Lookout Discovers Novel Confucius APT Android Spyware Linked to India-Pakistan Conflict

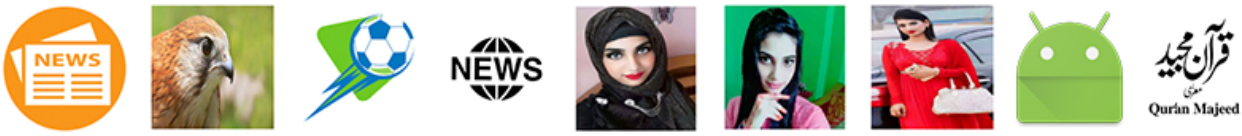
lookout.com/blog/lookout-discovers-novel-confucius-apt-android-spyware-linked-to-india-pakistan-conflict

February 10, 2021

The Lookout Threat Intelligence team has discovered two novel Android surveillanceware – Hornbill and SunBird. We believe with high confidence that these surveillance tools are used by the advanced persistent threat group (APT) Confucius, which first appeared in 2013 as a state-sponsored, pro-India actor primarily pursuing Pakistani and other South Asian targets.1 2

While primarily known for desktop malware, the Confucius group was previously reported to have started leveraging mobile malware in 2017, with the Android surveillanceware ChatSpy.3 However, our discovery of SunBird and Hornbill shows that Confucius may have been spying on mobile users up to a year before it started using ChatSpy.

Targets of these tools include personnel linked to Pakistan's military, nuclear authorities, and Indian election officials in Kashmir. Hornbill and SunBird have sophisticated capabilities to exfiltrate SMS, encrypted messaging app content, and geolocation, among other types of sensitive information.



SunBird has been disguised as applications that include:

- *Security services, such as the fictional "Google Security Framework"*
- *Apps tied to specific locations ("Kashmir News") or activities ("Falconry Connect" and "Mania Soccer")*
- *Islam-related applications ("Quran Majeed").*

The majority of applications appear to target Muslim individuals.

Lookout named Hornbill after the Indian Grey Hornbill, which is the state bird of Chandigarh and where the developers of Hornbill are located. SunBird's name was derived from the malicious services within the malware called "SunService" and the sunbird is also native to India.

Malicious functionality and impact of both SunBird and Hornbill

Hornbill and SunBird have both similarities and differences in the way they operate on an infected device. While SunBird features remote access trojan (RAT) functionality – a malware that can execute commands on an infected device as directed by an attacker – Hornbill is a discreet surveillance tool used to extract a selected set of data of interest to its operator.

Both of the malware can exfiltrate a wide range of data, such as:

- Call logs
- Contacts
- Device metadata including phone number, IMEI/Android ID, Model and Manufacturer and Android version
- Geolocation
- Images stored on external storage
- WhatsApp voice notes, if installed

Both malware are also able to perform the following actions on device:

- Request device administrator privileges
- Take screenshots, capturing whatever a victim is currently viewing on their device
- Take photos with the device camera
- Record environment and call audio
- Scrape WhatsApp messages and contacts via accessibility services
- Scrape WhatsApp notifications via accessibility services

SunBird-specific functionality

SunBird has a more extensive set of malicious capabilities than Hornbill. It attempts to upload all data it has access to at regular intervals to its command and control (C2) servers. Locally on the infected device, the data is collected in SQLite databases which are then compressed into ZIP files as they are uploaded to C2 infrastructure.

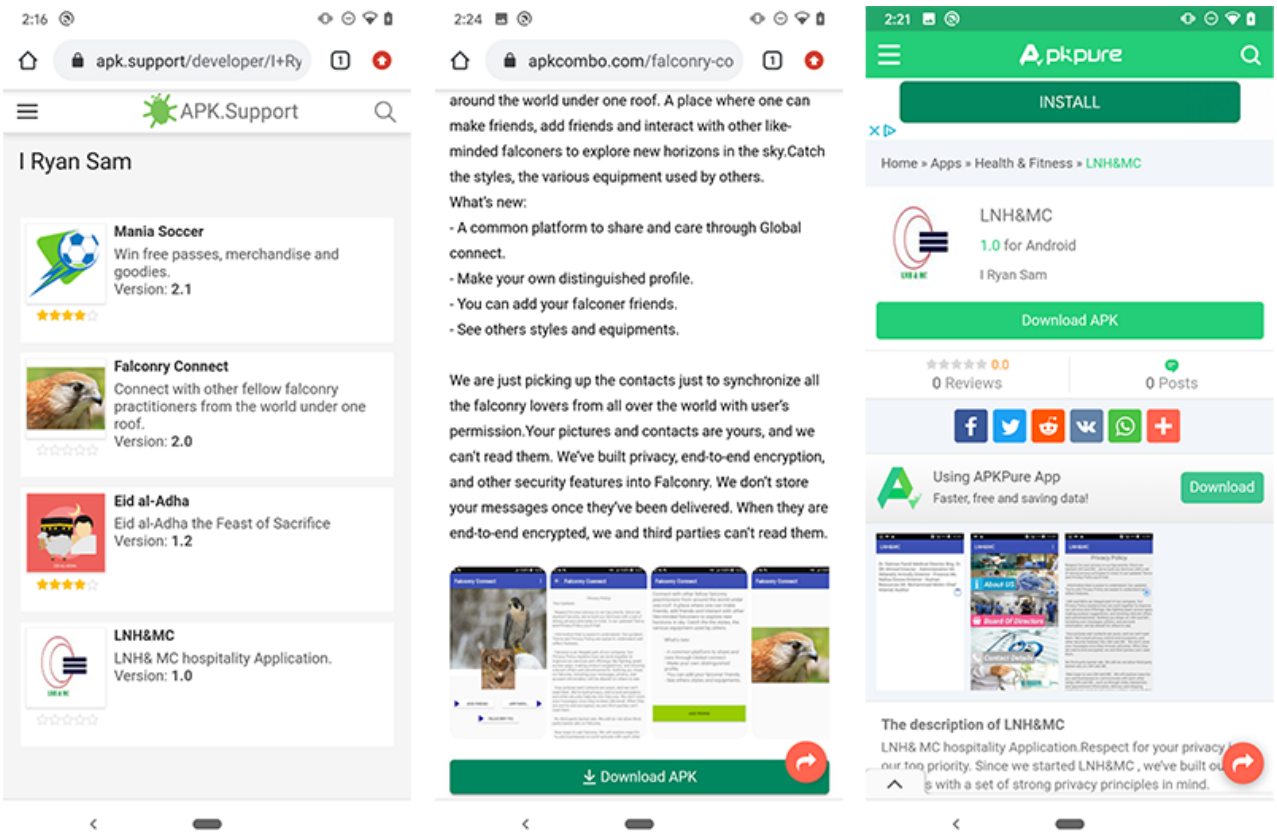
SunBird can exfiltrate the following list of data, in addition to the list above:

- List of installed applications
- Browser history
- Calendar information
- BlackBerry Messenger (BBM) audio files, documents and images
- WhatsApp Audio files, documents, databases, voice notes and images
- Content sent and received via IMO instant messaging application

In addition to the list of actions above, SunBird can also perform the following actions:

- Download attacker specified content from FTP shares
- Run arbitrary commands as root, if possible
- Scrape BBM messages and contacts via accessibility services

- Scrape BBM notifications via accessibility services



Samples of SunBird have been found hosted on third-party app stores, indicating one possible distribution mechanism. Considering many of these malware samples are trojanized – as in they contain complete user functionality – social engineering may also play a part in convincing targets to install the malware. No use of exploits was observed directly by Lookout researchers.

Hornbill-specific functionality

In contrast, Hornbill is more of a passive reconnaissance tool than SunBird. Not only does it target a limited set of data, the malware only uploads data when it initially runs and not at regular intervals like SunBird. After that, it only uploads changes in data to keep mobile data and battery usage low. The upload occurs when data monitored by Hornbill changes, such as when SMS, or WhatsApp notifications are received or calls are made from the device.

Hornbill is keenly interested in the state of an infected device and closely monitors the use of resources. For example, if the device is low on memory, it triggers the garbage collector. In addition to the list of exfiltrated data mentioned earlier, Hornbill also collects hardware information. For example, the malware can check if a device's screen is locked, the amount of available internal and external storage and whether WiFi and GPS are enabled.

Hornbill only logs location information if it deems the changes to be significant enough from the previously recorded location – if the difference between the corresponding latitudes and longitudes differ by more than 0.0006 which is roughly 70 metres.

Data collected by Hornbill is stored in hidden folders on external storage. Once call recordings or audio recordings are uploaded to C2 infrastructure they are deleted from the device to avoid suspicion.

Location on external storage	Type of data collected
/sdcard/.system0/.ia	Audio (environment) recordings
/sdcard/.system0/.cr	Call recordings
/sdcard/.system0/.tempo	Temporary location used for testing upload to C2 infrastructure
/sdcard/.system0/.is/.iss	Screenshots
/sdcard/.system0/.is/.ifcc	Front camera “clicks” (photos)
/sdcard/.system0/.is/.ircc	Rear camera “clicks” (photos)

List of hidden folders Hornbill creates and stores data to be exfiltrated to C2 infrastructure.

Hornbill uses a unique set of server paths to communicate to C2 infrastructure. These are listed below along with what action Hornbill takes when sending HTTP POST requests to each.

Unique Server Paths	Action
/SignUp	Registers either a Device ID or User ID with a hardcoded password for further data exfiltration
/UploadFile	Uploads file
/SaveMessages	Bulk saves messages
/SaveCallLogs	Bulk saves call logs
/SaveContactDetails	Bulk saves contacts
/SaveGpsDetails	Bulk saves GPS location
/UpdateMobileState	Saves directory structure
/UpdateMobileState	Queries C2 for queued and removed commands

The operators behind Hornbill are extremely interested in a user’s WhatsApp communications. In addition to exfiltrating message content and sender information of messages, Hornbill records WhatsApp calls by detecting an active call by abusing

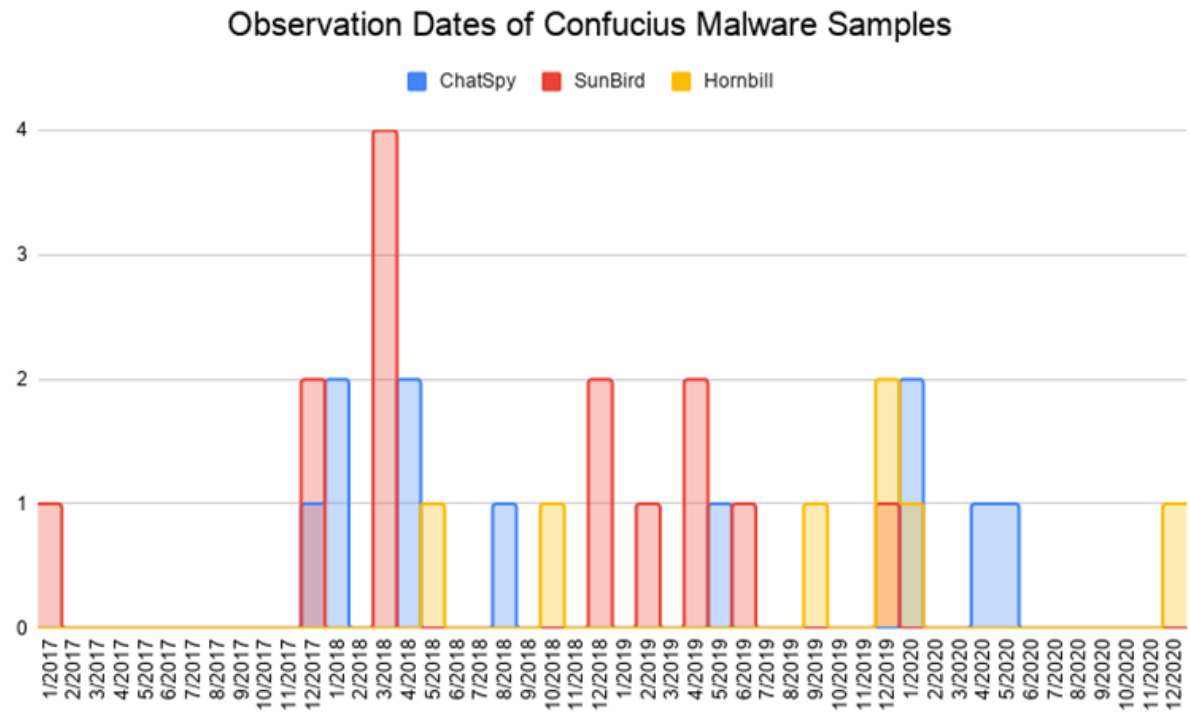
Android's accessibility services. The exploitation of Android's accessibility services in this manner is a trend we are observing frequently in Android surveillanceware. This enables the threat actor to avoid the need for privilege escalation on a device.

Lastly, Hornbill searches for and monitors activity on any documents stored on external storage with the following suffixes: ".doc", ".pdf", ".ppt", ".docx", ".xlsx", ".txt". Whenever a document is created, opened, closed, modified, moved or deleted, this action is logged by Hornbill. Functionality exists to modify this list of suffixes, but is incomplete in the samples we have observed. The latest samples of Hornbill show that this malware threat may still be under development.

Development timelines

The newest Hornbill sample was identified by Lookout's app analysis engine as recently as December 2020, suggesting the malware may still be active today. Both ChatSpy and Hornbill's packaging dates appeared to have been tampered with, but we first observed them in January 2018 and May 2018 respectively.

Lookout first observed SunBird in January 2017, but unlike the other two malware families, the packaging dates appear legitimate, indicating the malware was likely in development between December 2016 and early 2019.

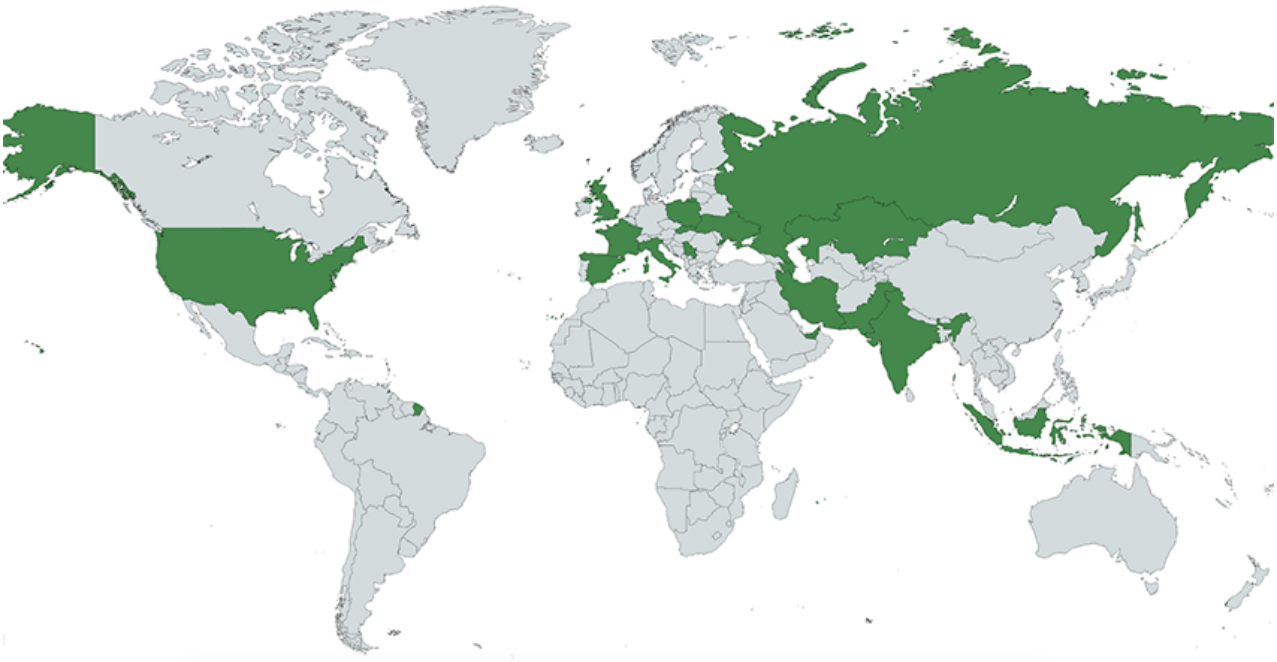


Hornbill, which Lookout first saw in May 2018, is actively deployed. We observed new samples as recently as December 2020. The first SunBird sample was seen as early as 2017 and as late as December 2019.

Targeting

To better understand who SunBird may have been deployed against, we analyzed over 18GB of exfiltrated data that was publicly exposed from at least six insecurely configured C2 servers. All data uploaded to the C2 infrastructure included the locale of the infected devices. This information, combined with the data content, gave us extensive insight into who was being targeted by this malware family and the kind of information the attackers were after.

Some notable targets included an individual who applied for a position at the Pakistan Atomic Energy Commission, individuals with numerous contacts in the Pakistan Air Force (PAF), as well as officers responsible for electoral rolls (Booth Level Officers) located in the Pulwama district of Kashmir.



Based on the locale and country code information of infected devices and exfiltrated content, we think SunBird may have roots as a commercial Android surveillanceware. The data included information on victims in Europe and the United States, some of which appear to be targets of spouseware or stalkerware. It also included data on Pakistani nationals in Pakistan, India and the United Arab Emirates that we believe may be targeted by Confucius APT campaigns between 2018 and 2019.

Malware development and commercial surveillance roots

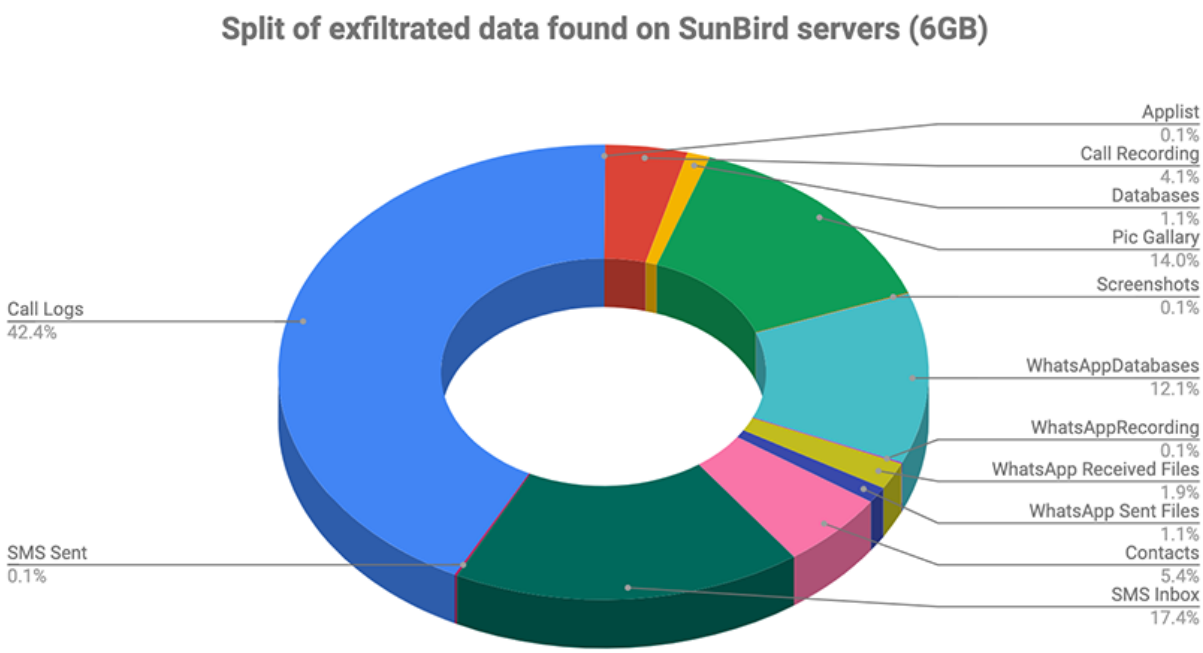
Both Hornbill and SunBird appear to be evolved versions of commercial Android surveillance tooling. Hornbill seems to be derived from the same code base as a previously active commercial surveillanceware product known as MobileSpy. 5 It is unclear how the developers of Hornbill acquired the code, but the company behind MobileSpy, Retina-X Studios, shut down their surveillance software products in May 2018 after being hacked twice. 6 Links between the Hornbill developers indicate they all appear to have worked together at a number of Android and iOS app development

companies registered and operating in or near Chandigarh, Punjab, India. In 2017, one developer claimed to be working at India's Defence Research and Development Organisation (DRDO) on their LinkedIn profile.

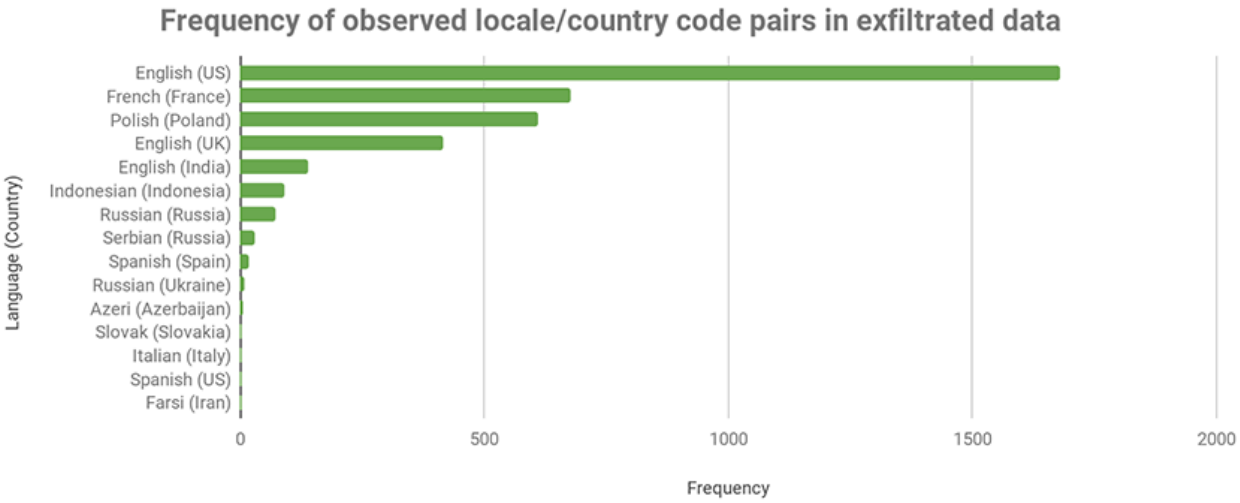
SunBird looks to have been created by Indian developers who also produced another commercial spyware product, which we dubbed BuzzOut. 7 The theory that SunBird's roots lay in stalkerware was also supported by the content found in the exfiltrated data we uncovered. The data included information on stalkerware victims, as well as Pakistani nationals living in Pakistan and traveling in the UAE and India. This data suggests that SunBird could have been sold to an actor that selectively deployed it to gather intelligence on targeted individuals. Similar behavior was observed with Stealth Mango and Tangelo, two nation state mobile surveillanceware Lookout researchers discovered in 2018. 8

Exfiltrated data

During this investigation, we were able to access exfiltrated data for SunBird whose C2 infrastructure had been insufficiently secured.



This is a breakdown of types of data SunBird exfiltrated. This data is from publicly-accessible exfiltrated content exposed on SunBird C2 servers for 5 campaigns between 2018 and 2019. We found another 12 GB of data exfiltrated on another C2 server 23.82.19[.]250. The default language of this server was set up as Chinese when discovered by Lookout researchers. This may be a false flag or may have been altered by a third party. This also makes it difficult to confirm if all of the data originated from infections of actual target devices.



Frequency of infected devices' locale and country code settings (translated to languages and countries) as packaged within publicly-accessible exfiltrated data. This data includes both the Confucius APT targets and spouseware victims of SunBird.

Left:*One particular SunBird C2 server was found to also be exposing a log file containing IP addresses of those that logged into the administrator panel. The majority of these were distributed throughout India.* ***Right:*** *Geo-location data captured from a publicly-exposed database found on another Sunbird C2 IP 23.82.19[.]250. Almost all data stored on this server referenced phone numbers of various locations in northern India. The second most common region for phone numbers was Pakistan.*

Within the exfiltrated data, one particular victim caught our interest. This individual was using WhatsApp to correspond with someone applying for a position at the Pakistan Nuclear Regulatory Authority in 2017. In 2018, messages were uncovered from someone applying for a position at the Pakistan Atomic Energy Commission.9

Additional exfiltrated data from late 2018 and early 2019 indicated that SunBird was being used to monitor Booth Level Officers10 responsible for field-level information regarding electoral rolls in the Pulwama district of Kashmir. This time and location is

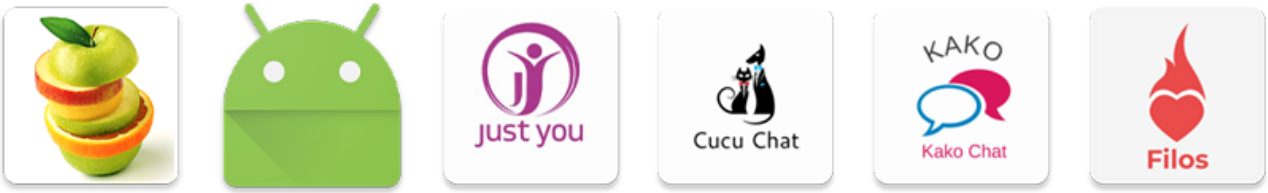
significant as Pulwama suffered a suicide bombing attack in February 2019, which increased tensions between India and Pakistan. The start date of active monitoring of this target on C2 servers coincided with the start of the Indian general elections held in April 2019.

1545971185database.zip 2018-12-28 04:26
1545973809database.zip 2018-12-28 05:10
1545981820database.zip 2018-12-28 07:23
1547835136database.zip 2019-01-18 18:12
1554948425database.zip 2019-04-11 02:07
1554948426database.zip 2019-04-11 02:07
1554948427database.zip 2019-04-11 02:07
1554948428database.zip 2019-04-11 02:07
1554948429database.zip 2019-04-11 02:07

Continuous data exfiltration data that occurred every ten minutes stopped at the end of 2018. Aside from one brief upload in January 2019, it suddenly picked up again on the 11th of April 2019. While this may be coincidence, this is also the same day that the Indian general elections of 2019 began.12

A total of 156 victims were discovered in this new dataset and included phone numbers from India, Pakistan and Kazakhstan.

Confucius connection



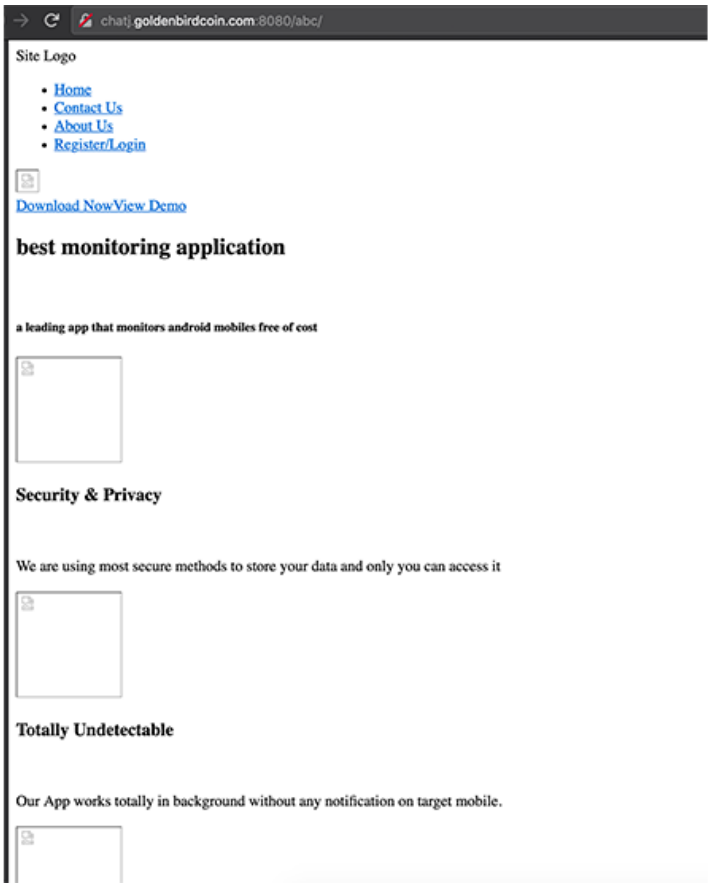
Hornbill application icons impersonate various chat and system applications.

Similar to previous Confucius tactics seen with ChatSpy, Hornbill samples often impersonate chat applications such as Fruit Chat, Cucu Chat and Kako Chat. The related C2 infrastructure communicates on port 8080, a pattern also seen on the desktop campaigns carried out by Confucius.14

The Confucius group is well known for impersonating legitimate services to cover their tracks and confuse its victims. Naming malicious apps similar to legitimate ones may be an attempt to gain a target's trust. For example, "kako chat" may have been named due to its similarity to KakaoTalk.15 However, Kako Chat's C2 server (chatk.goldenbirdcoin[.]com) references a defunct cryptocurrency by the same name.16 Cucu Chat may refer to a seemingly benign dating app of the same name that is available on third-party app stores such as APKPure.17, 18 However, Cucu Chat communicates to the site http://wangu[.]xyz19 (also on port 8080) and itself appears to be an

impersonation of Wangu, an application which advertises itself as a chat app for Zimbabweans.20 The latest sample of Hornbill titled “Filos” trojanizes the Mesibo21 Android application for legitimate chat functionality.

During our investigation, we noticed that Hornbill C2 infrastructure hosted HTML resources consistent with a commercial spyware page, but missing its image resources.



C2 servers for Hornbill were found to host HTML content from a commercial spyware.

Additionally, Hornbill carries out data exfiltration via the following unique set of server paths:

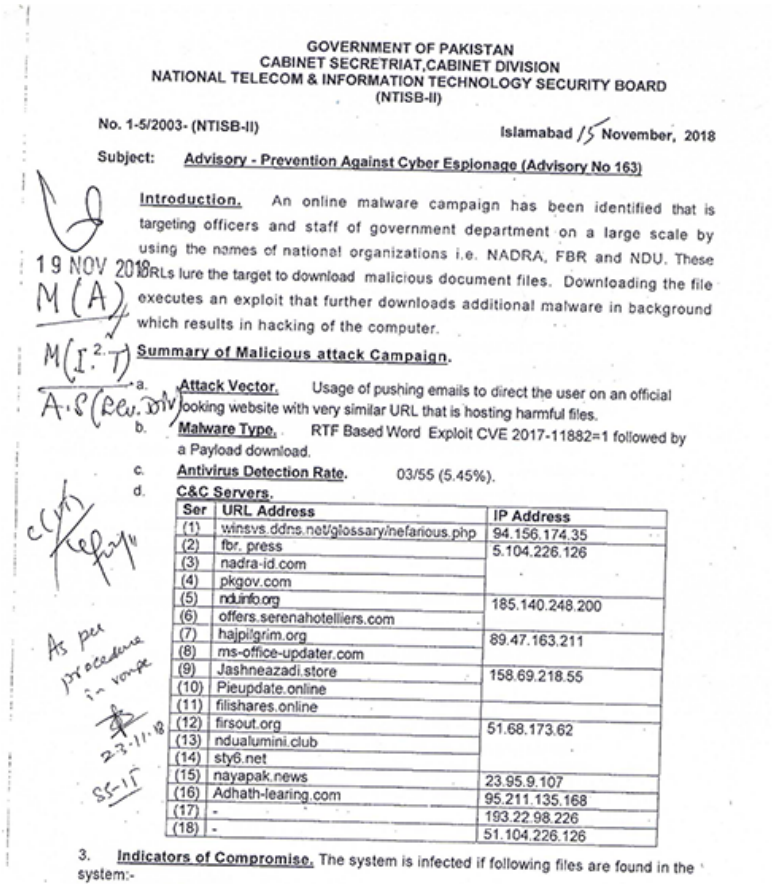
```
/SignUp
/UploadFile
/SaveMessages
/SaveCallLogs
/SaveContactDetails
/SaveGpsDetails
/UpdateMobileState
/UpdateMobileState
```

We found that the patterns noted above also existed on another domain samaatv[.]online. Although Lookout has not directly observed an APK communicating to this domain, we think one likely exists. samaatv[.]online has resolved to the IP address 91.210.107[.]104 since May 2019, which encompasses the activity of this campaign.

In addition to this, we found the SunBird C2 domain pieupdate[.]online resolved to 91.210.107.111 in between February 2019 and July 2019. This is also the timeframe in which we observed active campaigns by SunBird on that infrastructure.

With the help of public reporting and Lookout's dataset, we are confident that the Confucius APT group is actively using the IPs between 91.210.107[.]103-91.210.107[.]112 to host a large portion of their infrastructure, both presently and in the past.

Additional open-source intelligence (OSINT) searches confirmed the above connections. We found a publicly-accessible 2018 Pakistani government advisory warning of a desktop malware campaign targeting officers and government staff. The campaign described in it used phishing emails that impersonated various government agencies to deliver malicious Microsoft Word exploits. The Indicators of Compromise (IOCs) for this campaign included domains that were known Confucius infrastructure, leading us to believe the entire campaign could be attributed to that group.



GOVERNMENT OF PAKISTAN
CABINET SECRETRIAT,CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB-II)

No. 1-5/2003- (NTISB-II) Islamabad /5 November, 2018

Subject: Advisory - Prevention Against Cyber Espionage (Advisory No 163)

19 NOV 2018

Introduction. An online malware campaign has been identified that is targeting officers and staff of government department on a large scale by using the names of national organizations i.e. NADRA, FBR and NDU. These URLs lure the target to download malicious document files. Downloading the file executes an exploit that further downloads additional malware in background which results in hacking of the computer.

Summary of Malicious attack Campaign.

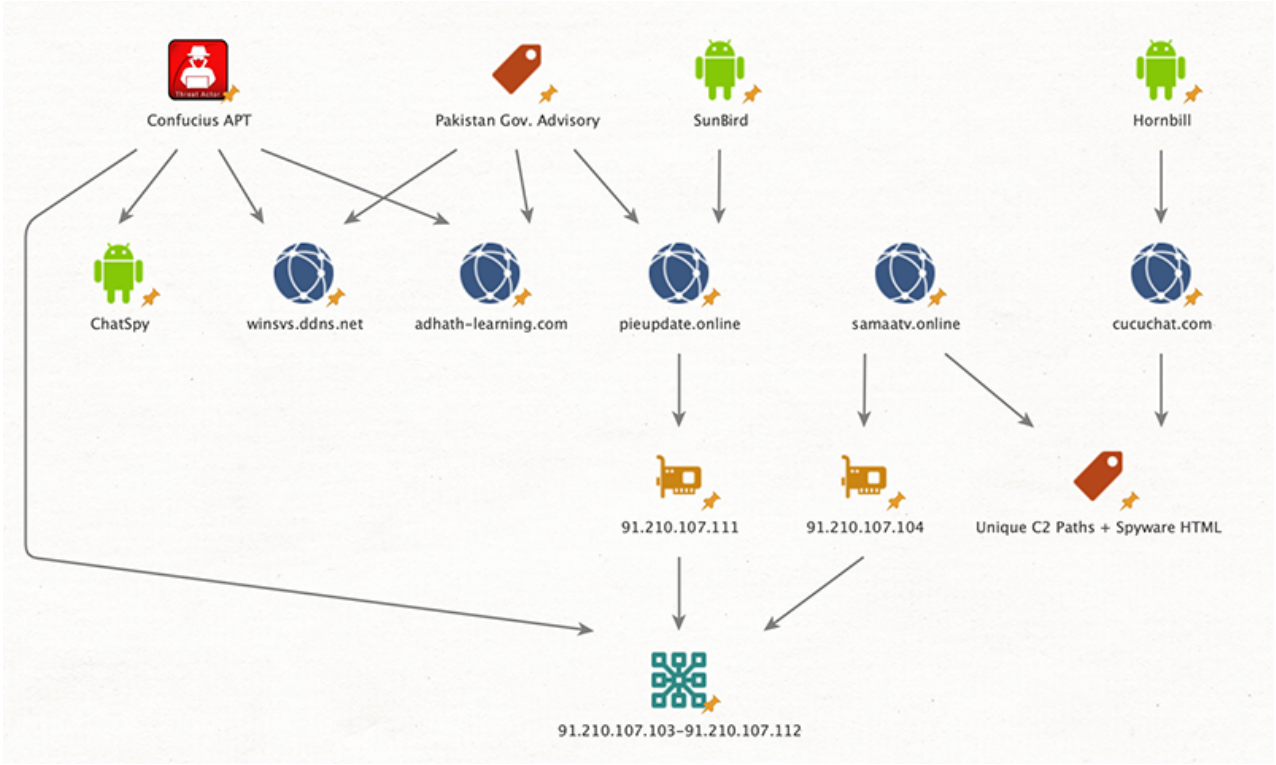
a. Attack Vector. Usage of pushing emails to direct the user on an official looking website with very similar URL that is hosting harmful files.
b. Malware Type. RTF Based Word Exploit CVE 2017-11882=1 followed by a Payload download.
c. Antivirus Detection Rate. 03/55 (5.45%).
d. C&C Servers.

Ser	URL Address	IP Address
(1)	winsvs.ddns.net/glossary/nefarious.php	94.156.174.35
(2)	fbr. press	5.104.226.126
(3)	nadra-id.com	
(4)	pkgov.com	
(5)	nduinfo.org	185.140.248.200
(6)	offers.serenahotelliers.com	
(7)	hajpilgrim.org	89.47.163.211
(8)	ms-office-updater.com	
(9)	Jashneazadi.store	158.69.218.55
(10)	Pieupdate.online	
(11)	filishares.online	
(12)	firsout.org	51.68.173.62
(13)	ndualumini.club	
(14)	sty6.net	
(15)	nayapak.news	23.95.9.107
(16)	Adhath-learing.com	95.211.135.168
(17)	-	193.22.98.226
(18)	-	51.104.226.126

3. Indicators of Compromise. The system is infected if following files are found in the system:-

Official Report from Pakistan's Federal Bureau of Revenue on Malicious Activity.

A particular point of interest on the advisory IoC list, and crucial in confirming Confucius connections, was pieupdate[.]online, a C2 server for malicious desktop activity as well as SunBird mobile malware.



Hornbill malware has unique file paths with which to communicate with C2 servers. They also display a unique Spyware HTML page. Lookout researchers uncovered another domain, samaatv[.]online, which shares the same unique file paths and Spyware HTML page found on a Hornbill C2 server, cucuchat[.]com. It is tied to known Confucius infrastructure by resolving to 91.210.107[.]104, in the Confucius IP range.

We are confident SunBird and Hornbill are two tools used by the same actor, perhaps for different surveillance purposes.

To the best of our knowledge the apps described in this article were never distributed through Google Play. Users of Lookout security apps are protected from these threats.

Lookout Threat Advisory Services customers have already been notified with additional intelligence on this and other threats. Take a look at ourThreat Advisory Services page to learn more.

Disclaimer

The information provided in this report is based upon discovery tools and methods which are inherently imperfect and though it is our belief the information in this report is accurate at the time of its publishing the information is provided “as is” with all faults, and Lookout Inc., assumes no liability for its accuracy or completeness, or one's use or reliance upon the information contained therein.

Acknowledgements

We would like to thank Michael Flossman for his contribution to the initial discovery and tracking of SunBird.

1 https://unit42.paloaltonetworks.com/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/

2 https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Confucius&n=1

3 https://www.trendmicro.com/en_us/research/18/b/deciphering-confucius-cyberespionage-operations.html

4 https://cdn.s3waas.gov.in/s3eb6fdc36b281b7d5eabf33396c2683a2/https://www.lookout.com/Uploads/2019/04/2019041885.pdf

5 https://www.mobile-spy.com/

6 https://www.vice.com/en/article/vvabv3/hackers-why-they-hit-stalkerware-flexispy-retina-x

7 https://www.bol7.com/mobile-tracking-spy/

8 https://info.lookout.com/rs/051-ESQ-475/images/lookout-stealth-mango-srr-us.pdf

9 https://en.wikipedia.org/wiki/Pakistan_Atomic_Energy_Commission

10 https://cdn.s3waas.gov.in/s3eb6fdc36b281b7d5eabf33396c2683a2/https://www.lookout.com/Uploads/2019/04/2019041885.pdf

11 https://en.wikipedia.org/wiki/2019_Pulwama_attack

12 https://en.wikipedia.org/wiki/2019_Indian_general_election

13 https://www.trendmicro.com/en_us/research/18/b/deciphering-confucius-cyberespionage-operations.html

14 https://www.virustotal.com/gui/file/8dccc3c76a474f106de639df9370b76e788cbff05b2345715454ab25309cd517/behavior

15 https://play.google.com/store/apps/details?id=com.kakao.talk&hl=en_US&gl=US

16 https://chasing-coins.com/coin/XGB

17 https://apkpure.com/cucu-free-chat-dating-app/crush.dating.app

18 https://apkpure.com/chat-xpress-pretty-people/cucuchat.android

19 https://web.archive.org/web/20180813100604/http://wangu.xyz/

20 https://play.google.com/store/apps/details?id=africa.wangu.app&hl=en_US&gl=US

21 https://play.google.com/store/apps/details?id=com.mesibo.mesiboapplication

22 https://unit42.paloaltonetworks.com/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites/

23 https://www.trendmicro.com/trendlabs-security-intelligence/deciphering-confucius-cyberespionage-operations/

SHA-1 Hashes

Hornbill

b6b239ccef57a261a254f5167357dc9096618939

1f1bab3c5a60275384083ef9e2a5b9fe6c194a35

704579a14a2ee80c89ad12019e19e50eb27dffea

3372458b73d3d5c3957a75dfe6cff62c5cd3cd4f

77867ddb68b68a340ccdb79bd9d46281d5956fa5

c504cef5e0e04b15d21388e6f9cc2c320071d50b

0cc49097778372fdf1ba2143e31a8f235342f9c9

SunBird

9b684cff07f98083bdb085cb846929ebca2c3df1

2ecb5b88b12ba44cfce2f51df7f16fbd4754aea2

665d23eda84cd008ccde013bde6a836976bcc4fc

a38931d68b26f04a94241f2155bcbf465b3fa99a

df5188225ab6de0a6e71635e997c4473c02d6527

e01729e5ceb827318e5198a24a12ae6d6bbc4ab3

8ae67888befb4f01f216d94f07051fc047150ceb

41268c45dc2453469ea8a0a0c615bdb562d1d9de

a4161cfe2d6146566094ee979ea893cd2fe3ae72

03d199cff2be8667932933d1bcb6bb58d364545a

fc2929a021ca1e83f0d87ca9c9c85df0057373e5

a6128100cd9c505e12af16a163d4fea35c42808a

6b75e6df7744a232a350658ad06e9574483a0b8b

be524a5a42b4b3f48f5571311f9be683024b6939

BuzzOut

2fd402c23f6827c049b92af19d4815c03cde407f

b847ffa3d097c9eb1ddfc0dd3133582988fde885

9b10e71f3d38e73d3637bf14d93404175bf4c276

ae1cd2a583082eeb540c567a051135d5147e97db

a0ed91b759a0015145ab301a3bba8f6cd868b394

afdc1db55e84e868e8ecdb3489309e1e19453779

27cabf2a24a87324f922becd5ae2dcf7bf4ae4bd

6779ebdd14113ce304172b078d859684248ee114

6bb91b2b97f08eb116982a5039d859ada94c37fd

e3cd30bbc7e9e0b8c4275c4d2b8ac876a7fc9b9b

07f1b2d8b34ce31296f6f5fe336ebae90293119e

15e18ac163275bdcf8e391a90127db5206ab4fdd

a5224bf9444736970dc357da3b309ad089aa7912

257bb82955818c1b3e2fc9581475c3d71df489e6

fde11af0c9ede7ad1f2b4e8bd6d55c1ef90eff72

01a91eb4cf0a8cfd048d98d3006e7b39a3d61f81

Command and control infrastructure

Hornbill

pieupdate[.]online

chatk.goldenbirdcoin[.]com

cucuchat[.]com

184.154.203[.]90
69.175.35[.]98

samaatv[.]online

tea-time[.]link

SunBird

data10.000webhostapp[.]com

global134.000webhostapp[.]com

wixten.000webhostapp[.]com

sunshinereal.000webhostapp[.]com

23.82.19[.]250

TAGS:

|

Threat Intelligence