

Confucius APT Android Spyware Targets Pakistani and Other South Asian Regions

blog.cyble.com/2021/02/17/confucius-apt-android-spyware-targets-pakistani-and-other-south-asian-regions

February 17, 2021

```
File: 'C:\Users\dungeon_hunter\Desktop\Confucius\confucius.rtf' - size: 473 bytes
-----+-----+-----
id | index | OLE Object
-----+-----+-----
0  | 00003F7Ch | format_id: 2 (Embedded)
   |           | class name: b'Package'
   |           | data size: 85812
   |           | OLE Package object:
   |           | Filename: 'bing.dll'
   |           | Source path:
   |           | 'C:\Users\Dev\Desktop\07082020_8570_S\bing.dll'
   |           | Temp path = 'C:\Users\Dev\AppData\Local\Temp\bing.dll'
   |           | MD5 = '70ab7f173c9ad785fc0d585c8ca685f9'
   |           | EXECUTABLE FILE
-----+-----+-----
1  | 000335AAh | format_id: 2 (Embedded)
   |           | class name: b'2333tion.3'
   |           | data size: 1024
   |           | MD5 = '15b8bc924f782057e0c263afd4d37646'
```

Two Android spyware strains named Hornbill and SunBird were recently discovered with possible connections to the advanced persistent threat (APT) group called Confucius. The group first appeared in 2013 as a hacking group, primarily pursuing Pakistani and other South Asian targets. Confucius has created mainly Windows malware in the past. However, after the spying app ChatSpy came into existence in 2017, the group has extended its mobile malware capabilities.

The two Android malware strains, Hornbill and SunBird, are embedded inside fake Android applications and used as spyware for monitoring and exfiltrating data from the mobile phones of their targets. These fake Android applications were used to spy on Pakistan’s military and nuclear authorities, along with election officials from Kashmir. The counterfeit apps contain advanced capabilities, including capturing photos from the camera, capturing the geolocation, scraping WhatsApp messages and media, and requesting elevated privileges. The data is first collected in SQLite databases, compressed to ZIP files and uploaded to the hacker’s C2 servers.

Counterfeit applications published by the APT group mimic various genuine-looking applications. The SunBird strain has been embedded into fake applications with legitimate-looking names such as “Google Security Framework,” “Falconry Connect,” “Mania Soccer,” and “Quran Majeed.” According to security researchers at [Lookout](#), apps embedded with SunBird have more extensive malicious capabilities than Hornbill.

While Hornbill works as spyware used to extract data of interest from the target device, SunBird additionally works as a remote access trojan (RAT), allowing hackers to execute commands on an infected device. Both malware programs can exfiltrate a wide range of data from target devices.

Data exfiltrated by Hornbill and SunBird:

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

Actions performed on target devices:

- Requesting device administrator privileges
- Taking screenshots and capturing whatever a victim is currently viewing on their device
- Taking photos with the device camera
- Recording environment and call audio
- Scraping WhatsApp messages, contacts, and notifications via accessibility services

The SunBird malware consists of certain additional malicious capabilities when compared with Hornbill. The additional data exfiltrated by SunBird includes:

- 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

Additional actions performed by SunBird include:

- Downloading attacker-specified content from FTP shares
- Running arbitrary commands as root, if possible
- Scraping BBM messages, contacts, and notifications via accessibility services

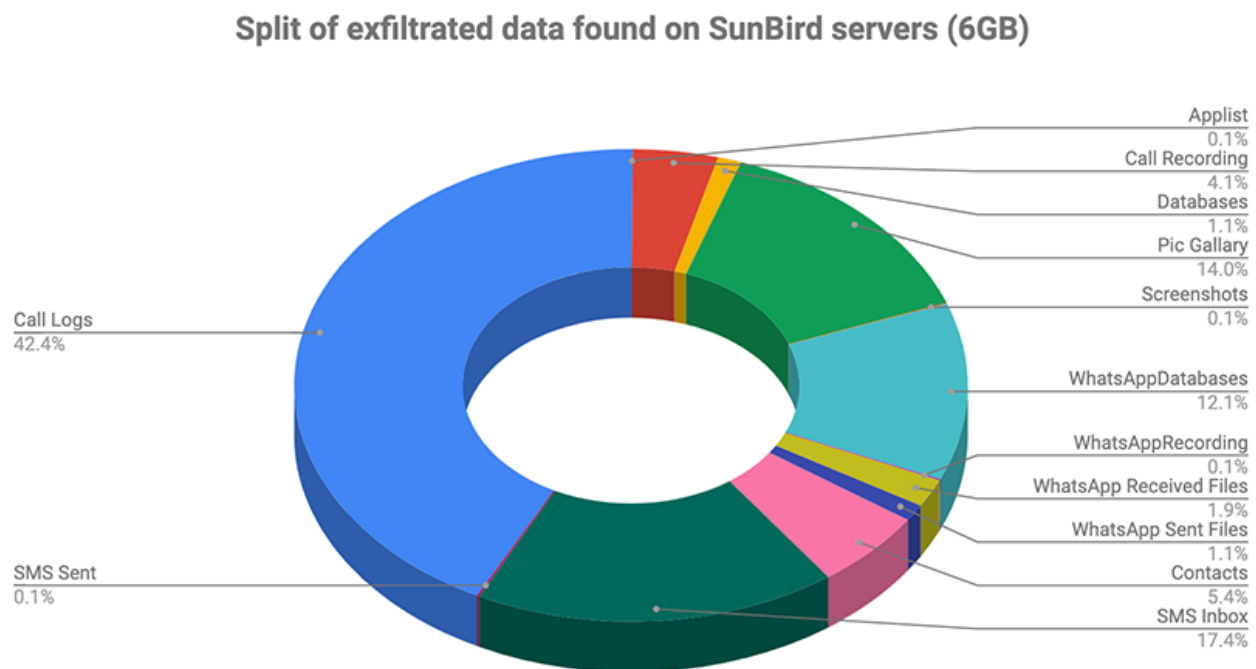
The Confucius APT malware campaign involves social engineering tactics for luring unsuspecting targets to download these applications from direct links. Multiple malicious applications with the SunBird and Hornbill strains are hosted on third-party app stores. Apps embedded with the Hornbill strain are more passive in nature, target a limited set of data, and are used as a reconnaissance tool. The malware only

uploads data to the C2 server when it runs for the first time on the infected device. Hornbill keeps mobile internet and battery usage low by only uploading new data from target devices. On the other hand, the SunBird strain uploads data in fixed intervals. Hornbill actors seem more interested in monitoring the user’s WhatsApp activity, and Hornbill abuses the Android accessibility services to detect an active WhatsApp call and record it.

Researchers believe that the same threat actor is behind both the malware, and neither of these apps were distributed via Google Play or any authorized app stores.

Possible targets of the campaign and exfiltrated data

Security researchers were able to get access to 18GB of exfiltrated data exposed on insecurely configured C2 servers of the SunBird malware. The data also included the location of the infected devices, which helped researchers determine the possible targets of this malware campaign. Some of the targets identified included individuals related to Pakistan Air Force (PAF), Pakistan Atomic Energy Commission, and other departments.



Publicly accessible exfiltrated content exposed on SunBird C2 servers for five campaigns, 2018-2019. (Image source: [Lookout](#))

The data exfiltrated by SunBird included information such as SMS messages, contacts, and call logs uploaded at fixed intervals.

Connection to Confucius APT

Similar to fake Android applications, the Confucius APT group also targets Windows systems. We analyzed a Confucius malware sample and observed that the attack kill chain starts with a word document delivered to the target. The document is crafted in a way that encourages the target to open that document. Once the user opens the document, it uses template injection to download the RTF exploit that downloads the final stage payload.

The RTF contains a DLL embedded in an OLE object, as shown in the image below.

```

=====
File: 'C:\Users\dungeon_hunter\Desktop\Confucius\confucius.rtf' - size:
473 bytes
-----
id | index | OLE Object
-----
0 | 00003F7Ch | format_id: 2 (Embedded)
   | | class name: b'Package'
   | | data size: 85812
   | | OLE Package object:
   | | Filename: 'bing.dll'
   | | Source path:
   | | 'C:\Users\Dev\Desktop\07082020_8570_S\bing.dll'
   | | Temp path = 'C:\Users\Dev\AppData\Local\Temp\bing.dll'
   | | MD5 = '70ab7f173c9ad785fc0d585c8ca685f9'
   | | EXECUTABLE FILE
-----
1 | 000335AAh | format_id: 2 (Embedded)
   | | class name: b'2333tion.3'
   | | data size: 1024
   | | MD5 = '15b8bc924f782057e0c263afd4d37646'
-----
C:\Users\dungeon_hunter\

```

DLL embedded in RTF file.

The embedded DLL file, bing.dll (SHA-256: 8b535452727edf06280c495b190c10e0a90522fad1c61cae8bfeef9b84a4879) contains an export “mark” and is responsible for downloading the payload. The name of the released .dll file is linknew.dll.

Offset	Name	Value	Meaning
128F0	Characteristics	0	
128F4	TimeStamp	601BD332	Thursday, 04.02.2021 10:57:54 UTC
128F8	MajorVersion	0	
128FA	MinorVersion	0	
128FC	Name	13922	linknew.dll
12900	Base	1	
12904	NumberOfFunc...	1	
12908	NumberOfNames	1	

Exported Functions [1 entry]					
Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
12918	1	1010	1392E	mark	

The malware also checks for the presence of a debugger and whether it is being executed in a virtual environment. The malicious `bing.dll` connects to “`hxxp://mlservices.online/content/upgrade`” to download the payload file. An LNK file named `update.lnk` and pointing to the payload file `update.exe` is dropped to the startup folders – “`%AppData%\Microsoft\Windows\Start Menu\Programs\Startup`” – for adding persistence. After dropping the payload, it runs in the background and performs spyware activities similar to Hornbill and SunBird. We are sharing indicators of compromise (IOCs) related to Confucius windows malware and fake Android applications.

Security recommendations

- Ensure antivirus software and associated files are up to date
- Search for existing signs of the indicated IOCs in your environment
- Consider blocking or setting up detection for all URL and IP-based IOCs
- Download applications from official app stores, such as Google Play Store and Apple App Store
- Avoid websites providing bootleg Android APKs and iOS APPs
- Keep applications and operating systems running at the current released patch level
- Exercise caution while opening attachments and links in emails
- Keep systems fully patched to mitigate vulnerabilities effectively

Indicators of compromise

SHA-1 Hashes

Hornbill

b6b239ccef57a261a254f5167357dc9096618939

1f1bab3c5a60275384083ef9e2a5b9fe6c194a35

704579a14a2ee80c89ad12019e19e50eb27dffa

3372458b73d3d5c3957a75dfe6cff62c5cd3cd4f

77867ddb68b68a340ccdb79bd9d46281d5956fa5

c504cef5e0e04b15d21388e6f9cc2c320071d50b

0cc49097778372fdf1ba2143e31a8f235342f9c9

SunBird

9b684cff07f98083bdb085cb846929ebca2c3df1

2ecb5b88b12ba44cfce2f51df7f16fbd4754aea2

665d23eda84cd008ccde013bde6a836976bcc4fc

a38931d68b26f04a94241f2155bcbf465b3fa99a

df5188225ab6de0a6e71635e997c4473c02d6527

e01729e5ceb827318e5198a24a12ae6d6bbc4ab3

8ae67888befb4f01f216d94f07051fc047150ceb

41268c45dc2453469ea8a0a0c615bdb562d1d9de

a4161cfe2d6146566094ee979ea893cd2fe3ae72

03d199cff2be8667932933d1bcb6bb58d364545a

fc2929a021ca1e83f0d87ca9c9c85df0057373e5

a6128100cd9c505e12af16a163d4fea35c42808a

6b75e6df7744a232a350658ad06e9574483a0b8b

be524a5a42b4b3f48f5571311f9be683024b6939

SHA-256 Hashes – Confucius

8b535452727edf06280c495b190c10eb0a90522fad1c61cae8bfeef9b84a4879

8ecf1c276e10e3f3e9f7bc9e728fde9abea23348a2af6ce70269008d632a412d

3ce48f371129a086935b031333387ea73282bda5f22ff78c85ee7f0f5e4625fe

1c41a03c65108e0d965b250dc9b3388a267909df9f36c3fefffbfd26d512a2126

07277c9f33d0ae873c2be3742669594acc18c7aa93ecadb8b2ce9b870baceb2f

ea52d6358d53fc79e1ab61f64cb77bb47f773f0aa29223b115811e2f339e85f5

686847b331ace1b93b48528ba50507cbf0f9b59aef5b5f539a7d6f2246135424

2f5fc653550b0b5d093427263b26892e3468e125686eb41206319c7060212c40

b9b5a9fa0ad7f802899e82e103a6c2c699c09390b1a79ae2b357cacc68f1ca8e

4500851dad1ac87165fc938fe5034983c10423f800bbc2661741f39e43ab8c8d

a3cd781b14d75de94e5263ce37a572cdf5fe5013ec85ff8daeee3783ff95b073

59ccfff73bdb8567e7673a57b73f86fc082b0e4eeaa3faf7e92875c35bf4f62c

59cd62ad204e536b178db3e2ea10b36c782be4aa4849c10eef8484433a524297

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

Confucius

Mlservices[.]online

msoffice.user-assist[.]site

msoffice.user-assist[.]site

Wordupdate[.]com

[http://wordupdate\[.\]com/refresh/content](http://wordupdate[.]com/refresh/content)

[http://mlservices\[.\]online/content/upgrade](http://mlservices[.]online/content/upgrade)

[http://wordupdate\[.\]com/recent/update](http://wordupdate[.]com/recent/update)

About Cyble

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the darkweb. Cyble's prime focus is to provide organizations with real-time visibility into their digital risk footprint. Backed by Y

Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Startups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.