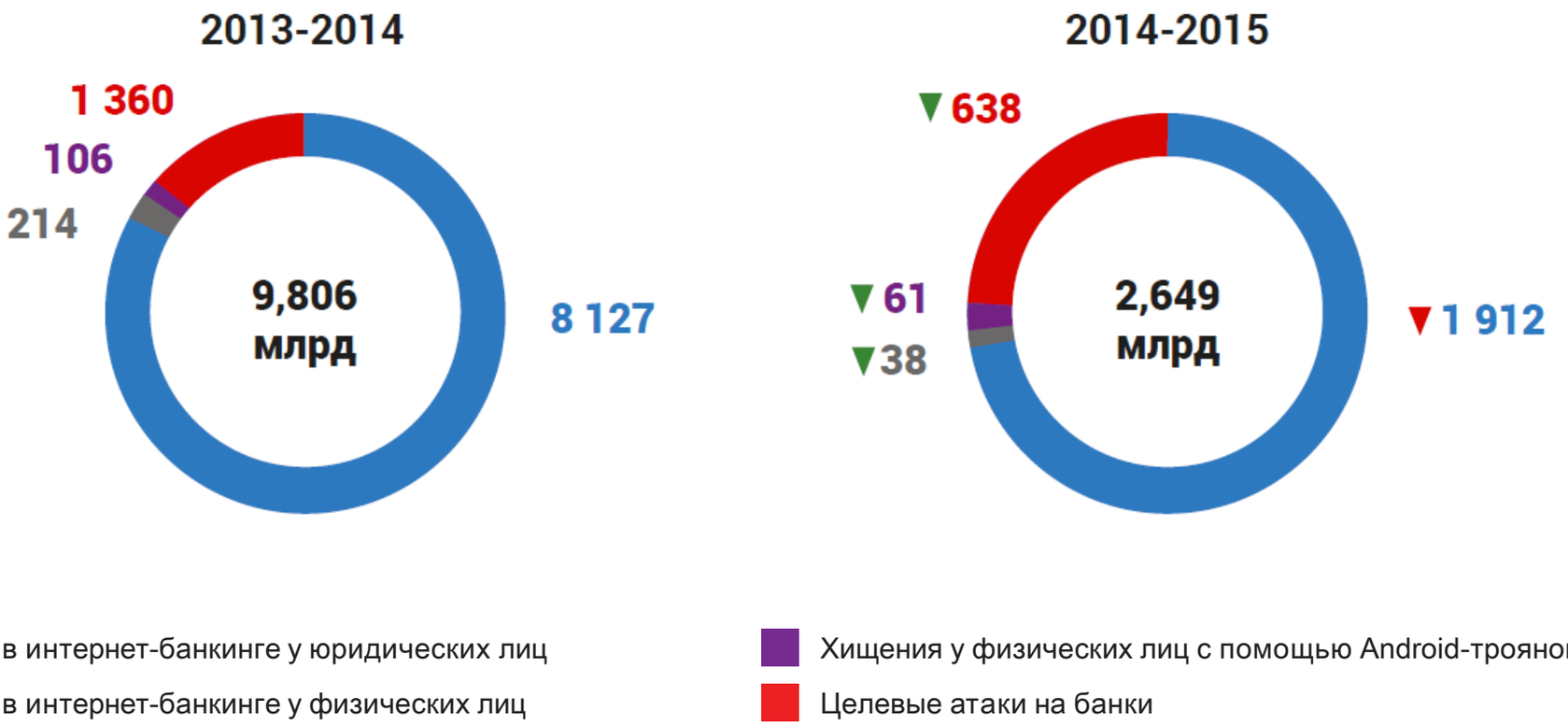
Тенденции развития преступности в области высоких технологий 2015

GROUP IB

GLOBAL CYBER SECURITY COMPANY

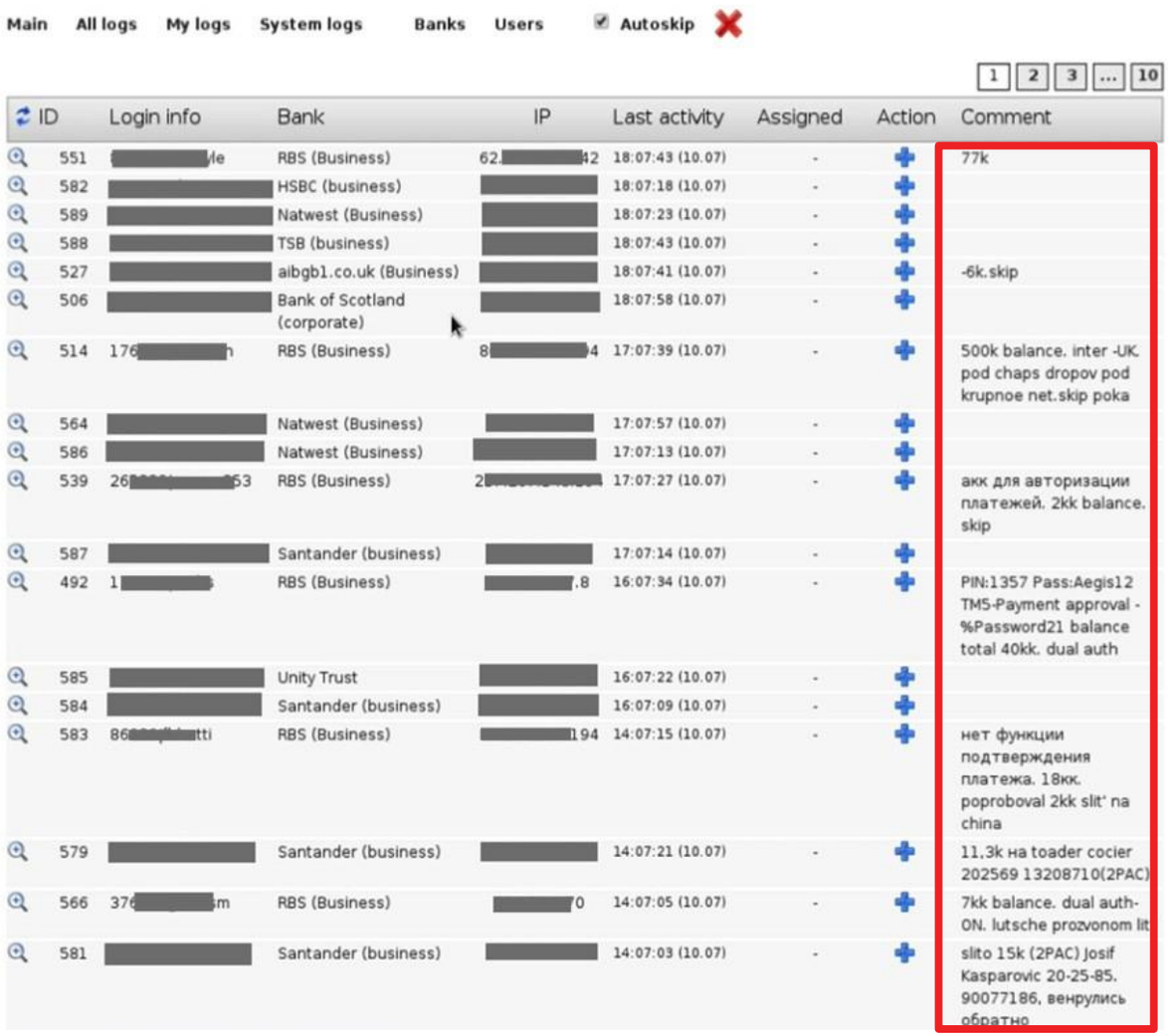
ТРЕНД №1:
СНИЖЕНИЕ УЩЕРБА ПРИ РОСТЕ КОЛИЧЕСТВА АТАК

Оценка рынка высокотехнологичных преступлений, тренд (млн руб.)



ТРЕНД №2
ПРОФЕССИОНАЛЫ УХОДЯТ С РЫНКА РОССИИ

- Один банк
- 13 клиентов
- 120 миллионов фунтов баланса



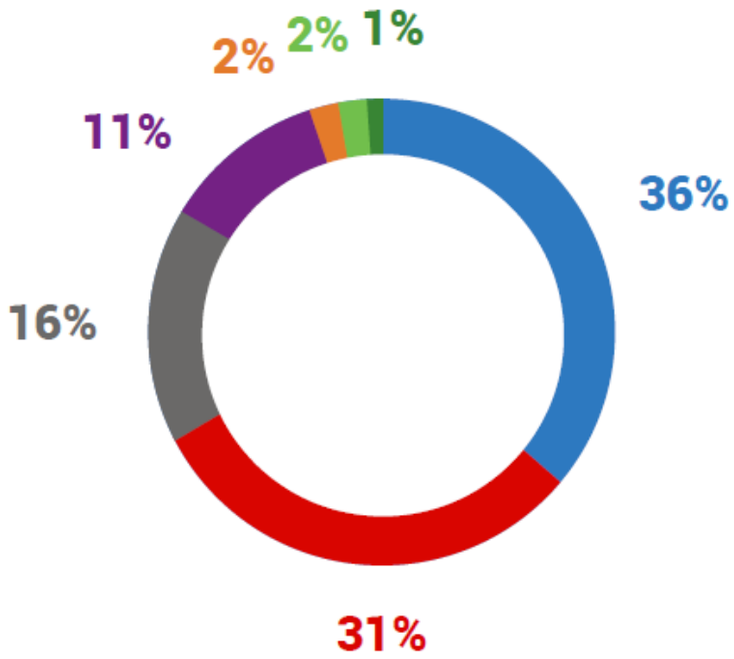
ТРЕНД №2
ПРОФЕССИОНАЛЫ УХОДЯТ С РЫНКА РОССИИ

Рост числа преступных групп: вместо 3х старых мы получаем 6 новых групп
Новички приносят старые методы хищений - удаленное управление

Группы, работающие по компаниям:

- ~~Shiz~~
- ~~Ranbyus~~
- ~~Infinity~~
- Lurk
- Cork
- Kontur (Buhtrap) NEW
- Toplel NEW
- Uni_chthonic NEW
- Prosecutor NEW
- Kronos_Nalog NEW
- Yebot NEW

Инциденты по группам



ТРЕНД №3
ПЕРЕОРИЕНТАЦИЯ РУССКОГОВОРЯЩИХ ХАКЕРОВ НА ЗАПАД

Из-за девальвации рубля хакерам стало выгоднее атаковать клиентов иностранных банков

Самые опасные банковские трояны для Запада написаны или управляются русскоговорящими хакерами

Резкий рост количества троянов: за III квартал 2015 сразу три новых банковских трояна

- ***Shifu***
- ***Corebot***
- ***Sphinx***

Самые популярные трояны для атак на клиентов европейских и американских банков	Количество групп
Dyre (Dyreza)	1
Dridex (Bugat, Feodo, Cridex)	1
Qadars	1
Emotet	1
Vawtrak (Neverquest, Papras)	4
ISFB (Ursnif)	3
Kronos	2
MMBB (Money Maker Bank Bot)	2
Tinba (Zusy)	>8
Zeus 2.0.8.9	>11
Citadel	>17
KINS (ZeusVM)	>18

ТРЕНД №4
КАРДИНАЛЬНАЯ СМЕНА МЕТОДА АТАК НА ФИЗИЧЕСКИЕ ЛИЦА
РЕЗКИЙ РОСТ МОБИЛЬНЫХ УГРОЗ

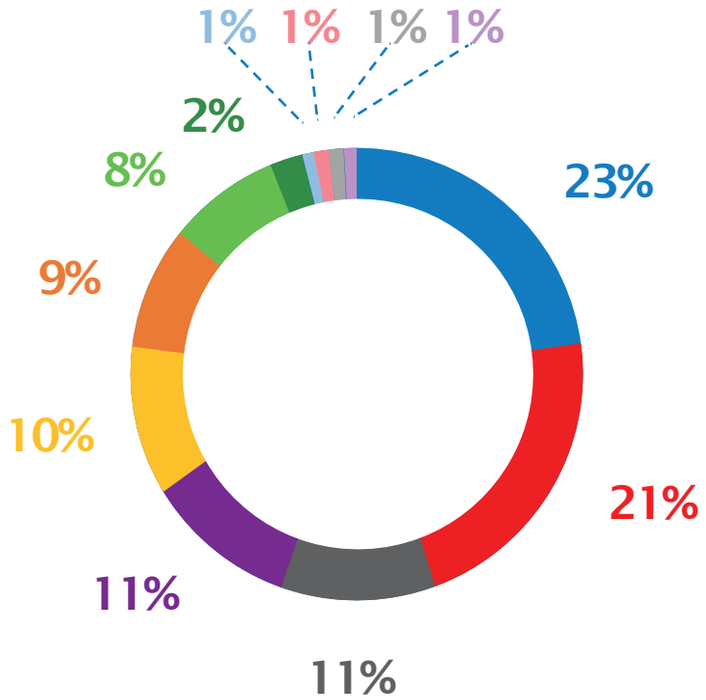
Группы, работающие по физическим лицам через Web-банкинг

- ~~PhishEye~~
- ~~Infinity~~ Proxy

Группы, работающие по физическим лицам через мобильный клиент-банк

- ~~Reich~~
- ~~Waplook~~
- Ada
- March
- Greff
- Sizeprofit NEW
- Cron NEW
- Group 404 NEW
- Ada2 NEW
- ApiMaps NEW
- Tark NEW
- Xruss NEW
- MobiApps NEW
- Mikorta NEW
- Webmobil NEW

Инциденты по мобильным группам



Количество преступных групп, работающих с мобильными троянами, увеличилось на 200% и продолжает расти

ТРЕНД №5
УСИЛЕНИЕ ИНТЕРЕСА К ТОРГОВЫМ / БРОКЕРСКИМ СИСТЕМАМ

Группа Corkow

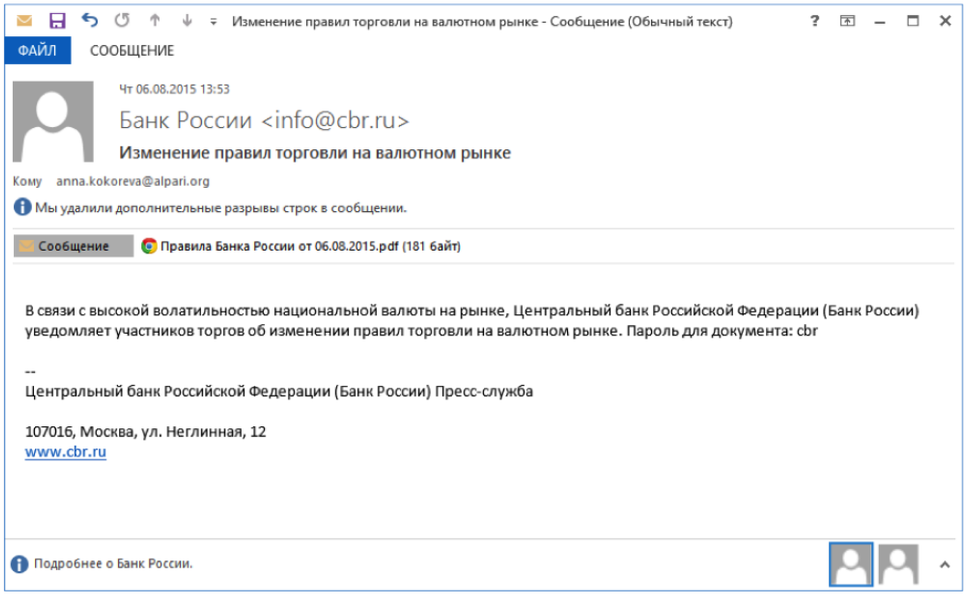
- Специальный троян с модулями для брокерских систем
- Первая атака в России в феврале 2015
- Были спровоцированы 10-рублевые скачки курса доллара
- Атака длилась всего 14 минут
- Подготовка 5 месяцев
- **Ущерб около 300 миллионов рублей**

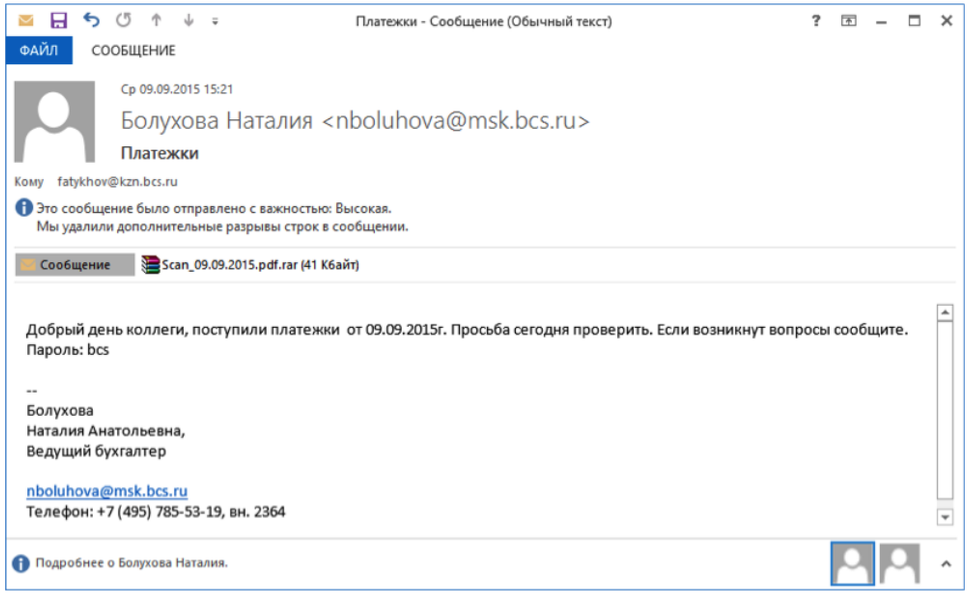
ТРЕНД №5
УСИЛЕНИЕ ИНТЕРЕСА К ТОРГОВЫМ/БРОКЕРСКИМ СИСТЕМАМ

Группа Anunak

Примеры атак на:

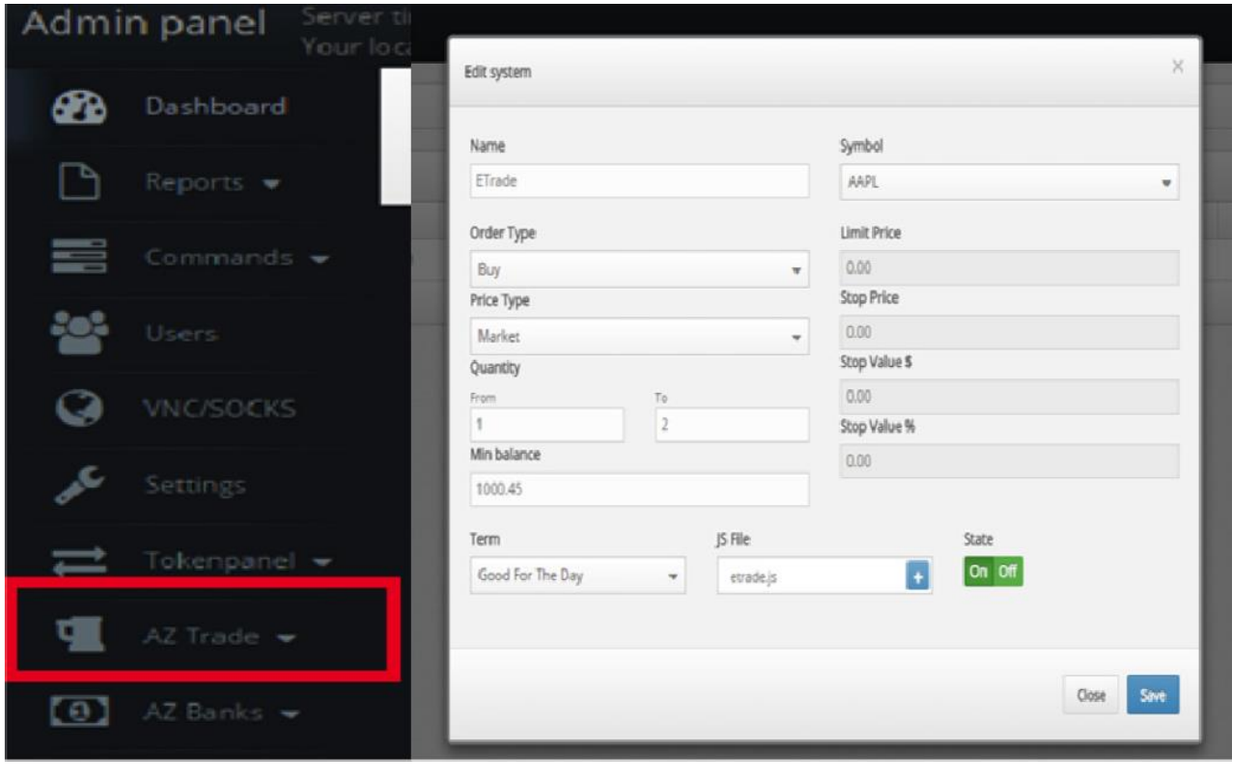
- брокера ФГ БКС
- форекс-брокер Alparic





Минимум 5 групп собирают данные о логинах торговых систем.
Есть модули для автоматического хищения.

Троян	Цель
Dyre	invest.etrade.com.au
Dyre	subastas.scotiainlatrade.com
KINS	dab-bank.com
Zeus	*.etrade.com
ISFB	wintrade-international.com.au



ТРЕНД №6
СМЕНА ПРИОРИТЕТОВ

- Вначале атаковали только клиентов банков
- Потом начали атаковать сами банки
- Позже начали атаковать брокеров
- Теперь под атакой и расчетные системыс

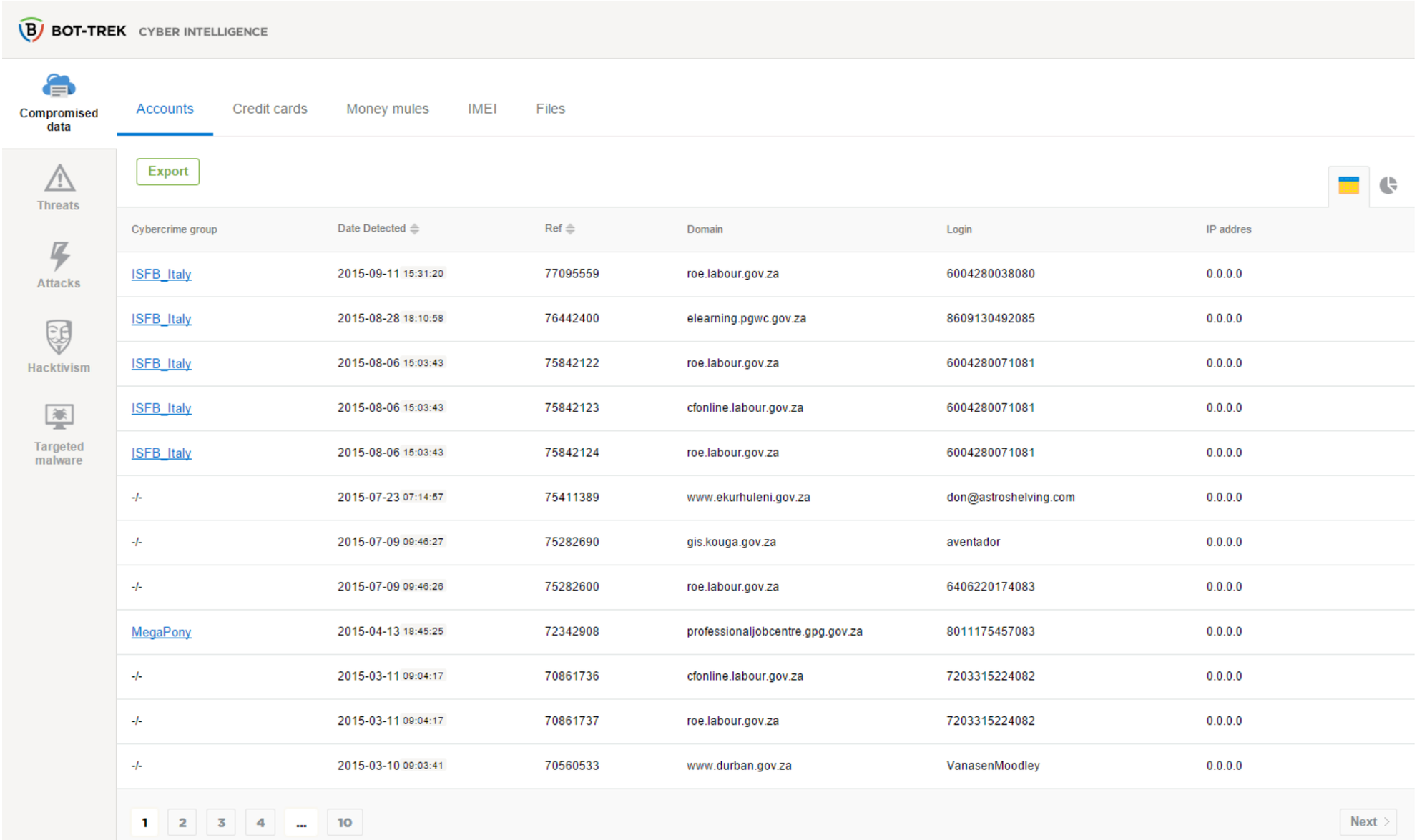
но и отклиентов не отказались...

и отбанков не отказались...

и отброкеров не отказались.

BOT-TREK INTELLIGENCE

Cyber Intelligence subscription



Cybercrime group	Date Detected	Ref	Domain	Login	IP addres
ISFB_Italy	2015-09-11 15:31:20	77095559	roe.labour.gov.za	6004280038080	0.0.0.0
ISFB_Italy	2015-08-28 18:10:58	76442400	elearning.pgwc.gov.za	8609130492085	0.0.0.0
ISFB_Italy	2015-08-06 15:03:43	75842122	roe.labour.gov.za	6004280071081	0.0.0.0
ISFB_Italy	2015-08-06 15:03:43	75842123	cfonline.labour.gov.za	6004280071081	0.0.0.0
ISFB_Italy	2015-08-06 15:03:43	75842124	roe.labour.gov.za	6004280071081	0.0.0.0
-/-	2015-07-23 07:14:57	75411389	www.ekurhuleni.gov.za	don@astroshelving.com	0.0.0.0
-/-	2015-07-09 09:46:27	75282690	gis.kouga.gov.za	aventador	0.0.0.0
-/-	2015-07-09 09:46:26	75282600	roe.labour.gov.za	6406220174083	0.0.0.0
MegaPony	2015-04-13 18:45:25	72342908	professionaljobcentre.gpg.gov.za	8011175457083	0.0.0.0
-/-	2015-03-11 09:04:17	70861736	cfonline.labour.gov.za	7203315224082	0.0.0.0
-/-	2015-03-11 09:04:17	70861737	roe.labour.gov.za	7203315224082	0.0.0.0
-/-	2015-03-10 09:03:41	70560533	www.durban.gov.za	VanasenMoodley	0.0.0.0

BOT-TREK THREAT DETECTION SERVICE

Detects threats within your corporate network

TDS

BOT-TREK SECURE BANK

Innovative protection for online payments

ПРОГНОЗЫ на 2016 год

- Атаки на клиентов банков – физических лиц с помощью троянов для персональных компьютеров прекратятся.
- Количество инцидентов и суммы похищаемых средств увеличатся за счет перехвата на Android-устройствах данных банковских карт, логинов и паролей для интернет-банкинга.
- Вырастет количество инцидентов с фишингом в отношении клиентов банков в результате появления новых преступных групп и автоматизации процесса хищения денежных средств.
- У юридических лиц увеличится количество инцидентов с программами, шифрующими данные для последующего вымогания денег за их расшифровку («криптолокерами»).
- Эффективность троянов, позволяющих переводить деньги с банковских счетов посредством подмены реквизитов («автозалива»), для юридических лиц будет снижена за счет внедрения новых систем защиты крупными банками, а злоумышленники могут переключить свое внимание на хищения с удаленным доступом.
- Количество инцидентов с POS-терминалами продолжит расти, поскольку количество программ для этих целей постоянно растет. Часть таких программ находится в открытом доступе.
- Количество целевых атак продолжит расти за счет новых игроков, но их эффективность в количественном показателе останется невысокой.

GROUP IB

GLOBAL CYBER SECURITY COMPANY

+7 (495) 984 33 64

www.group-ib.ru

info@group-ib.ru

facebook.com/groupib

youtube.com/groupib

twitter.com/groupib

linkedin.com/company/group-ib