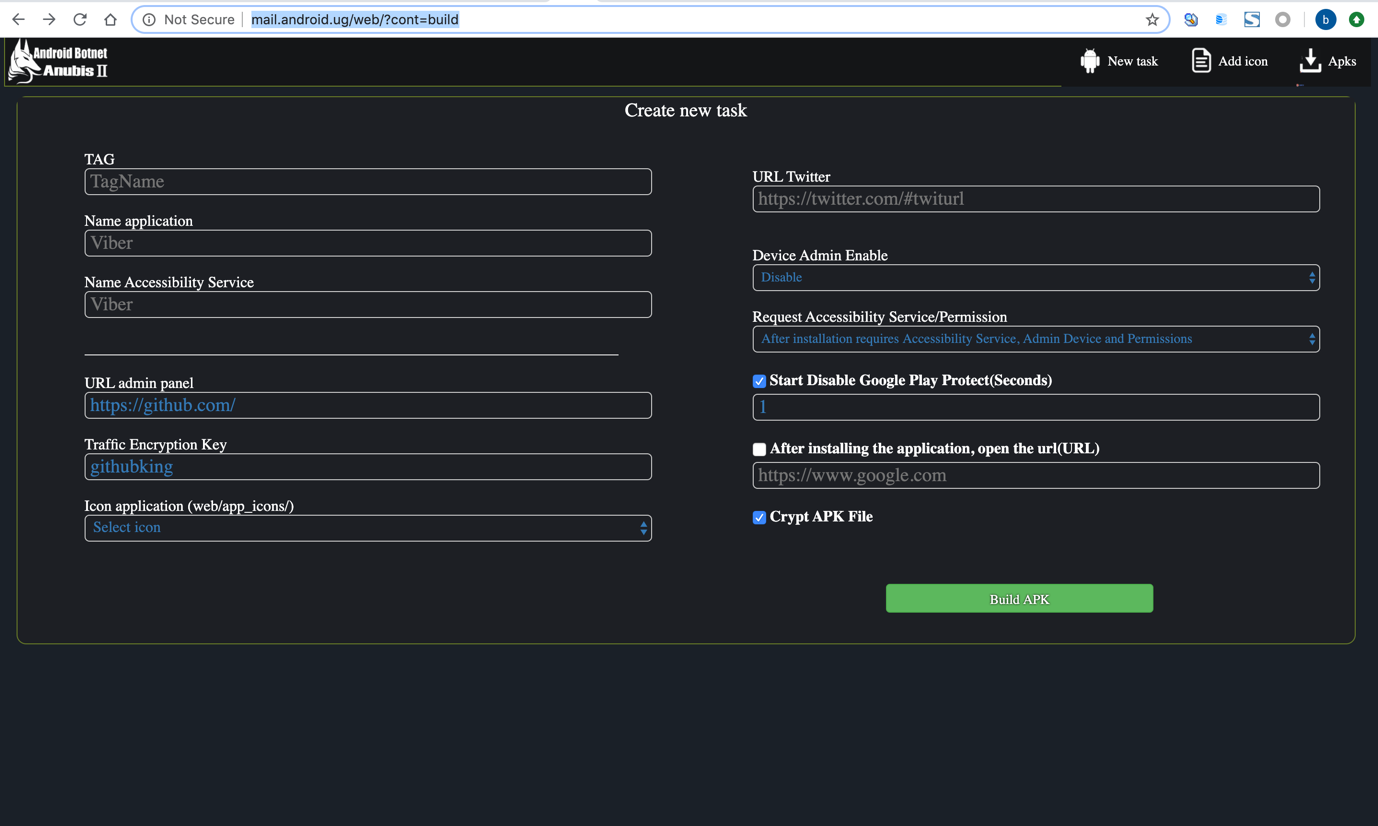
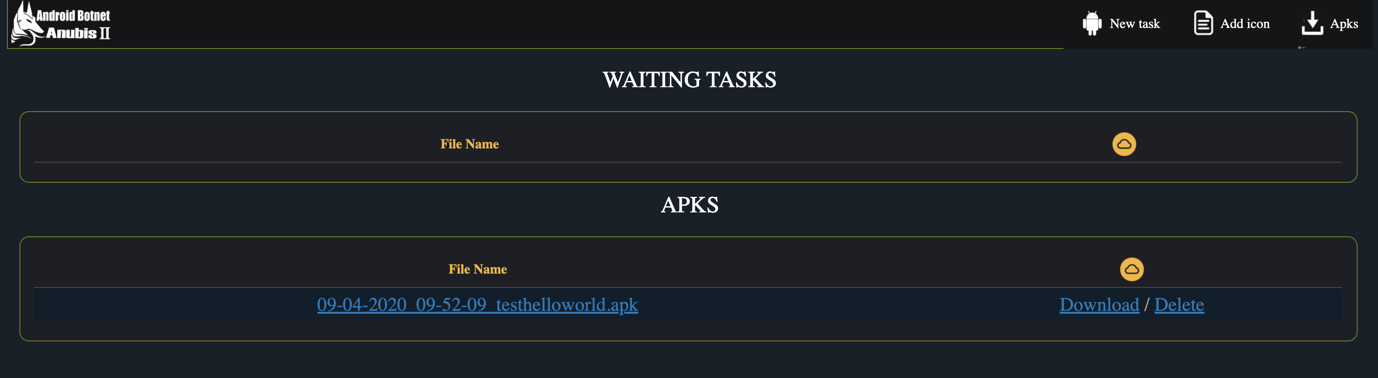
1. Base on C2 domain[files.ug], I found old Anubis Build Server[hxxp://mail.android.ug/web/?cont=build]

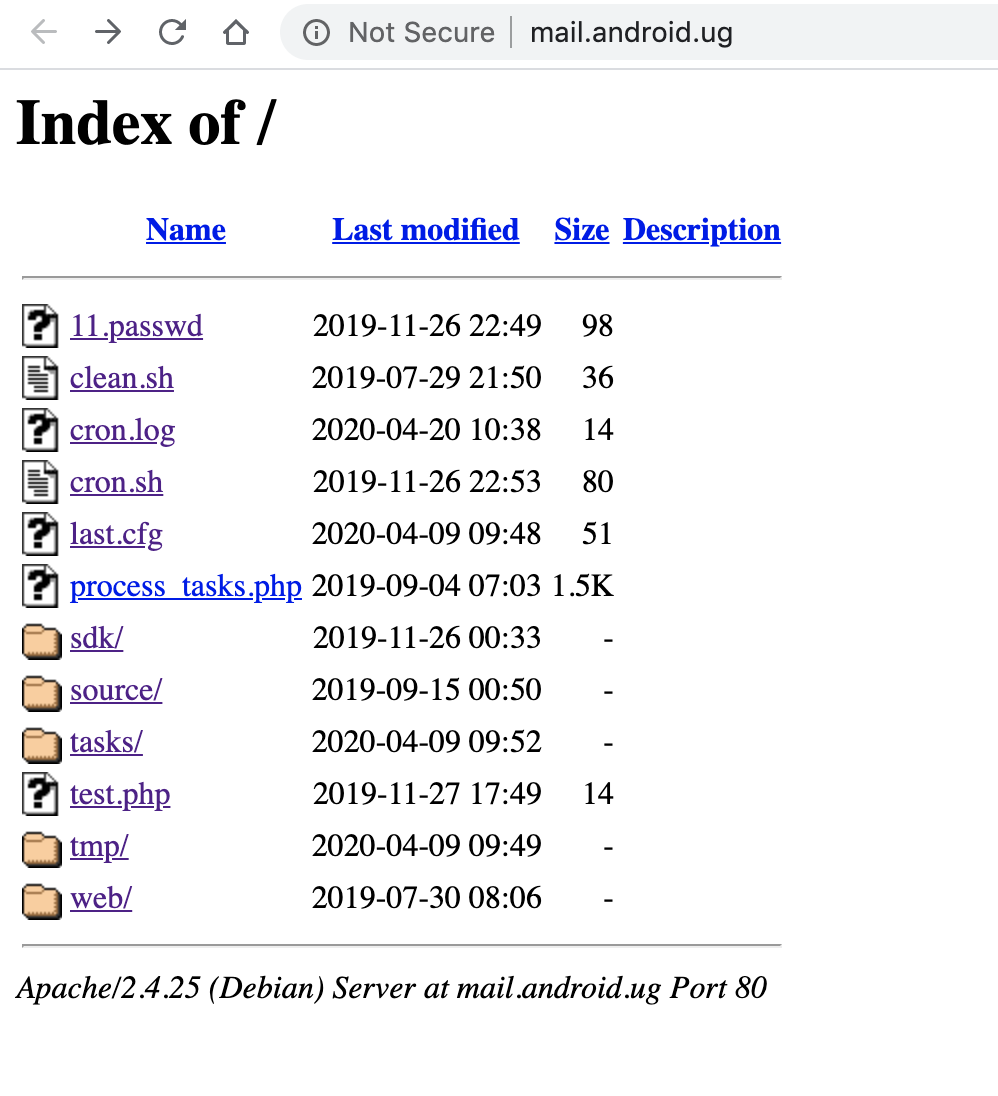




Icon Application table:

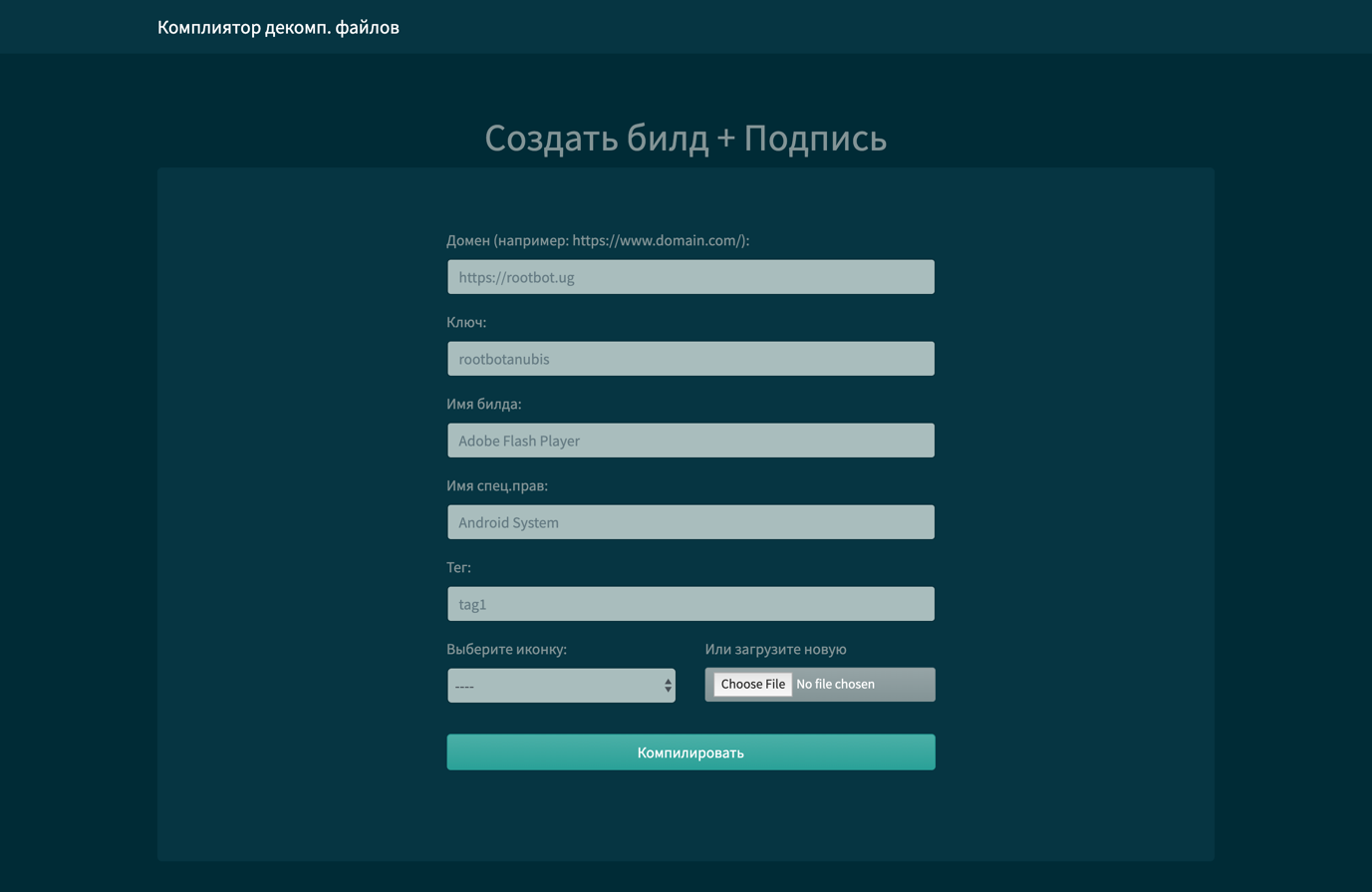
|  |
| --- |
| mobile\_legend\_cheats |
| freefire\_cheat |
| bitcoin\_1 |
| Your\_safety |
| Wallet\_pro |
| Update1 |
| Update |
| Turkcell-10gb |
| TiM.it.telecom |
| Talklog |
| SystemSecurity |
| Stand\_Off |
| Shareit |
| Setting |
| Samsung\_Pay |
| PromoCodes |
| PlayMarket |
| Pizza-Darom |
| Photo\_1 |
| Photo |
| Option\_Signal |
| Modus\_Fashion |
| MinerBitcoins |
| Look |
| KasperskyInternetSecurity |
| Invoice |
| InstagramMass |
| Instafiltrs |
| Insta\_pro |
| Gvrt |
| Google\_Maps |
| Google |
| Document |
| Cryptobot |
| Critical\_Ops |
| CoinMarketApp |
| Chat\_private\_XL |
| CashbackPlus |
| CHEAT |
| Bitpanda |
| Bitcoin |
| Bankia\_Wallet |
| Bankia |
| Android\_SystemUl |
| Android\_Explorer |
| AndroidSystemWebView |
| AdobeFlashPlayerUpdate |
| 20GB-İnternet |

Other info:



2. New Building page:

hxxp://android.ug/



Samples that the actor has builded:



All had been detected as AndroidOS\_AnubisDropper.HRX

276ebe2ff5b1234e8f9bfb7e116bece349a7b91b7326cfd057ef3095b29a5ccd  01\_04\_2020\_16-56-15\_pubg.apk

276ebe2ff5b1234e8f9bfb7e116bece349a7b91b7326cfd057ef3095b29a5ccd  02\_04\_2020\_15-15-47\_pubg.apk

540418afc7e75f27befcb6b33381a21b9842a5d13f7d18bbe8f233e3b5e4e740  02\_04\_2020\_16-38-15\_tag1.apk

42ecb107a212d16cd3d0c59edf42b6be1489df316b12dddce2a8fb11cd990e5a  03\_04\_2020\_23-39-14\_tag10.apk

9630356c8c51944748eadc68ba8f3a4974339bef1c811a520d7529e0962a4141  05\_04\_2020\_05-07-39\_.apk

f6e773ea059b5701a428dd5a1ef3ea9bcaa33b2960f00cef922de91497f15f6c  09\_04\_2020\_07-06-59\_testhelloworld.apk

774f3e875f477213a2fbe727aaf125d840ec4b449c2843a5cf2447d1d72c7b4e  10\_04\_2020\_15-32-27\_pubg.apk

1568f9b3484ea343c2676b6f5f712ea27f66b8ef8e11e62d9a6547a882d7aa29  10\_04\_2020\_15-47-20\_king.apk

612839537cd23e35aefa2a874ae25a11df3dbb92fd770e682275d1bffb9402a5  14\_04\_2020\_01-17-55\_reintermediate.apk

711f77b88811dca261ee7c2949a4fffa415efc20e3cfc9134f38db9d89f4d230  14\_04\_2020\_01-19-15\_Georgia.apk

06a3cfd553ebdc4e124ffc4025aecd144b06604853f3c0c59336a5322737adbd  14\_04\_2020\_01-19-53\_.apk

8ec16967b86b71a901028e66082a99fccb8c77bc6344b856d4cc0f1307fab072  14\_04\_2020\_01-20-33\_Georgia.apk

638c43defcb81956cd81358e3cba06e0267751a4f4e6ecc4317726d919458364  14\_04\_2020\_01-21-22\_.apk

1504725144efcb57270a69693088fe2029ca12c84756343f16be425ce5d64a9f  14\_04\_2020\_01-22-01\_Georgia.apk

9630356c8c51944748eadc68ba8f3a4974339bef1c811a520d7529e0962a4141  14\_04\_2020\_01-22-44\_.apk

be2edcfc60c0bd84a4db2022c2ab6ecdb5fc635dd8278b287df24cc5631e4ca0  14\_04\_2020\_01-23-23\_Georgia.apk

177e084b64f8e635ff74fab8b9d69a8047a09e5ab06a078e44660379a459f578  14\_04\_2020\_01-24-04\_.apk

764d94fcf048c7c68f81fbe8ce8c44732a0601ad9043c1f4a3b73a8abb38e332  14\_04\_2020\_01-24-41\_Georgia.apk

05c9428115e742580396853f68d051a662959def67863b38421bc9736cd21ebc  14\_04\_2020\_01-28-31\_microchip.apk

5cc1261cc7b78182f0ca916b94964e72c6d2d91d7cd564d8addba8d8c81f807f  14\_04\_2020\_01-29-17\_.apk

258f6592b779d898efbbceb4f161577c0330a2b0cce719639931a16f51a866fc  14\_04\_2020\_01-31-33\_ROI.apk

3cdfe3b165712427455008647b5af028342e444813a126679c9af0e45bd0a46c  14\_04\_2020\_01-32-50\_synthesize.apk

c28a55f2d2282273e8d9a5e72ef63a6672016be91701d9a6d271c56fda97332e  14\_04\_2020\_01-33-32\_.apk

22a031dca85f5fabdf8e7d3477ae39b58fea819f646f76a183f28e3831286a0f  14\_04\_2020\_01-34-16\_synthesize.apk

970f95dfd8783bfb453ccdc8e3b0966d9af5d4dfa7800edb6bc902729b7b298d  14\_04\_2020\_01-34-59\_.apk

32678dd89dc68553ee8fb0090b8742cf9f9c47436d839320dbc1fe102857c6d1  14\_04\_2020\_01-35-50\_synthesize.apk

20f39226bd067651d4a21b16108a43c8fb8269b8c765585edcdda80d546764d4  19\_04\_2020\_18-47-05\_Spur.apk