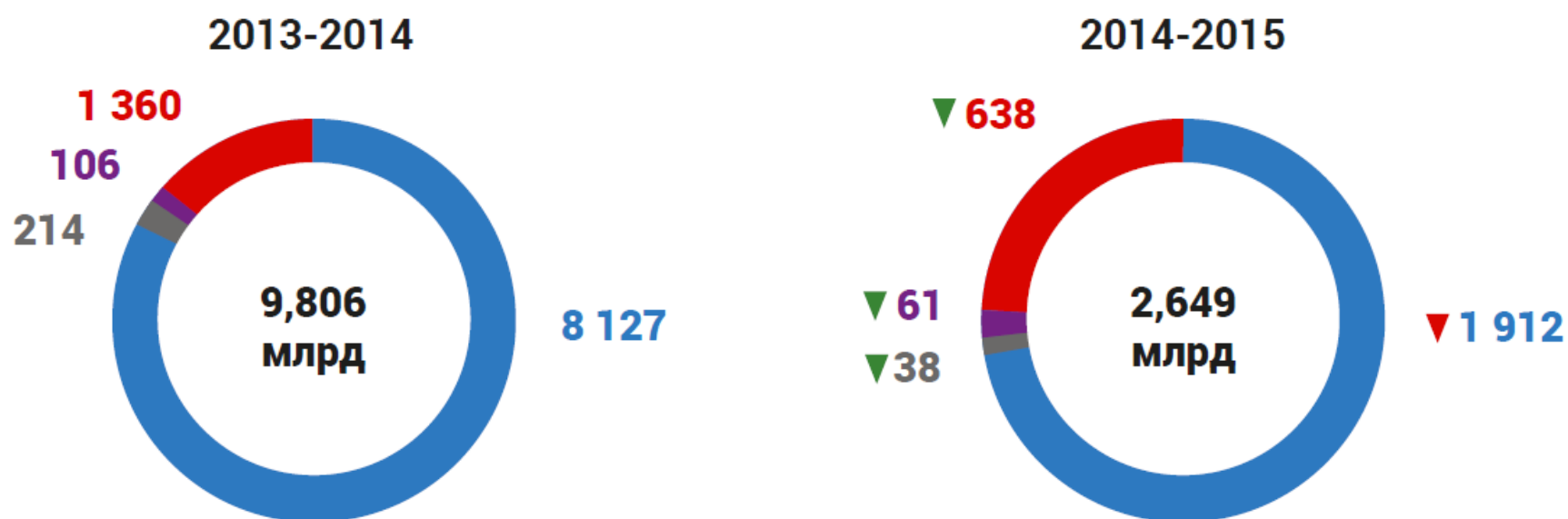


Тенденции развития
преступности в области
высоких технологий **2015**

|GROUP|IB|
GLOBAL CYBER SECURITY COMPANY

ТРЕНД №1: СНИЖЕНИЕ УЩЕРБА ПРИ РОСТЕ КОЛИЧЕСТВА АТАК

Оценка рынка высокотехнологичных преступлений, тренд (млн руб.)



■ Хищения в интернет-банкинге у юридических лиц
■ Хищения в интернет-банкинге у физических лиц

■ Хищения у физических лиц с помощью Android-троянов
■ Целевые атаки на банки

ТРЕНД №2 ПРОФЕССИОНАЛЫ УХОДЯТ С РЫНКА РОССИИ

- Один банк
- 13 клиентов
- 120 миллионов фунтов баланса

Main All logs My logs System logs Banks Users Autoskip X

1 2 3 ... 10

ID	Login info	Bank	IP	Last activity	Assigned	Action	Comment
551	[REDACTED]@le	RBS (Business)	62[REDACTED]42	18:07:43 (10.07)	-	+	77k
582	[REDACTED]	HSBC (business)	[REDACTED]	18:07:18 (10.07)	-	+	
589	[REDACTED]	Natwest (Business)	[REDACTED]	18:07:23 (10.07)	-	+	
588	[REDACTED]	TSB (business)	[REDACTED]	18:07:43 (10.07)	-	+	
527	[REDACTED]	aibgb1.co.uk (Business)	[REDACTED]	18:07:41 (10.07)	-	+	-6k. skip
506	[REDACTED]	Bank of Scotland (corporate)	[REDACTED]	18:07:58 (10.07)	-	+	
514	176[REDACTED]h	RBS (Business)	8[REDACTED]4	17:07:39 (10.07)	-	+	500k balance. inter -UK. pod chaps dropov pod krupnoe net. skip poka
564	[REDACTED]	Natwest (Business)	[REDACTED]	17:07:57 (10.07)	-	+	
586	[REDACTED]	Natwest (Business)	[REDACTED]	17:07:13 (10.07)	-	+	
539	26[REDACTED]53	RBS (Business)	2[REDACTED]	17:07:27 (10.07)	-	+	акк для авторизации платежей. 2kk balance. skip
587	[REDACTED]	Santander (business)	[REDACTED]	17:07:14 (10.07)	-	+	
492	1[REDACTED]	RBS (Business)	[REDACTED].8	16:07:34 (10.07)	-	+	PIN:1357 Pass:Aegis12 TMS-Payment approval - %Password21 balance total 40kk. dual auth
585	[REDACTED]	Unity Trust	[REDACTED]	16:07:22 (10.07)	-	+	
584	[REDACTED]	Santander (business)	[REDACTED]	16:07:09 (10.07)	-	+	
583	86[REDACTED]tti	RBS (Business)	[REDACTED]194	14:07:15 (10.07)	-	+	нет функции подтверждения платежа. 18kk. poproboval 2kk slit' na china
579	[REDACTED]	Santander (business)	[REDACTED]	14:07:21 (10.07)	-	+	11.3k na toader cocier 202569 13208710(2PAC)
566	376[REDACTED]m	RBS (Business)	[REDACTED]0	14:07:05 (10.07)	-	+	7kk balance. dual auth-ON. lutsche prozvonom lit
581	[REDACTED]	Santander (business)	[REDACTED]	14:07:03 (10.07)	-	+	slito 15k (2PAC) Josif Kasparovic 20-25-85. 90077186, венулись обратно

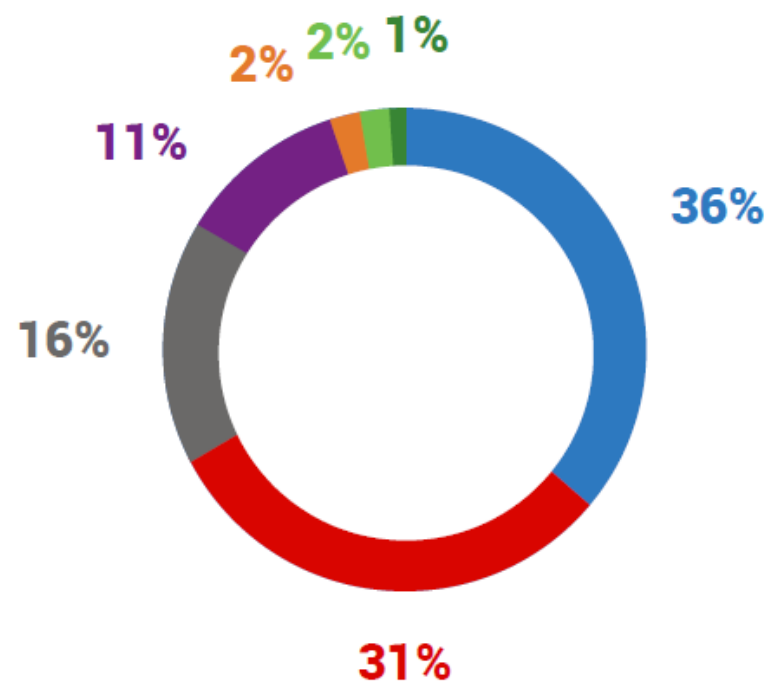
ТРЕНД №2 ПРОФЕССИОНАЛЫ УХОДЯТ С РЫНКА РОССИИ

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

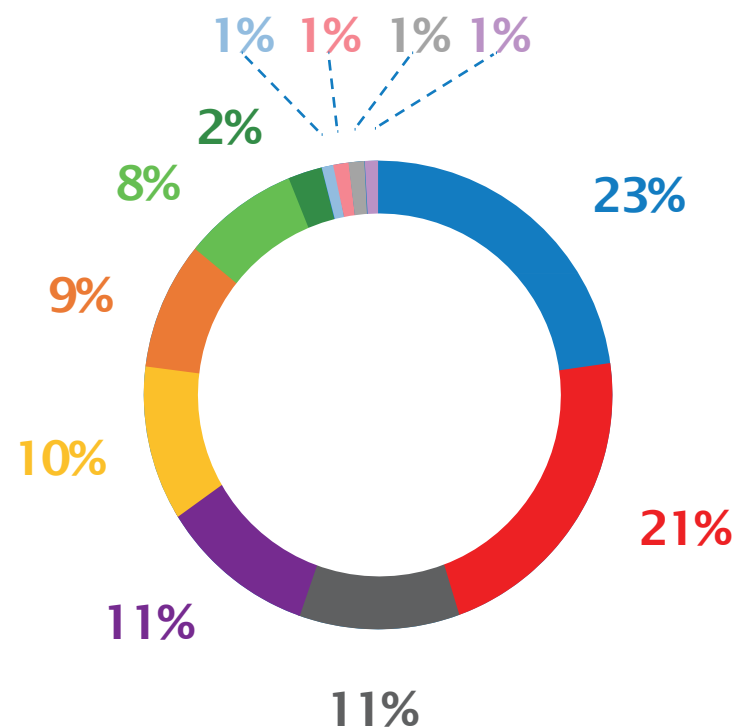
Группы, работающие по физическим лицам
через Web-банкинг

- PhishEye
- Infinity Proxy

Группы, работающие по физическим лицам
через мобильный клиент-банк

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

Инциденты по мобильным группам



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

ТРЕНД №5

УСИЛЕНИЕ ИНТЕРЕСА К ТОРГОВЫМ / БРОКЕРСКИМ СИСТЕМАМ

Группа Corkow

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

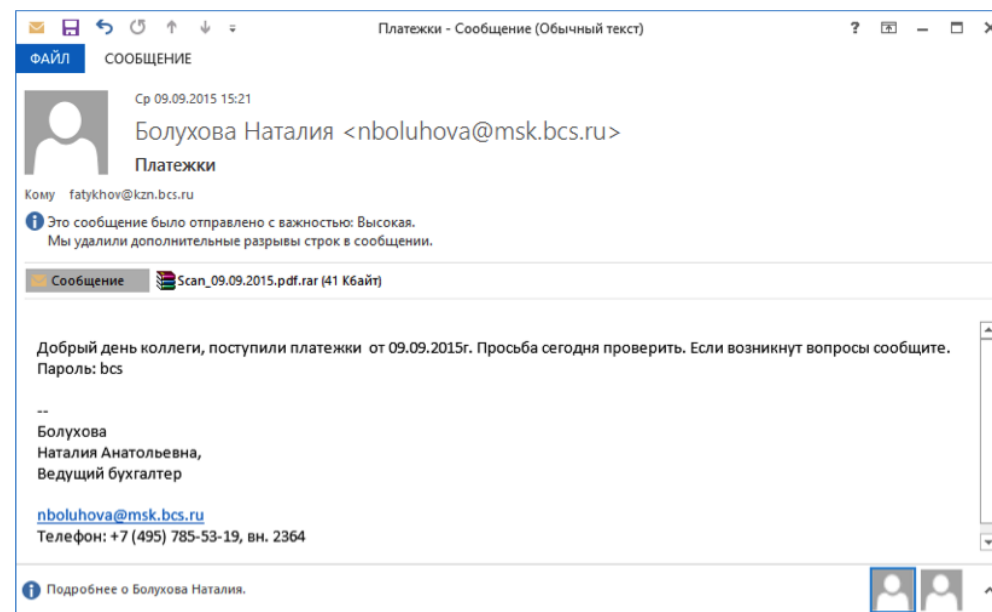
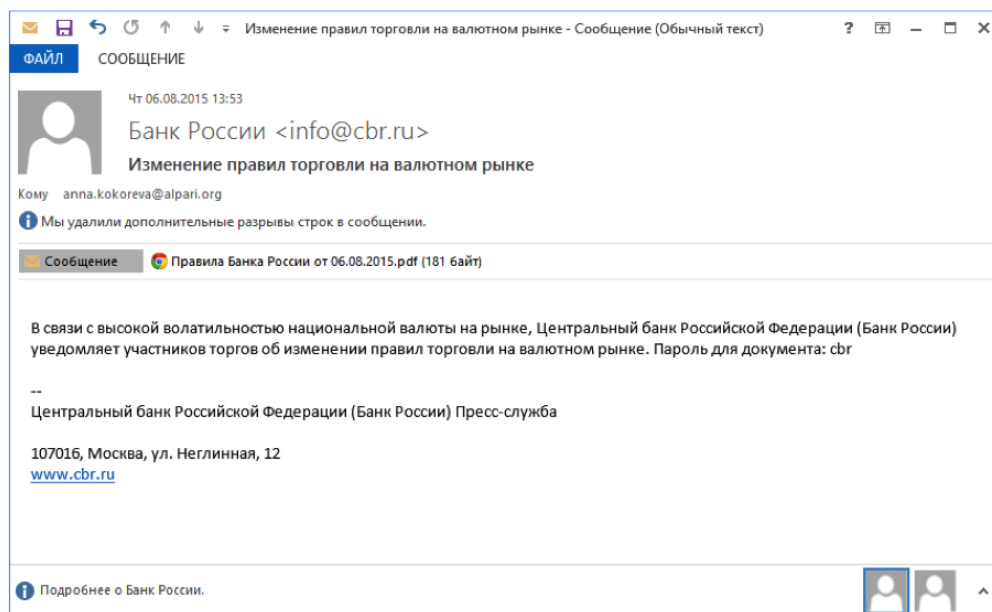


ТРЕНД №5 УСИЛЕНИЕ ИНТЕРЕСА К ТОРГОВЫМ/БРОКЕРСКИМ СИСТЕМАМ

Группа Anunak

Примеры атак на:

- брокера ФГ БКС
- форекс-брокер Alpari

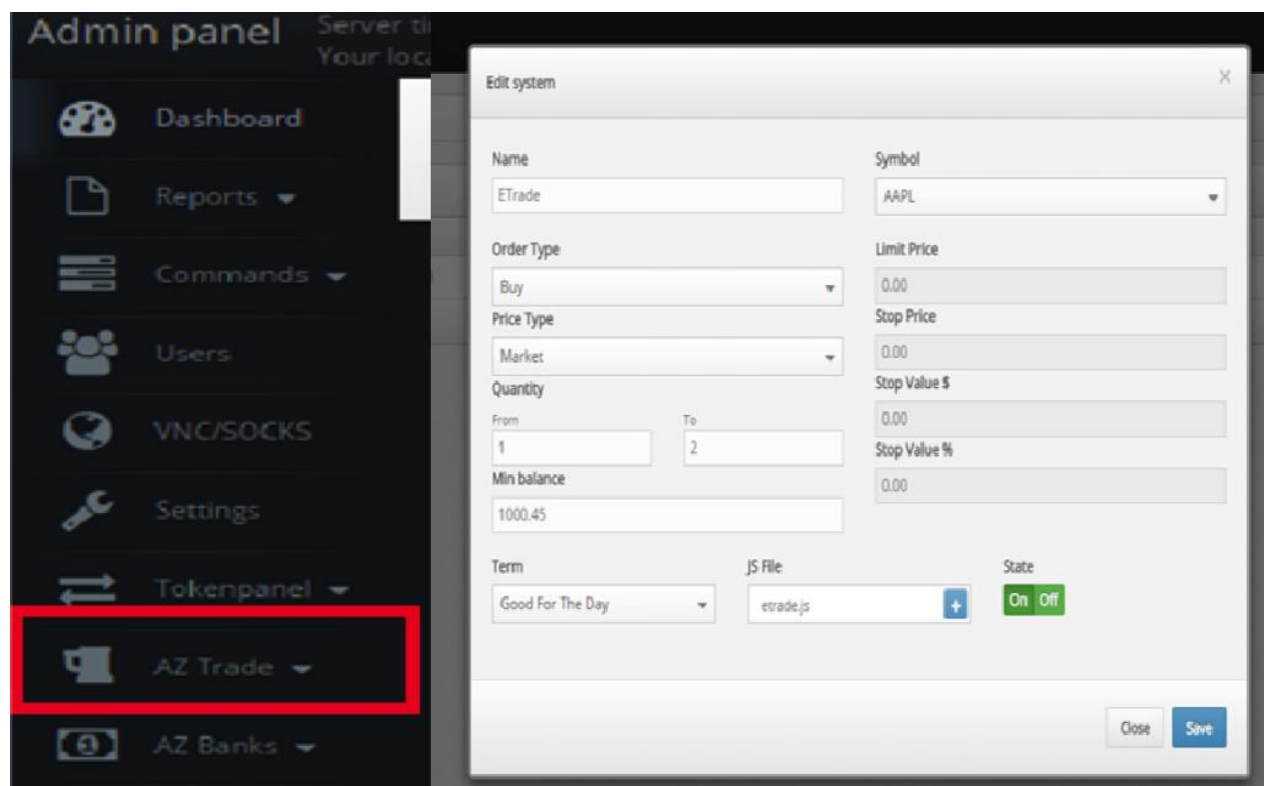


Минимум 5 групп собирают данные о логинах торговых систем.
Есть модули для автоматического хищения.

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 системы

*но и отклиентов не отказались...
и отбанков не отказались...
и отброкеров не отказались.*



BOT-TREK INTELLIGENCE

Cyber Intelligence subscription



Compromised data

Accounts

Credit cards

Money mules

IMEI

Files

Export



Threats



Attacks



Hacktivism



Targeted malware

Cybercrime group	Date Detected	Ref	Domain	Login	IP address
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

1 2 3 4 ... 10

Next >

BOT-TREK THREAT DETECTION SERVICE

Detects threats within your corporate network



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.





+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