ANTIY | Antiy Labs

Analysis Report on Android Trojan HongTouTou (ADRD)

Antiy Labs

(February 2011)

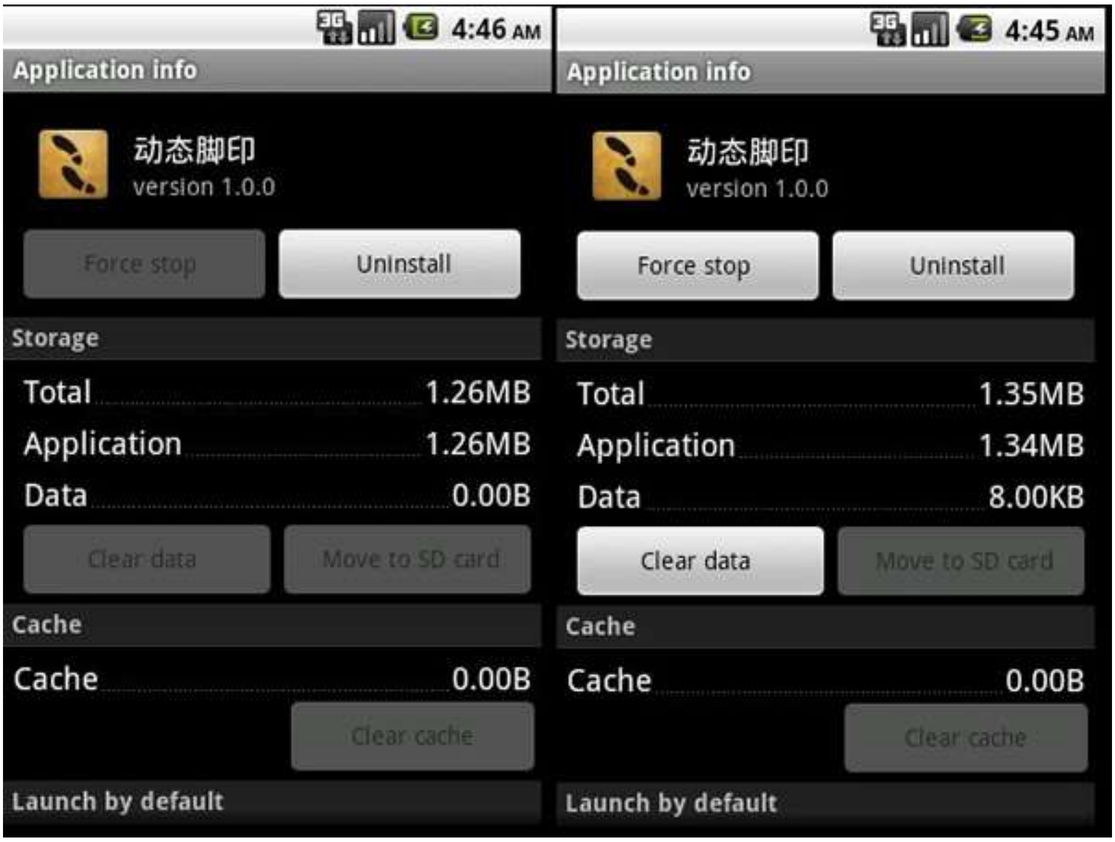
Contents

Basic Information

Virus Name: Trojan/Android.Adrd.a[Clicker]
Virus Alias: HongTouTou、ADRD
Type：Trojan
Sample MD5：A84997B0D220E6A63E2943DA64FFA38C
Sample CRC32:A42850DE
Sample Length:1,316,981 bytes
Original File Name: Newfpwap_com_liveprintslivewallpaper.apk
Appearance Time: Jan. 27, 2011
Systems Infected: Android 2.0 and higher versions

Overview

ADRD Trojan (HongTouTou Trojan) has been embedded into more than 10 legal applications (Figure 1) and it spreads through a number of forums and downloads. It can open several system services. It can also upload infected cell phone’s information (IMEI, IMSI, and version) to the control server every 6 hours and then receive its commands. In addition, it can obtain 30 URLs from the data server and access them individually. What’s worse, it can download an installation file (.apk) to a specified directory of the SD card. Infected cell phones will generate lots of network traffic and cause users a lot of extra expenses. Users can use our Android malware cleansing tool AVL for Android to detect whether the phone is infected or not, and then decide to delete corresponding applications.



动态脚印
version 1.0.0

Total 1.26MB
Application 1.26MB
Data 0.00B
Cache 0.00B

动态脚印
version 1.0.0

Total 1.35MB
Application 1.34MB
Data 8.00KB
Cache 0.00B

Figure 1 Normal application and the application injected

Sample Signature

Antiy Labs has detected that ADRD (also known as HongTouTou Trojan) is injected into the following Android applications:

- Live Prints Live Wallpaper
- TurboFly 3D
- Robo 3
- iReader
- Fancy Widget Pro
- Light Grid
- Compass
- FingerPrint

Ø Silhouette Donation

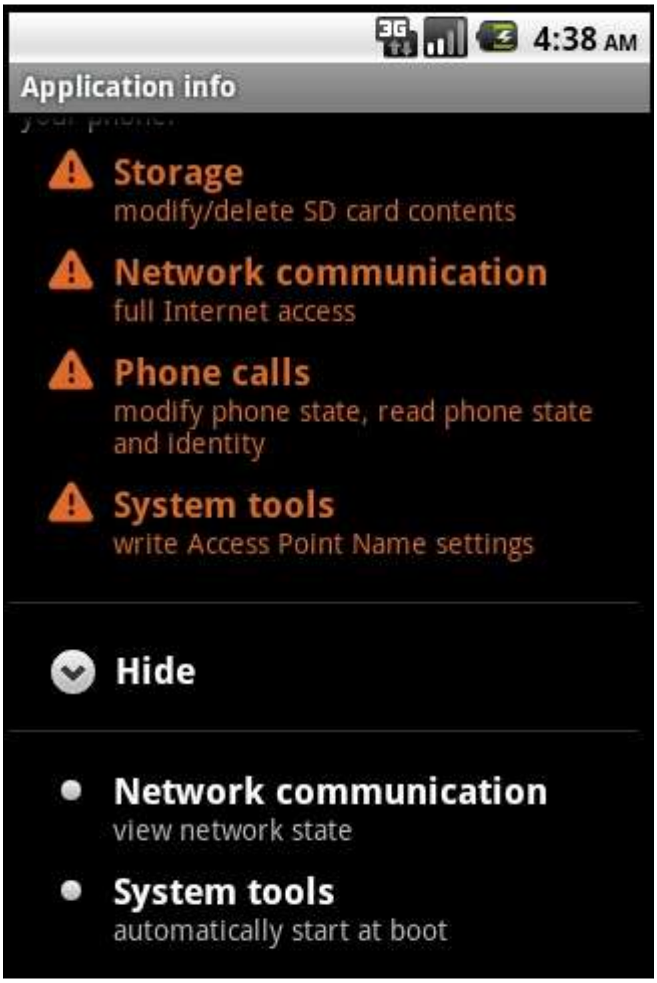
ADRD is embedded into Live Prints Live Wallpaper, which was discussed in mainstream domestic forums on January 27th. The embedded app includes 2 parts:

1. a normal program liveprints：
1） service LivePrints：android.service.wallpaper.WallpaperService
2） Activity：.LivePrintsSettings

2.malware com.xxx.yyy：
1） receiver com.xxx.yyy.MyBoolService, used to start（android.intent.action.BOOT_COMPLETED）
2） receiver com.xxx.yyy.MyAlarmReceiver，customer service（com.lz.myservicestart）
3） receiver com.xxx.yyy.NetWorkReceiver， responds to the network changes（android.net.conn.CONNECTIVITY_CHANGE）
4）receiver com.xxx.yyy.CustomBroadCastReceiver， responds to the phone state（android.intent.action.PHONE_STATE）
5） service com.xxx.yyy.MyService

ADRD needs to obtain the following system privileges(Figure2）:

• read the contact data
• fully access the Internet
• modify / delete the contents of the SD card
• read and modify the call state
• Write the APN (Access Point Name) settings
•check the network and Wi-Fi state
• auto-start



4:38 AM

Application info

⚠ Storage
modify/delete SD card contents

⚠ Network communication
full Internet access

⚠ Phone calls
modify phone state, read phone state and identity

⚠ System tools
write Access Point Name settings

Hide

● Network communication
view network state

● System tools
automatically start at boot

Figure 2 Malicious code needs many system privileges

Behavior Analysis

Receiver Analysis

com.xxx.yyy.MyBoolService

The Trojan starts automatically at boot by the receiver, and then sends com.lz.myservicestart broadcast message and sets an alarm which will be activated in 2 minutes.

com.xxx.yyy.MyAlarmReceiver

After receiving com.lz.myservicestart, it will start MyService.

com.xxx.yyy.NetWorkReceiver

Check the state mark in phone_start to decide whether MyService is started or not. If the service is not started, the receiver will start it.

com.xxx.yyy.CustomBroadCastReceiver

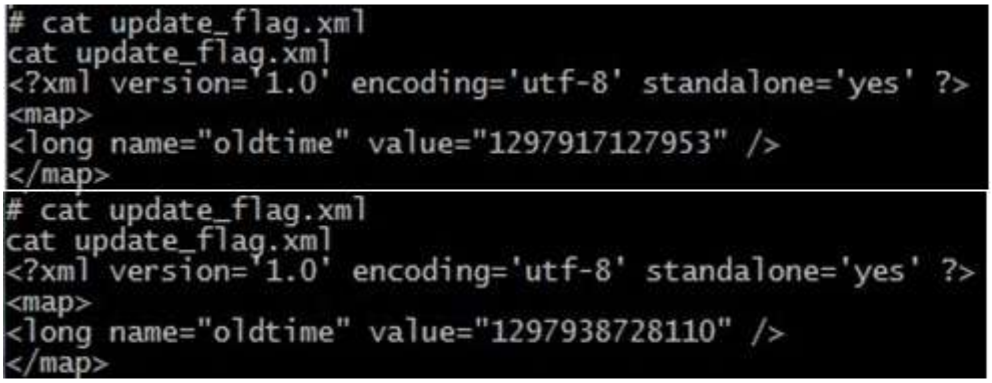
If the phone state is idle, it will modify the state mark of phone_start as start and enable MyService.

MyService

After the MyService starts, it attempts to obtain IMEI and IMSI of phone. If it fails, it will attempt in 6 minutes.

The second step is to check network communication. If there is no connection, it will attempt to open network connection. If it fails, it will attempt in 6 minutes. Access the configuration information in APN settings, and compare it with UNINET, UNIWAP, cmnet and cmwap to decide the connection type.

The next step is to check the time when the sample saved in oldtime field of update_flag.xml communicated with control server. If the time is more than 6 hours, it collects local information and sends data to control server, and update the oldtime. (Figure 3)



```
# cat update_flag.xml
cat update_flag.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<long name="oldtime" value="1297917127953" />
</map>
```

```
# cat update_flag.xml
cat update_flag.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<long name="oldtime" value="1297938728110" />
</map>
```

Figure 3 Sample connects control server every 6 hours

Malicious Actions Analysis

Figure 4 shows the main malicious actions of samples. All the actions run in background, so they are invisible for users.

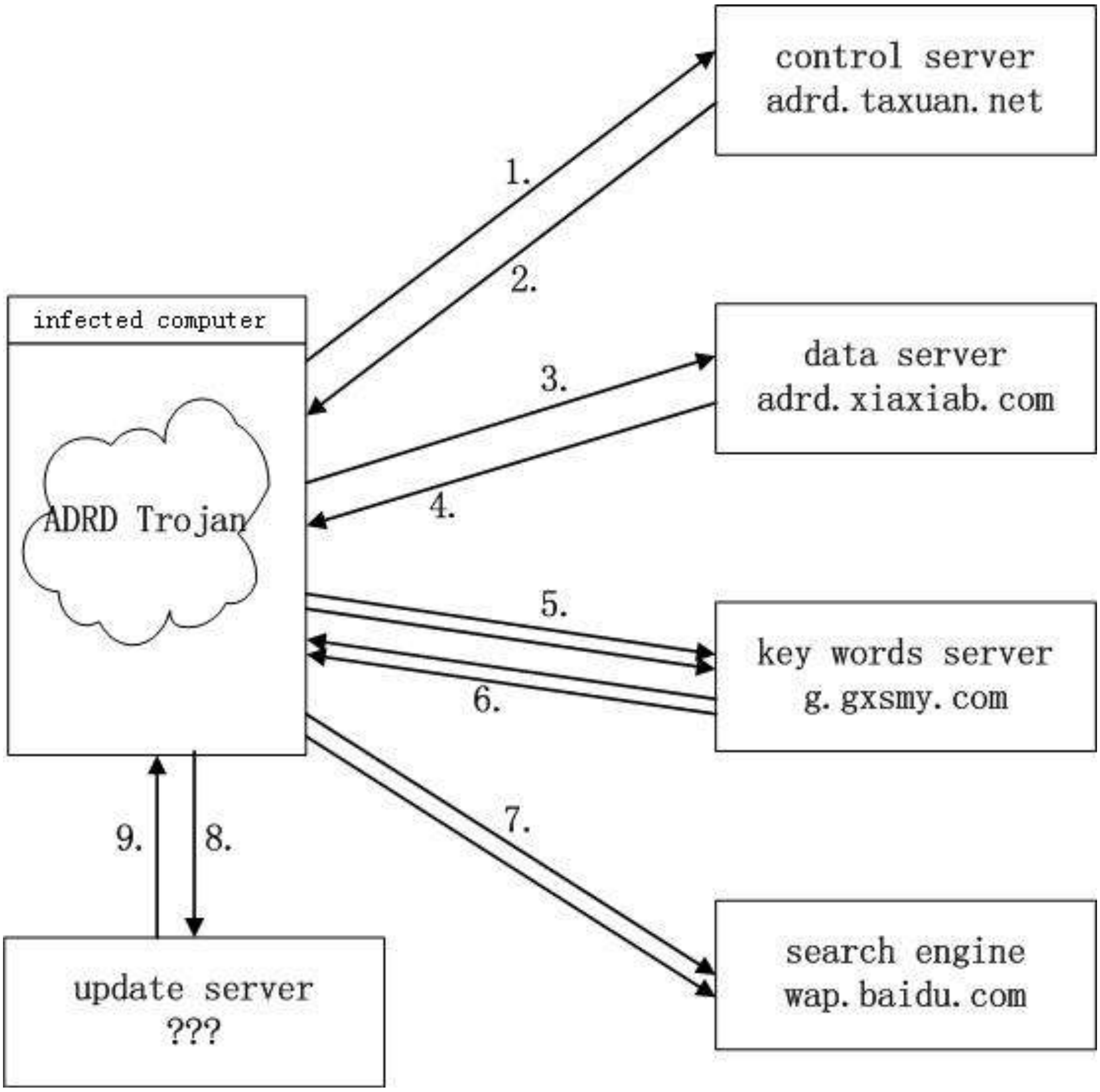


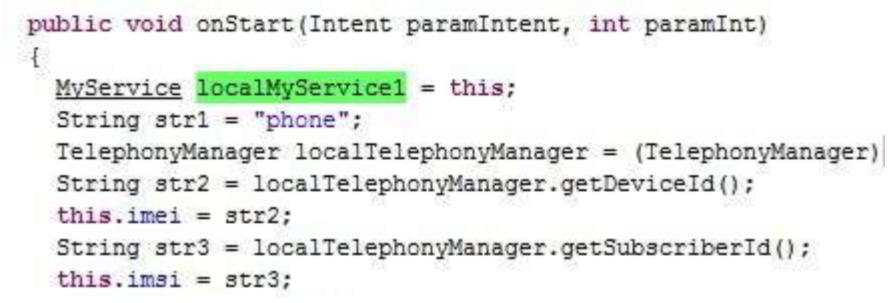
Figure 4 Main malicious actions

Send IMEI/IMSI and Version Information to Control Server

MyService obtains the following information from phone (Figure 5):

- Imei: the IMEI code of compromised phone
- Imsi: the IMSI code of compromised phone
- Iversion: the version of sample, 1 as default
- Oversion: the version of compromised Android system

l Netway: if the value is 1, it means normally visit; if the value is 0, it means visit by proxy.



```
public void onStart(Intent paramIntent, int paramInt)
{
  MyService localMyService1 = this;
  String str1 = "phone";
  TelephonyManager localTelephonyManager = (TelephonyManager)
  String str2 = localTelephonyManager.getDeviceId();
  this.imei = str2;
  String str3 = localTelephonyManager.getSubscriberId();
  this.imsi = str3;
```

Figure 5 Get IMEI and IMSI codes

Next, structure a plain text string according to the following methods and orders:

<string> = Imei + “&” + imsi + “&” + netway + “iversion” + “oversion”

Encrypt the above string with DES arithmetic (use key “48734154”) and get encrypted text string <enstring>. Then combine the encrypted text string with the link of control server as a complete URL:

http://adrd.taxuan.net/index.aspx?im=<enstring>

At last, send a HPPT POST request to this URL, thus send the encrypted IMEI, IMSI and version information of phone to control server adrd.taxuan.net.

Receive Control instructions from control server

Sample receives response message from control server adrd.taxuan.net. The response data is encrypted text encrypted with DES and decrypted with key “48734154”. And then it executes next step according to the second character of decrypted plaintext:

Instruction 0: current function returns the subsequent character string to call function;

Instruction 1: start to execute step 3 (connect to data server);

Instruction 2: current function returns the subsequent character string to call function;

Instruction 3: start to execute step 8 (connect to update server).

Send IMEI/IMSI to data server

Structure a plain text string according to the following methods and orders：

<string> = Imei + “&” + imsi

Encrypt the above string with DES arithmetic (use key “48734154”) and get encrypted text string <enstring>. Then combine the encrypted text string with the link of data server as a complete URL:

http://adrd.xiaxiab.com/pic.aspx?im=<enstring>

At last, send a HTTP POST request to this URL, thus send IMEI, IMMSI code of phone to data server adrd.xiaxiab.com

Receive URL entry from data server

Sample receives response information from data server adrd.xiaxiab.com. The response data is encrypted test encrypted with DES and decrypted with key “48734154”. Get following plain text (omitting middle section):

```
B#1#963a_w1|http://59.173.12.105/g/g.ashx?w=963a_w1|1|http://59.173.12.105/add
/pk.aspx$B#1#961a_w1|
http://59.173.12.105/g/g.ashx?w=961a_w1|1|http://59.173.12.105/add/pk.aspx$B#1#
964a_w1|
http://59.173.12.105/g/g.ashx?w=964a_w1|1|
………..
http://59.173.12.105/add/pk.aspx$B#1#961a_w1|http://59.173.12.105/g/g.ashx?w=96
1a_w1|1|
http://59.173.12.105/add/pk.aspx$
```

It contains 30 recorders. First recorder, for example, whose each field has following meanings:

Field value	Meanings
B	Beginning delimiter
1	Expected visit count(docount)
963a_w1	Identity
http://59.173.12.105/g/g.ashx?w=963a_w1	Key words server(URL gwurl)
1	Hmul
http://59.173.12.105/add/pk.aspx	prul
$	Ending delimiter

It should be pointed out that these 30 recorders, which remain stable in much analysis, is irrelevant with IMEI, IMSI code sent to data server.

We call string gwurl as key words server URL. The IP of key words server is 59.173.12.102. Between these 30 recorders, server address also appears with g.gxsmy.com.

Visit Key words server repeatedly

After parsing these 30 recorders, sample obtains 30 difference key words server's URL. Then, orderly visit these URLsat the speed of one per second (in HTTP request, refer field is set to prul value).

Get key words and search links

Key words server g.gxsmy.com returns data to sample, the data has following way:

1|http://wap.baidu.com/s?word=%e8%9d%8e%e5%ad%90&vit=uni&from=963a_w1

With "|" as separator, the second part is search links. This link points to one search result page of Baidu WAP.

For the examples above, "%e8%9d%8e%e5%ad%90" is Unicode corresponding with a string Chinese character. It is the search key words from wap.baidu.com. During analysis, same key words server URL visiting will return difference key words, and these key words have no obvious relevance. So we think that, these key words are generated by key words servers at random.

We also notice that, between search links, appear a parameter from and this parameter is same with w parameter which exist in corresponding key word server URL. For example, the 963a_w1 appears at example of above section.

On the other hand, 30 recorders got at step 4 correspond with 30 identifiers. For these 30 identifiers, key words server will return search links. But for other identifiers, key words server will return null.

So, key words server maintains the list of these 30 identifiers and checks visiting request. This identifier information, which remains the same in the main attack, is significant.

Visit search links

Finally, the sample will access the search link and download the page, so it will cause lots of network traffic.

When the sample finish step 5, 6 and 7, then the interaction with the control server is done. Related processes will exit and the sample will establish connection with the control server in 6 hours.

Connect the update server

When the control server send back command 3 in step 2, the sample will execute step 2. It will access a URL that is used for update.
The value of the URL is appended after the commands.
But in the analysis, we never found command 3 be returned, so we can't get the address of the update server. We believe the sample hasn't started this function.

Download and install the installation package

After the sample access the update server, it will download an installation file (.apk), rename it as myupdate.apk， and then store it in directory \sdcard\uc\. In addition, the sample will add the attribute "is_new" to update_flag.xml.

Detection and Removal method

User could download free tool AVL PK for Android provided by Antiy Labs to detect this Trojan. Below is the information of the installation file:

Download: http://www.antiy.com/download/avlpk/AVLPK_for_Android_1.02.zip

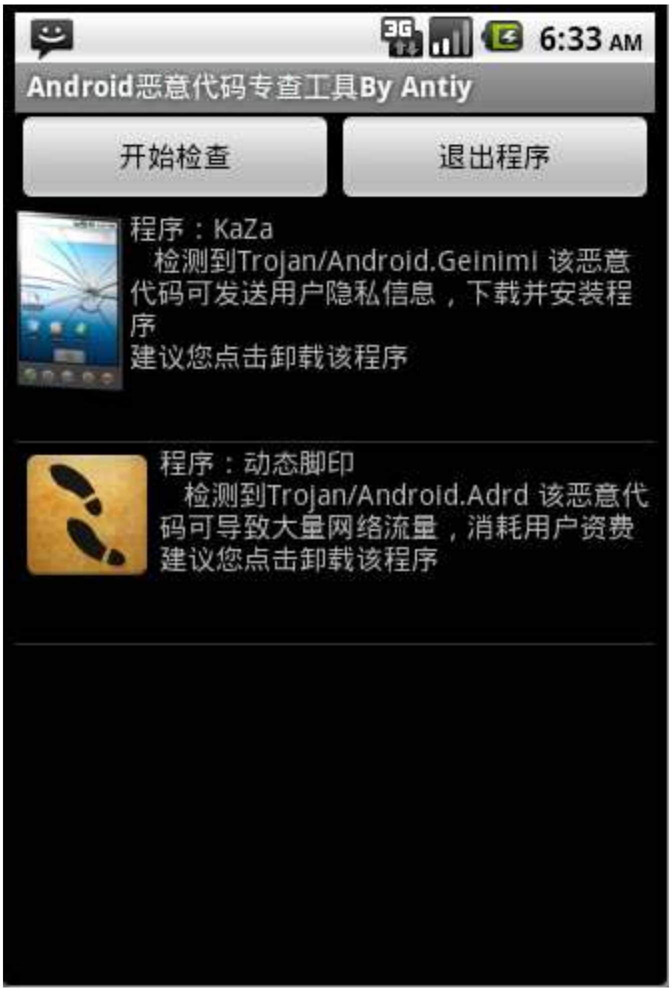
Name: AVL PK for Android.apk

Size: 143, 412 bite

MD5: 2721be6205102dada7e1fa7e5c544606

Version: 1.02

After installing AVL PK for Android, run this tool, select "start detection" and wait. If it appears "detect a Trojan/Android.Adrd" (figure 3), we could uninstall related software and then the Trojan would be cleared. In addition.AVL PK for Android also detects and clears Geinimi Trojan.



Android恶意代码专查工具By Antiy

程序：KaZa
检测到Trojan/Android.Geinimi 该恶意代码可发送用户隐私信息，下载并安装程序
建议您点击卸载该程序

程序：动态脚印
检测到Trojan/Android.Adrd 该恶意代码可导致大量网络流量，消耗用户资费
建议您点击卸载该程序

Figure 7 AVL for Android has detected ADRD Trojan

Conclusion

In recent years, more and more cell phones are using Android systems. As a result, the Android system becomes a major attack target. Cell phone malware has various spreading methods and it is good at hiding itself.

On the other hand, according to a research, more than 10% users don’t even know there is phone malware, and more than 30% don’t worry about cell phone malware. Users’ carelessness makes it much easier for malware to spread. It is reported that since Jan. 27th, ADRD had infected almost a million users.

Currently, there are many forums on Android applications and cell phones. They do convenient the users, but they also convenient the malware. ADRD and Geinimi both spread via forums and download websites. So, we suggest that users download phone applications from trusted sources.

In addition, when installing an app, users should pay attention to the required privilege. If it requires strangely high privilege, users should be careful.

Any technical information that is made available by Antiy Labs is the copyrighted work of Antiy Labs and is owned by Antiy Labs.

NO WARRANTY. Antiy Labs makes no warranty as to this document's accuracy or use. The information in this document may include typographical errors or inaccuracies, and may not reflect the most current developments; and Antiy Labs does not represent, warrant or guarantee that it is complete, accurate, or up-to-date, nor does Antiy Labs offer any certification or guarantee with respect to any opinions expressed herein or any references provided. Changing circumstances may change the accuracy of the content herein. Opinions presented in this document reflect judgment at the time of publication and are subject to change. Any use of the information contained in this document is at the risk of the user. Antiy Labs assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. Antiy Labs reserves the right to make changes at any time without prior notice.

About Antiy Labs

Antiy Labs is an antivirus vendor which makes advanced research and technology contributions to the field. Currently, there are tens of thousands of firewalls, UTM and security devices deployed with our antivirus engine. More information is available at www.antiy.net.

ANTIY

Antiy Labs