



Russian cybercrime Intelligence

|GROUP|IB|

Group-IB

→ ONE OF THE LEADING INTERNATIONAL COMPANIES DEALING WITH PREVENTION AND INVESTIGATION OF CYBER CRIME COMMITTED USING IT

Main activities:



1 → Monitoring and cyber threats prevention



2 → Investigation of cybercrime and theft committed using IT



3 → Computer forensic and malware research

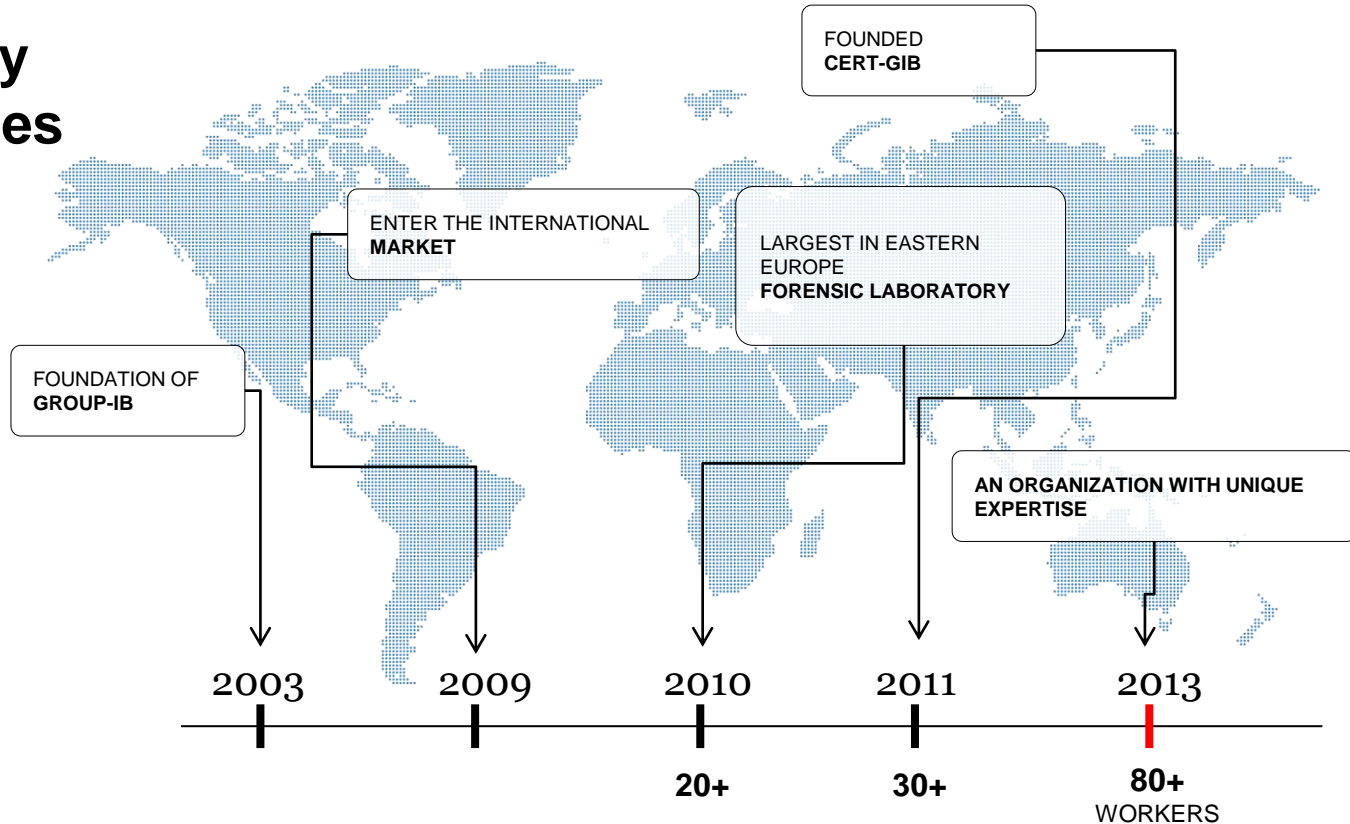


4 → Information security audit



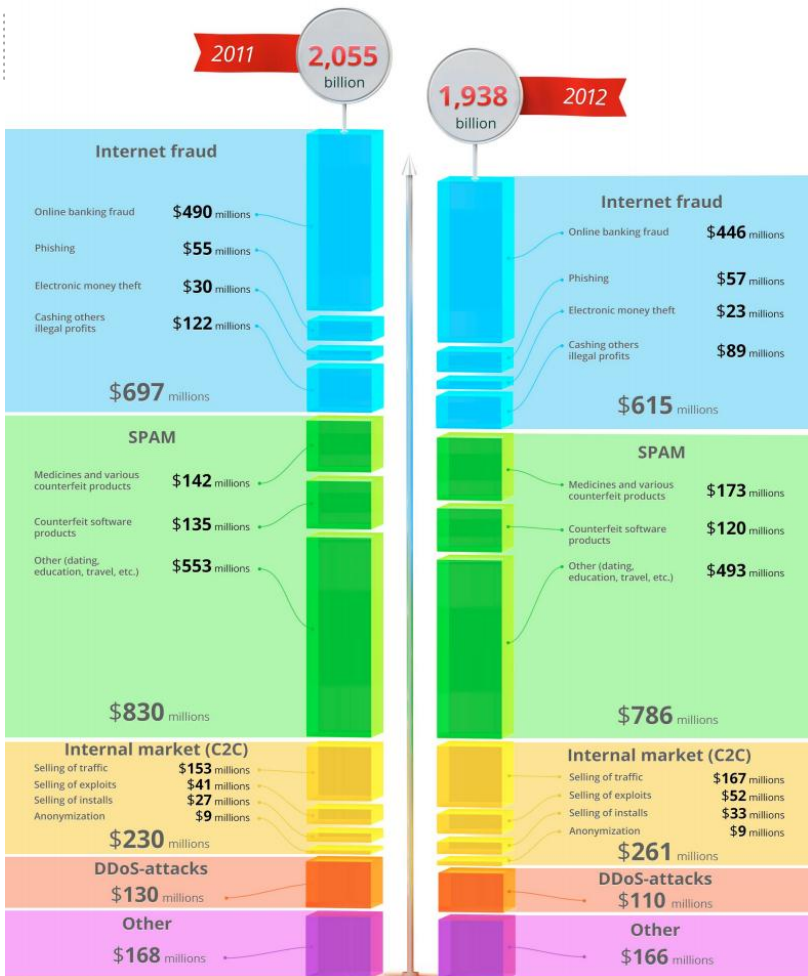
5 → Development of innovative information security products

Company Milestones

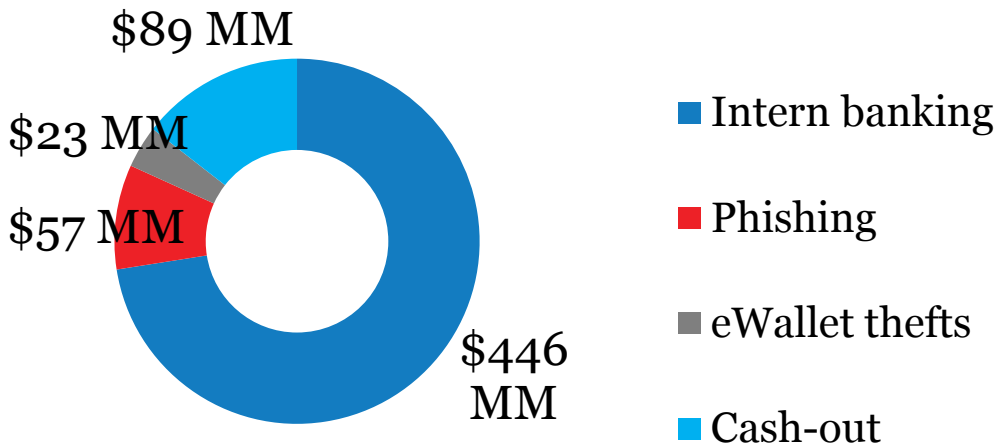


Trends

- *Internet-banking theft decrease*
- *Automatic payments (autoloads)*
- *Attacks on trading systems*
- *Attacks on POS-terminals*
- *Mobile threats*
- *Bank robbery*

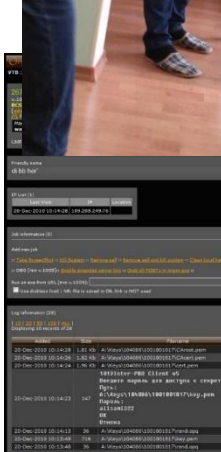
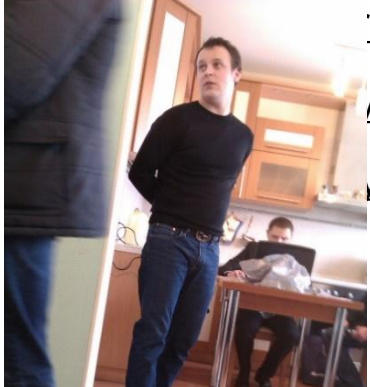


↓ **12%** Internet fraud



Internet-banking theft decrease

- *Successful cybercriminals arrests*
- *Interbank list of “money mules”*
- *Antifraud system implementation in banks*
- *Botnet data interception*
- *Modest newcomers*



Имя	Имя пользователя	Почта
Александр	alexander86@mail.ru	8060V
Александр	alexander86@mail.ru	s593
Орлов	orlov@k.ru	pt9n
Иванов	ivanov@yandex.ru	qwe05
Иванов	ivanov@yandex.ru	9804
Иванов	ivanov@yandex.ru	2560348
Иванов	ivanov@yandex.ru	Vik039
Иванов	ivanov@yandex.ru	P58
Иванов	ivanov@yandex.ru	19021989
Иванов	ivanov@yandex.ru	yn020
Иванов	ivanov@yandex.ru	KU25
Иванов	ivanov@yandex.ru	OVGLST.RU
Иванов	ivanov@yandex.ru	10018
Иванов	ivanov@yandex.ru	236@mail.ru
Иванов	ivanov@yandex.ru	h418
Иванов	ivanov@yandex.ru	8823
Иванов	ivanov@yandex.ru	malikseyaslich
Иванов	ivanov@yandex.ru	VolkovS
Иванов	ivanov@yandex.ru	8524
Иванов	ivanov@yandex.ru	andreyaslich
Иванов	ivanov@yandex.ru	029v0i
Иванов	ivanov@yandex.ru	11_5
Иванов	ivanov@yandex.ru	6@gmail.ru
Иванов	ivanov@yandex.ru	2389
Иванов	ivanov@yandex.ru	magdofowers.ru
Иванов	ivanov@yandex.ru	1296
Иванов	ivanov@yandex.ru	11@gmail.ru
Иванов	ivanov@yandex.ru	7211
Иванов	ivanov@yandex.ru	36@mail.ru
Иванов	ivanov@yandex.ru	864
Иванов	ivanov@yandex.ru	724
Иванов	ivanov@yandex.ru	1ca

Страна	Количество битов	Живых битов
Russia	1	0
New Zealand	9	0
Oman	2	0
Nepal	10	1
Philippines	15	0
Poland	12	1
Poland	203	12
Polishian Territory	5	0
Portugal	120	0
Qatar	3	0
Romania	101	3
Russia	1443642	64750
Ukraine	27	0
United States	4	0
Sydney	107	3
Singapore	5	1

Automatic payments

Portable Executable:

- *System infection*
- *Process injection*
- *CommandLine interception*

Java Agent:

- *Modifying java banking software on the fly*
- *Java banking software full data control*
- *Automatic creation of payment documents (Autoloads)*

Trends 2012-2013



837 banks in Russia:

- 650 000 companies
- 450 000 private persons

180 bank in Ukraine:

- 300 000 companies
- 145 000 private persons

Attack on Ibank2

- *Interception of login/password*
- *Screenshots creation*
- *Automatic payments*

Trends 2012-2013

Рабочие | Исполненные | Шаблоны

Документы: любые с . . . по . . . Обновить

N док. v2	Дата док. v1	Сумма	Получатель	Назначение платежа	Ст
168	13.02.2013	123 000.00	[REDACTED]	Налог на добавленную стоимост...	На
167	13.02.2013	1 496.00	[REDACTED]	Регистрационный номер в Упра...	На
166	13.02.2013	1 758.00	[REDACTED]	Регистрационный номер в Упра...	На
165	13.02.2013	4 688.00	[REDACTED]	Регистрационный номер в Упра...	На
164	13.02.2013	177.00	[REDACTED]	Взносы на обязательное социа...	На обработке
163	13.02.2013	849.00	[REDACTED]	Взносы на обязательное социа...	На обработке
162	13.02.2013	3 809.00	[REDACTED]	НДФЛ, НДС не облагается	На обработке
161	13.02.2013	403 560.00	[REDACTED]	Служба по связям: № 15 02 104	На обработке

Ваши счета:

Счет	БИК	Текущий остаток	Дебет за сегодня
[REDACTED]	[REDACTED]	2 079 703.85 RUR	

Последние сеансы работы (скрыть):

Дата и время	Владелец ключа ЭП	Информация
19.02.2013 16:49	[REDACTED] Группа подписи: 1	IP: [REDACTED] Регион: Russian Federation, Moscow City, Moscow

```
[+] save login data, login num: 1
protocol: file
[~] new ClientInfo
[+] LOGIN_DATA:
locale=русский
keystoreFile=W:\keys\rfi_keys2\Технологии\keys3
keystoreType=Ключ на диске
password=09041979
keys=Техно[REDACTED]3
protocol=file
```

← → offset 0 limit 50 total 306 order by ID order_dir ASC Show

ID	Бот	БИК	Номер	Баланс	Валюта	Получен	Обновлен	Клиент
1	292	044525976	40802810522000039174	483 481.01	RUR	2013-07-15 14:48:24	2013-07-16 15:54:45	ИП С
4	191	044525219	40702810600670000771	34 038.22	RUR	2013-07-15 14:50:06	2013-07-19 14:31:54	ООО
5	376	044525976	40702810222000004680	4 145 296.01	RUR	2013-07-15 14:50:25	2013-07-19 15:47:16	ЗАО *
12	321	046568941	40702810816000000425	75 324.04	RUR	2013-07-15 14:50:26	2013-07-15 14:50:26	Обще "Баро
13	276	044525976	40702810322000037418	3 931.53	RUR	2013-07-15 14:50:28	2013-07-19 08:46:42	ООО
16	276	044525976	40702810622000038816	1 802 339.57	RUR	2013-07-15 14:55:16	2013-07-19 17:02:43	ООО
19	127	044030881	40702810604040000072	447 181.66	RUR	2013-07-15 14:57:36	2013-07-15 18:07:01	ООО
24	148	048073855	40702810400010007006	381 142.87	RUR	2013-07-15 14:58:20	2013-07-17 08:56:02	ООО
25	304	048073855	40802810600100000464	962.31	RUR	2013-07-15 15:00:34	2013-07-15 15:02:48	ИП Ш
26	388	042748705	40702810700000073807	595 241.40	RUR	2013-07-15 15:01:21	2013-07-19 11:28:11	ООО
27	380	044525219	40702810100880000252	231 138.44	RUR	2013-07-15 15:03:40	2013-07-19 14:03:25	ООО
33	304	048073855	40802810400100000457	969.64	RUR	2013-07-15 15:05:18	2013-07-15 15:05:18	ИП Б
34	142	042282832	40702810100490003523	6 378.22	RUR	2013-07-15 15:05:21	2013-07-19 09:13:06	ООО
35	310	044583679	40702810400004665001	351.87	RUR	2013-07-15 15:13:55	2013-07-19 10:18:42	ООО
36	321	046568941	40702810016000000445	242 793.80	RUR	2013-07-15 15:14:56	2013-07-17 08:35:04	ООО
37	262	044525976	40802810900000003036	237 731.08	RUR	2013-07-15 15:16:29	2013-07-16 08:47:00	ИП Не
41	204	047003729	40802810300000002158	626 049.13	RUR	2013-07-15 15:16:49	2013-07-19 16:14:44	Каме
42	372	048073855	40702810500090000185	29 787.86	RUR	2013-07-15 15:20:04	2013-07-18 15:20:07	ООО
43	225	040349841	40702810022680000827	48 115.25	RUR	2013-07-15 15:20:53	2013-07-18 14:04:37	ООО
46	191	044525521	40702810401260017223	33 143.07	RUR	2013-07-15 15:27:21	2013-07-15 15:27:21	Обще "Горо
47	262	049205916	40701810500000000057	695 677.06	RUR	2013-07-15 15:30:09	2013-07-19 14:43:31	ООО
48	350	044525205	40702810900450000186	1 424 737.80	RUR	2013-07-15 15:31:11	2013-07-19 15:45:40	ООО

Online trading and stock brokerage

Серверное время: 16:28:14

[Главная](#)
Боты 10480 (+672 last 24h)
[ibank-граббер](#)
Банки
Акции
 Puty 19
 Western Union 0
 WebMoney 13
 quik 9
 mstsc 0

[Поиск](#)
[Демон](#)
[Настройки](#)

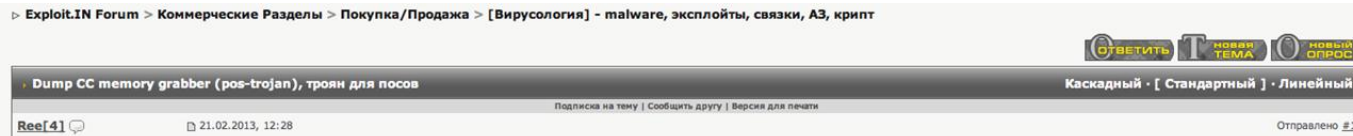
Акки > quik

#	ID	Дата	IP	Комментарий	Actions
1	microsofe27f22_70180af4_def01265	07:55 13.05.2013	RU 79.126.23.69		Подробнее (2) Комментарий Удалить
2	lhxku2pthm_ce092fa1_9d396e59	01:50 30.04.2013	RU 46.20.187.148		Подробнее (2) Комментарий Удалить
3	0u1pWxYs_a2dd4de9_6iffafa21	01:42 30.04.2013	RU 212.5.70.172		Подробнее (2) Комментарий Удалить
4	darja_2a403df8_2738ff2b	09:12 30.04.2013	RU 94.181.32.196		Подробнее (1) Комментарий Удалить
5	24608bf7535253_b969fe69_47fbc1e1	07:49 30.04.2013	RU 95.26.216.5		Подробнее (5) Комментарий Удалить
6	djel4a734e0567_c53cbb4_9172fedb	04:25 29.04.2013	RU 109.172.59.39		Подробнее (6) Комментарий Удалить
7	microsoftf11e70_ad9b76bd_f481be40	04:57 26.04.2013	RU 176.192.175.232		Подробнее (3) Комментарий Удалить
8	microsoft489b6_96bec1ef_31d9c78	02:44 26.04.2013	RU 217.66.157.40		Подробнее (13) Комментарий Удалить
9	Artem_12d2967d_dfd3330	11:17 15.04.2013	RU 213.87.240.251		Подробнее (9) Комментарий Удалить

6	user-56264ef3ea_fc2254b5_32eb549b	17:17 07.12.2012	-		Подробнее Комментарий Удалить
7	040ded60da6d468_8bba797d_20eb07da	13:58 05.12.2012	-		Подробнее Комментарий Удалить
8	hays_9a046963_29d899a2	21:15 03.12.2012	-		Подробнее Комментарий Удалить

Attacks on POS-terminals

- December, 2012 «**Dexter**», Seculert
- March, 2013 «**vSkimmer**», McAfee Labs
- March, 2013 «**Dump Memory Grabber**» Group-IB



This trojan is written on pure C++ without any additional libraries, for grabbing of dumps of CC from RAM memory of all processes

Works on any version of OS Windows including x64. Very stable.

Uses mmon.exe to scan memory.

Very silent on the host, add itself to Autorun, timeout of auto start is 3 hours (can be changed)

Re-launch grabbing of dumps. Log sends to the gate via FTP. Every log has date of sending, like 1.09.56-16.02.2013.txt

Can be changed to send to email


Attacks on POS-terminals

Простые POS терминалы / FAKE POS

Сообщений в теме: 12

OFFLINE

Cashout D+P service / Fake POS

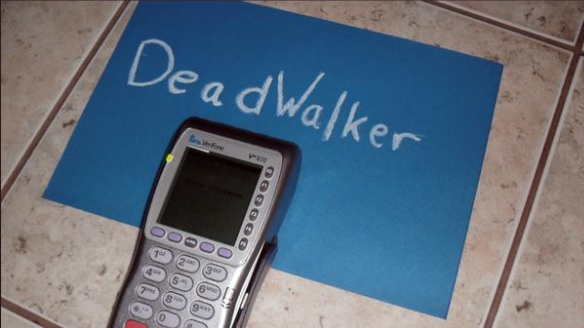


Save TRACK1 + TRACK2 + PIN in internal memory + has functionality to send data via SMS on your number. Uses GSM SIM.
Languages: RUS\ENG
Available to save your data + logo during check printing.

Seller
Регистрация: 05 Ноя 2012
Сообщений: 131
Депозит: 2100\$

3 000\$ - покупка.
или
2 000\$ + 20% от Вашего материала мои.

Видео работы девайса: <http://www.sendspace.com/file/wuujd>



Attacks on mobile platforms

- *Android trojans*
- *SMS on premium numbers*
- *Evolution to the banking theft in 2013*

Comands					
Name	Number	Mesage	Issued	Complete	
7515	7515	5964hib	56	17	Del
					Save

Comand & Bots					
Group	Comand				
telefon	7515(56,17)	<input checked="" type="checkbox"/> Zamenat	<input type="checkbox"/> Obnulat	<input checked="" type="checkbox"/> Offline	Go

Bots in process					
					Online
Imei	Group	Comment	Command Name		
					Offline
Imei	Group	Comment	Command Name		
353426056492465	group1		7515	Cancel	
351565050633624	group1		7515	Cancel	
358841041829958	group1		7515	Cancel	
357952004383536	group1		7515	Cancel	
355019120360442	group1		7515	Cancel	
353139050697357	group1		7515	Cancel	
353922054293392	group1		7515	Cancel	
357446041884531	group1		7515	Cancel	
355769041282865	group1		7515	Cancel	
354912052650908	group1		7515	Cancel	
356525041728524	group1		7515	Cancel	
352176011593789	group1		7515	Cancel	

Imei(3)
Sms(C)

Imei(3)
Sms(C)

Imei(3)
Sms(C)

Imei(3)
Sms(C)

Imei(3)
Sms(C)

Imei(3)
Sms(C)

Attacks on mobile platforms

- Development
- Start of inf
- Detection
- Remove from

		Обновить		Показать всех ботов		Показать онлайн ботов		UID: <input type="text"/>		Искать бота	
		-1000 -100 -10 -5 -1 +1 +5 +10 +100 +1000									
	bot_uid	phone_number	sms	auth_pin	reg_date	last_date					
Q	0cabb24d15a814562fd56142eba7a9c		0	10799	15.12.12 [13:25:42]	15.12.12 [13:25:42]					
Q	a7be38b5b253d2b46e6f2c82f5862481		0	10798	15.12.12 [10:15:32]	15.12.12 [10:15:32]					
Q	5dc4a91a5e5b404fa2c4223cb649b20		0	10797	14.12.12 [08:46:23]	14.12.12 [08:46:23]					
Q	edde2a296cf9f564bd699a4900f340ae		0	10796	14.12.12 [01:40:54]	14.12.12 [01:40:54]					
Q	2bf1deb9614f273527ca06274460fa73		0	10795	13.12.12 [19:15:37]	13.12.12 [19:15:37]					
Q	8838e994a928f374e37a96f93e833736		0	10794	13.12.12 [15:37:34]	13.12.12 [15:37:34]					
Q	99e91180f6b02d904a6794c93bdc454d		0	10793	13.12.12 [10:46:30]	13.12.12 [10:46:30]					
Q	19c58b5b73bd11f989a8bc92d8e8c488		0	10792	13.12.12 [06:37:01]	13.12.12 [06:37:01]					
		8 [REDACTED] 8	0	10791	12.12.12 [21:10:30]	12.12.12 [22:19:39]					
Q	b538b10592b541561c688315077621c9		0	10790	12.12.12 [20:26:44]	12.12.12 [20:26:44]					
		8 [REDACTED] 6	5	10789	12.12.12 [19:19:57]	13.12.12 [13:43:17]					

Отправитель: 1234	Дата сообщения: 13-12-12 [08:26:24]
MTC. Настройки MTS Internet и MTS MMS в следующем сообщении. Сохраните их //Мобильное ТВ - более 100 каналов, всего 8 рубл/день, трафик бесплатно! Подключай *999#	
Отправитель: 900	Дата сообщения: 13-12-12 [08:09:53]
VISA3902: 13.12.12 09:09 оплата услуг на сумму 100.00 руб. МОБИКОМ-КА/КАЗ (92 [REDACTED] 5) выполнена успешно. Доступно: 4155.57 руб. ПЕРЕВОД 89XX1234567 500 – перевести 500 руб. на карту Сбербанка, зная только телефон получателя.	
Отправитель: 900	Дата сообщения: 13-12-12 [08:08:29]
Для оплаты с карты VISA3902 телефона MegafonKV 92 [REDACTED] 5 на 100 руб. отправьте код #5969 на номер 900.	
Отправитель: 900	Дата сообщения: 13-12-12 [08:06:34]
VISA3902: 13.12.12 09:06 оплата услуг на сумму 200.00 руб. МОБИКОМ-КА/КАЗ (9287336055) выполнена успешно. Доступно: 4255.57 руб. ПЕРЕВОД 89 [REDACTED] 7 500 – перевести 500 руб. на карту Сбербанка, зная только телефон получателя.	
Отправитель: 900	Дата сообщения: 13-12-12 [08:05:47]
Для оплаты с карты VISA3902 телефона MegafonKV 9 [REDACTED] 5 на 200 руб. отправьте код #6170 на номер 900.	


10:53 AM

Phone number verification

Введите номер телефона:

8

Do authorization



СБЕРБАНК

Всегда рядом

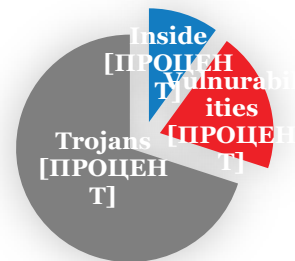
Why rob banks, not customers?

- *Facts of successful compromise of banks*
- *Websites and Web resources of banks successfully "hacked"*
- *Criminal have necessary experience and skills*
- *Banks are not ready to withstand against such threats*
- *Steal 100 million at a time is easier, rather than steal a hundred times by 1 million*

Types of robberies

- *Robbery as a result of insider*
- *Robbery as a result of vulnerabilities exploitation in the banking systems*
- *Robbery as a result of penetration of the banking network with the use of Trojans*

Sources of robberies



■ Инсайд ■ Уязвимость в банковском ПО ■ Трояны

The use of Trojans

1 The process of compromise

- *Infecting computer in bank network*
- *Installing Trojan RDPdoor*
- *Installing legal remote management tools, Ammy Admin, TeamViewer*
- *Compromising the domain and mail server*
- *Search for servers with banking services*
- *Removing Malware*
- *Preparing to cash out*

2 How to Rob

- *Selecting rich clients*
- *Generate new bank digital signature*
- *Reset passwords to internet-banking*
- *Transfer money*

The screenshot shows a Windows XP desktop with a banking application window titled "ПК АРМ КБР. Оператор [Комбинированный]". The window has a menu bar (Файл, ЭЗД, ЭСЗД, Превка, Операции, Вид, Помощь) and a toolbar with icons for Exit, ESD, ESDZ, Change, Control, Print, Sign, Protocol, Monitoring ESD, and Monitoring ES. Below the toolbar is a navigation bar with "Введенные/Полученные из АС клиента" and "Принятые из ЦОИ".

The main area contains a table with the following data:

Иден.	Состояние	Имя польз.	Имя файла	Время помещения в хранилище	Тип	УИИС ЭД	Дата ЭД	Номер ЭД	Сумма ЭД	Отправитель	Пр
1	Получен ответ	vetlugina	b4N73803.7PT	09.12.10	ED210	5773803000	23.04.2013	10001		Ручной ввод	П
2	Отрицательный результат	vetlugina	b4N73803.7PV	10.02.03	ED101	5773803000	23.04.2013	10003	12000000-00	Ручной ввод	П
3	Передан в транспортную систему	vetlugina	b4N73803.7PW	10.26.27	ED101	5773803000	23.04.2013	10004	12000000-00	Ручной ввод	П

Below the table is a toolbar with icons for file operations and a status bar showing "1" and "3".

The bottom part of the window shows a file explorer view for "C:\uarm2\Explor" dated "23.04.2013". It displays a list of files and folders, including "Назначение платежа" and "ПОДПИСИ". The "ПОДПИСИ" folder is expanded, showing a list of log entries:

- Начало обработки файла C:\uarm2\Explor\b4N73803.7PW
- (23.04.2013 10:26:39.75) [USER293] [vet.lugina] [Формирование КА]
- Выходной файл b4N73803.7PV помещен в каталог C:\uarm2\expl\ctc
- (23.04.2013 10:26:39.77) [USER293] [vet.lugina] [Формирование КА]
- Завершение обработки файла b4N73803.7PW
- (23.04.2013 10:26:39.85) [USER293] [vet.lugina] [Отправка сообщений]
- Начало обработки файла C:\uarm2\Expl\ctc\b4N73803.7PW
- (23.04.2013 10:26:39.96) [USER293] [vet.lugina] [Отправка сообщений]
- Выходной файл b4N73803.7PW помещен в каталог C:\uarm2\Expl\ctc
- (23.04.2013 10:26:39.96) [USER293] [vet.lugina] [Отправка сообщений]
- Завершение обработки файла b4N73803.7PW

The status bar at the bottom of the window shows "2" errors, "0" warnings, "57" messages, "1" action, and "60" total items.

The taskbar at the bottom of the desktop shows the Start button, several application icons, and the system tray with the date "10:28".

Банк - [Имя пользователя] - Сервер ДБО BS-Client v.3

Файлы Исполнение БЭЗ Справочники Администрирование Сервис Подпись

Интернет-пользователи

ID	Login	Ф.И.О.	Состояние	Ограничен	Язык	Подразделение
57	000		активен с 22.01.2013	1	RUSSIAN	Я ФИЛИ
58	000		активен с 22.01.2013	1	RUSSIAN	Я ФИЛИ
60	000		блокирован	1	RUSSIAN	Я ФИЛИ
61	ИП.З	овин	активен с 25.01.2013	1	RUSSIAN	Я ФИЛИ
62	000	и Михайловск"	активен с 25.01.2013	1	RUSSIAN	Я ФИЛИ
63	000		активен с 31.01.2013	1	RUSSIAN	Я ФИЛИ
64	ИП.С	евна	активен с 05.02.2013	1	RUSSIAN	Я ФИЛИ
65	ИП.С	ьвен	активен с 05.02.2013	1	RUSSIAN	Я ФИЛИ
69	ИП.П	льевич	активен с 08.02.2013	1	RUSSIAN	Я ФИЛИ
66	000		активен с 08.02.2013	1	RUSSIAN	Я ФИЛИ
67	000		активен с 08.02.2013	1	RUSSIAN	Я ФИЛИ
68	0A0	льние культуры"	активен с 13.02.2013	1	RUSSIAN	Я ФИЛИ
70	ИП.З	ьирович	активен с 19.02.2013	1	RUSSIAN	Я ФИЛИ
71	000	ности"	активен с 19.02.2013	1	RUSSIAN	Я ФИЛИ
93	000		активен с 28.02.2013	1	RUSSIAN	Я ФИЛИ
94	000		активен с 28.02.2013	1	RUSSIAN	Я ФИЛИ
72	ИП.Н	ьирович	активен с 01.03.2013	1	RUSSIAN	Я ФИЛИ
74	ИП.С	данович	активен с 22.04.2013	1	RUSSIAN	Я ФИЛИ
75	000		активен с 06.03.2013	1	RUSSIAN	Я ФИЛИ
73	ИП.Я	ьирова	активен с 06.03.2013	1	RUSSIAN	Я ФИЛИ
95	000		активен с 07.03.2013	1	RUSSIAN	Я ФИЛИ
96	000		активен с 11.03.2013	1	RUSSIAN	Я ФИЛИ
76	000		активен с 18.04.2013	1	RUSSIAN	Я ФИЛИ
77	ИП.Н	ич	активен с 15.03.2013	1	RUSSIAN	Я ФИЛИ
78	ИП.Е	инович	активен с 25.03.2013	1	RUSSIAN	Я ФИЛИ
97	000		активен с 05.04.2013	1	RUSSIAN	Я ФИЛИ
98	ИП.Г	ьвич	активен с 05.04.2013	1	RUSSIAN	Я ФИЛИ
79	000	"	активен с 09.04.2013	1	RUSSIAN	Я ФИЛИ
80	ИП.И	ьвич	активен с 09.04.2013	1	RUSSIAN	Я ФИЛИ
81	ИП.С	ович	активен с 09.04.2013	1	RUSSIAN	Я ФИЛИ
82	000		активен с 10.04.2013	1	RUSSIAN	Я ФИЛИ
99	ИП.Н	ович	активен с 12.04.2013	1	RUSSIAN	Я ФИЛИ
00	000		активен с 16.04.2013	1	RUSSIAN	Я ФИЛИ
83	ИП.З	ьвич	активен с 29.04.2013	1	RUSSIAN	Я ФИЛИ
84	000		активен с 22.04.2013	1	RUSSIAN	Я ФИЛИ
85	000		активен с 22.04.2013	1	RUSSIAN	Я ФИЛИ
81	ИП.Е		активен с 22.04.2013	1	RUSSIAN	Я ФИЛИ
82	000	льней Рязок"	активен с 25.04.2013	1	RUSSIAN	Я ФИЛИ
86	ИП.С	ьевич	активен с 29.04.2013	1	RUSSIAN	Я ФИЛИ
87	ИП.Н	ьевич	активен с 30.04.2013	1	RUSSIAN	Я ФИЛИ
88	000		блокирован	1	RUSSIAN	Я ФИЛИ
03	000		активен с 14.05.2013	1	RUSSIAN	Я ФИЛИ

Ok Отмена

Пуск | C:\Program Files\Total Commander | Отправлен... | RE: заявка... | Z Radwin... | C:\WINDOWS... | 10:41 вторник, 14.05.2013

Боты

Очистить фильтр

Online only

Online time min

Bot ID

Ammyy ID

Diversion

firstdatetime

Edition

Comment

Фильтровать

Удалить выбранные Экспорт keylog Экспорт процессов Экспорт линков

log	Bot ID	Ammyy ID	HDD serial	Bot IP	GEO	Last Date	First Date	DLL Version	Win User
<input type="checkbox"/>	7337	0	813944109	87.245.155.90/ 10.0.11.117	RU	2013-07-26 14:36:38	2013-03-15 14:43:31	5.0.1	user1 USER P/ Администр DC
<input type="checkbox"/>	7445	19[REDACTED]95	1621506197	31.23.46.17/ 192.168.0.57	RU	2013-07-26 16:27:55	2013-05-17 11:19:09	5.0.3	Admin USER PASSW PASS:
<input type="checkbox"/>	7448	19[REDACTED]60	2023860611	178.207.136.5/ 192.168.0.6	RU	2013-05-20 14:14:32	2013-05-17 15:29:36	5.0.3	User2
<input type="checkbox"/>	7593	0	2[REDACTED]58	77.[REDACTED].234/ 192.168.4.181	RU	2013-07-23 16:56:54			
<input type="checkbox"/>	7594	3[REDACTED]	37[REDACTED]92	[REDACTED] 192.168.0.3	RU	2013-07-26 15:42:35	2013-07-18 15:29:21	5.0.3	Администратор
<input type="checkbox"/>	7596	221[REDACTED]44	384[REDACTED]72	[REDACTED] 192.168.6.4	RU	2013-07-26 09:11:29			
<input type="checkbox"/>	7597	221[REDACTED]58	1171[REDACTED]31	217.[REDACTED].129/ 192.168.24.74	RU	2013-07-26 16:59:28			
<input type="checkbox"/>	7511	19[REDACTED]81	1618148822	31.129.2.198/ 192.168.2.21	RU	2013-07-22 14:17:59	2013-06-24 11:06:23	5.0.3	Admin
<input type="checkbox"/>	7539	2[REDACTED]60	2827292861	85.21.122.30/ 192.168.0.132	RU	2013-07-26 15:46:38	2013-06-25 11:19:33	5.0.3	PanovaJA
<input type="checkbox"/>	7547	2[REDACTED]74	2766827362	217.15.151.229/ 192.168.30.15	RU	2013-07-26 16:07:38	2013-06-27 09:17:25	5.0.3	admin
<input type="checkbox"/>	7549	212[REDACTED]62	1812530106	85.237.43.156/ 192.168.20.103	RU	2013-06-28 12:19:53	2013-06-27 10:18:01	5.0.3	Admin

```
inetnum: 77.108.100.232 - 77.108.100.239
netname: COMCOR-AKB-ZOLOSTBANK
descr: Network for AKB "ZOLOSTBANK"
country: RU
admin-c: MKV16-RIPE
tech-c: MKV16-RIPE
status: ASSIGNED PA
mnt-by: AS8732-MNT
source: RIPE # Filtered
```

2013-07-18 15:29:21 5.0.3 Администратор

```
inetnum: 217.168.244.128 - 217.168.244.135
netname: VOCBANK-NET
descr: ZAO 'VOCBANK' network
country: RU
admin-c: ABS24-RIPE
tech-c: ABS24-RIPE
status: ASSIGNED PA
mnt-by: ENIN-MNT
source: RIPE # Filtered
```

Экспорт таблицы ботов

Client O	Client	IP	OS	Arch	Job	Time
	[REDACTED]VA		Windows XP	x86	IdleJob	2013-07-26 17:53:50
	GLAVBUCH		Windows XP	x86	IdleJob	2013-07-26 17:53:50
	PC0325		Windows XP	x86	IdleJob	2013-07-26 18:53:50
	[REDACTED]VA		Windows XP	x86	IdleJob	2013-07-26 18:53:50
К стоит нилко						
BSS L						



+7 (495) 984-33-64



www.group-ib.ru



info@group-ib.ru



facebook.com/group-ib



twitter.com/group-ib