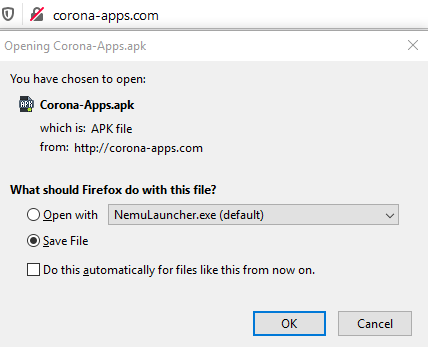
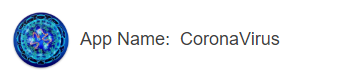
Cerberus and Anubis may be collaborators, not competitors

We found that Cerberus back again as coronavirus at 2020/3/19.

[http://corona-apps.com/Corona-Apps.apk](https://www.virustotal.com/gui/url/074047bf4c7fe335641797267993cc75cf5001106516dcced3ce4e1277372000)





sha256: 93288d18a7b43661a17f96955abb281e61df450ba2e4c7840ce9fd0e17ab8f77

packager: bpbdwemefb.sktkcxzsdgsasrbiqoodhkw.sqmrea

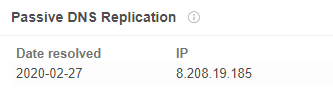
label: CoronaVirus

Cerberus Payload

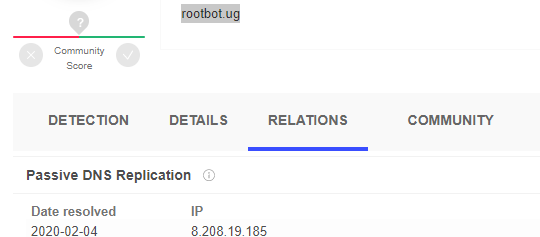
Sha256: 6A22EEA26C63F98763AA965D1E4C55A70D5ADF0E29678511CF303CB612395DF0

Interesting things:

We found that Cerberus C&C(botduke1[.]ug) has been seen to resolve the following IP address.



At the same time, we also found that Anubis C&C(rootbot[.]ug) has been seen to resolve the same IP address.

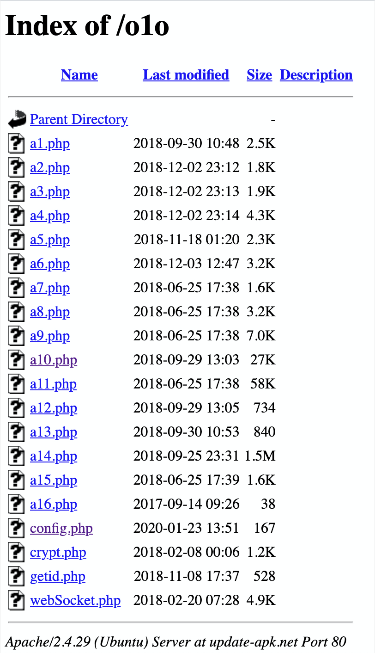
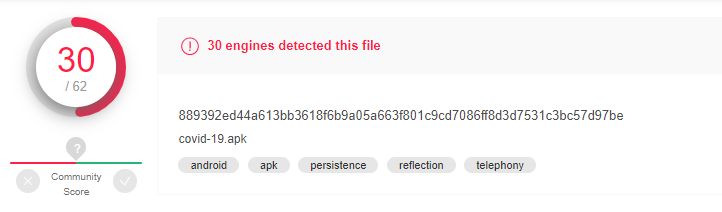


Previously Anubis also used coronavirus to attack, such as:

DownloadName: covid-19.apk

Sha256: 889392ed44a613bb3618f6b9a05a663f801c9cd7086ff8d3d7531c3bc57d97be

C&C: <http://update-apk[.]net>



The Anubis C&C(update-apk[.]net) has been seen to resolve the following IP address.

|  |  |
| --- | --- |
| Time | IP |
| 2020-02-10 | 161.117.239[.]0 |

And Other Anubis C&C had been seen to resolve the same IP address.

|  |  |
| --- | --- |
| Date resolved | Anubis C&C |
| 2020-02-06 | oleose[.]info |
| 2020-01-30 | sevenapp[.]info |

At the same time, the Cerberus C&C has been seen to resolve the same IP address.

|  |  |
| --- | --- |
| Date resolved | Cerberus C&C |
| 2020-02-11 | owallet[.]space |
| 2020-01-31 | honminer[.]com |
| 2020-01-30 | arm-pay[.]ru |

Based on the above research, we suspect that Anubis has a good relationship with Cerberus.

In addition, we also found Anubis new wild fishing attack.

Fishing url:

<http://weatherr[.]xyz/Flash>

<http://z99541uj.beget[.]tech/Flash>

