Anubis Android Malware Returns with Over 17,000 Samples

***By: Tony Bao (Mobile Threats Analyst)***

Last year’s [mobile threat landscape](https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2018-mobile-threat-landscape) showed banking trojans diversifying in tactics and techniques to evade detection and further monetize their malware — and in the case of the Anubis Android malware, retooled for other malicious activities. Since it first emerged, Anubis underwent several changes, from being used for [cyberespionage](https://blog.trendmicro.com/trendlabs-security-intelligence/cyberespionage-campaign-sphinx-goes-mobile-anubisspy/) to being retooled as a banking malware, combining information theft and [ransomware](https://www.trendmicro.com/vinfo/us/security/definition/ransomware)-like routines. In mid-January this year, we saw Anubis use a plethora of techniques, including the use of [motion-based sensors](https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/) to elude sandbox analysis and overlays to steal personally identifiable information.

The latest samples of Anubis (detected by Trend Micro as AndroidOS\_AnubisDropper) we recently came across are no different. When we tracked Anubis’ activities, we saw two related servers containing 17,491 samples. Some of the new variants now sport an additional routine of dropping payloads twice, with the first being a still-in-development Dalvik executable (DEX) file, which we think was done to further evade anti-virus (AV) detection. And based on these latest samples, we also found other Anubis samples on Google Play, which have since been taken down.

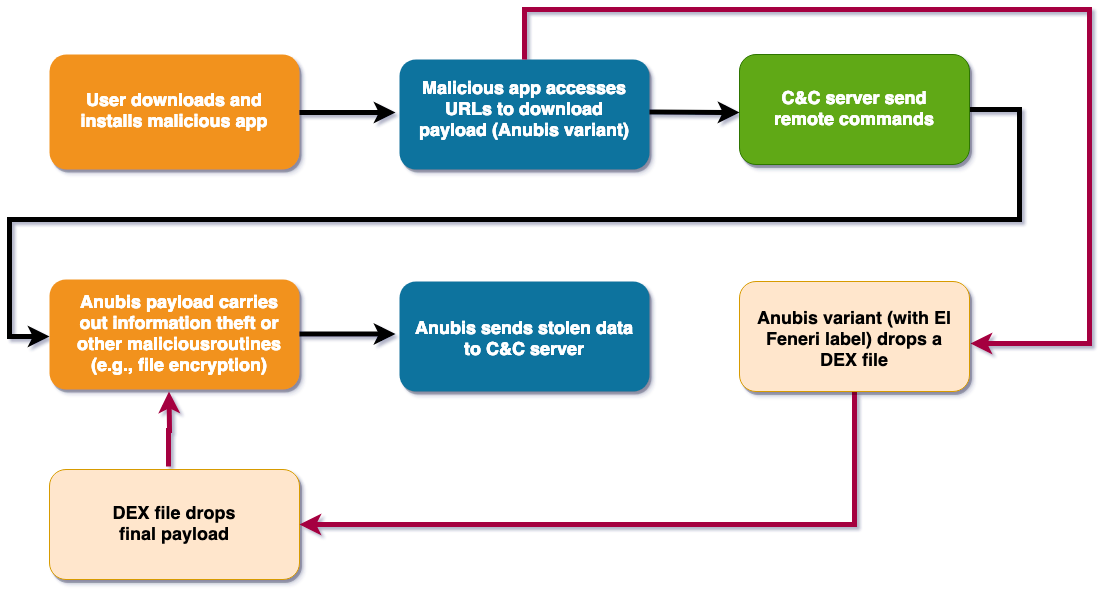


Figure 1. Anubis’ infection chain

## Coming Across 17,491 Anubis Samples

We used the following samples (SHA-256) to analyze Anubis and further track this threat’s activities:

These variants of Anubis will request the following URLs and parse an XML file to download a malicious app:

* hxxp://markuezdnbrs[.]online/deneme/api[.]php?xml=8c6c029e-153b-41e1-a061-2699a45b69f9
* hxxp://successiondar[.]xyz/continuing/resigned[.]php?xml=7e393286-925c-41f4-ac81-b7e2625473d0

The malicious Android application packages (APKs) will be retrieved from here:

* hxxp://markuezdnbrs[.]online/deneme/apk/6928[.]apk
* hxxp://successiondar[.]xyz/continuing/kan/5425[.]apk



Figure 2. Code snippets showing Anubis dropper’s request URLs (highlighted)

Checking on other Anubis-related URLs, we uncovered that they hosted 17,491 samples:

* hxxp://markuezdnbrs[.]online/deneme/apk/[0-7810] [.]apk
* hxxp://successiondar[.]xyz/continuing/kan/[1-9680] [.]apk



Figure 3. Screenshot showing Anubis samples

We found three labels in these samples: “Operatör Güncellemesi”, “Google Services”, and “El Feneri”. In Turkish, “Operatör Güncellemesi” means “Operator Update”, while “El Feneri” can be translated as “Flashlight”. These are probably meant as social engineering lures to encourage unwitting users into downloading a malicious app.

## Technical Analysis

The labels are also notable in that the samples bearing specific labels appear to have different routines from others. We analyzed an Anubis variant with the Operatör Güncellemesi label (SHA-256: 6079af3bab8bb0ba445cd0dd896d8c8d7845da3757755b4ef3af584d227e0490) and found its information-stealing capabilities similar to the malware’s previous iterations:

* Taking ss of the infected device’s screen
* the device via virtual network computing()
* audio
* , receive, and delete SMS
* Enable or configure istration settings
* the device’s s
* Steal the device’s list
* a specified
* Lock the device’s s
* or initiate unstructured supplementary service data(), which the technology used to send text messages between a mobile device and application
* Encrypt files, including those stored on the SD card as
* or locate
* the device’s
* Retrieve rsocial media channels like

Anubis also has the capability to inject a specified [Activity](https://developer.android.com/reference/android/app/Activity) (where an app starts its process). Anubis monitors the activity of the targeted apps (Figure 5 and Table 1), and once it determines that these apps are open or being used, the attacker can abuse the [WebView](https://developer.android.com/reference/android/webkit/WebView) feature to display the apps’ content on a web page. This can then be used as an attack vector for phishing, or using it to carry out overlay techniques to steal payment data. Anubis can also initiate an Activity via push notification and sending the information strings contained in the notification to the C&C server.

These iterations of Anubis have a list of targeted financial apps from which it steals personal and financial data, as shown in Figure 5 and Table 1. Like its previous versions, these new variants can still detect if they are being tested on virtual machines via motion-based sensors. It can also detect if it is being run on an Android emulator (e.g., Genymotion or x86-based machines).



Figure 4. Anubis sample with the label Operatör Güncellemesi

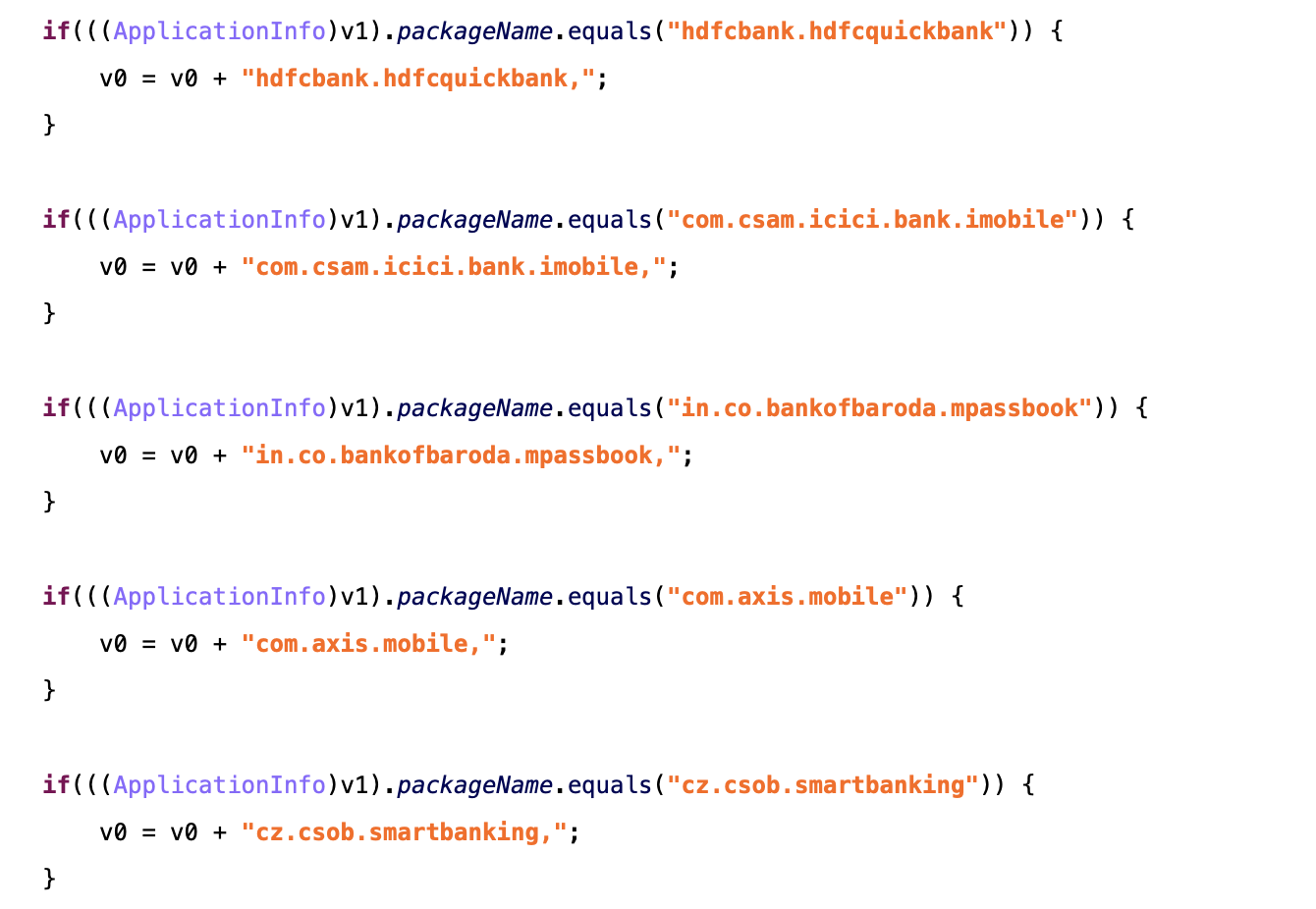


Figure 5. Code snippet showing the financial apps targeted by Anubis

|  |  |
| --- | --- |
| com.orangefinanse | Kompakt Finanse produkty bankowe dostarcza mBank |
| pl\_pl.ceneo | The largest price comparison app in Poland |
| may.maybank.android | Malayan Banking Berhad |

Table 1. Other newly added apps targeted by Anubis

The financial targets distribution:

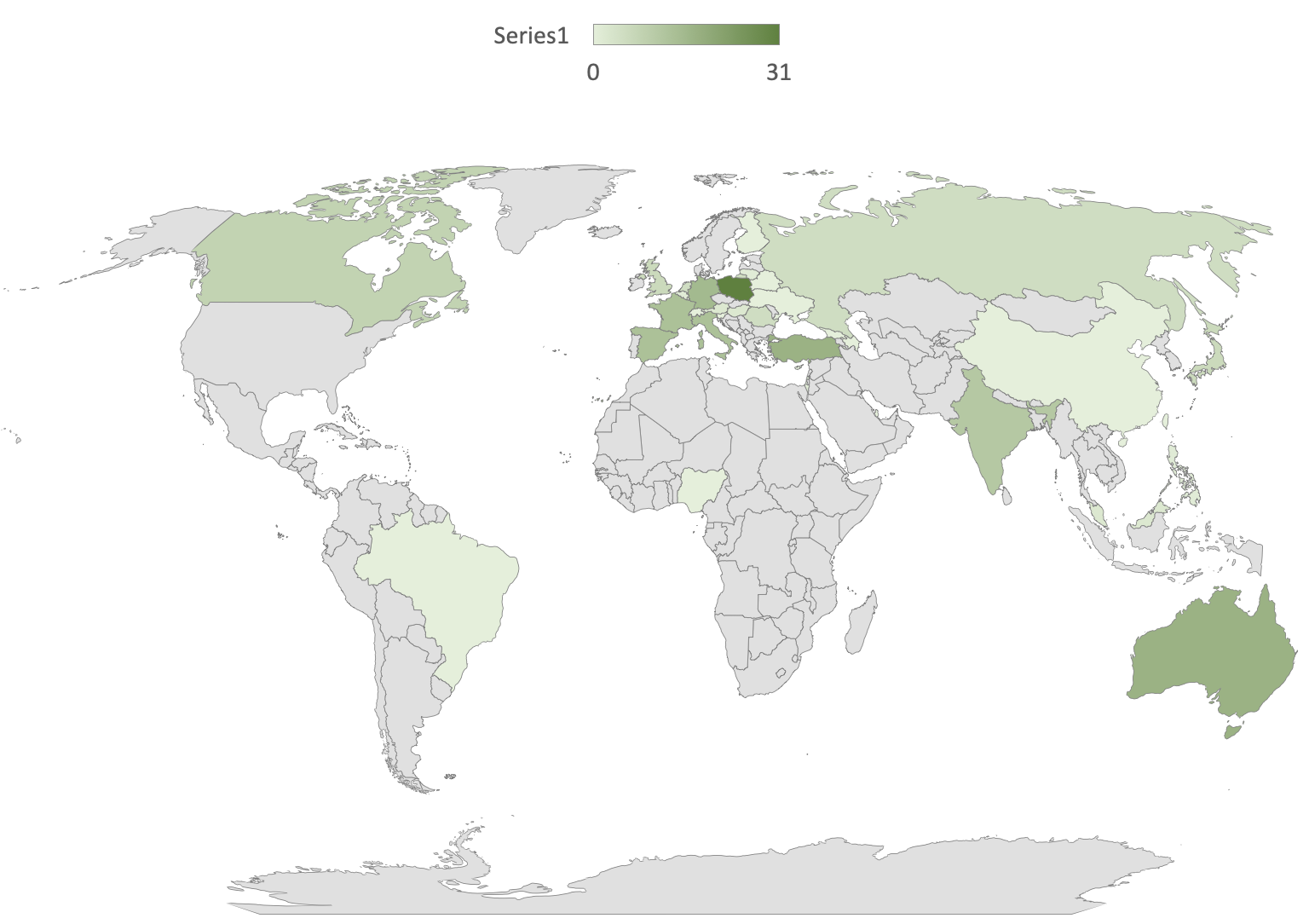


Figure 6, The financial targets distribution

For the variant of Anubis with the Google Services label, we analyzed a sample (SHA-256: 77a602217b272955ca255634da9a9736431ac6e244b104fd2bb6656f99ab6cab) and found that it first had to be unpacked. The samples with Google Services label have similar information-stealing and environment-detecting capabilities as those with the Operatör Güncellemesi label.

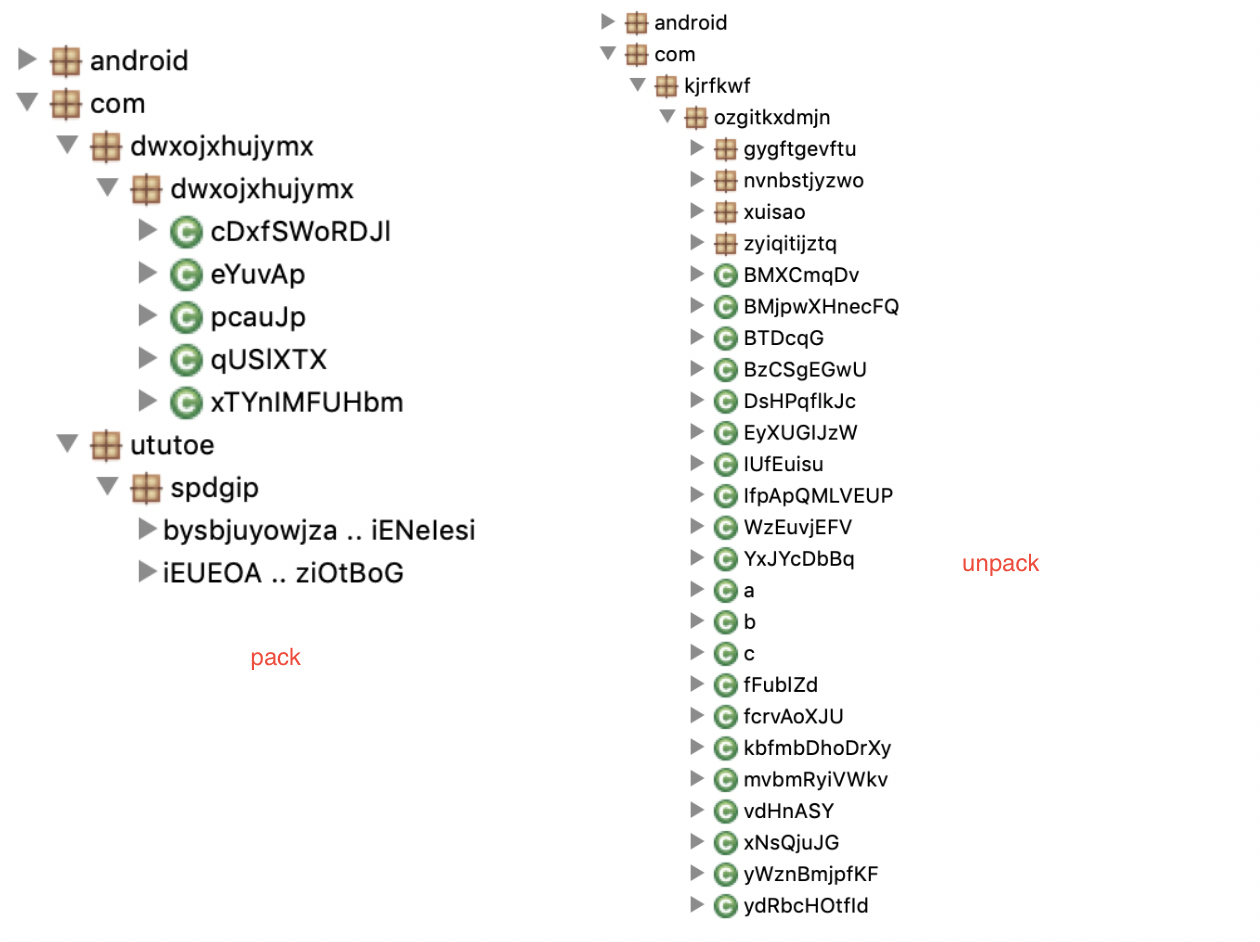
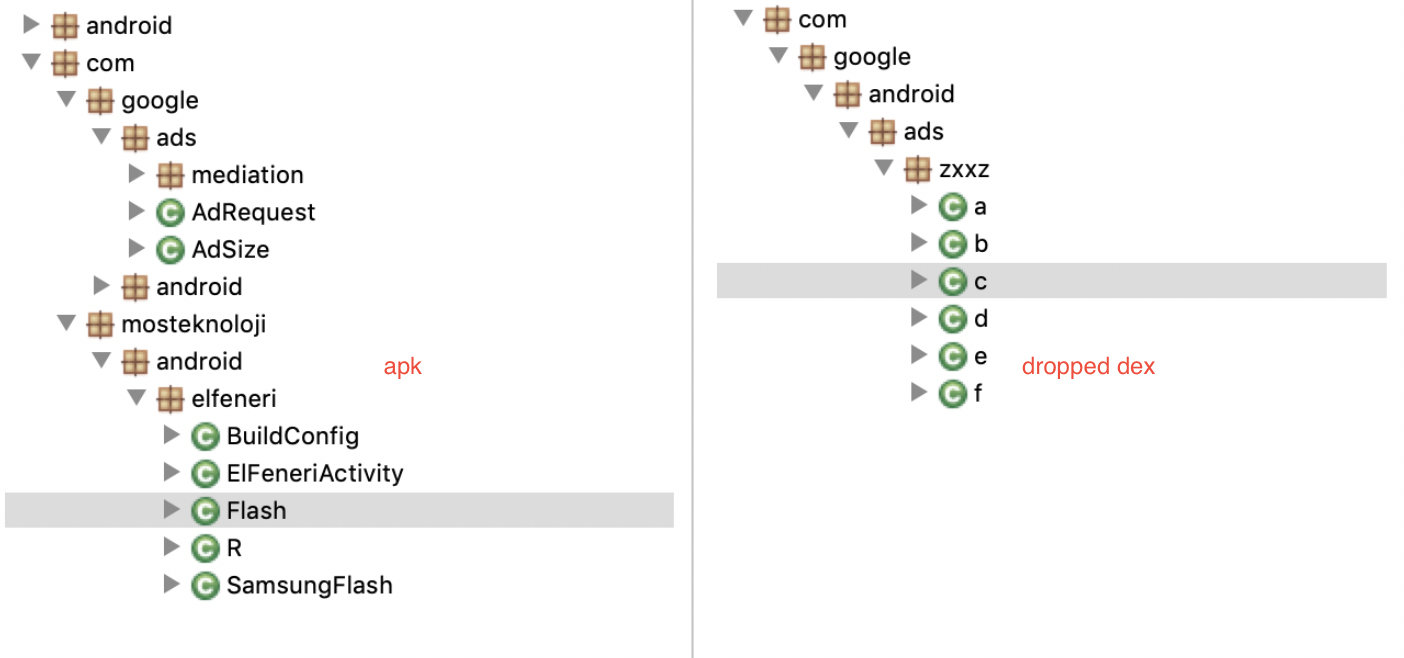


Figure 7. A sample of Anubis with the Google Services label

The Anubis variants with the El Feneri label, however, have an additional routine. Our analysis of a sample (SHA-256: 003582253ed11bdc328fcaa26437d8c5d3bd9dad15f217eb092771f241975879) revealed that these variants are still in development, as some of their functions are still not working properly.

These variants use a two-pronged approach, shown in Figure 7 (bottom), to deliver the final payload.

It will first drop a DEX file (SHA-256: a70c073c41cac0d28f259c335ec7d551488697c1624fb87924220ba4ea7fbbb7). The DEX file, which is what we’ve seen as unfinished or still-in-development, was likely intended this way to avoid AV detection.



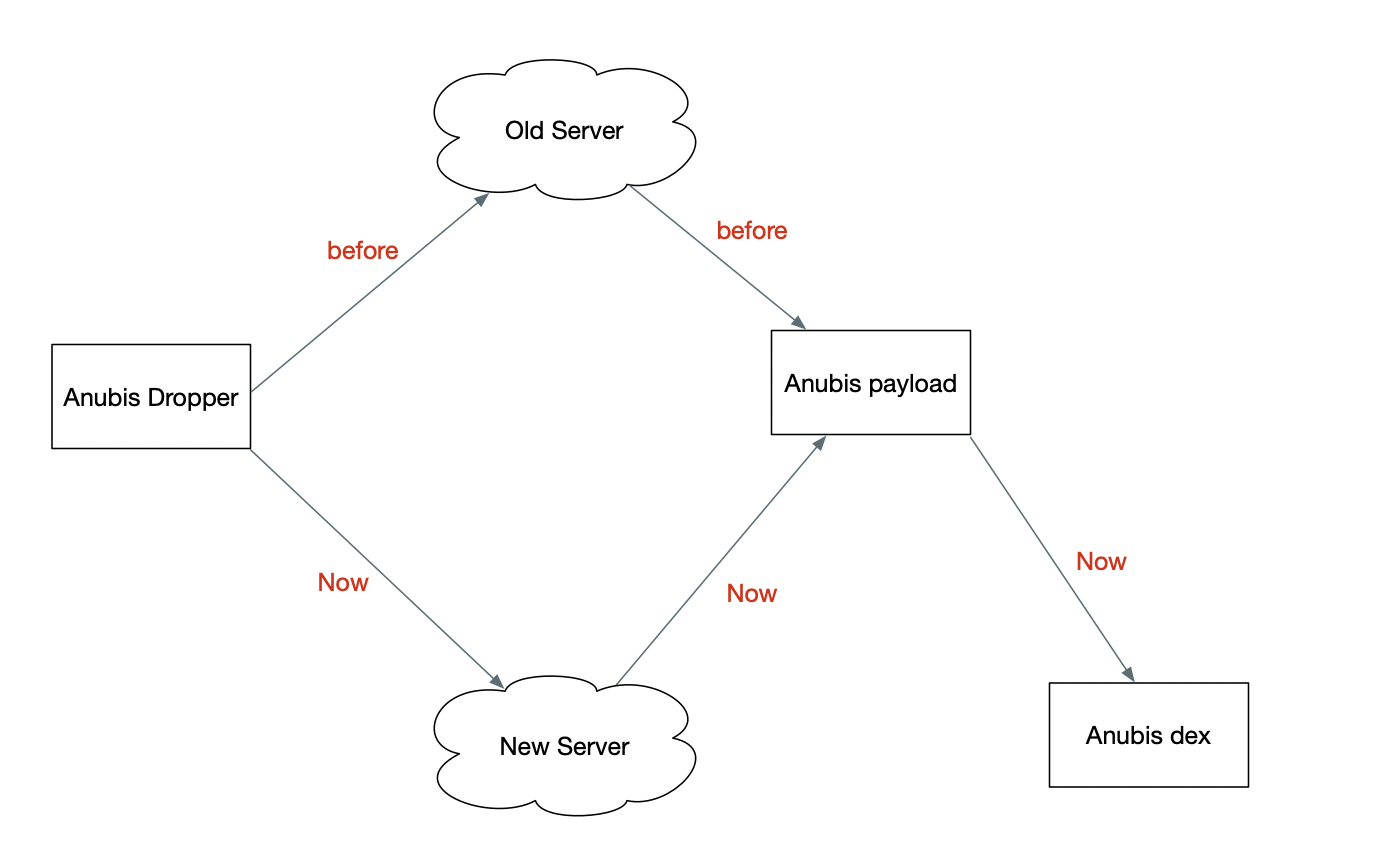


Figure 8. A sample of Anubis with the El Feneri label (top); the DEX file’s structure, which is similar to the initial dropper/APK (center); and its infection flow/how it drops the DEX file (bottom)

Using these samples, we were able to find Anubis samples on Google Play. Like the El Feneri label suggests, these apps are disguised as flashlight apps, as shown in Figure 8. While these apps are already taken down on Google Play, some of these apps had significant downloads, with one of them being downloaded and installed over a hundred thousand times.

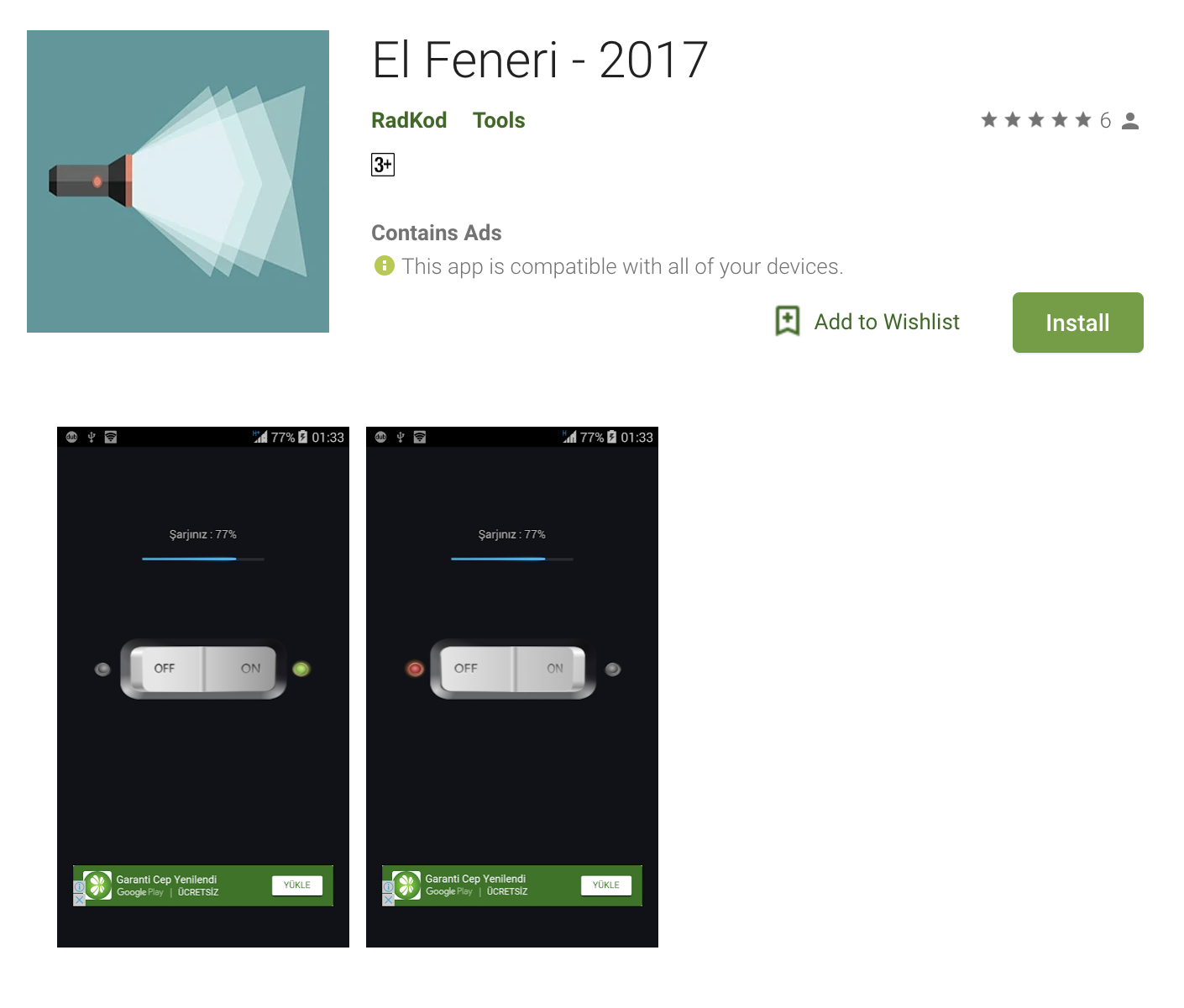


Figure 9. An example of an Anubis-embedded app in Google Play and dropped dex structure

## Correlating Anubis’ Command-and-Control (C&C) Communications

Anubis’ C&C servers are distributed in different countries, some are deployed by abusing a cloud service, some are IDC server, but all in a botnet, the botnet is not only the Anubis C&C server, but also the C&C server for Windows malware.

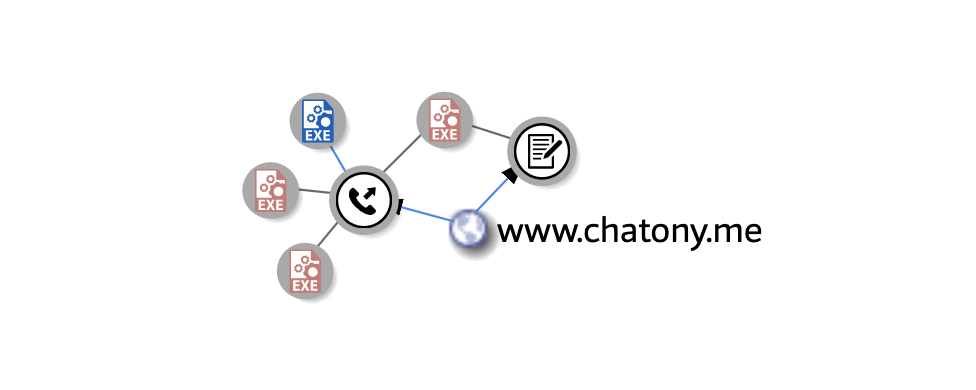


Figure 10. the C&C server in the botnet for Windows malware

In terms of impact, the Android devices affected by these new iterations of Anubis were mostly located in China and Turkey. As shown in Figure 9, Anubis connects to certain domains to download the payloads.

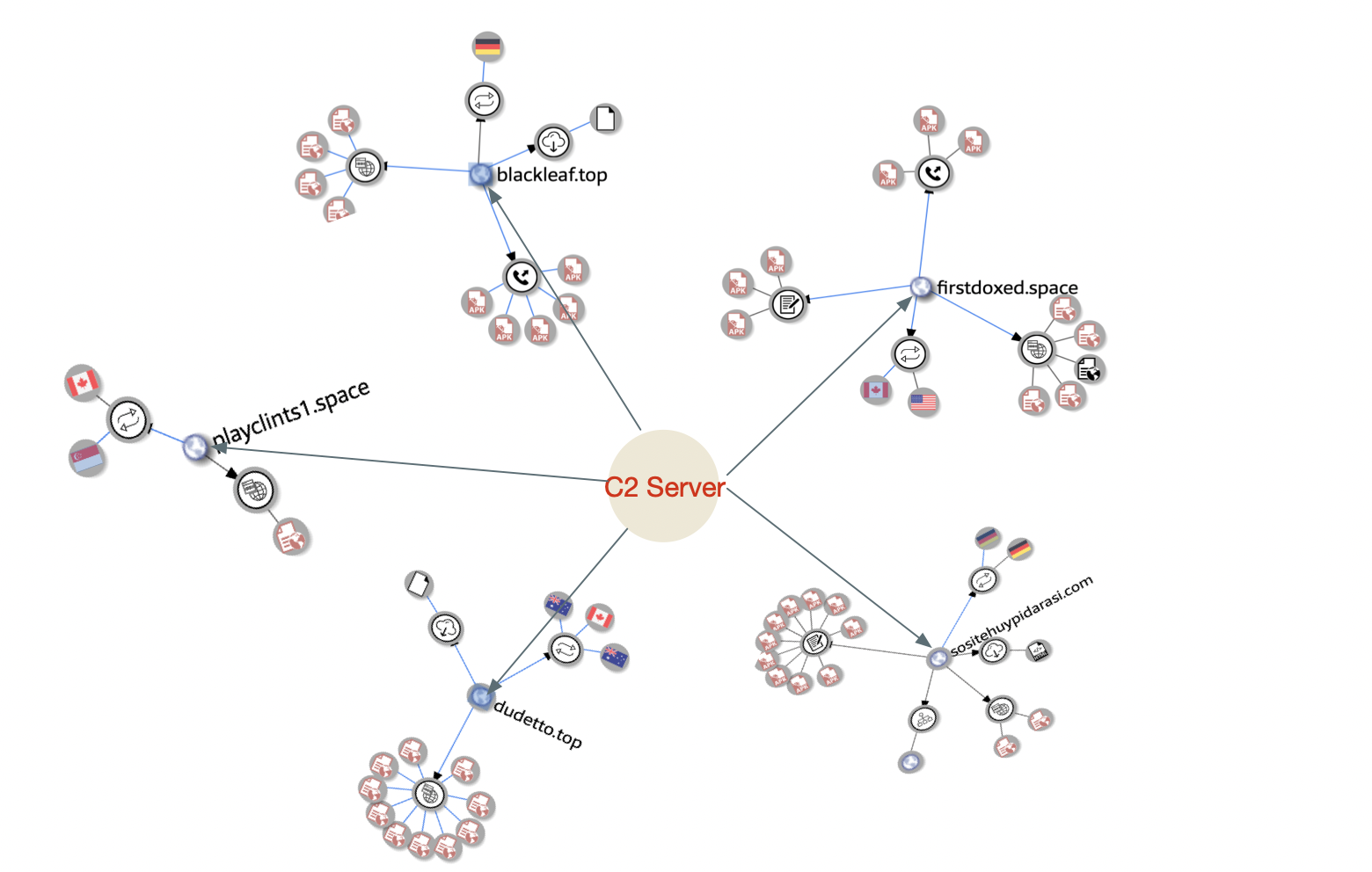


Figure 11. Anubis’ C&C infrastructure, including the domains where the payload is retrieved



Further tracking Anubis’ C&C activities, we found that the malware have been using social media channels like Twitter (with the attacker-owned Twitter accounts’ followers mostly using Turkish) and Google short links to send commands since 2014. According to the registration time of one of the accounts, the attacker has probably been active for about 12 years. We also found that Anubis is abusing Facebook for its C&C communication.







Figure 12. Twitter accounts abused by Anubis’ operators to issue C&C commands (top); how Google and Facebook short links were abused for C&C communications

The sheer amount of samples we uncovered reflect how Anubis’ authors and operators are actively using their malware. And given how some of them are still in development, we expect these to have additional techniques geared toward evading AV detection or obfuscating its trails, like how it connects to its C&C servers or deploy the final information-stealing or file-encrypting payloads. Users should always [practice](https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/a-practical-guide-to-mobile-safety) [security hygiene](https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/best-practices-securing-your-mobile-device) when installing apps, especially when the mobile devices are used in [BYOD settings](https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-devices-in-the-workplace-security-risks-and-threats-to-byod-environments).

End users and enterprises can also benefit from [multilayered mobile security solutions](https://www.av-test.org/en/antivirus/mobile-devices/android/november-2017/trend-micro-mobile-security--antivirus-9.1-174421/) such as [Trend Micro™ Mobile Security for Android™](https://www.trendmicro.com/us/home/products/mobile-solutions/android-security/) (available on Google Play). [Trend Micro™ Mobile Security for Enterprise](https://www.trendmicro.com/us/enterprise/product-security/mobile-security/) provides device, compliance and application management, data protection, and configuration provisioning, as well as protects devices from attacks that exploit vulnerabilities, preventing unauthorized access to apps, and detecting and blocking malware and fraudulent websites. Trend Micro’s [Mobile App Reputation Service](https://mars.trendmicro.com/) (MARS) covers Android and iOS threats using leading sandbox and [machine learning](https://www.trendmicro.com/vinfo/us/security/definition/machine-learning/) technologies, protecting devices against malware, zero-day and known exploits, privacy leaks, and application vulnerabilities.

A list of indicators of compromise (IoCs) is in this appendix.

Google Play IOC:

|  |  |  |
| --- | --- | --- |
| Sha256 | Packge Name | Downloads |
| 94274A97B96A14F687DE8A5ACEBAC0AAA4FC3CA9CF5FF3949449A3DC879EFA0A | com.eka.flash | 100+ |
| 2272167BCA81BB25D8171B21A03B062524B9BB2A17F8F5013D0CF9B58BE98209 | com.slck.elfeneri | 100,000+ |
| 158C0595B6AEC09428032E02093A3067F4560E8C9F6C06C055A59759E93F911D | com.mobikolik.screenlightpro | 100+ |
| E0935615B27678CDBA0CE8D587C4BBF8C1E630340BF983AEE03CC36EB7C9499A | com.nullovy.simpleflashlight | 1,000+ |
| B030D89AB285465F0B500C47726D695BB8C50395381A52518526E46EFF582447 | com.yilmazteknoloji.elfeneri | 50,000+ |
| 33B00B27648FA191255028D92F05194E57D0ECBCC60F366DE94C099684819DC0 | com.dogusumit.elfeneri | 1,000+ |
| 1421F4605C10CBBA1A52A8EEB86CD168F08C87376674BADCC11FB17994755D45 | com.inddir.elfeneri | 100+ |
| AAFEC2001B04AC5C3E22E52ED7B72FF7723DAE5F0321BE3D73FA126893F65E9C | com.radkod.radkod | 10+ |
| 5F23FDD7FF3320B438C8F651AC5B4C7ECB7455ABBDCF4DBF98CE4B1566B2CC32 | tr.com.cevoapps.elfeneri | 10+ |
| 155F50823B43D2B28157E325789D6B7181F10267E46BC6C4F70817476749A9A5 | com.flash.nuri.elfeneri | 1+ |
| A52FE42FFC9C8B571900F02CC3620F0DFE3F5E5702660B7E50A1BC12A025CA42 | com.umitkose.flash\_light\_el\_feneri\_isik | 10+ |
| 1AC14EF09F8995910D27796C24A3DBA008BE16F1D471C4B5FAD284B2570395A0 | com.yusufdesign.flashlights | 100+ |
| BFF816C88F5470CBEBEEA9F0160DD1349572AA04D0CEA113910529B0AFF7FD6B | com.ankabilisim.elfeneri | 10+ |
| D6C9405F8E32F33B7FB45C0777C27C137239DC348C5537069702C49C6C78D5C3 | com.Ps.Fener | 50+ |
| 0665CCB30F5C50FDD40C685EC5833F538CFCF7ADF7B9F7E98CA50D100A829685 | elci.elfeneri | 10+ |
| 415EA20B25090A8454C88F663A65DD639190E94383A46B94099F49CEDFA5556C | com.flashlighttr | 10+ |

C2:

|  |
| --- |
| hxxp://marksteylor.us/ |
| hxxp://ktosdelaetskrintotpidor.com |
| hxxp://sositehuypidarasi.com |
| hxxps://t.me/unite11 |
| hxxp://demo.website.com/ |
| hxxps://t.me/newpaparoni |
| hxxps://twitter.com/qweqweqwe |
| hxxps://www.chatony.me |
| hxxps://playclints1.space |
| hxxps://blackleaf.top |
| hxxps://lskbfidsbvkjsfgakfjsdffsdfupdate.net/o1o/a16.php |
| hxxps://firstdoxed.space |
| hxxps://sositehuypidarasi.com |
| hxxps://ndudetto.top |
| hxxps://lskbfidsbvkjsfgakfjsdffsdfupdate.net |
| hxxps://t.me/thethe123 |