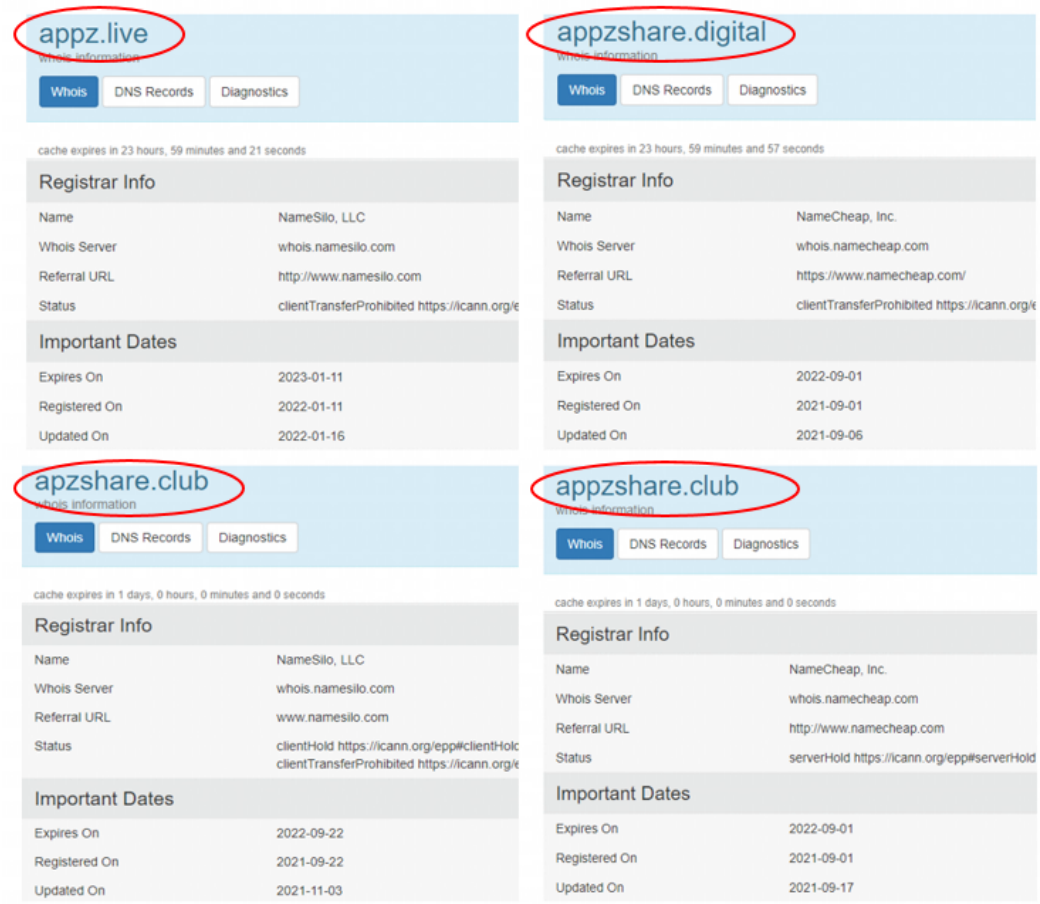


Figure 2. 2 part of the domain name payload server who is the situation

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 's what we get from attacker C 2The photos and information of some victims' mobile phones were intercepted on the server .

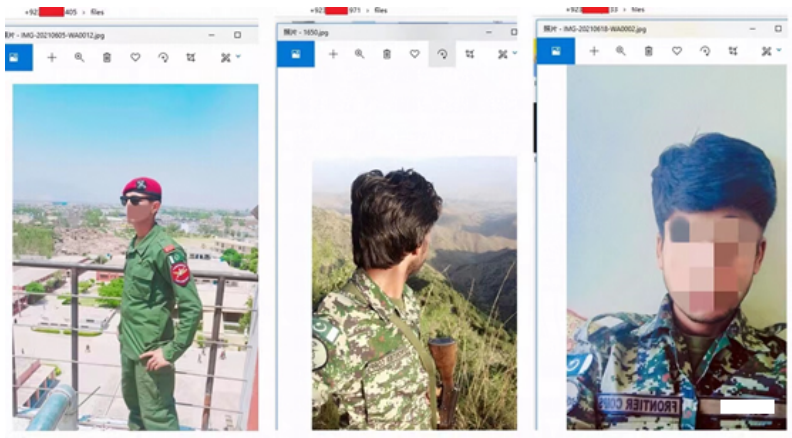


Figure 3.1 Stolen photos of Pakistan Frontier Guard (FC , F ro n ti e r C o r p s) personnel _ _ _

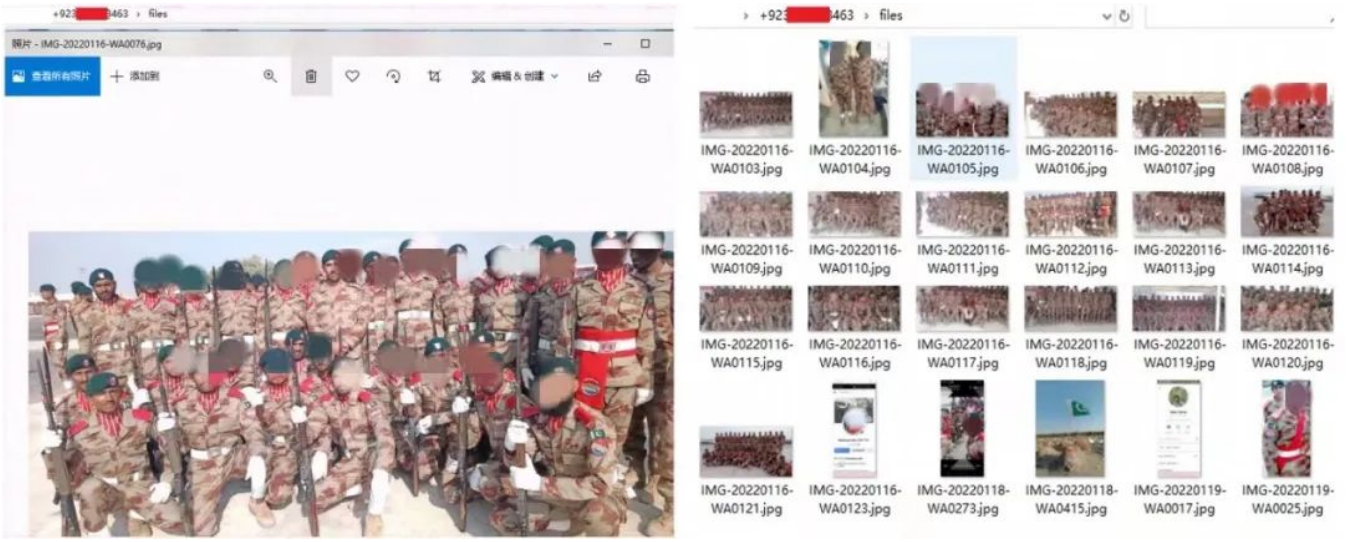


Figure 3.2 Stolen photos of Pakistani Balochistan Border Guard (FC B L N , FC Balochistan) personnel _ _ _ _ _ _ _ _ _ _ _ _ _ _

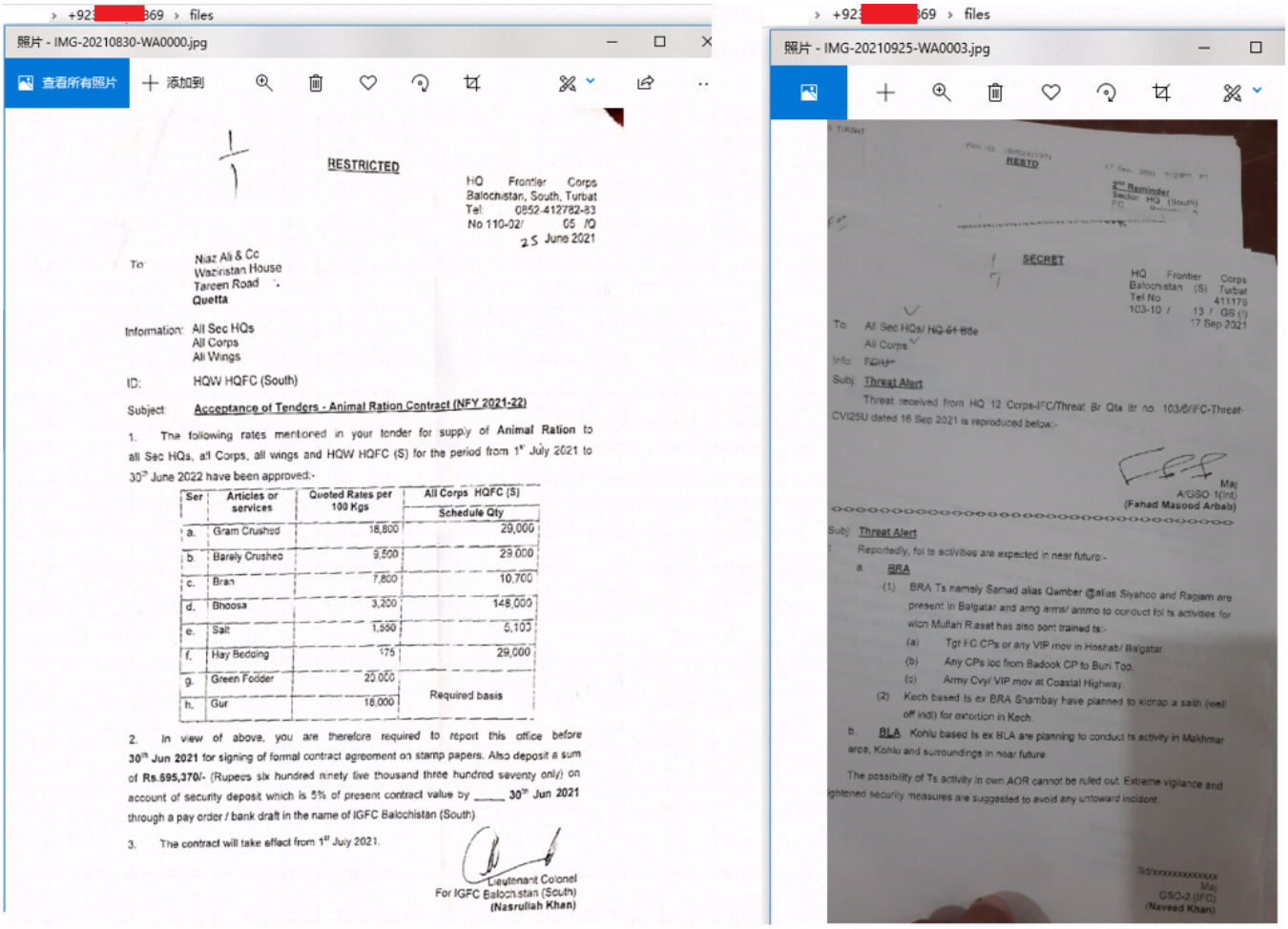


Figure 3.3 Information stolen from Balochistan border guards _ _

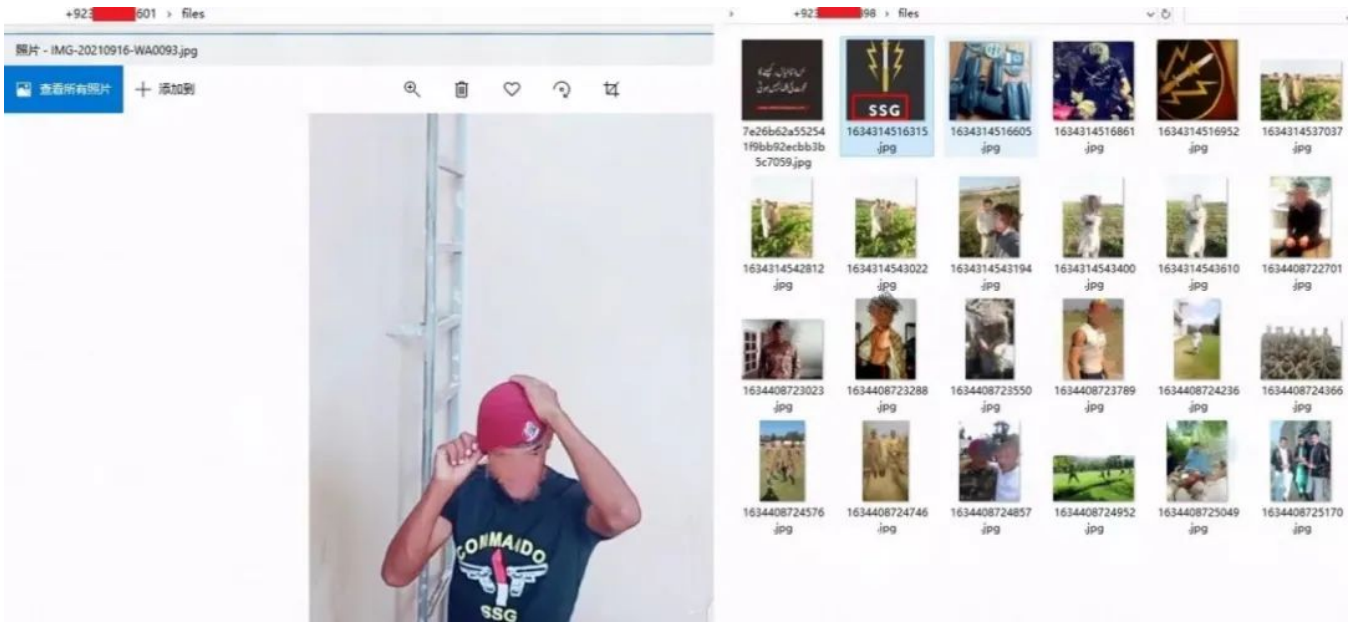


Figure 3.4 Stolen photos of Pakistani special forces _

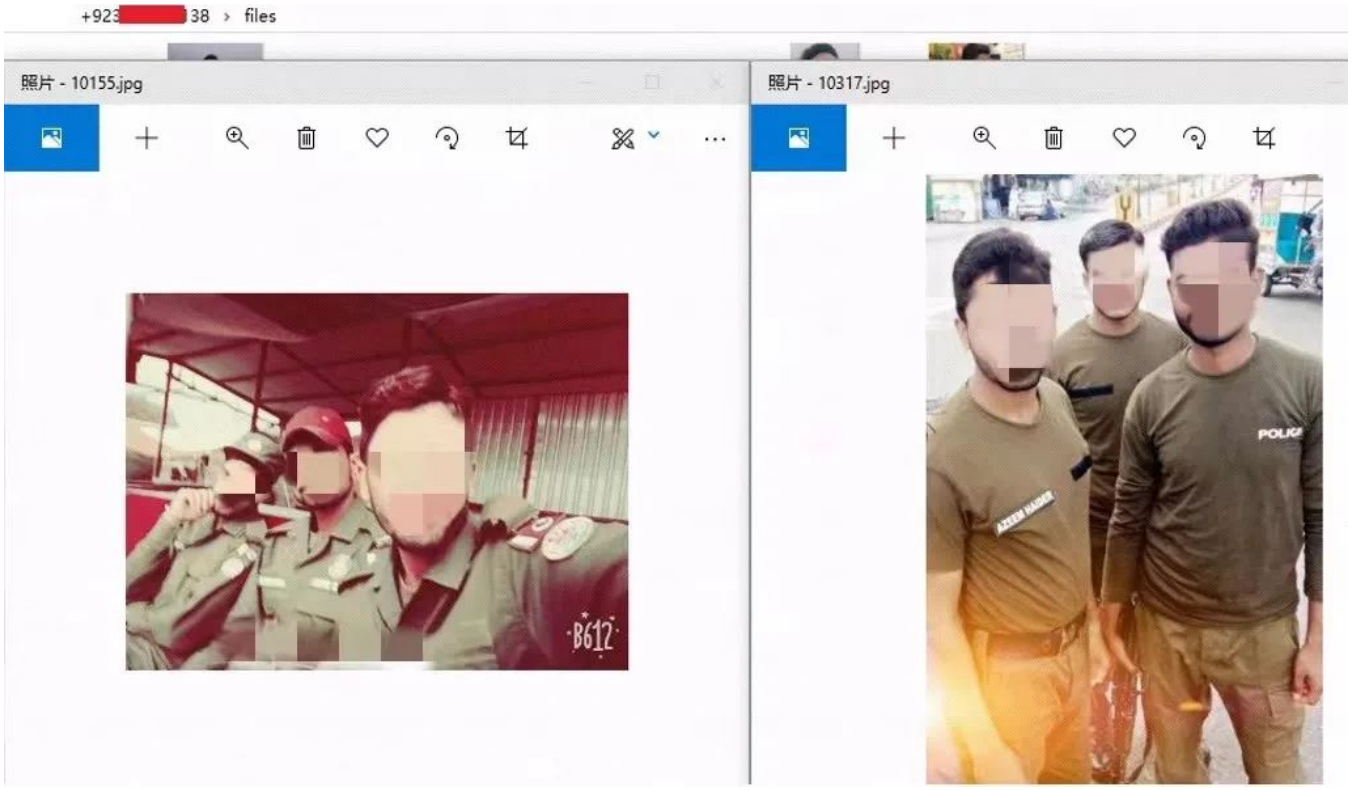
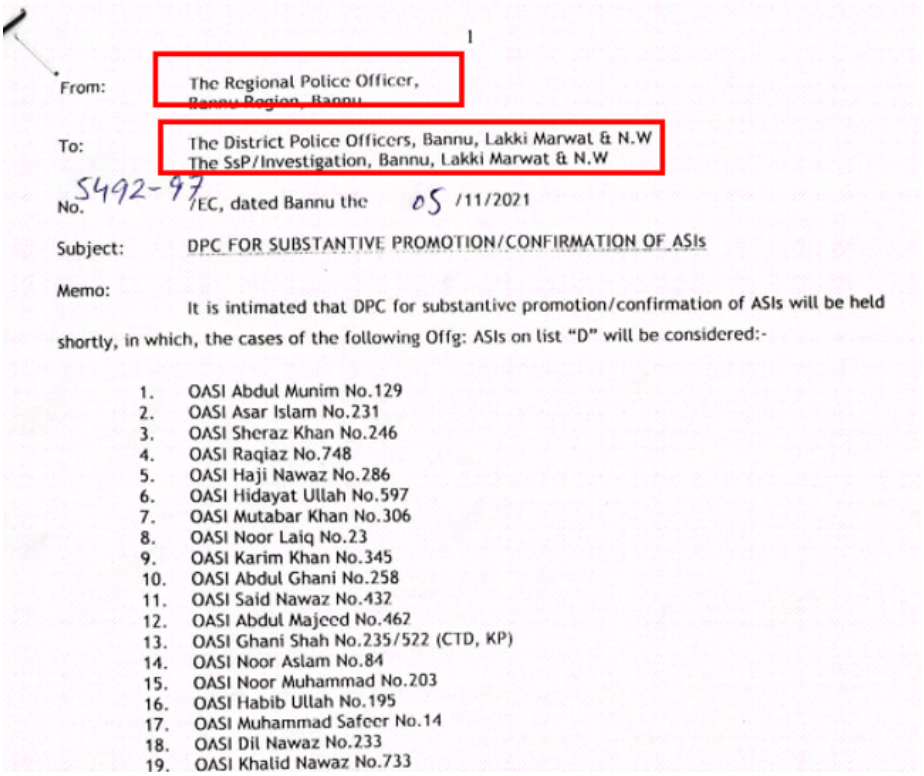


Figure 3.5 Stolen photos of Pakistani police _



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

Figure 3.6 Pakistani Police Stolen Information _ _

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

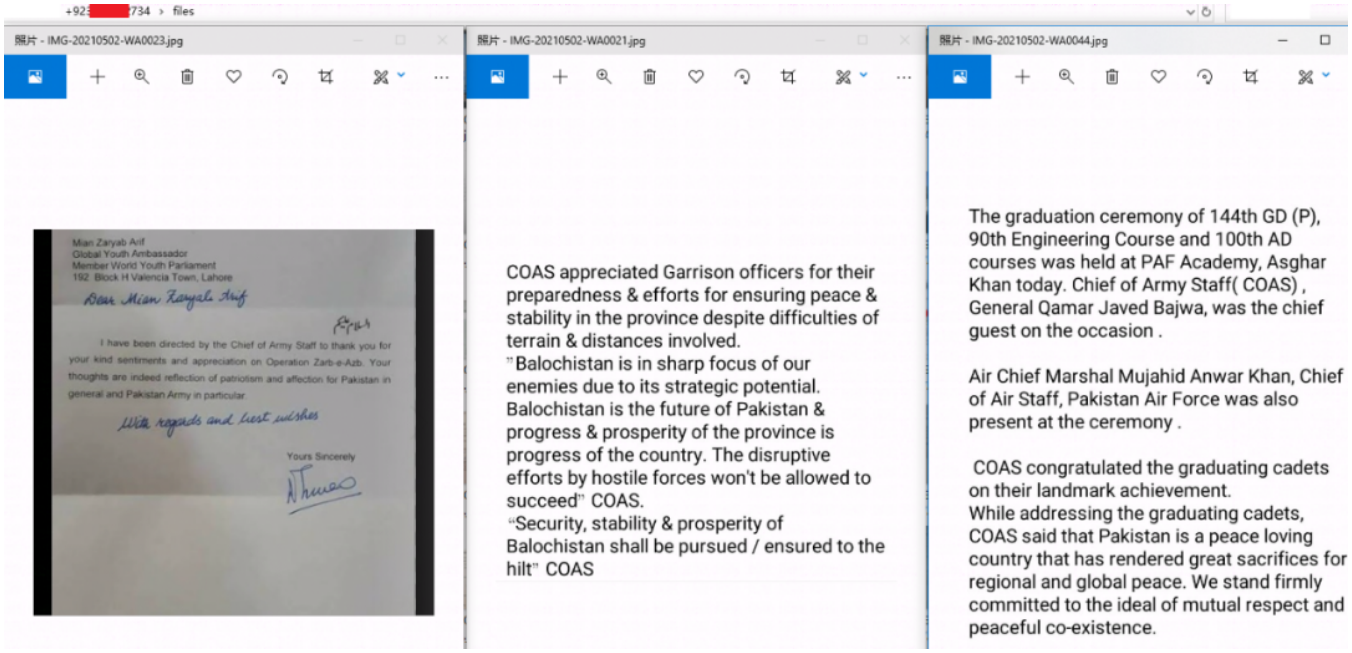


Figure 3.8 Stolen Information on the Chief of Staff of the Army _

4. Technical Analysis _

Through analysis , it is found that the attack RA T invested by the King Kong Elephant Organization is currently targeting the Android platform . _ Analysis shows that the organization has a high degree of R A T customization , and weNamed V a j r a Sp y . _ _ V a j r a Spy 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	l o g s . j s o n
steal address book	c o n t a c t s . j s o n
Steal SMS	s m s . j s o n
Steal 1 5 types of files in the specified directory of the SD card	file / filename _ _ _ _ _
Steal notification bar information	n o t i / 1 3 -bit timestamp . j s o n
Steal device information	d e v i c e . j s o n
Steal installed application information _ _ _	a p p d e t a i l s . j s o n
Stealing three versions of WhatsApp information _ _ _ _ _ _ _	w a . j s o n / w a b . j s o n / w a b s . j s o n

Table 2 V a j r a S p y R A T main stealing functions _ _

```
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()));
```

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 (P _ _o l ic e) 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 thethe 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 byBecause of launching attacks 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 A P T activities targeting developing countries will be more or less Via mobile platforms , social platformsto proceed . For example , the Nuo Chong Lion Organization , the Blade Eagle Organization and the Diamond Elephant Organization disclosed this time all target the An d r oi d platform and _ _ _ _ _ network of social platformsattack 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 ? App for mobile platforms and social platforms _What is the impact of T 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 trueIt 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’ postsUnknown 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 strictSupervision 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 . sameInstall 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 . _ move , 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 .

Part IOC _ _

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

AndroidMD5	package name
7a47d859d5ee719340184433e3ab7ed5b	com.cr.chat_ _
0c980f475766f3a57f35d19f44b07666	com.crazy.talk

Appendix 1 Qi Anxin Virus Response Center

Qi'anxin Virus Response Center is **a** virus identification and response professional team under Beijing Qi'anxin Technology Co., Ltd. (Qianxin Group) , backed by the core of Qi'anxin Cloud platform , with daily tens of millionsSample detection and disposal capabilities , daily 100 million -level safety data correlation analysis capabilities . Combining years of anti- virus core security technology and operational experience , based on the Q O W L and Q D E independently developed by the group(artificial intelligence) engine , forming cross- platform Trojan virus and vulnerability detection and repair capabilities , and has powerful big data analysis and realization of full platform security . Full protection and early warning capabilities .

Qi'anxin Virus Response Center is responsible for supporting the virus detection of Qi'anxin 's entire line of security products , actively responding to security feedback from customers , and can provide customers with the first time Eliminate intractable diseases . _ Center ZengHe has dealt with major virus incidents many times and participated in the security work of major events , which has been highly recognized by customers , which has enhanced Qi Anxin 's brand influence in the industry .

Appendix 2 Qi'anxin Virus Response Center Mobile Security Team _

The mobile security team of **Qi'anxin Virus Response Center** has been committed to the research in the field of mobile security and Android security ecology . At present , Qi Anxin 's mobile security products can not only detect and kill commonIt can also accurately detect and kill popular software such as brushing , fraud , gambling , violations , pornography and other black products . _ _ _ _ _ It can effectively support traceability through its internal analysis systemAnalysis and other tracking . Through its high-value mobile attack discovery process , it has captured a number of attack events , released a number of mobile black industry reports , and disclosed multiple A P T groups . weaving activities , _Two years ago , new APT organizations under the background of 4

countries have been disclosed for the first time (Nuo Chong Lion Organization Si l en c e r L ion , Blade Eagle Organization B l a d e H aw k , Aiye Leopard Organization S _no w L e o par d and this time the Vajra Eleph) . _ _ _ _ _ _ _ _ _ _ _ _ In the future , we will continue to be at the forefront of global mobile security research , tracking and analyzing the first timeThe latest mobile security incidents , in -depth exploration and tracking of domestic mobile - related black and gray products , are striving to maintain the network security on the mobile terminal .

Appendix 3 Introduction of Qi'anxin Mobile Products

Qi'anxin Mobile Terminal Security Management System (Tianji) **is** aimed at customers in public security , justice , government , finance , operators , energy , manufacturing and other industries . Terminal control and strong terminal security features _A unique mobile terminal security management product . The product is based on Qi Anxin 's security technology accumulation and operation experience on massive mobile terminals , from hardware , OS , application , data to link and other multi - levelSecurity protection solutions to ensure the security of enterprise data and applications in mobile terminals .

Qi'anxin Mobile Situational Awareness System is a mobile situational awareness management product jointly launched by Qi'anxin Security Supervision BG Situational Awareness First Division and its partner Qi'anxin Virus Response Center Mobile Team. Different from traditional mobile security vendors, which focus on APP production and release, and provide customers with APP reinforcement, detection, analysis, etc.; mobile situational awareness is oriented to customers with regulatory responsibilities, focusing more on APP download and use, and find out the scope of the jurisdiction. The use of APP provides customers with functions such as APP illegal detection, compliance analysis, and traceability.