Fighting against Cybercrimes in Russia.

Trends and Experience.

Alexander Pisemskiy, CISM, CISA, MCP

Deputy CEO
Group-IB
pisemskiy@group-ib.ru

About us

- Major activity: Information security incident investigation and response
- Starting from 2003
- Computer forensics facility
- The first and the one in Russia

The last case

ИЗВЕСТИЯ RU
ОБЩЕНАЦИОНАЛЬНАЯ ГАЗЕТА

http://www.izvestia.ru/obshestvo/article3145621/index.html

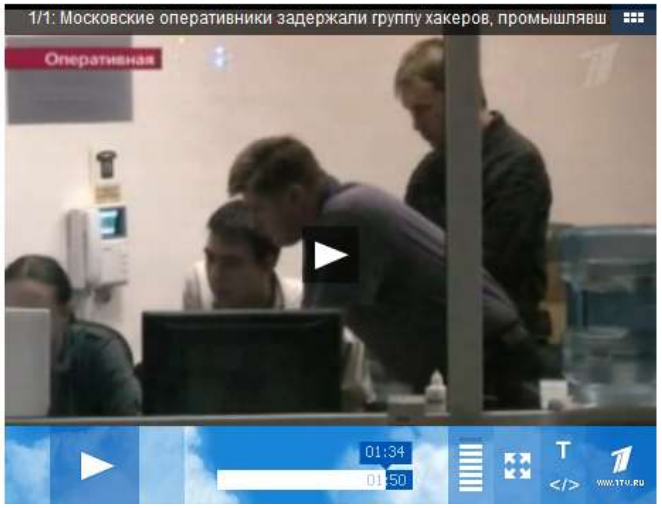
Хакеров сняли с золотой жилы

Дмитрий Евстифеев

Столичные оперативники задержали группу молодых хакеров, которые зарабатывали миллиарды рублей на вирусах. Владелец зараженного компьютера должен был отправить платную СМС, чтобы избавиться от заразы. Жертвами мошенников стали десятки тысяч людей не только в России.

Московские оперативники задержали группу хакеров, промышлявших интернет-рэкетом

Версия для печати Код для вставки в блог



Group-IB помогла УБЭП и отделу "К" ликвидировать группу хакеров

≡ Безопасность | пресс-релизы | 01.09.2010 15:15

комментировать
версия для печати

Специалисты компании Group-IB – первой компании в России, которая комплексно занимается расследованием ИТ-инцидентов и нарушений информационной безопасности – совместно с опер отдела "К" и УБЭП ГУВД г. Москвы приняли участие в ликвидации преступной группы хакеров, з вирусами-блокираторами персональные компьютеры пользователей сети Интернет.

Major types of cybercrimes

- Internet banking fraud
- Malware
- DDoS-attacks
- Sensitive data theft
- Intellect property piracy
- SMS – fraud
- Internet hacking

The aim of criminals

The main aim of criminals is to get as much profit as possible.

16 years old boy earns up to $1.700.000 in 1.5 year

Botnet owner's billing page

2007-07-0610670	4645	$1.16	$41	1:35	132	0	$5377.56	$418.56	$5796.12
2007-07-0512550	5222	$0.83	$37	1:44	118	0	$4331.42	$379.23	$4710.65
2007-07-045851	2385	$0.91	$34	1:37	64	0	$2175.91	$311.24	$2487.15
2007-07-033870	1628	$0.88	$29	1:33	50	0	$1440.75	$519.3	$1960.05
2007-07-021814	955	$1.88	$43	1:23	42	0	$1793.96	$347.92	$2141.88
2007-07-011593	850	$1.17	$43	1:37	23	0	$996.56	$140.33	$1136.89
2007-06-301661	910	$3.94	$38	1:10	94	0	$3582.42	$482.99	$4065.41
2007-06-291951	949	$7.26	$39	1:5	175	0	$6893.41	$816.3	$7709.71
2007-06-281500	789	$4.36	$45	1:10	76	0	$3443.09	$425.6	$3868.69
2007-06-273050	1703	$0.94	$42	1:45	38	0	$1604.47	$274.16	$1878.63
2007-06-263918	2175	$0.52	$34	1:66	33	0	$1134.23	$174.86	$1309.09
2007-06-254263	2472	$0.74	$45	1:60	41	0	$1826.93	$109.1	$1936.03
Total	14811	19891	49118	$0.18	$45	1:257	3564399	$1604494.72	$128997.71	$1733492.43

Internet Banking Fraud

Group-IB data:

- More than 200% growth compare with 2009
- Each month in Moscow police registers 10 cases in average
- Total number of incidents is Moscow minimum 2 times bigger than number of reports
- Average loss on incident is 1.500.000 Rubles
- Loss in particular case may vary from 100.000 to 40.000.000 Rubles

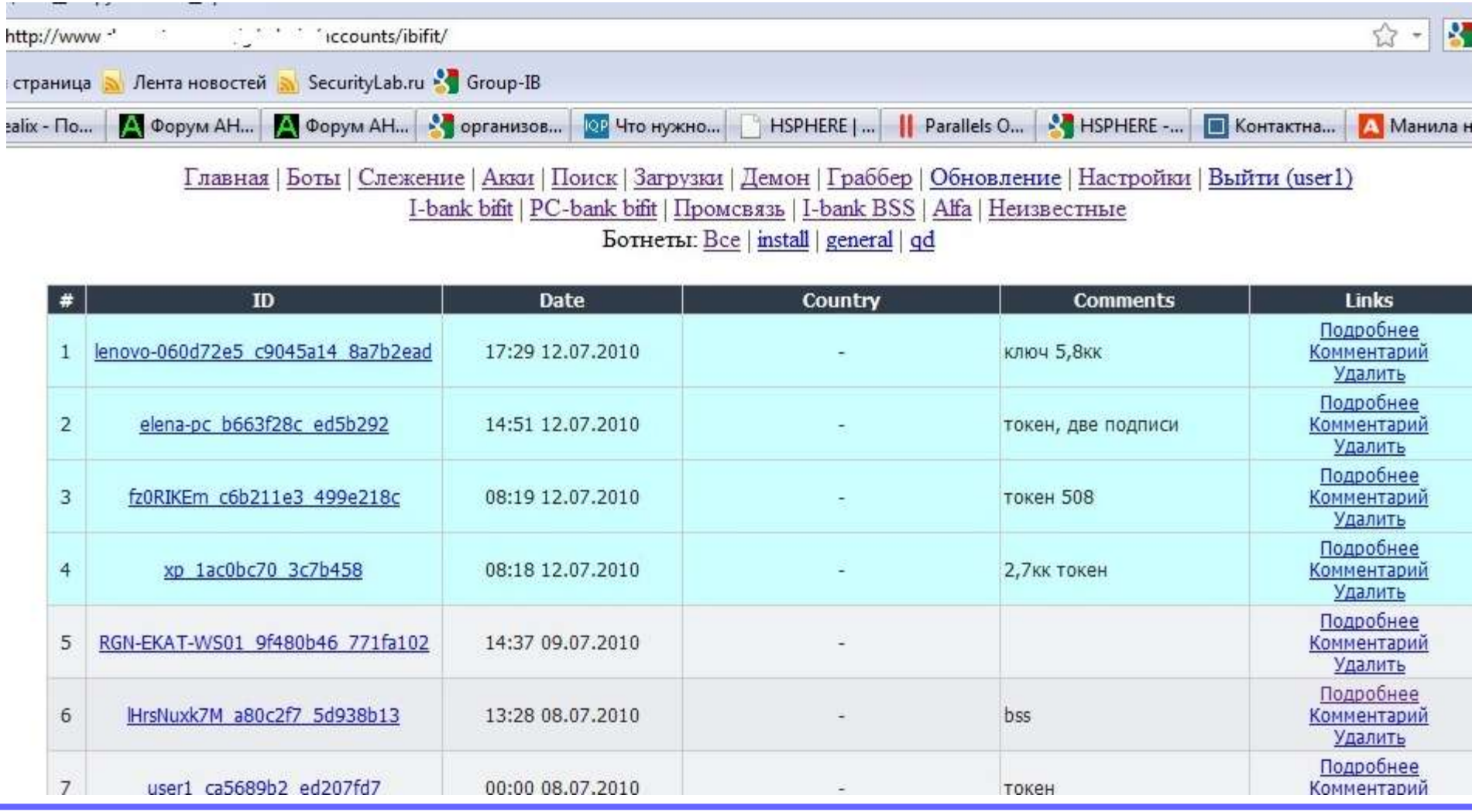
Trends of 2010

- New malware customized for particular Internet Banking system
- DDoS-attacks are not used any more to hide fraud
- Sending fraudulent payment from victim’s PC using remote access
- Using new ways to cash money
- Anti-forensics activities

Trojan-banker CC console

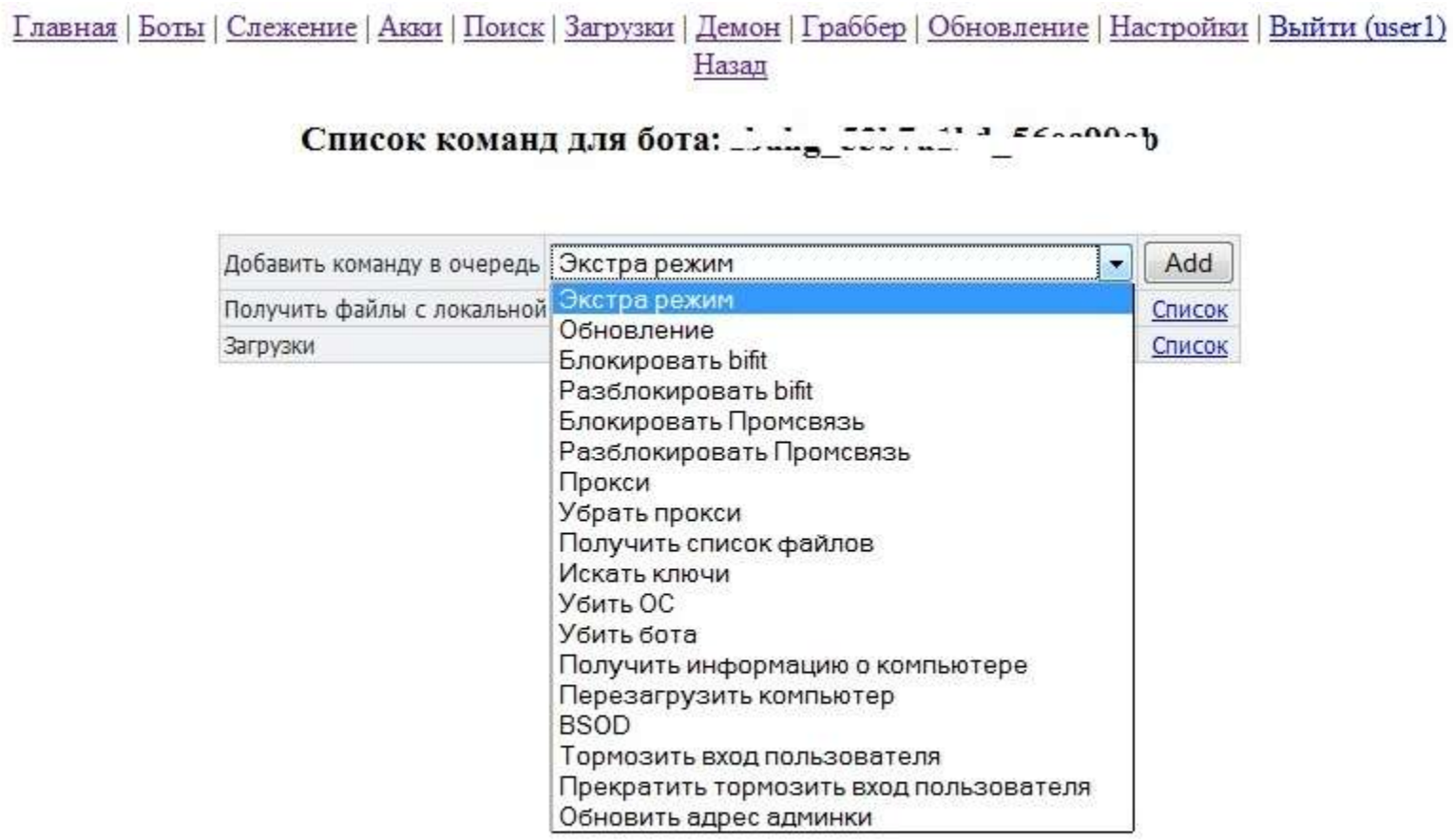
4	xp_1ac0bc70_3c7b458	08:18 12.07.2010	-		Подробнее Комментарий Удалить
5	RGN-EKAT-WS01_9f480b46_771fa102	14:37 09.07.2010	-		Подробнее Комментарий Удалить
6	lHrsNuxk7M_a80c2f7_5d938b13	13:28 08.07.2010	-		Подробнее Комментарий Удалить
7	user1_ca5689b2_ed207fd7	00:00 08.07.2010	-		Подробнее Комментарий Удалить
8	bos_dde6cd8f_935812d0	08:54 07.07.2010	-		Подробнее Комментарий Удалить
9	516c2954c5ac410_9755e5a9_68c47b8e	08:52 07.07.2010	-		Подробнее Комментарий Удалить
10	microsof-02e5d0_b8b24a9_33d125d0	13:57 06.07.2010	!	ИСПОЛЬЗОВАН. 500к	Подробнее Комментарий Удалить
11	GlavBux_4d519b63_6728dafe	11:47 06.07.2010	-		Подробнее Комментарий Удалить
12	Rzhevskaja_c4939ba0_16355dab	10:00 05.07.2010	-		Подробнее Комментарий Удалить
13	dom_73923851_5b82d85c	08:43 05.07.2010	-		Подробнее Комментарий Удалить

Trojan-banker CC console



#	ID	Date	Country	Comments	Links
1	lenovo-060d72e5_c9045a14_8a7b2ead	17:29 12.07.2010	-	ключ 5,8кк	Подробнее Комментарий Удалить
2	elena-pc_b663f28c_ed5b292	14:51 12.07.2010	-	токен, две подписи	Подробнее Комментарий Удалить
3	fz0RIKEm_c6b211e3_499e218c	08:19 12.07.2010	-	токен 508	Подробнее Комментарий Удалить
4	xp_1ac0bc70_3c7b458	08:18 12.07.2010	-	2,7кк токен	Подробнее Комментарий Удалить
5	RGN-EKAT-WS01_9f480b46_771fa102	14:37 09.07.2010	-		Подробнее Комментарий Удалить
6	lHrsNuxk7M_a80c2f7_5d938b13	13:28 08.07.2010	-	bss	Подробнее Комментарий Удалить
7	user1_ca5689b2_ed207fd7	00:00 08.07.2010	-	токен	Подробнее Комментарий

Trojan-banker CC console

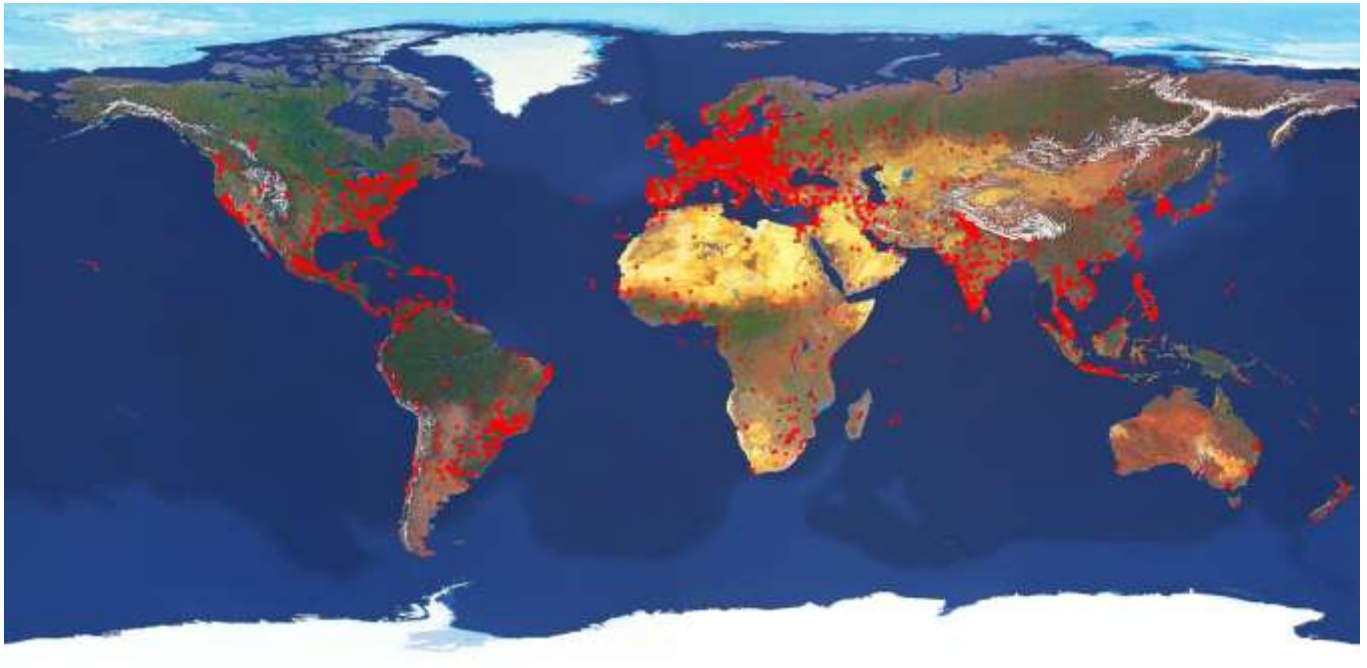


Malware trends 2010

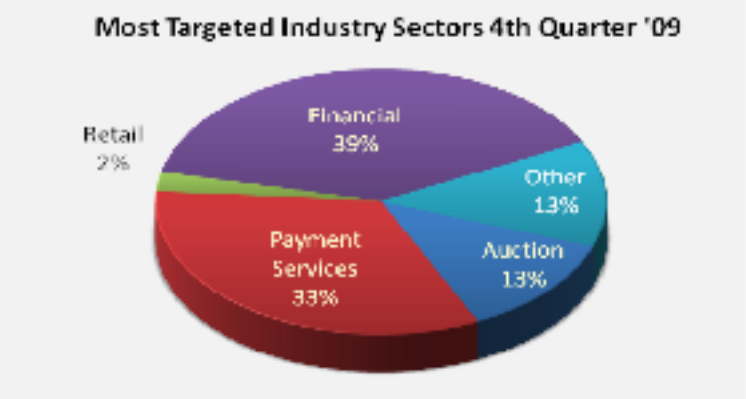
- Intellectual setup
- Encrypted communication with CC
- Capture Bank crypto keys from RAM
- Substitution of payment document during signing
- Emulation of OTP
- Remote access tools
- Winlocker

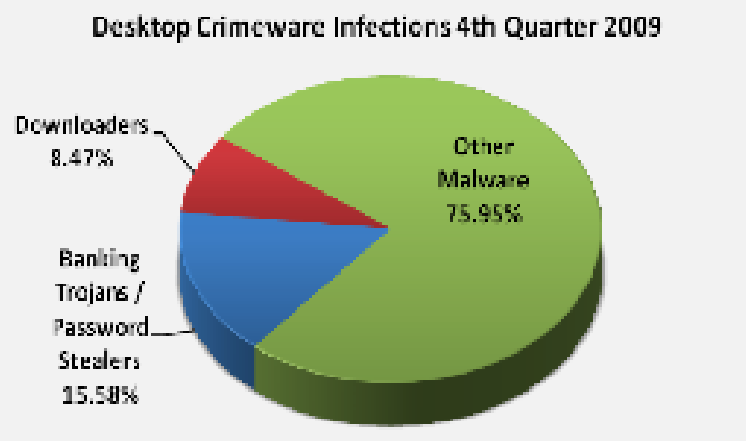
Botnets and DDoS

- Multifunctional bots
- “Non-professional” botnets made in constructor
- “Partner” botnets



Phishing





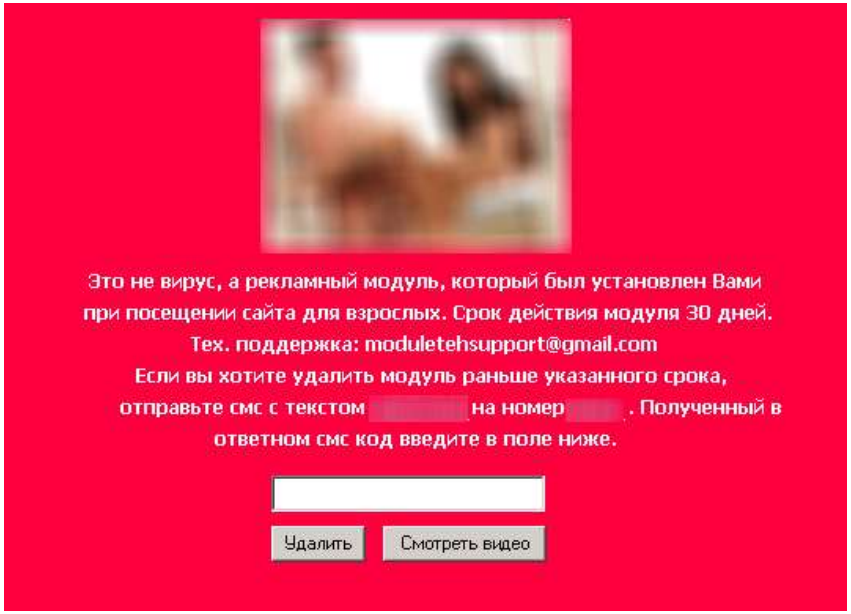
Countries Hosting Phishing Sites – 4th Quarter 2009

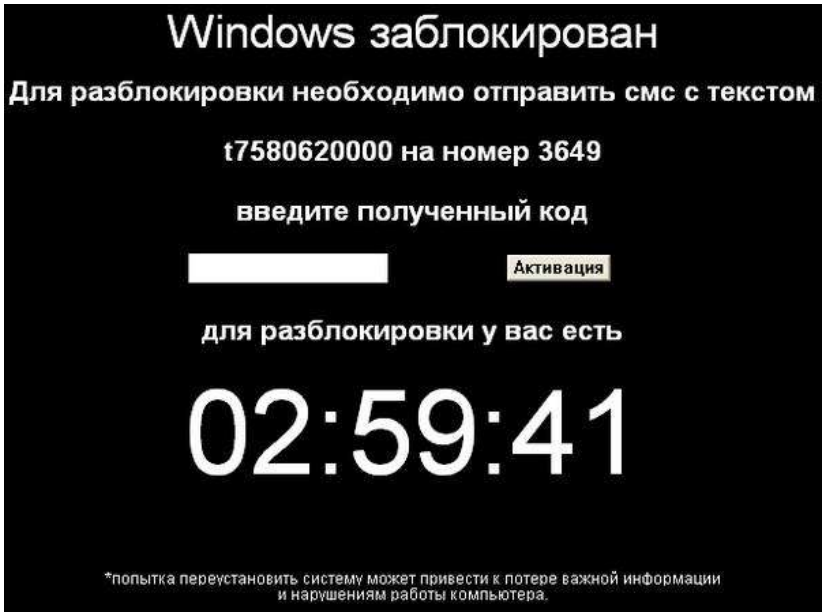
October		November		December	
USA	91.51%	USA	90.14%	USA	72.92%
Hong Kong	3.76%	Hong Kong	3.22%	China	5.24%
China	0.96%	China	1.73%	Canada	3.65%
Brazil	0.89%	Russia	1.01%	Germany	2.12%
Rep. Korea	0.47%	Rep. Korea	0.55%	Hong Kong	1.65%
Germany	0.40%	Germany	0.53%	Rep. Korea	1.47%
UK	0.29%	UK	0.28%	Russia	1.46%
Russia	0.20%	Canada	0.28%	UK	1.44%
France	0.18%	France	0.26%	Netherlands	1.23%
Canada	0.17%	Netherlands	0.17%	France	1.07%

SMS-Fraud

Combination of Trojan-Winlockers + SMS-based payment

Average month revenue of “black” partner of SMS-aggregator is $1M





Problems

- Corruption in police
- Not enough amount of cybercrime investigators
- People do not believe in justice
- Victim do not know what to do in case of cybercrime
- Low level of security awareness
- Not effective international cooperation
- Weak laws

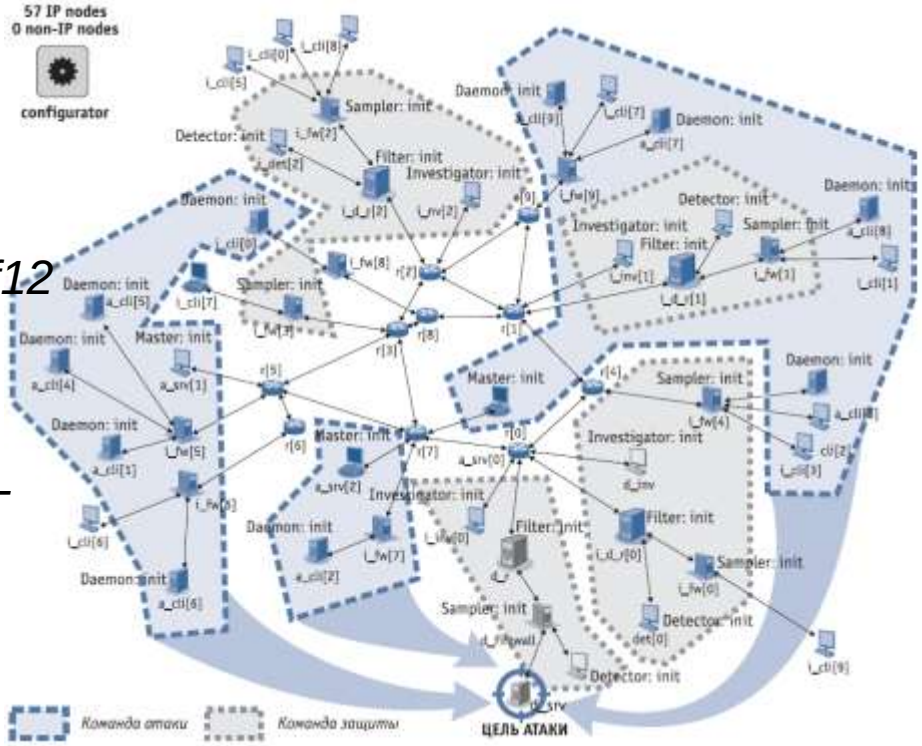
What we do

- Create Law practice in fighting cyber crimes: SMS-Fraud, Torrent-based piracy, Illegal Internet casinos, etc.
- Create new methodologies in computer forensics to investigate new types of incidents.
- Stop and investigate DDoS-attacks. Provide free data about bots and attacks to ISP's, victims and police.
- Participate in Russian Honeynet Project.
- Computer forensics services to government law-enforcement bodies and commercial organizations.
- Participate in police investigations as technical experts and consultants.
- Free consulting to citizens and organizations about cybercrimes.
- Provide science researches.
- Increase level of awareness in cybercrimes of commercial organizations and citizens

Stop DDoS-attack free method

- Honeynet

GET /main/rand/test.php?ver=0001id=151D4f12E2&cmd=0102 HTTP/1.0
Host: zlozlozlo.cn
HTTP/1.1 200 OK
Date: Tue, 26 Aug 2009 16:16:50 GMT
Server: Apache/2
X-Powered-By: PHP/5.0.11
Vary: Accept-Encoding,User-Agent
Content-Length: 17
Connection: close
Content-Type: text/html



StopDDoS.ru

- Страна: ru (48 IPs)
  - BEE-AS AS16345 (5 IPs) dump
  - Unknown Unknown (4 IPs) dump
  - ROSTOV-TELEGRAF-AS AS21479 (3 IPs) dump
  - COMCOR-AS AS8732 (2 IPs) dump
  - NTK AS31200 (2 IPs) dump
  - RIALCOM-AS AS34456 (2 IPs) dump
  - Fiord-AS AS28917 (2 IPs) dump
  - COMSTAR AS8359 (2 IPs) dump
  - CIFRA-AS AS41025 (2 IPs) dump
  - EXTREME-AS AS39709 (1 IPs) dump
  - STC-AS AS25490 (1 IPs) dump
  - ZTELECOM-AS AS41733 (1 IPs) dump
  - MF-NWGSM-AS AS31213 (1 IPs) dump
  - RU-CTSRND-AS AS6767 (1 IPs) dump
  - HOMELINK AS39618 (1 IPs) dump
  - MAcomnet AS8470 (1 IPs) dump
  - SEVEREN-TELECOM AS24739 (1 IPs) dump
  - BWCCJSC-AS AS41592 (1 IPs) dump
  - URAL AS5563 (1 IPs) dump
  - TKT-AS AS38951 (1 IPs) dump
  - INFOLINE-AS AS8416 (1 IPs) dump
  - SIBIRTELECOM-AS AS41440 (1 IPs) dump
  - ASN-TVT AS29194 (1 IPs) dump
  - magistraly-ru AS43970 (1 IPs) dump
  - CORBINA-AS AS8402 (1 IPs) dump
  - LEALTA-AS AS41275 (1 IPs) dump
  - BTL-AS AS43687 (1 IPs) dump
  - SOVAM-AS AS3216 (1 IPs) dump
  - ROSTELECOM-AS AS12389 (1 IPs) dump
  - TATTELECOM-AS AS28840 (1 IPs) dump
  - ASTRARU-AS AS42268 (1 IPs) dump
  - UNNET-AS AS31323 (1 IPs) dump
  - RTCOMM-AS AS8342 (1 IPs) dump
- Страна: UA (25 IPs)

- Страна: UA (25 IPs)
  - BANKINFORM-AS AS13188 (5 IPs) dump
  - UKRTELNET AS6849 (2 IPs) dump
  - UARNET-AS AS3255 (2 IPs) dump
  - VOLIA-AS AS25229 (2 IPs) dump
  - FARLINE AS42239 (1 IPs) dump
  - ELIS-NET AS6789 (1 IPs) dump
  - UACITY-AS AS29370 (1 IPs) dump
  - LUGANET-AS AS39728 (1 IPs) dump
  - APEXNCC-AS AS6702 (1 IPs) dump
  - AVANET AS35533 (1 IPs) dump
  - NetLux-AS AS5598 (1 IPs) dump
  - UMC-AS AS21497 (1 IPs) dump
  - DYTYNETS-AS AS34814 (1 IPs) dump
  - EVPANET-AS AS43936 (1 IPs) dump
  - MICROSYSTEM-AS AS16047 (1 IPs) dump
  - DORIS-AS AS8343 (1 IPs) dump
  - RENOME-AS AS34187 (1 IPs) dump
  - GROZA-AS AS42501 (1 IPs) dump
- Страна: KZ (2 IPs)
  - KAZTELECOM-AS AS9198 (2 IPs) dump
- Страна: UZ (1 IPs)
  - UZPAK AS8193 (1 IPs) dump
- Страна: Others (331 IPs)
  - Unknown Unknown (331 IPs) dump

Cooperation

We provide all our efforts to organize effective and pleasant cooperation between interested organizations to make our world securely.

We communicate with:

- Russian and CIS force agencies
- Forensics organizations and institutes
- CERTS all over the world
- Commercial organizations and ISP’s
- Antivirus and vulnerability labs
- Information security vendors

We are opened to new contacts and partnership.

Thank You!

Alexander Pisemskiy
CISM, CISA, MCP
Group-IB

pisemskiy@group-ib.ru
www.group-ib.ru