Digital Crimes in Russia and Criminal Prosecution
First 24/7 CERT in Eastern Europe
CERT-GIB is the first private Computer Emergency Response Team in Russia.

Service package
- Pre-incident consulting;
- Response;
- Forensics;
- Investigation;
- Legal support;
- Post-incident consulting.

Skolkovo resident
The CyberCop project, an integrated system for counteracting cybercrime.

Leader on the Russian market
The first and only company in the CIS providing comprehensive services in investigating IT security incidents.

Group-IB is founded

Acquisition by Leta Group

International Expansion

Creation of CERT-GIB

Dedicated Certified Professionals

2003

2010

2011

2011

2012

60+ employees
A report on the results of a comprehensive study of the state of the Russian-speaking cybercrime market:

- Financial performance estimates;
- Analysis of the main trends and threats;
- Overview of key events;
- Legal aspects;
- Forecasts.
Russian-Speaking Market

- Russian Federation
- CIS
- Baltic states
- Immigrants from former USSR
Russian Cybercrime vs. Global Market

Total Cybercrime Market
IN U.S. DOLLARS

$12.5 billion
$4.5 billion

SIZE OF GLOBAL CYBERCRIME MARKET
RUSSIAN SPEAKING CYBERCRIME MARKET
CERT-GIB

First 24/7 CERT in Eastern Europe
CERT-GIB is the first Eastern European 24/7 Computer Emergency Response Team, and the first private CERT in Russia (second overall)

Around-the-clock geographical deployent
Passing the relay for monitoring, analyzing, and mitigating: Europe ➔ North America ➔ Asia – for smooth uninterrupted incident handling

Providing help and assistance for:
Phishing, Spam, Scam, DDoS attacks, malware, and many other fraudulent schemes

.RU, .РФ, .SU: special emphasis
Official ccTLD.ru-assigned expert organization for handling phishing, malware, and botnets

CERT-GIB: Europe, North America, Asia
Unique Expertise

Competent Organizations

The League for Safer Internet

As per the Agreement, the organization’s area of expertise includes combating negative online content, especially child pornography. The League for Safer Internet is one of the most effective non-governmental organizations countering negative online content. Over the past ten months more than 20,000 reports were received regarding online child pornography resources. After processing these reports, more than 8,000 websites containing unlawful content were removed. Interaction regulations.

Group IB

As per the Agreement, the organization’s area of expertise includes combating the use of domain names for the purposes of phishing, unauthorized access to third-party information systems, malware distribution, and controlling botnets. Group IB is a nongovernmental organization providing information security incident investigation.

Contacts
CERT-GIB Accreditation

Authorized user of the “CERT” trademark

Accreditation in progress

TI-listed
<table>
<thead>
<tr>
<th><strong>CONVENTION ON CYBERCRIME</strong></th>
<th><strong>RUSSIAN CRIMINAL LAW</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 2 – Illegal access</td>
<td>Article 138, 272, 274</td>
</tr>
<tr>
<td>Article 3 – Illegal interception</td>
<td>Article 138, 272, 274</td>
</tr>
<tr>
<td>Article 4 – Data interference</td>
<td>Article 272, 273, 274</td>
</tr>
<tr>
<td>Article 5 – System interference</td>
<td>Article 272, 273, 274</td>
</tr>
<tr>
<td>Article 6 – Misuse of devices</td>
<td>Article 138.1, 273</td>
</tr>
<tr>
<td>Article 7 – Computer-related forgery</td>
<td>Article 272, 273, 274</td>
</tr>
<tr>
<td>Article 8 – Computer-related fraud</td>
<td>Article 272, 273, 274</td>
</tr>
<tr>
<td>Article 9 – Offences related to child pornography</td>
<td>Article 158-160, 165, 272, 273, 274</td>
</tr>
<tr>
<td>Article 10 – Offences related to infringements of copyright and related rights</td>
<td>Article 242.1, 242.2</td>
</tr>
<tr>
<td></td>
<td>Article 146, 180</td>
</tr>
</tbody>
</table>
Pavel Vrublevsky (RedEye)

CEO of Chronopay, a payment processing company

✓ Member of the Antispam Working Group at the Russian Ministry of Communication;
✓ Chairman of the Russian Committee on Electronic Commerce;
✓ Member of the Russian Association of Electronic Communications.
Pavel Vrublevsky (RedEye)

aka RedEye

Porn affiliation programs:
cash.pornocruto.es
etu-cash.com
Pavel Vrublevsky (RedEye)

Crutop.nu: the largest spammer forum
Pavel Vrublevsky (RedEye)

Pharmaceutical affiliate program:
Rx-promotion.com
DDoS Attack on Assist

ChronoPay Co-Founder Arrested

Hello there! If you are new here, you might want to subscribe to the RSS feed for updates on this topic. You may also subscribe by email in the sidebar.

Russian authorities on Thursday arrested Pavel Vrublevsky, co-founder of ChronoPay, the country’s largest processor of online payments, for allegedly hiring a hacker to attack his company's rivals.

Vrublevsky, 32, is probably best known as the co-owner of the Rx-Promotion rogue online pharmacy program. His company also consistently has been involved in credit card processing for—and in many cases setting up companies on behalf of—rogue anti-virus or “scareware” scams that use misleading PC security alerts in a bid to frighten people into purchasing worthless security software.

Vrublevsky was arrested on June 23. Financial Times reporter Joe Menn writes that Vrublevsky was arrested without bail and a hearing was set for a month’s time.

As I reported earlier this week, Vrublevsky fled the country after the arrest of a suspect who confessed that he was hired by Vrublevsky to launch a debilitating cyber attack against Assist, a top ChronoPay competitor. According to Russian news organizations, the ChronoPay executive wanted to sideline rival payment processing firms who were competing for a lucrative contract to process payments for Aeroflot, Russia's largest airline. Sources close to the investigation said Vrublevsky was arrested at the Sheremetyevo airport outside of Moscow as he returned from a trip to the Maldives.

The arrest comes just 24 hours after authorities seized computers and servers in the United States and seven other countries this week as part of an ongoing investigation of a hacking gang that stole $72 million via scareware scams.

Accused of organizing a DDoS attack on Assist, a payment processing company (Accused executor of the attack: Igor Artimovich)
Заместитель Генерального прокурора Российской Федерации Виктор Гринь направил в суд уголовное дело об умышленном блокировании работы системы оплаты и приобретения электронных билетов на сайте ОАО «Аэрофлот».

Расследованием по делу установлено, что Врублевский, являясь генеральным директором ЗАО «Конопля», в начале июля 2010 г. решил предпринять меры к разрыву контракта между ОАО «Аэрофлот» и ООО «Ассист» об оказании услуг по продаже электронных авиабилетов, устраивая тем самым конкурента своей фирмы в данной сфере. Для этого он в г. Москве создал организованную группу, куда помимо него входили подчиненные ему ведущий специалист службы информационной безопасности Пермяков, а также брат Артемьев, занимающийся оказанием хакерских услуг.

Руководя указанной организованной группой, Врублевский в июле 2010 г. через Пермякова поставил задачу братьям Артемьевым, имеющим в пользовании созданный ими же с использованием вредоносных программ сервер заказов ИТ-компании (Вет-сети), провести хакерскую атаку на сайт ОАО «Аэрофлот» по продаже билетов. За указанные действия Врублевский выдал денежные средства предприятия в размере более 20 тыс. долларов США, которые Пермяков по мере необходимости перечислил братьям Артемьевым за работу.

Артемьева, получившего незаконное указание, находился в съемной квартире в г. Москве, и действуя со своего мобильного телефона, имеющего подключение к сети Internet в период с 15 по 24 июля 2010 г. осуществлял компьютерную DDoS-атаку (также названную в обходе) на информационные ресурсы ООО «Ассист», которая заключалась в одномногородном обращении множества компьютеров, находящихся в Вет-сети, с запросами на обслуживание.

Однако данные компьютерной атаки привели к блокированию работы системы оплаты и приобретения электронных билетов на сайте ОАО «Аэрофлот» на весь период атаки и причинен погибшим фирмам крупный ущерб: ООО «Ассист» — на сумму свыше 15 млн. руб., ООО «Аэрофлот» — на сумму свыше 146 млн. руб.

Уголовное дело рассмотрено Следственным управлением Федеральной службы безопасности Российской Федерации.

После утверждения обвинительного заключения уголовное дело направлено в Тушинский районный суд г. Москвы для рассмотрения по существу.
Maxim Glotov (Two-Face)

Accused of committing fraud, unauthorized access to computer information, and creating and distributing malware.
Russian police arrest notorious Trojan gang

Huge crime spree brought to an end

By John Leyden + Get more from this author
Posted in Crime, 20th March 2012 14:02 GMT

Russian police are reported to have arrested a group of eight online banking scammers arrested in Russia

Gambling cyberblackmailers_steps_selection

Stolen Twitter selling for $1

Worldwide drop 2012

The arrested suspects included eight hackers who allegedly sold $4.5 million in the last three years using an estimated 90 compromised accounts. The gang, prior to the withdrawal of the statement by the Russian Interior Ministry, was said to be the ringleaders.

The investigation involved three malware: Stucct and Win32/Ralphdor malware.

The gang also conducted DDoS attacks.

Commonly associated with Blackhole Exploit Kit, Carberp achieved the banking worm as a follow-up attack in the aftermath of the Internet.

Related articles:

- Eight online banking scammers arrested in Russia
- Gambling cyberblackmailers_steps_selection
- Stolen Twitter selling for $1
- Worldwide drop 2012

News

Eight online banking scammers arrested in Russia

Hackers mainly targeted Russian, Eastern European and Dutch banks

Seven Russians and one person in Lithuania arrested

The Russian Federal Security Service has arrested eight hackers who allegedly sold $4.5 million in the last three years using an estimated 90 compromised accounts. The gang, prior to the withdrawal of the statement by the Russian Interior Ministry, was said to be the ringleaders.

Apart from the Russian group, the group was also said to be active in many other countries, including the Netherlands.

The criminals used the Carberp Trojan, a remote control tool, and Windows/Officetab malware.

The gang also conducted DDoS attacks.

The Carberp Group is commonly associated with Blackhole Exploit Kit, Carberp achieved the banking worm as a follow-up attack in the aftermath of the Internet.
Method of Propagation
### Carberp Control Panel

#### Поиск бота:
- **по UID:**
- **по IP:**
- **Искать:** Q

#### Список ботов:
- **Предфикс:** Все
- **Показать**

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Bot UID</th>
<th>Reg Date</th>
<th>Last Date</th>
<th>Live</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>bece9154f0e49804e9b77847344be59</td>
<td>28.01.11 [15:20:20]</td>
<td>28.01.11 [15:20:20]</td>
<td>06, 06, 06, 06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a56b6e39f156a74479807d3b51952236</td>
<td>28.01.11 [15:09:41]</td>
<td>28.01.11 [15:09:41]</td>
<td>06, 06, 06, 06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>226ba247a47213e78e1641855767e931</td>
<td>28.01.11 [14:48:56]</td>
<td>28.01.11 [14:48:56]</td>
<td>06, 06, 06, 06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ca9278773d2b083707ae750db632694</td>
<td>28.01.11 [14:41:12]</td>
<td>28.01.11 [14:41:12]</td>
<td>06, 06, 06, 06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a771c9fa7201725469449367af7635</td>
<td>28.01.11 [13:08:10]</td>
<td>28.01.11 [15:03:14]</td>
<td>06, 1ч, 55м</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5360e73525a6556e5e80a79836441</td>
<td>28.01.11 [11:33:57]</td>
<td>28.01.11 [12:29:30]</td>
<td>06, 5ч, 55м</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### RDPdor Control Panel

#### Table: The Way To The Future

<table>
<thead>
<tr>
<th>No</th>
<th>Bot UID</th>
<th>IP</th>
<th>State</th>
<th>Locale</th>
<th>OS Ver</th>
<th>First Connect</th>
<th>Last Knock</th>
<th>User</th>
<th>Passwds</th>
<th>Ver</th>
<th>Cmd</th>
<th>Comment</th>
<th>Ru</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>542b50c74d2325f8e8f31317b162900b8</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>10/10/11,12 23/11/11,03</td>
<td>Admin</td>
<td>Admin:MECI</td>
<td>2.1.27</td>
<td>cmd</td>
<td>500k:call 350</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>56a34e0f53f22b7e0e7f3f93297b5a</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>14/11/11,19 25/11/11,01</td>
<td>Admin</td>
<td>Admin:MECI</td>
<td>2.1.27</td>
<td>cmd</td>
<td>S</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>f002be9003b9c3d7e6eb55e191934b6f2</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>14/11/11,14 23/11/11,16</td>
<td>vika</td>
<td>vika:HOME</td>
<td>2.1.27</td>
<td>cmd</td>
<td>S</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>312121a17713f292979c3e2385calif9c0b</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>10/10/11,21 25/11/11,01</td>
<td>Admin</td>
<td>Admin:MECI</td>
<td>2.1.27</td>
<td>cmd</td>
<td>S</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>4587ec09d562573b7b2b6ec3a2a7c1bad</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>10/10/11,22 25/11/11,04</td>
<td>user2:12345</td>
<td>2.1.27</td>
<td>cmd</td>
<td>S</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>03336f0e892eb3a05760e947931cb1f</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>26/10/11,02 23/11/11,12</td>
<td>Admin</td>
<td>Admin:PO12</td>
<td>2.1.27</td>
<td>cmd</td>
<td>--</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>eab3444e866e29c821749fd458e9cf</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>11/10/11,00 25/11/11,07</td>
<td>User</td>
<td>User:HOME</td>
<td>2.1.27</td>
<td>cmd</td>
<td>S</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>c929d864e2c5946b5eac07274e6f8d6</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>11/10/11,00 25/11/11,09</td>
<td>Пользователь</td>
<td>Пользователь</td>
<td>2.1.27</td>
<td>cmd</td>
<td>S</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>c50414b25832318624760fed7089f7</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>11/10/11,00 25/11/11,07</td>
<td>Иванов111</td>
<td>2.1.27</td>
<td>cmd</td>
<td>S</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>2ff2177b7b83bf196a7cb37b8b5759</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>11/10/11,01 23/11/11,08</td>
<td>Admin</td>
<td>Admin:1-Ad1</td>
<td>2.1.27</td>
<td>cmd</td>
<td>etbanikai</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>5726f3f50e6356746fb7d266b6e446</td>
<td>OK</td>
<td>en-US</td>
<td>2:5:1:2600</td>
<td>21/11/11,01 25/11/11,08</td>
<td>Виктор</td>
<td>Виктор:VK1</td>
<td>2.1.27</td>
<td>cmd</td>
<td>S</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>d193b01d183e4e4896e8649b3089c0f</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>14/11/11,08 25/11/11,12</td>
<td>Лариса</td>
<td>Лариса:ONE</td>
<td>2.1.27</td>
<td>cmd</td>
<td>S</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>9eb22a698e595374b3d38816b1f82c</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>11/10/11,01 25/11/11,08</td>
<td>Admin</td>
<td>Admin:MELT</td>
<td>2.1.27</td>
<td>cmd</td>
<td>belorus</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>911b2d601d392955917a7337df7</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>11/10/11,02 25/11/11,08</td>
<td>User:SUH</td>
<td>2.1.27</td>
<td>cmd</td>
<td>S</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>3aa6b35eb8e449e3a2c32650966667eaf</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>14/11/11,16 25/11/11,00</td>
<td>Аргир</td>
<td>Аргир:ACC</td>
<td>2.1.27</td>
<td>cmd</td>
<td>S</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>0c253e2ed6d9f818777eca7a5543de9</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>21/11/11,13 22/11/11,11</td>
<td>Сергей</td>
<td>Сергей:RU1</td>
<td>2.1.27</td>
<td>cmd</td>
<td>S</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>1914bc4b8b9dd2b232b30998910c3</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>14/11/11,16 25/11/11,00</td>
<td>Аргир</td>
<td>Аргир:ACC</td>
<td>2.1.27</td>
<td>cmd</td>
<td>S</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>71b402016493fdd41ee40c13edd69358b6</td>
<td>OK</td>
<td>ru-RU</td>
<td>2:5:1:2600</td>
<td>13/10/11,02 25/11/11,05</td>
<td>User</td>
<td>User:12332</td>
<td>2.1.27</td>
<td>cmd</td>
<td>bilo.parator, йдем нома</td>
<td>S</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Results of the Investigation

✓ Joint investigation in close cooperation with the FSB and MVD of the Russian Federation and FOX-IT;

✓ Results of the investigation is the detention of the criminal group (8 persons);

✓ World’s first case when the entire online-banking criminal chain was arrested.
### Статистика Ботов

<table>
<thead>
<tr>
<th>Статистика Ботов</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ботов всего:</td>
<td>1543926</td>
</tr>
<tr>
<td>Ботов онлайн:</td>
<td>69874 (4.53%)</td>
</tr>
<tr>
<td>Ботов всего новых:</td>
<td>124017 (8.03%)</td>
</tr>
<tr>
<td>Ботов всего активных:</td>
<td>1413982 (91.58%)</td>
</tr>
<tr>
<td>Ботов за 24 часа:</td>
<td>129510 (8.39%)</td>
</tr>
<tr>
<td>Ботов за 7 дней:</td>
<td>204787 (13.26%)</td>
</tr>
<tr>
<td>Ботов за 1 месяц:</td>
<td>652746 (42.28%)</td>
</tr>
<tr>
<td>Размер БД (инфо ботов):</td>
<td>383.93 МВ из 256 ТВ (0.00%)</td>
</tr>
</tbody>
</table>
## Carberp Control Panel

### Log Entries

**Program:** Carberp

**Hash of program:** 0x321ECF12

<table>
<thead>
<tr>
<th>Bot</th>
<th>OBNOVLJCKYOE4B5F8767C8D9A1B</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP (Country)</td>
<td></td>
</tr>
</tbody>
</table>

**Hash launch:** 4012

**Date added:** 2011-12-20 13:12:58

**Hash launch:** 3400

**Date added:** 2011-12-20 13:13:03

**Hash launch:** 3308

**Date added:** 2011-12-20 13:13:04

**Log Entries:**

- iq2w3e

**Log Entries:**

- iq2w3e

**Log Entries:**

- iq2w3e
RDPdor Control Panel

### xTerm Control center v3.0 (Extended)

- **Main** | **Online hosts** | **All hosts** | **Update** | **Upload** | **Search** | **Key Logs** | **GAZ Sync** | **Service** | **Bot log** | **Access log** | **Debug logs** | **Users** |

- **Statistics**
  - Online: 132
  - Offline: 1144
  - Download: 22
  - Error: 47
  - Total: 1344

### Types

<table>
<thead>
<tr>
<th>Time</th>
<th>User</th>
<th>Last Log</th>
<th>User Action</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 min</td>
<td>Admin</td>
<td>9 min ago</td>
<td>Admin</td>
<td></td>
</tr>
<tr>
<td>5 sec</td>
<td></td>
<td>8 min ago</td>
<td>Admin</td>
<td></td>
</tr>
<tr>
<td>3 hrs</td>
<td>Admin</td>
<td>6 min ago</td>
<td>Admin</td>
<td></td>
</tr>
<tr>
<td>3 hrs</td>
<td>Admin</td>
<td>5 min ago</td>
<td>Admin</td>
<td></td>
</tr>
<tr>
<td>41 min</td>
<td>Admin</td>
<td>5 min ago</td>
<td>Admin</td>
<td></td>
</tr>
<tr>
<td>17 min</td>
<td>Anna</td>
<td>5 min ago</td>
<td>Anna</td>
<td></td>
</tr>
<tr>
<td>50 min</td>
<td>DDDDD</td>
<td>5 min ago</td>
<td>DDDDD</td>
<td></td>
</tr>
</tbody>
</table>
Results of the Investigation

- Joint investigation in close cooperation with the MVD of the Russian Federation, Sberbank and ESET;
- Results of the investigation is the detention of the criminal group (6 persons).
Conclusion

✓ Two of six active groups arrested;

✓ Remaining four groups are under investigation;

✓ Law enforcement officials are becoming more interested in such crimes;

✓ With proper support, at least three criminal groups can be neutralized within eight months;

✓ We expect a surge in theft, including from individuals, in June and July 2012.
Group-IB

Sergey Grudinov
Deputy CEO

+7 (495) 661-55-38
grudinov@group-ib.ru
www.group-ib.com