Утечки конфиденциальной информации в России в 2016 году. Экспертный взгляд

Информационные технологии завтра. C-News – FORUM.
Секция «Информационная безопасность: в мире киберугроз»

ГАЗПРОМБАНК

10/11/2016 Москва

#информацияутекает

Латентность

Масштабность

!?

Технологичность

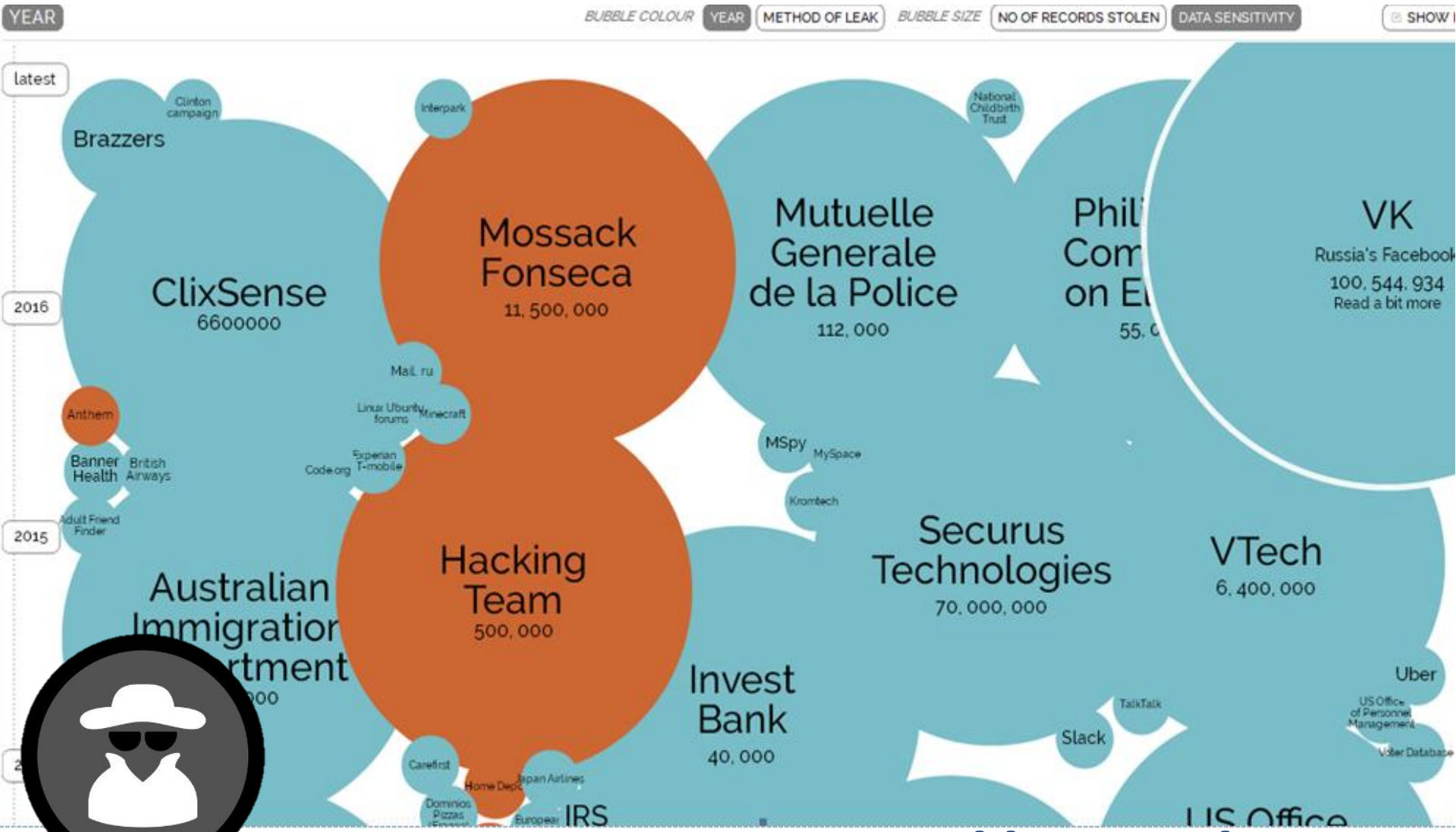
Доступность

#КТООНИ

?

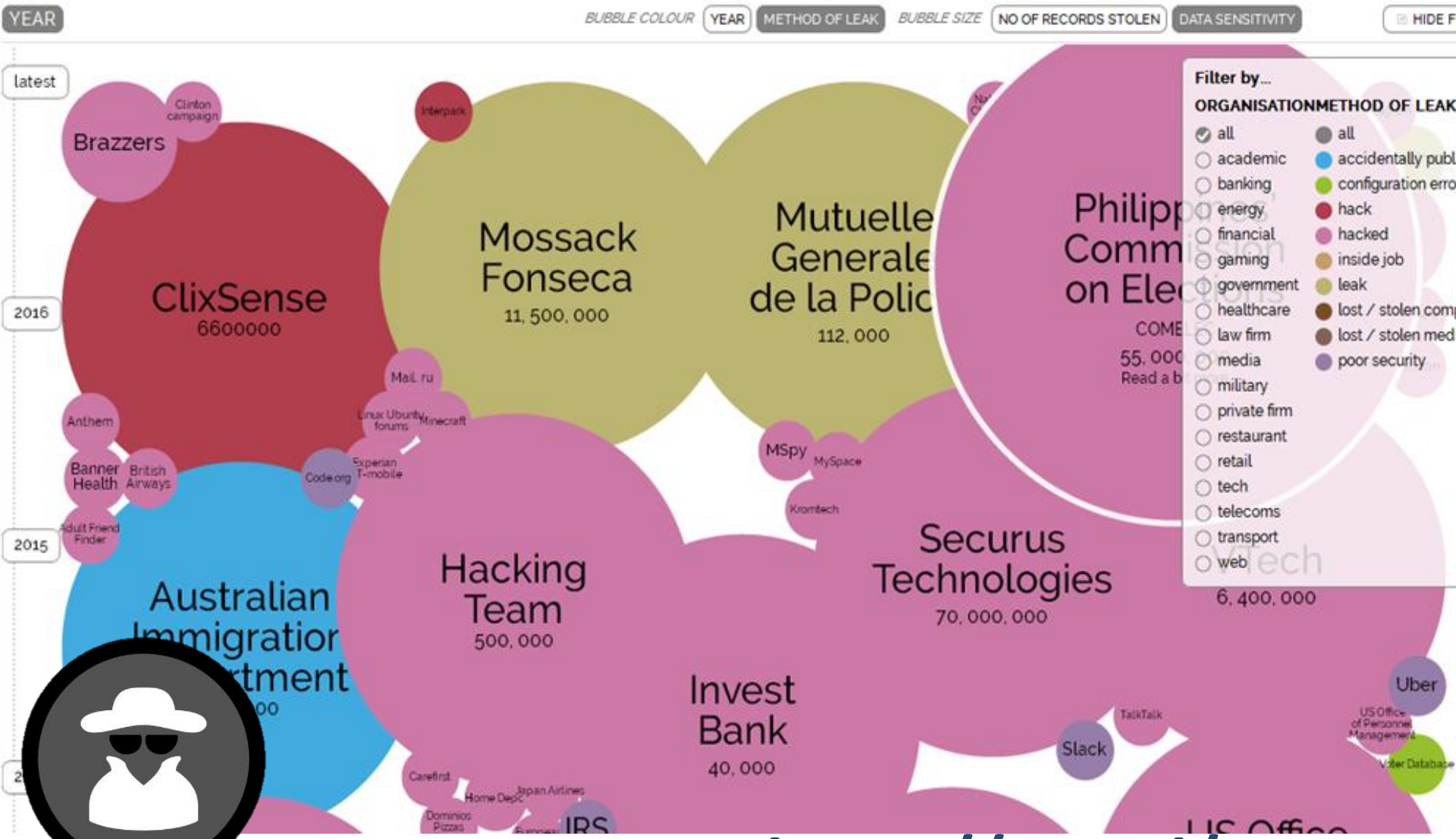
!

#информацияутекает

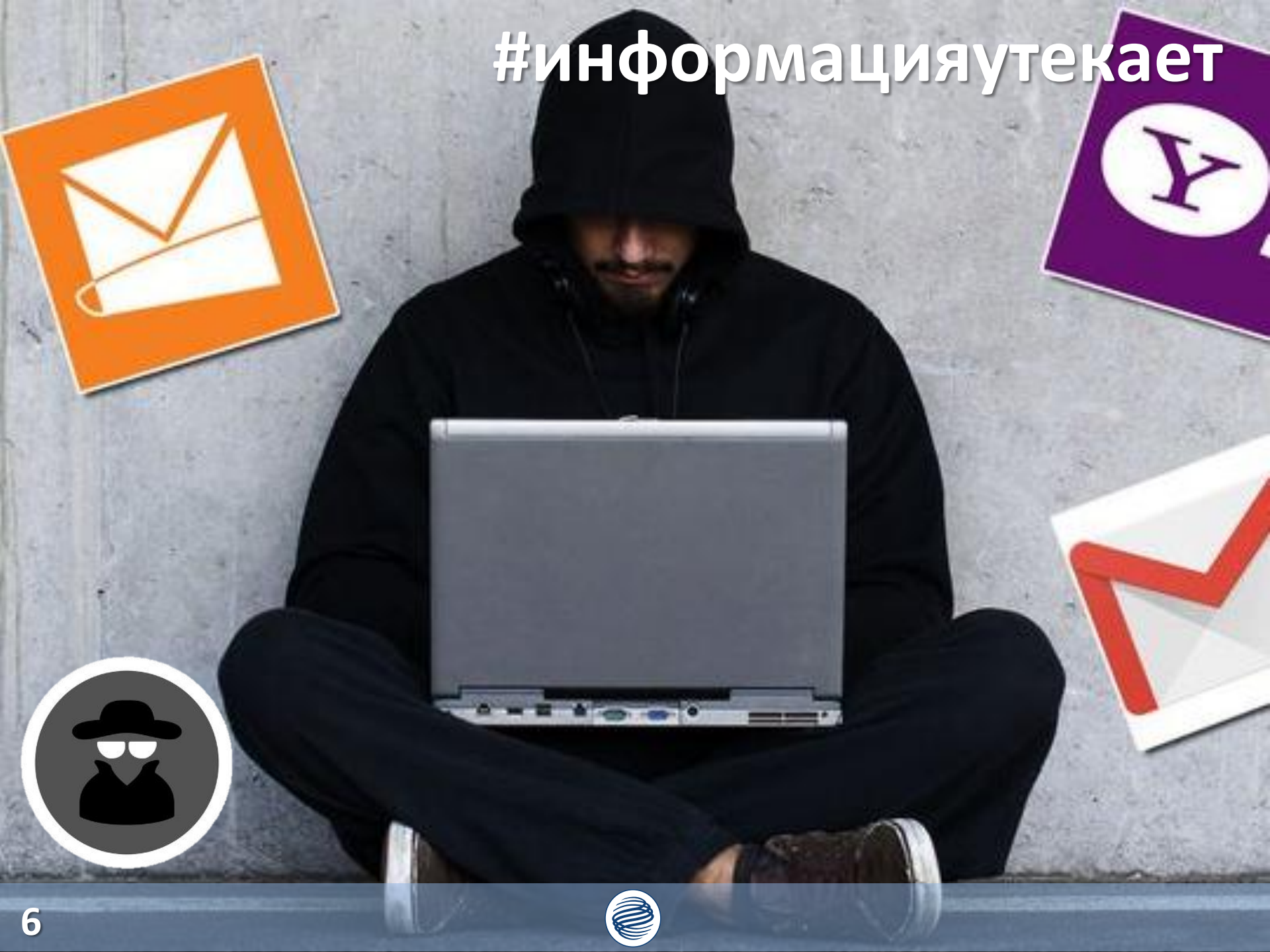


источник: https://goo.gl/a0pGe

#информацияутекает



источник: https://goo.gl/s2ogFS


#информацияутекает

LEAKEDSOURCE

HAS YOUR INFORMATION BEEN LEAKED?

2,293,680,424

скомпрометированных учетных записей в базе

Структура данных:

- Username
- Reg e-mail address
- Password (clear/SHA1/MD5)
- Source IP-address
- other info

Последние поступления:

- DVDrBase.info - 90,174 users - October 8th, a:2013
- AllGsmun.com - 134,859 users - September 15th, a:2016
- SprintUsers.com - 422,681 users - September 16th, a:2016
- Enworld.org - 284,586 users - September 14th, a:2016

1	@yahoo.com	126,053,325	24	@NONE	790,159	47	@qamail.msprod.msp	328,267
2	@hotmail.com	79,747,231	25	@yahoo.fr	741,962	48	@peoplepc.com	325,192
3	@gmail.com	25,190,557	26	@att.net	685,951	49	@music.msprod.msp	324,173
4	@aol.com	24,115,704	27	@earthlink.net	652,769	50	@yahoo.ca	320,579
5	@aim.com	5,345,585	28	@hotmail.es	612,748	51	@tmail.com	314,187
6	@live.com	4,728,497	29	@yahoo.co.id	604,816	52	@gmx.net	310,143
7	@hotmail.co.uk	4,701,850	30	@yahoo.com.my	601,114	53	@netzero.com	308,410
8	@msn.com	4,378,167	31	@yahoo.com.br	551,956	54	@yahoo.it	307,122
9	@myspace.com	4,257,451	32	@charter.net	548,031	55	@optonline.net	306,284
10	@comcast.net	3,275,651	33	@yahoo.de	543,823			
11	@ymail.com	2,866,796	34	@live.fr	518,523			
12	@sbcglobal.net	2,793,292	35	@netscape.net	510,577			
13	@hotmail.fr	2,335,422	36	@live.co.uk	502,121			
14	@web.de	1,486,602	37	@libero.it	490,151			
15	@rocketmail.com	1,420,819	38	@googlemail.com	430,112			
16	@yahoo.co.uk	1,384,943	39	@wp.pl	401,928			
17	@verizon.net	1,255,478	40	@live.com.mx	397,944			
18	@cox.net	1,082,304	41	@yahoo.es	389,453			
19	@mail.ru	1,040,442	42	@yahoo.co.jp	351,781			
20	@hotmail.it	1,018,406	43	@btinternet.com	349,642			
21	@bellsouth.net	961,018	44	@mail.com	343,346			
22	@gmx.de	959,852	45	@excite.com	335,215			
23	@hotmail.de	852,256	46	@yahoo.com.mx	330,927			

#статистика

LEAKEDSOURCE

HAS YOUR INFORMATION BEEN LEAKED?

LEAKEDSOURCE
HAS YOUR INFORMATION BEEN LEAKED?

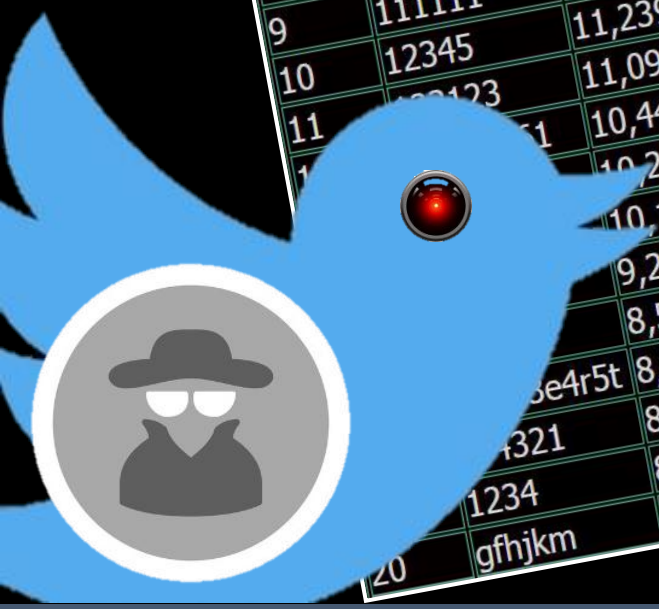
#доказательства

Rank	Password	Frequency
1	123456	120,417
2	123456789	32,775
3	qwerty	22,770
4	password	17,471
5	1234567	14,401
6	1234567890	13,799
7	12345678	13,380
8	123321	13,161
9	111111	12,138
10	12345	11,239
11	[illegible]	11,099
[illegible]	[illegible]	10,444
[illegible]	[illegible]	[illegible]231
[illegible]	[illegible]	[illegible]10,124
[illegible]	[illegible]	9,264
[illegible]	[illegible]	8,586
[illegible]	[illegible]e4r5t	8,386
[illegible]	[illegible]321	8,358
[illegible]	1234	8,257
20	gfhjkm	7,77

Rank	Country	Frequency
1	United States	13,711,788
2	Turkey	3,984,906
3	United Kingdom	3,646,707
4	Poland	2,569,583
5	Italy	2,084,394
6	Germany	2,054,638
7	Canada	1,633,484
[illegible]	France	1,606,438
[illegible]	Netherlands	1,420,732
[illegible]	[illegible]	[illegible]

Rank	Password	Frequency
1	homelesspa	855,478
2	password1	585,503
3	abc123	569,825
4	123456	487,945
5	myspace1	276,915
6	123456a	244,641
7	123456789	191,016
8	a123456	165,132
9	123abc	159,700
10	(POSSIBLY INVALID)	158,462

Rank	Password	Frequency
1	123456	753,305
2	linkedin	172,523
3	password	144,458
4	123456789	94,314
5	12345678	63,769
6	111111	57,210
7	1234567	49,652
8	sunshine	39,118
9	qwerty	37,538
10	654321	33,854
[illegible]	000000	32,490
[illegible]	password1	30,981
[illegible]	abc123	30,398
[illegible]	charlie	28,049
[illegible]	linked	25,334
[illegible]	maggie	23,892
[illegible]	michael	23,075
[illegible]	666666	22,888
[illegible]	princess	22,122
[illegible]	123123	21,826



#монетизация

Цена для физических лиц

Period	Bitcoin		PayPal
1 Day trial	$2.00	||	$4.00
7 Days	$8.00	||	$11.00
14 Days	$15.00	||	$18.00
28 Days	$25.00	||	$30.00
3 Months (90 Days)	$70.00	||	$85.00
6 Months (180 Days)	$135.00	||	$165.00
12 Months (365 Days)	$265.00	||	$320.00

Цена для юридических лиц

Very small companies 1 Month:	$1,000 (per month USD)	||	$1,000,000(per breach)
Small companies 1 Month:	$ 5,000 (per month USD)	||	$10,000,000(per breach)
Me… large companies 1 Month:	$10,000 (per month USD)	||	$30,000,000(per breach)
…s with hundreds of M of users 1 Month:	Contact us for a quote	||	Unlimited

source: e-mail leakedsource.com

PHONE TO NUMBER

137,090,136

скомпрометированных учетных записей в базе

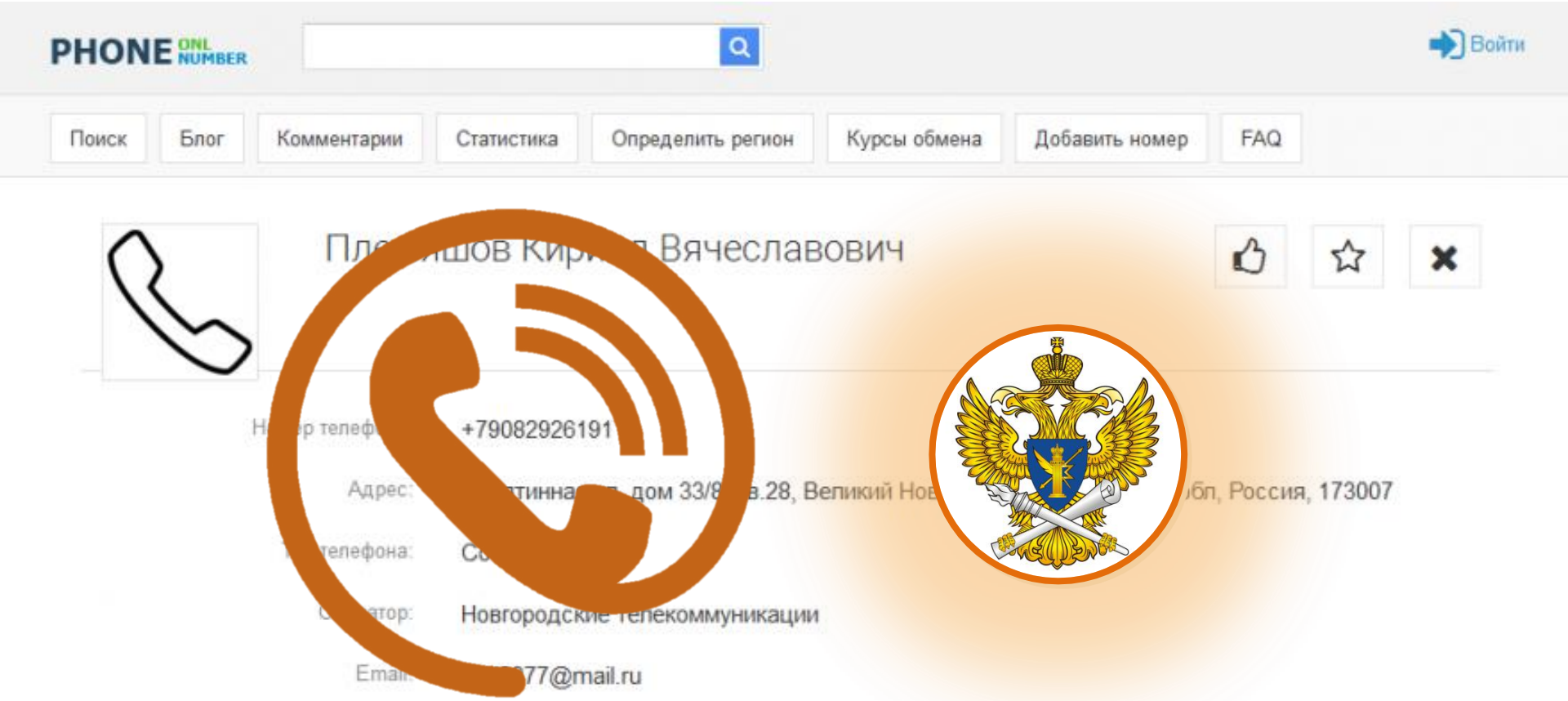
Структура данных

- ФИО
- Phone number
- Local address
- Type of service
- Reg e-mail address
- other info

Источники поступления данных

- Общедоступные данные
- API других сайтов и специальных сервисов
- Индивидуальные «коллекторы»
- Информация от пользователей сервиса при регистрации ☺

#доказательства



(c) Жалоба: противозаконное размещение моих персональных данных в интернете

Без моего согласия на сайте https://phonenumber.to в открытом доступе размещены мои персональные данные. Ссылка на страницу с личной информацией: https://phonenumber.to/phone/79128318281 Прошу Роскомнадзор разобраться в ситуации и помочь удалить мои конфиденциальные данные. Большое спасибо!

#монетизация

Любой пользователь сети Интернет может заплатить организаторам сайта phonenumber.to за исключением своих данных из базы общего доступа при помощи **bitcoin** по текущему курсу 1 BTC = ~40 000 рублей.

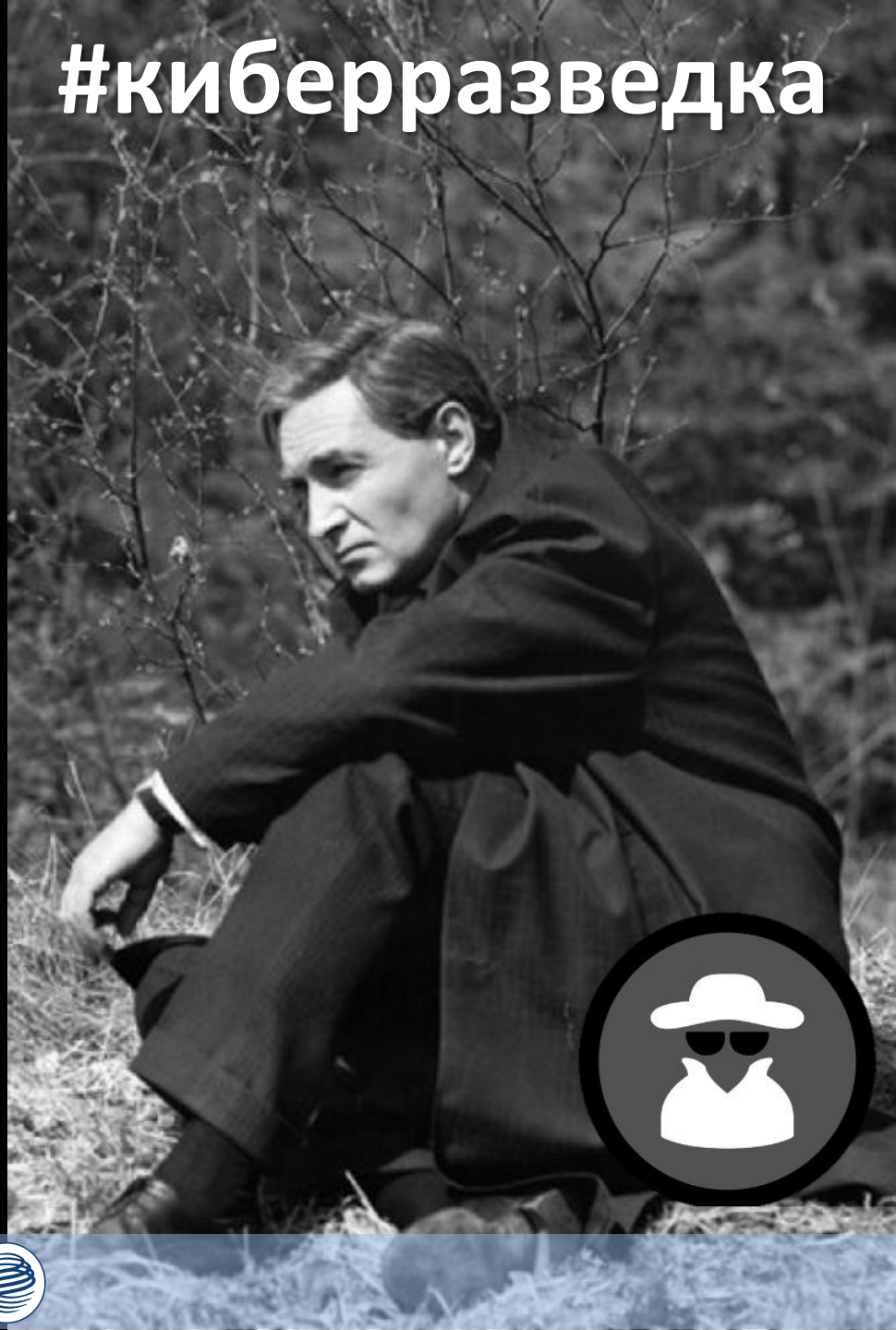
Условия обсуждаются индивидуально.

+ популяризация **bitcoin** ☺

phonenumber.to

#киберразведка

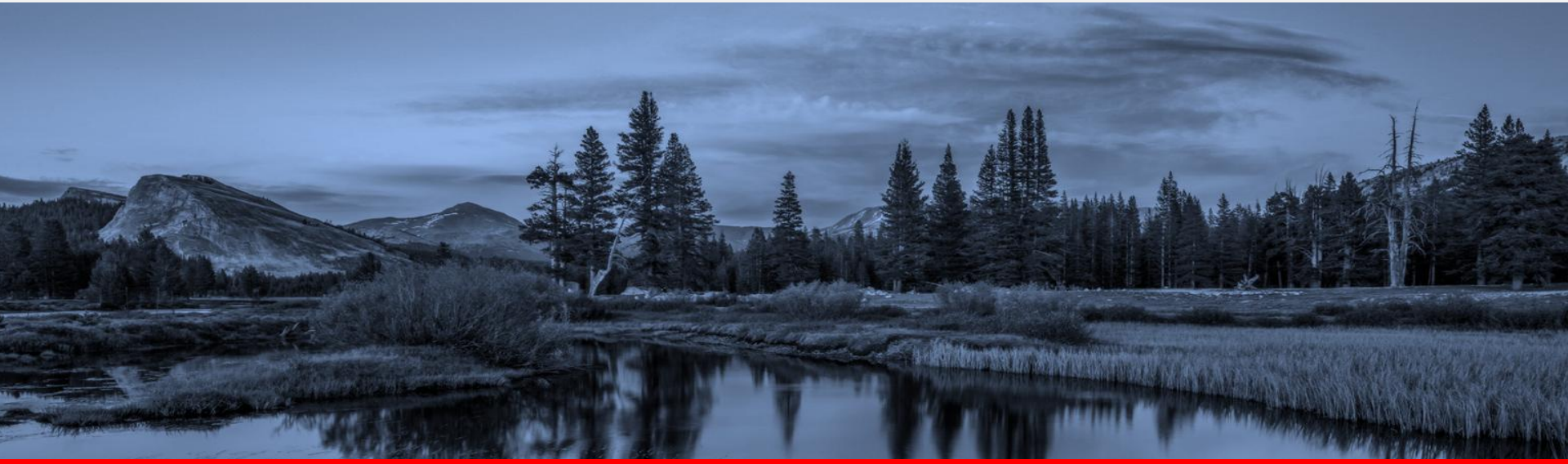
- ✓ Принцип «знай своего врага»
- ✓ Работа с первоисточником по уязвимостям
- ✓ …
- ✓ Сбор и анализ актуальной информации о методах и инструментах злоумышленников
- ✓ Оценка угроз для собственной системы защиты информации
- ✓ Мониторинг утечек со стороны черного рынка
- ✓ Работа на опережение по подтвержденным утечкам
- ✓ Получение и реализации информации по смежным областям
- ✓ …



#зоныразвития

- Привлечение внутренних и внешних ресурсов для проведения кибербразведки
- Формирование и актуализация критериев
- Машинное и персональное обучение, повышение квалификации
- Поиск и отбор продавцов/владельцев достоверной информации
- Верификация полученных данных
- Определение источника и канала утечки
- Проведение внутренних мероприятий по минимизации вероятности рецидивов
- Подтверждение эффективности

Благодарю за внимание!



Готов ответить на Ваши вопросы

ГАЗПРОМБАНК

Плешков Алексей Константинович

начальник Управления
режима информационной безопасности
Департамент защиты информации
Банк ГПБ (АО) г. Москва

e-mail: Alexey.Pleshkov@gazprombank.ru
тел: 8(495)-428-5045