PANDA SECURITY | One step ahead.

The Business of Cybercrime

Luis Corrons

PandaLabs Technical Director

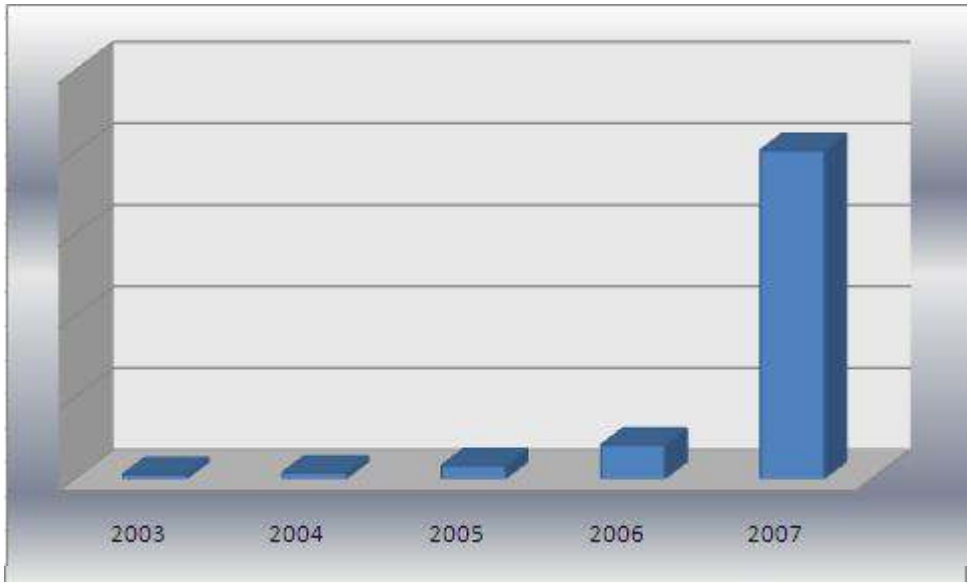
Agenda

1. Malware figures
2. Who is behind this?
3. Web Attack Toolkits
4. A Real Case
5. Underground Shopping Cart
6. Where to buy?

Malware figures

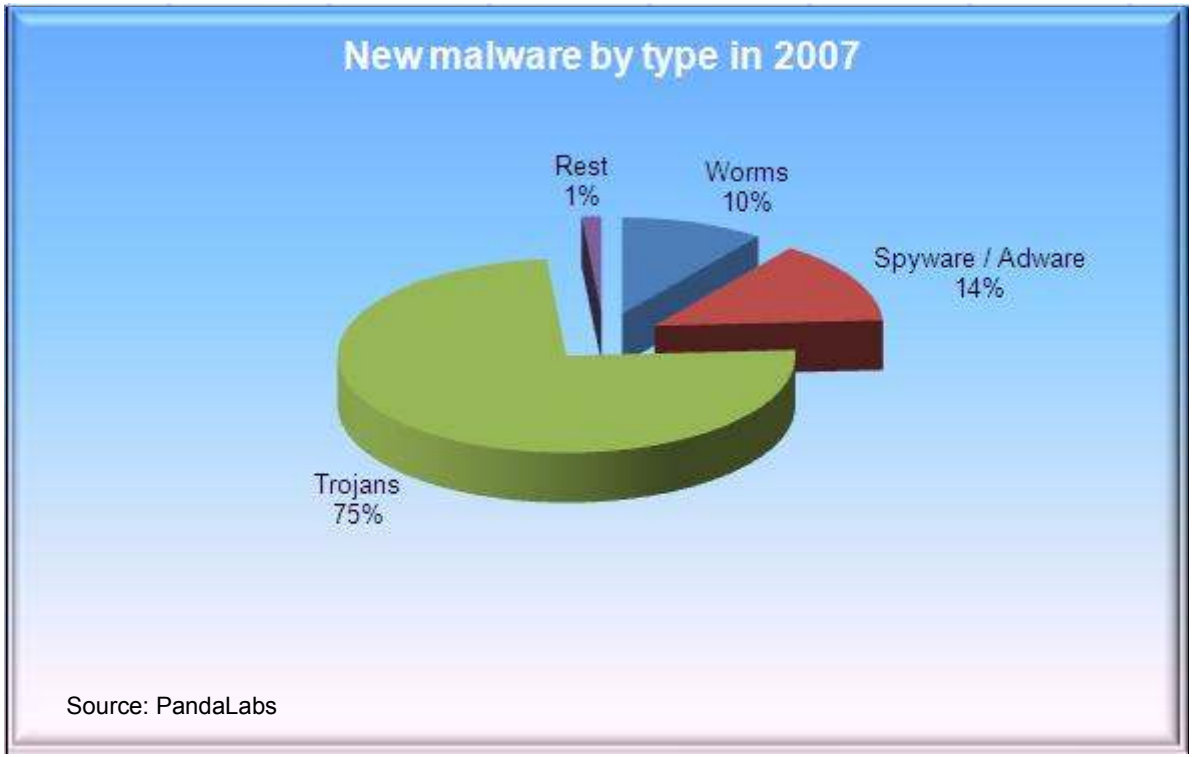
Malware evolution

Malware detected per year



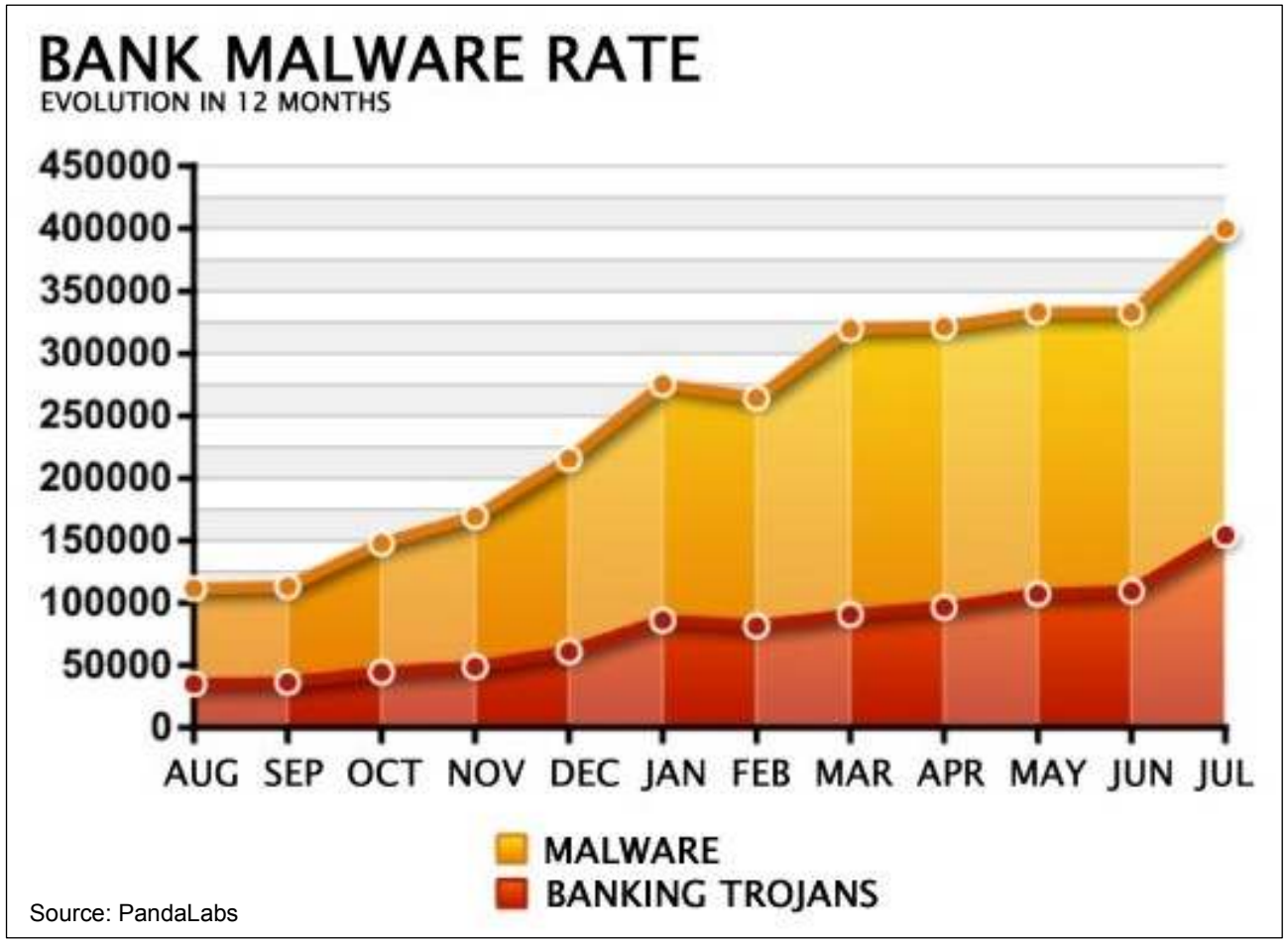
Source: PandaLabs

Malware evolution by type



Source: PandaLabs

Malware evolution by type



Source: PandaLabs

Who is behind this?

Yesterday's Bad Guys

Blaster.B	Nestky / Sasser	CIH	29-A
Jeffrey Lee Parson	Sven Jaschan	Chen Ing-Hau	Benny

Today's Bad Guys

Spam

James Ancheta

Phishing

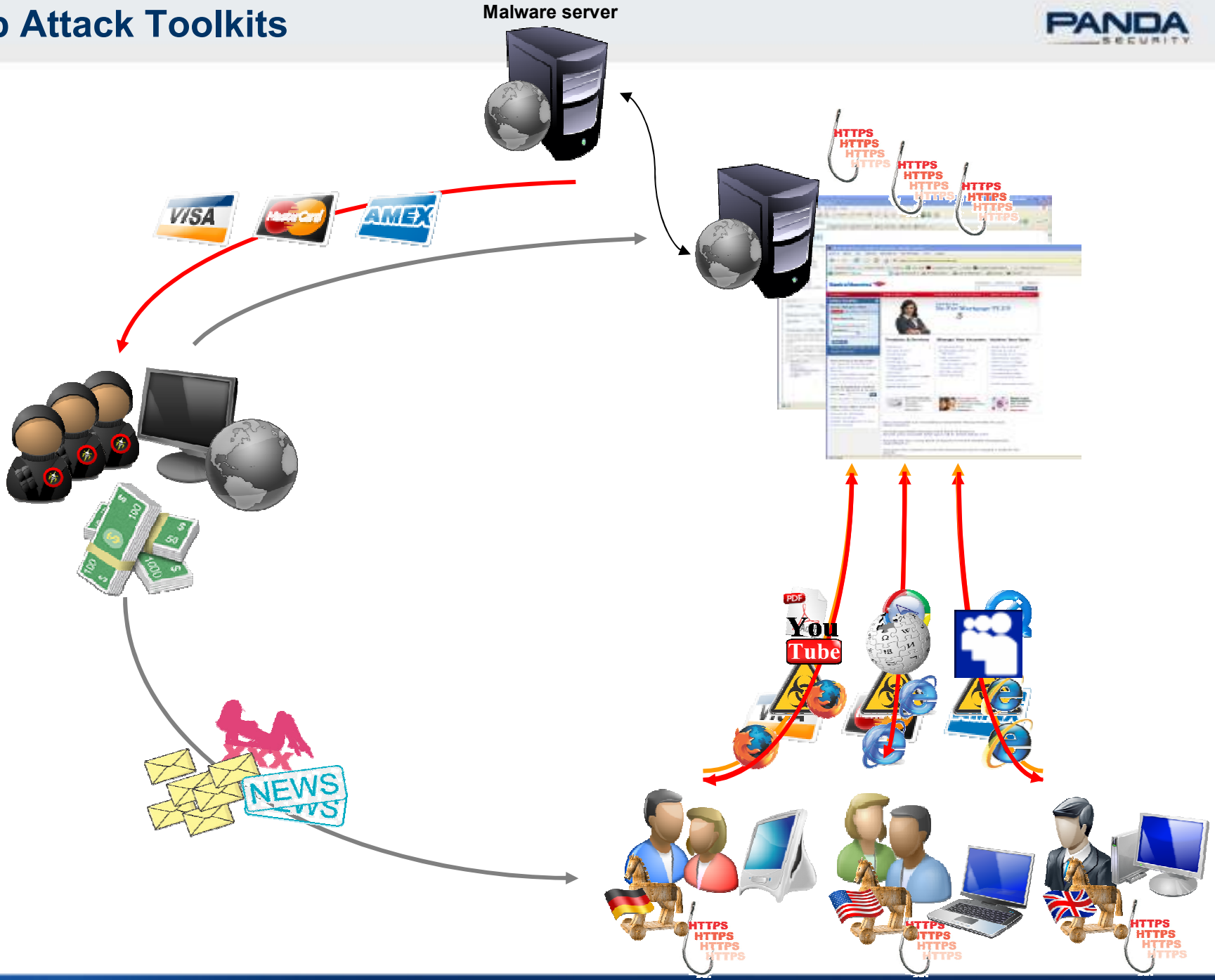
Andrew Schwarmkoff

Spam

Jeremy Jaynes

Web Attack Toolkits

Web Attack Toolkits



MPack

virus BULLETIN Fighting malware and spam
www.aec.eu
Mpack packs punch in Italy
Massive MPACK Compromise
Published: 2007-06-18,
Last Updated: 2007-06-18 21:34:24 UTC
by Lorna Hutcheson (Version: 1)
Crippling malware attack strikes in Italy
Researchers claim hundreds of sites compromised
Shaun Nichols in California, vnunet.com 18 Jun 2007
Italy is suffering from a barrage of remote attacks launched from hundreds of compromised websites, security experts have warned.
Researchers at Symantec reported that attackers have injected 'iframe' tags within the HTML files on compromised sites.
ADVERTISEMENT
intel Centrino Duo
More peace of mind for less.
Wednesday, June 20, 2007
Massive Embedded Web Attack in Italy
The Web is abuzz with news stories regarding the MPACK web exploitation kit installed on over 10,000 mostly Italian based sites, and in the spirit of previous analyses of malicious URLs here's an overview of the strategy of the attack, the outcome, and IPs in quesiton, thus the ones that should get blacklisted or CYBERINT applied for further juicy details on the severity of the attack.
The strategy of the attack
Picture yourself in the position of a malicious

MPack

- **Tracking Mpack for 2 months (April & May 2007):**
  - **41 different servers with Mpack running**
  - **366,717 web pages “iframed”**
  - **More than 1 million users infected (1,217,741)**

MPack

MPack v0.90 stats

Attacked hosts (total - uniq)	
IE XP ALL	114721 - 96104
QuickTime	2175 - 2048
Win2000	7033 - 6260
Firefox	12885 - 12514
Opera7	1271 - 1264

Traffic (total - uniq)	
Total traff	159073 - 129089
Exploited	44804 - 35574
Loads count	17408 - 15968
Loader's response	38.85% - 44.89%
Efficiency 10.94% - 12.37%	

Browser stats (total)	
MSIE	4 0%
Opera	1 0%

Modules state	
Statistic type	MySQL-based
User blocking	ON
Country blocking	OFF

Country	Traff	Loads	Efficiency
RU - Russian federation	112793 70.9%	12653 72.7%	11.22%
UA - Ukraine	16666 10.5%	1670 9.6%	10.02%
IT - Italy	7045 4.4%	593 3.4%	8.42%
GE - Georgia	5775 3.6%	673 3.9%	11.65%
BY - Belarus	5419 3.4%	657 3.8%	12.12%
KZ - Kazakstan	3098 1.9%	376 2.2%	12.14%
US - United states	1117 0.7%	50 0.3%	4.48%
AZ - Azerbaijan	1060 0.7%	128 0.7%	12.08%
MD - Moldova, republic of	683	101	14.79%

IcePack

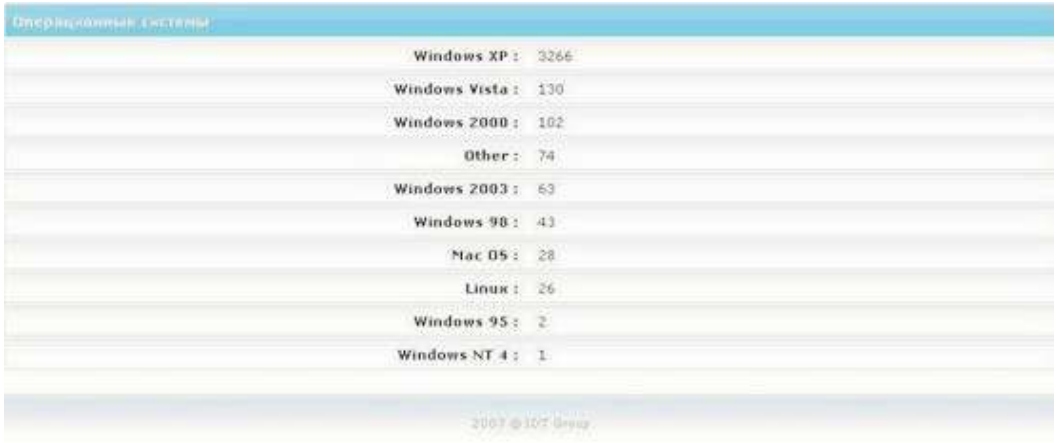
Login

IcePack

IcePack
Главная страница
Добро пожаловать
PHP :
MySQL :
Safe Mode :
IP сервера :
Ваш IP :
Общее кол-во трафика :

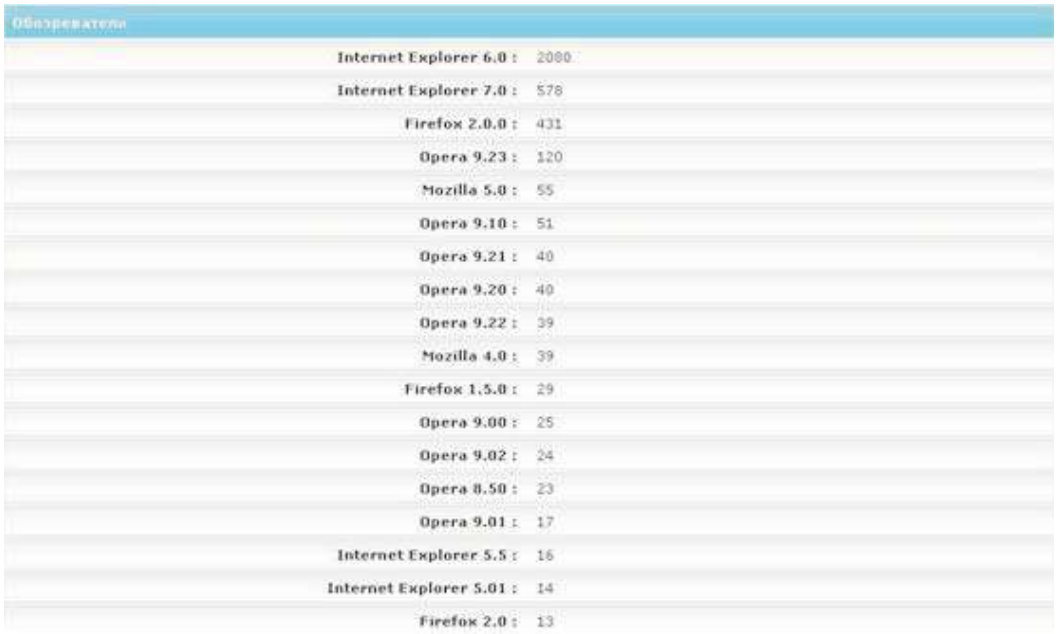
IcePack

Operating System



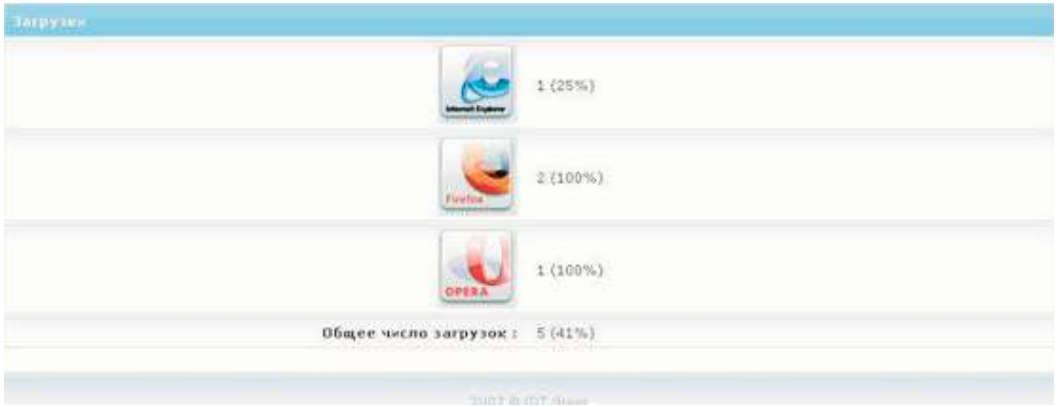
IcePack

Browser



Обозреватель	
Internet Explorer 6.0 :	2080
Internet Explorer 7.0 :	578
Firefox 2.0.0 :	431
Opera 9.23 :	120
Mozilla 5.0 :	55
Opera 9.10 :	51
Opera 9.21 :	40
Opera 9.20 :	40
Opera 9.22 :	39
Mozilla 4.0 :	39
Firefox 1.5.0 :	29
Opera 9.00 :	25
Opera 9.02 :	24
Opera 8.50 :	23
Opera 9.01 :	17
Internet Explorer 5.5 :	16
Internet Explorer 5.01 :	14
Firefox 2.0 :	13

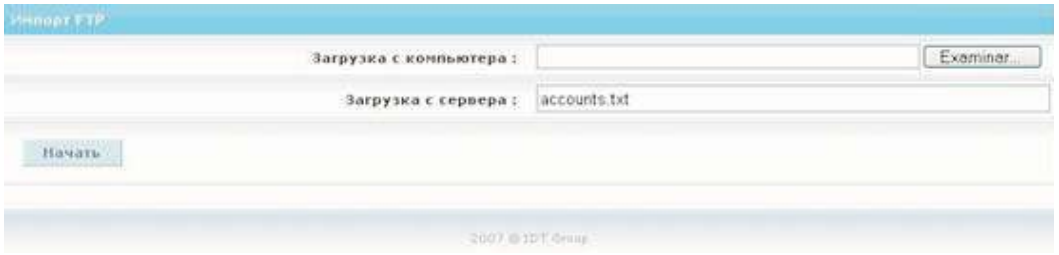
IcePack



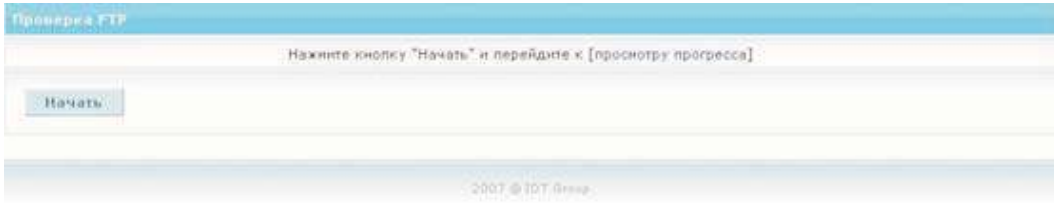
IcePack

Referrers

FTP import



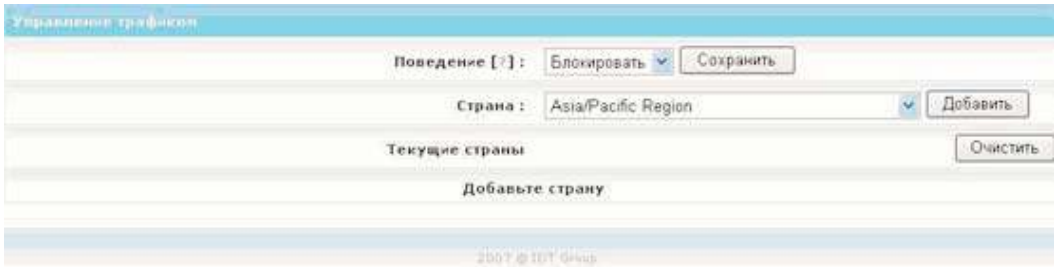
FTP checker



IcePack

iFramer

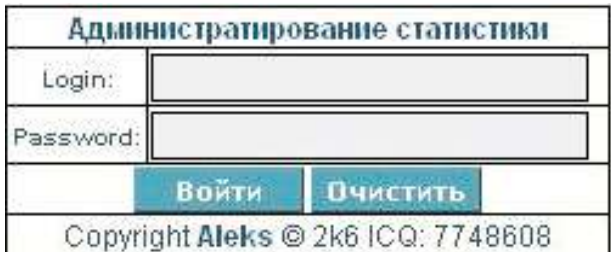
Country blocking

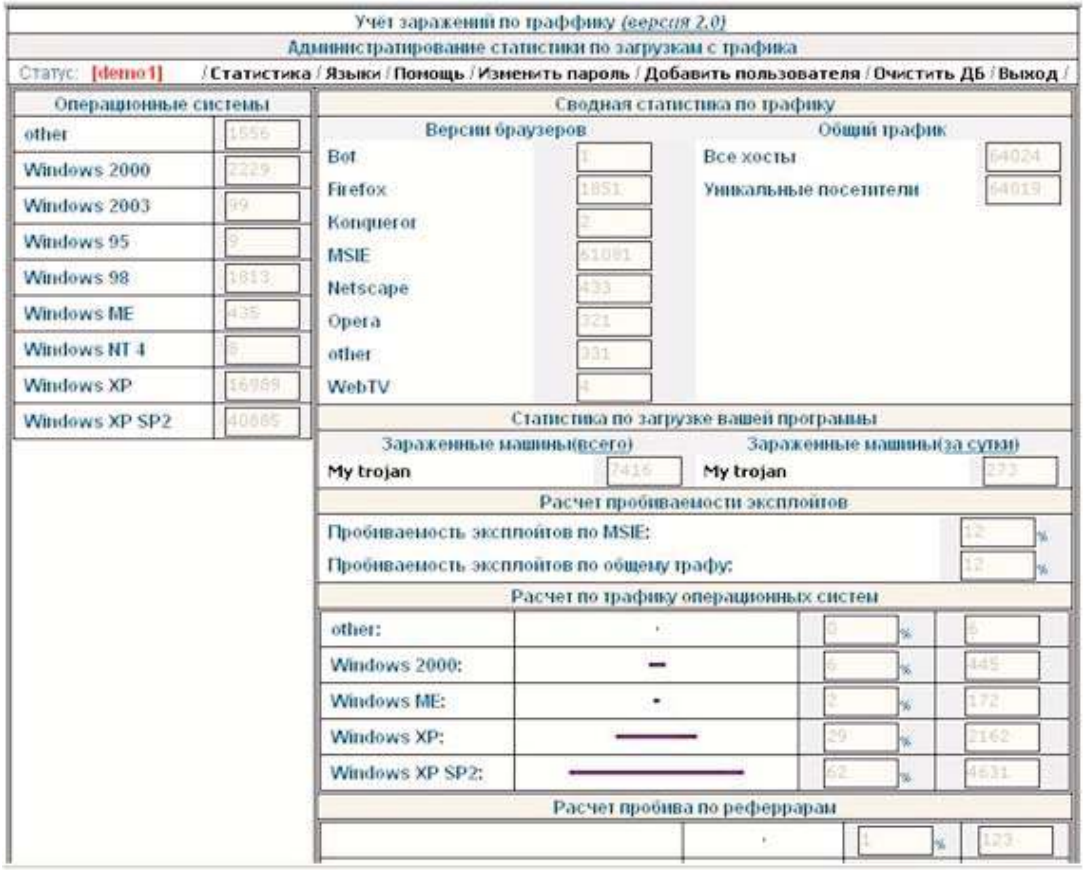


FirePack

FIREPACK
Статистика
Рефери
Очистка статистики
Статистика
По браузерам
Загрузок:0
Пробито:0
Пробив:
0%
Загрузок:0
Пробито:0
Пробив:
0%
Загрузок:0
Пробито:0
Пробив:
0%
Статистика
По операционным системам

Traffic Pro


Администратирование статистики
Login:
Password:
Войти
Очистить
Copyright Aleks © 2k6 ICQ: 7748608


Учет заражений по траффику (версия 2.0)
Администратирование статистики по загрузкам с трафика
Статус: [demo1] / Статистика / Языки / Помощь / Изменить пароль / Добавить пользователя / Очистить ДБ / Выход /
Операционные системы
other
Windows 2000
Windows 2003
Windows 95
Windows 98
Windows ME
Windows NT 4
Windows XP
Windows XP SP2
Сводная статистика по трафику
Версии браузеров
Bot
Firefox
Konqueror
MSIE
Netscape
Opera
other
WebTV
Общий трафик
Все хосты
Уникальные посетители
Статистика по загрузке вашей программы
Зараженные машины(всего)
My trojan
Зараженные машины(за сутки)
My trojan
Расчет пробиваемости эксплойтов
Пробиваемость эксплойтов по MSIE:
Пробиваемость эксплойтов по общему трафу:
Расчет по трафику операционных систем
other:
Windows 2000:
Windows ME:
Windows XP:
Windows XP SP2:
Расчет пробива по реферрарам

Neosploit

Main Menu

Total Stats

Logout

Total Stats

	Username	Traffic							Loads						Acti
							Redirect	Total					Total	Loader hits	
	Active users														
	user1	15483	3686	215	5	4417	0	23806	1778 (11.483%)	0 (0%)	0 (0%)	0 (0%)	1778 (7.468%)	0 (0%)	Res
	user22	3396	344	30	0	215	0	3985	810 (23.851%)	7 (2.034%)	0 (0%)	0 (0%)	817 (20.501%)	0 (0%)	Res
	user212	55	11	19	0	21	0	106	10 (18.181%)	1 (9.090%)	0 (0%)	0 (0%)	11 (10.377%)	0 (0%)	Res
	user5	0	1	0	0	0	0	1	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	Res
	user31	3939	1394	134	3	1199	0	6669	520 (13.201%)	78 (5.595%)	0 (0%)	0 (0%)	598 (8.966%)	0 (0%)	Res
	user32	2453	1256	110	4	1009	0	4832	377 (15.368%)	62 (4.936%)	0 (0%)	0 (0%)	439 (9.085%)	0 (0%)	Res
	Passive users														
	admin	0	0	0	0	0	0	0	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	Res

And many more…

- *E-corepack*
- *Nuclear traffic*
- *Multi exploits pack*
- *Nuclear Malware Kit*
- *Prime Exploit System*
- *Web-Attacker*
- *SmartPack*

A Real Case

The Business of Cybercrime

Infected Team

- **Proxy**
  - 5 - $2.5
  - 1,000 - $300
- **DDoS**
  - 1 hour - $20
  - 24 hours - $100
  - Major projects starting at $200
  - 10 minutes for free!

Infected Team

– **Spam: < 192,000,000 e-mail addresses**

- **USA (home users) – 117,000,000**
  - **US$150 / million messages**
- **USA (enterprises) – 4,000,000**
  - **US$150 / million messages**
- **Western Europe (home users) – 45,000,000**
  - **US$130 / million messages**
- **Western Europe (enterprises) – 902,256**
  - **US$130 / million messages**
- **Russia (home users) – 20,700,000**
  - **US$100 / million messages**
- **Russia (enterprises) – 5,000,000**
  - **US$120 / million messages**

Infected Team

- Personal cryptor ($15, updates $5)
- ABLoader ($60, builder $500)
- RooT iFrame ($25 Russian, $50 English)
- SpamPHP Script ($2)
- FTPCheckIframe ($25)

Infected Team

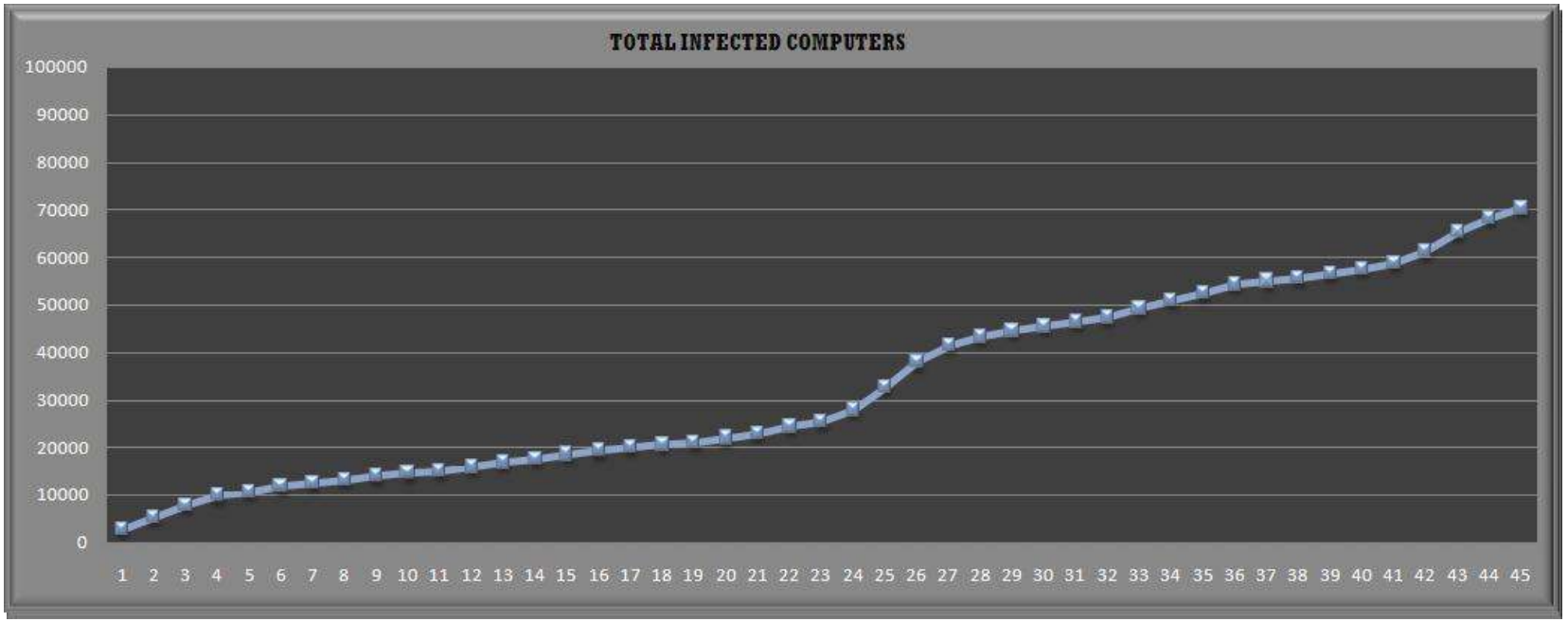
MPack

Dream Downloader

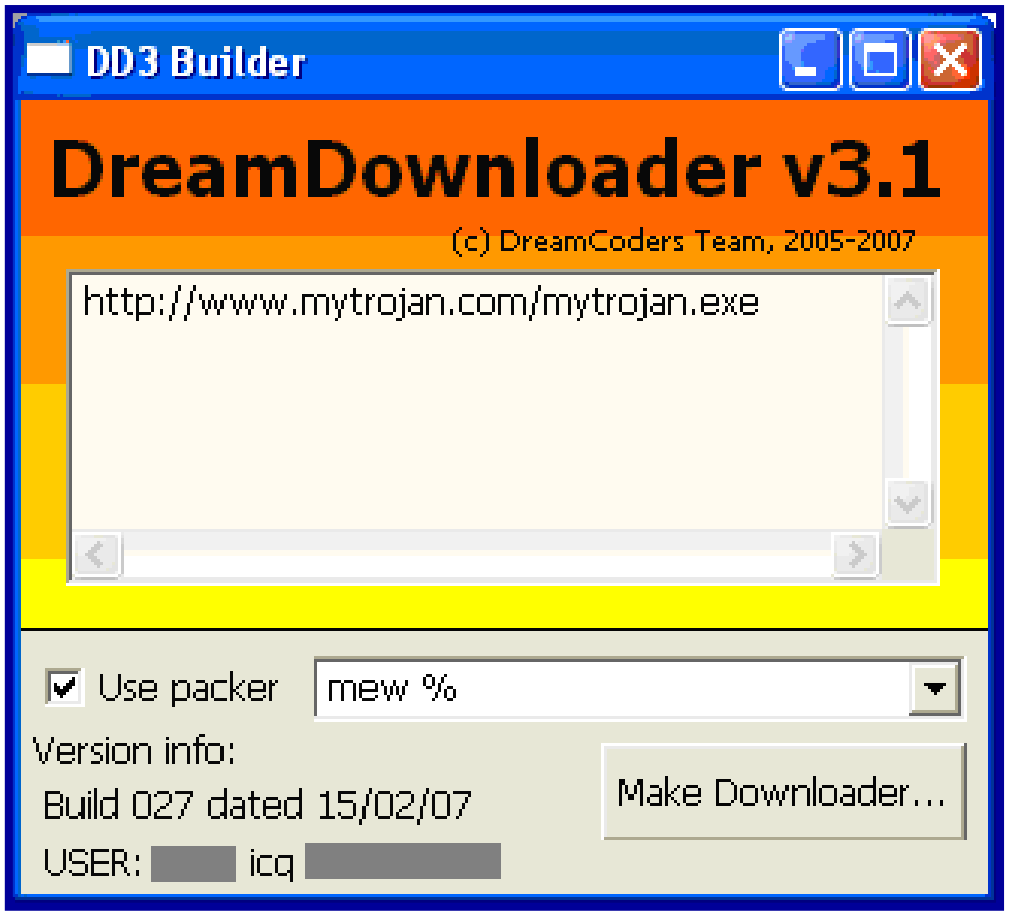
Limbo

Total Investment:
1,500$

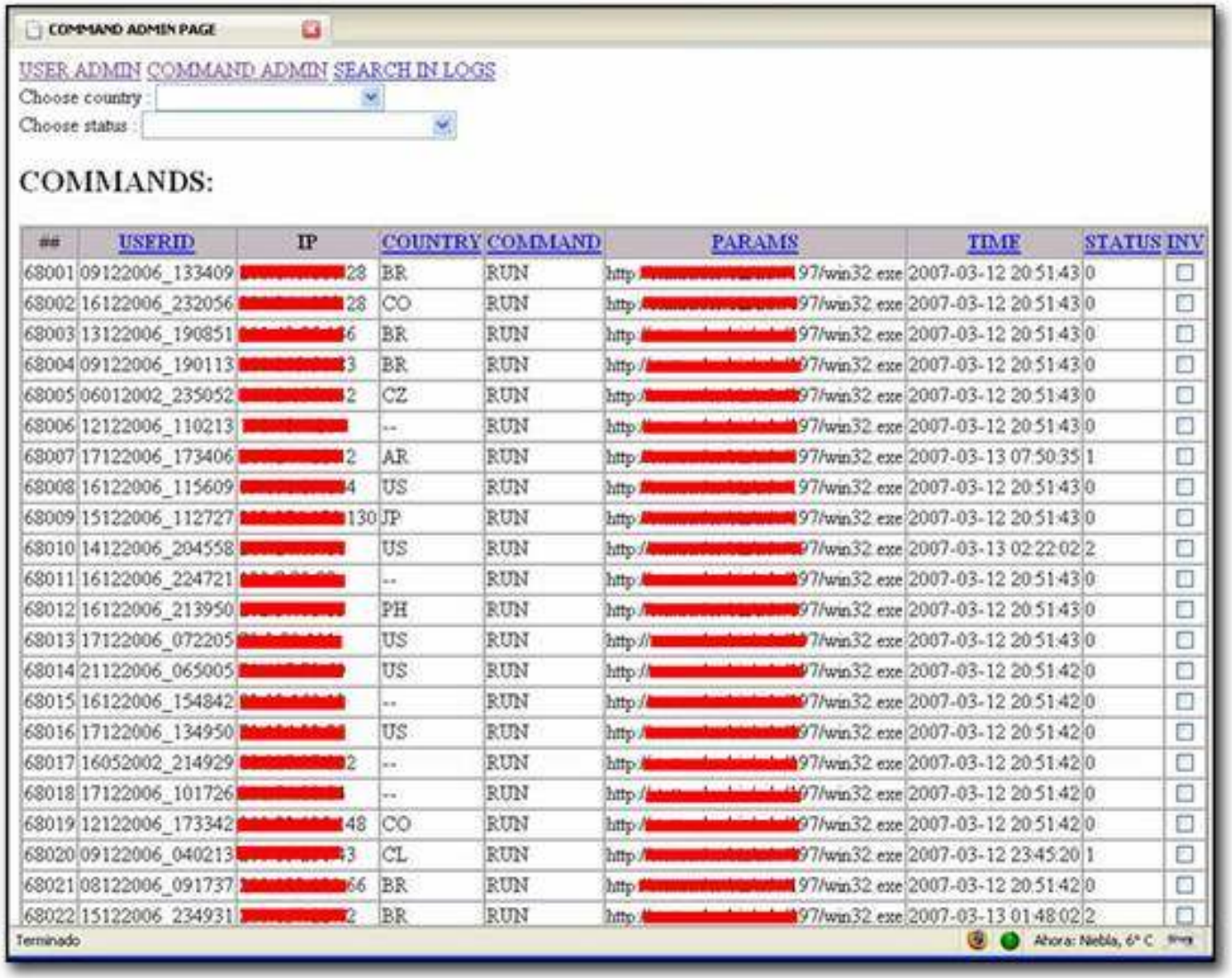
Infected Team



Infected Team



Infected Team



COMMAND ADMIN PAGE

USER ADMIN COMMAND ADMIN SEARCH IN LOGS

Choose country :

Choose status :

COMMANDS:

##	USERID	IP	COUNTRY	COMMAND	PARAMS	TIME	STATUS	INV
68001	09122006_133409	[redacted]28	BR	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:43	0	☐
68002	16122006_232056	[redacted]28	CO	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:43	0	☐
68003	13122006_190851	[redacted]6	BR	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:43	0	☐
68004	09122006_190113	[redacted]3	BR	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:43	0	☐
68005	06012002_235052	[redacted]2	CZ	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:43	0	☐
68006	12122006_110213	[redacted]	--	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:43	0	☐
68007	17122006_173406	[redacted]2	AR	RUN	http [redacted]97/win32.exe	2007-03-13 07:50:35	1	☐
68008	16122006_115609	[redacted]4	US	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:43	0	☐
68009	15122006_112727	[redacted]130	JP	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:43	0	☐
68010	14122006_204558	[redacted]	US	RUN	http [redacted]97/win32.exe	2007-03-13 02:22:02	2	☐
68011	16122006_224721	[redacted]	--	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:43	0	☐
68012	16122006_213950	[redacted]	PH	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:43	0	☐
68013	17122006_072205	[redacted]	US	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:43	0	☐
68014	21122006_065005	[redacted]	US	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:42	0	☐
68015	16122006_154842	[redacted]	--	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:42	0	☐
68016	17122006_134950	[redacted]	US	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:42	0	☐
68017	16052002_214929	[redacted]2	--	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:42	0	☐
68018	17122006_101726	[redacted]1	--	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:42	0	☐
68019	12122006_173342	[redacted]48	CO	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:42	0	☐
68020	09122006_040213	[redacted]3	CL	RUN	http [redacted]97/win32.exe	2007-03-12 23:45:20	1	☐
68021	08122006_091737	[redacted]66	BR	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:42	0	☐
68022	15122006_234931	[redacted]2	BR	RUN	http [redacted]97/win32.exe	2007-03-13 01:48:02	2	☐

Terminado

Ahora: Niebla, 6° C

Infected Team

Win32.exe = Trojan downloader

Installed:

Spammer Trojan
Rogue AntiSpyware

Infected Team

Rogue AntiSpyware

Commissions paid per installation:

$0.40 USA, Canada
$0.20 UK, France, Germany, Italy, Spain, Belgium, Luxembourg, Monaco
$0.05 Austria, Denmark, Finland, Sweden, Norway, The Netherlands
$0.01 China, Korea, Japan

Infected Team

Let's do some maths

China, Korea, Japan:	$0.01 * 70,300 = $703
Finland, Norway…:	$0.05 * 70,300 = $3,515
UK, France…:	$0.20 * 70,300 = $14,060
USA, Canada:	$0.40 * 70,300 = $28,120

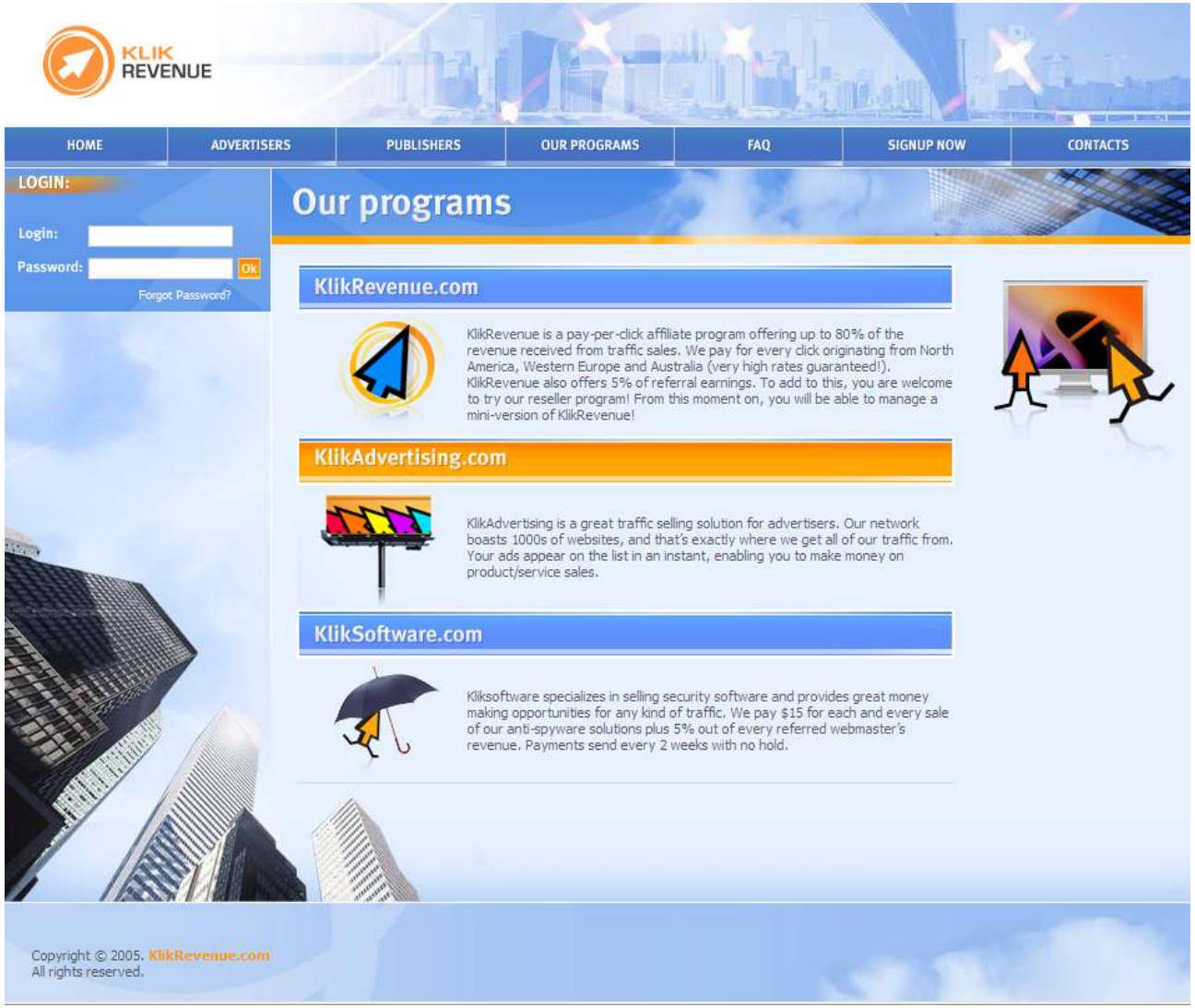
And the same numbers in 30 days…

China, Korea, Japan:	$0.01 * 70,300 * 30 = $21,090
Finland, Norway…:	$0.05 * 70,300 * 30 = $105,450
UK, France…:	$0.20 * 70,300 * 30 = $421,800
USA, Canada:	$0.40 * 70,300 * 30 = $843,600

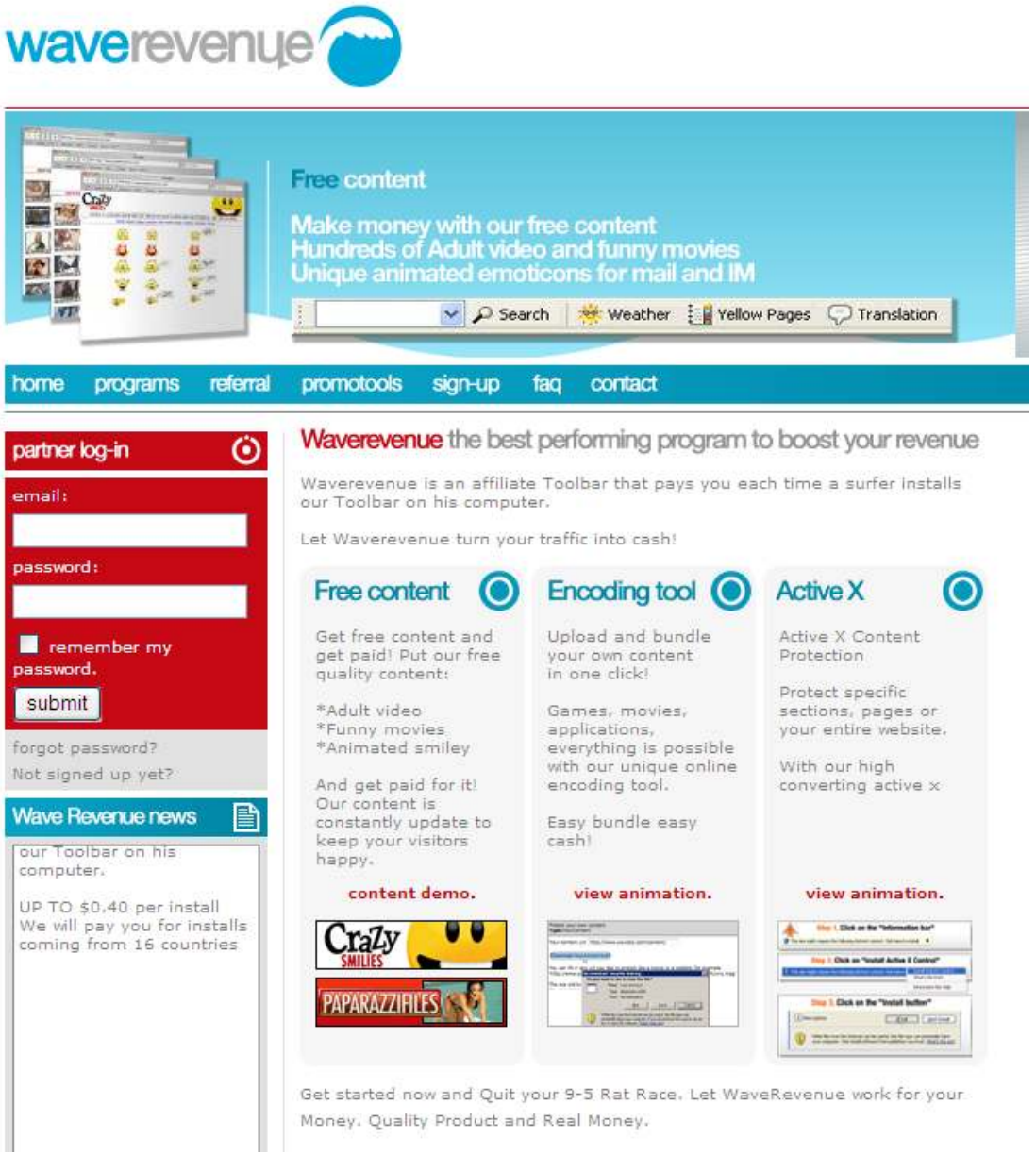
Infected Team

Who's paying these Rogue AntiSpyware installations?

The Business of Cybercrime



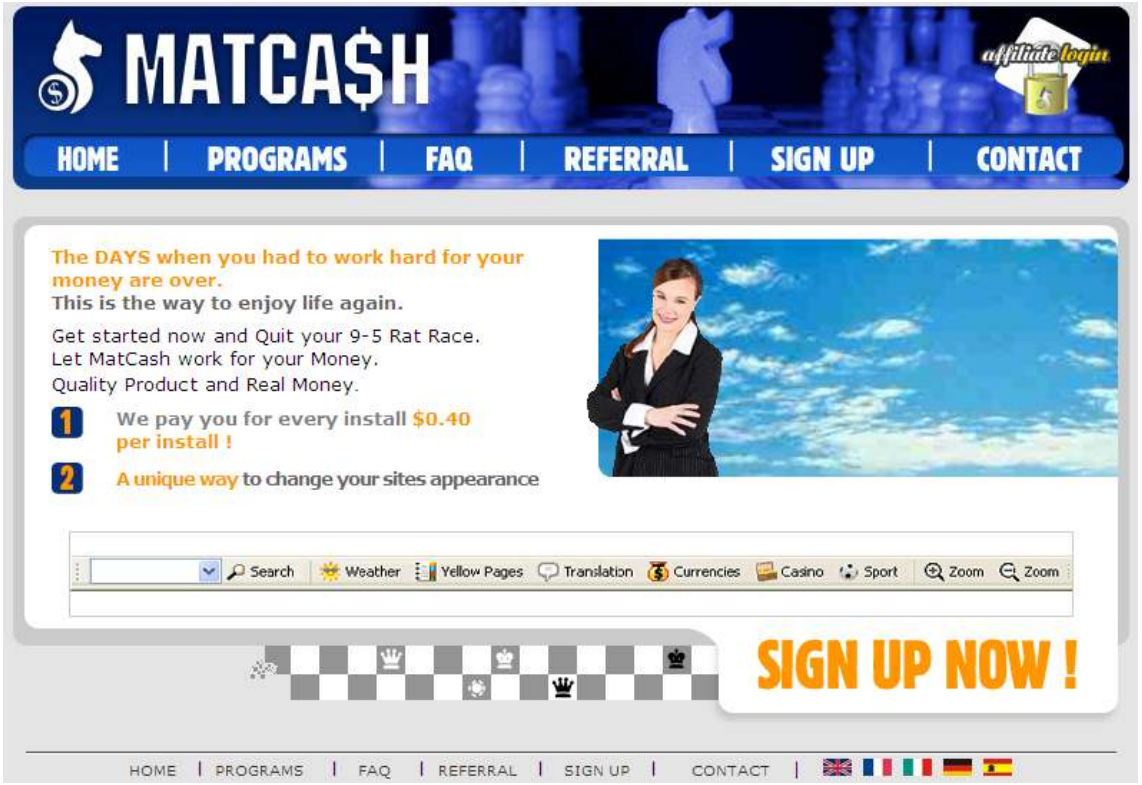
The Business of Cybercrime



The Business of Cybercrime

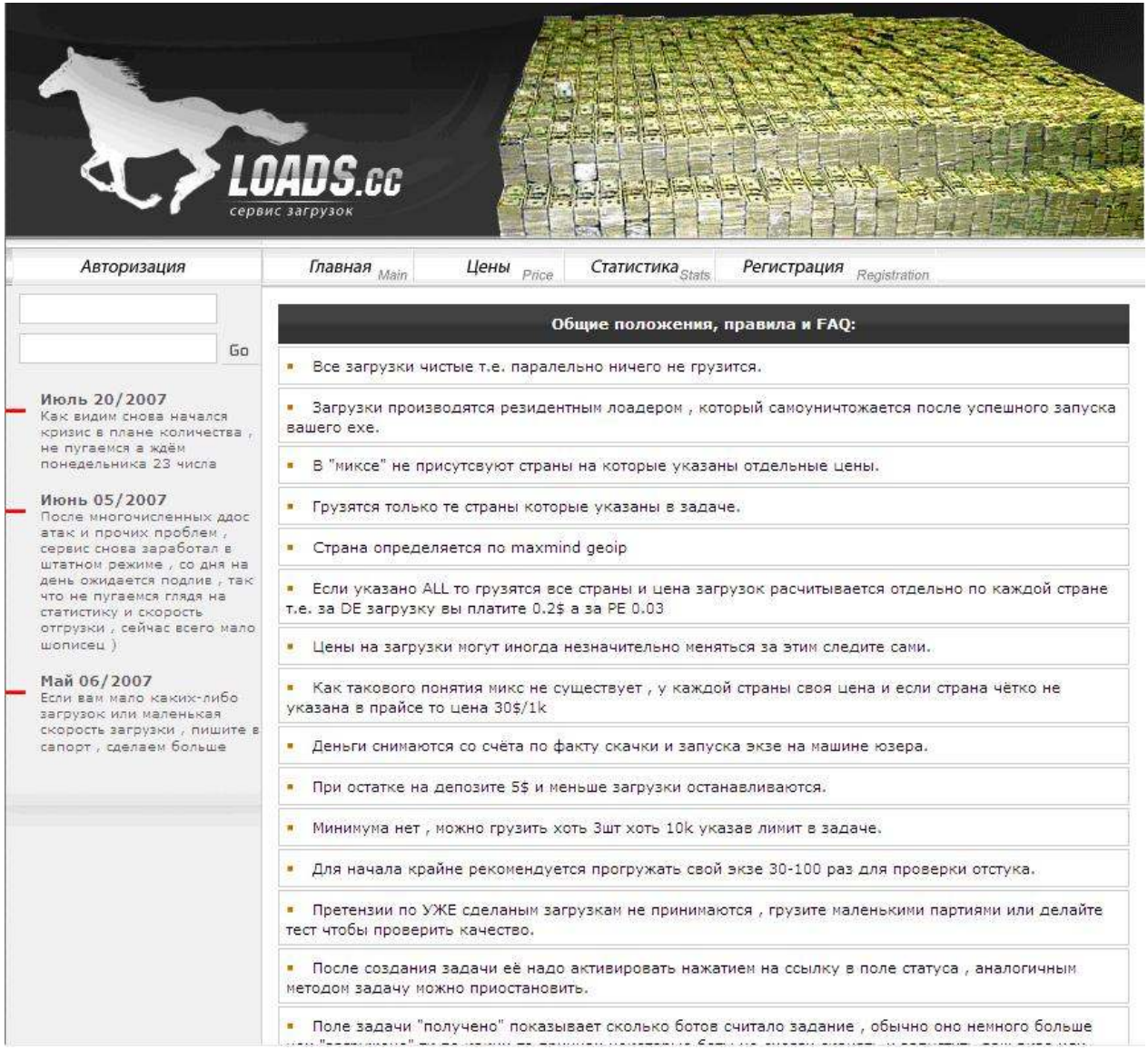
The Business of Cybercrime

The Business of Cybercrime



The Business of Cybercrime

The Business of Cybercrime

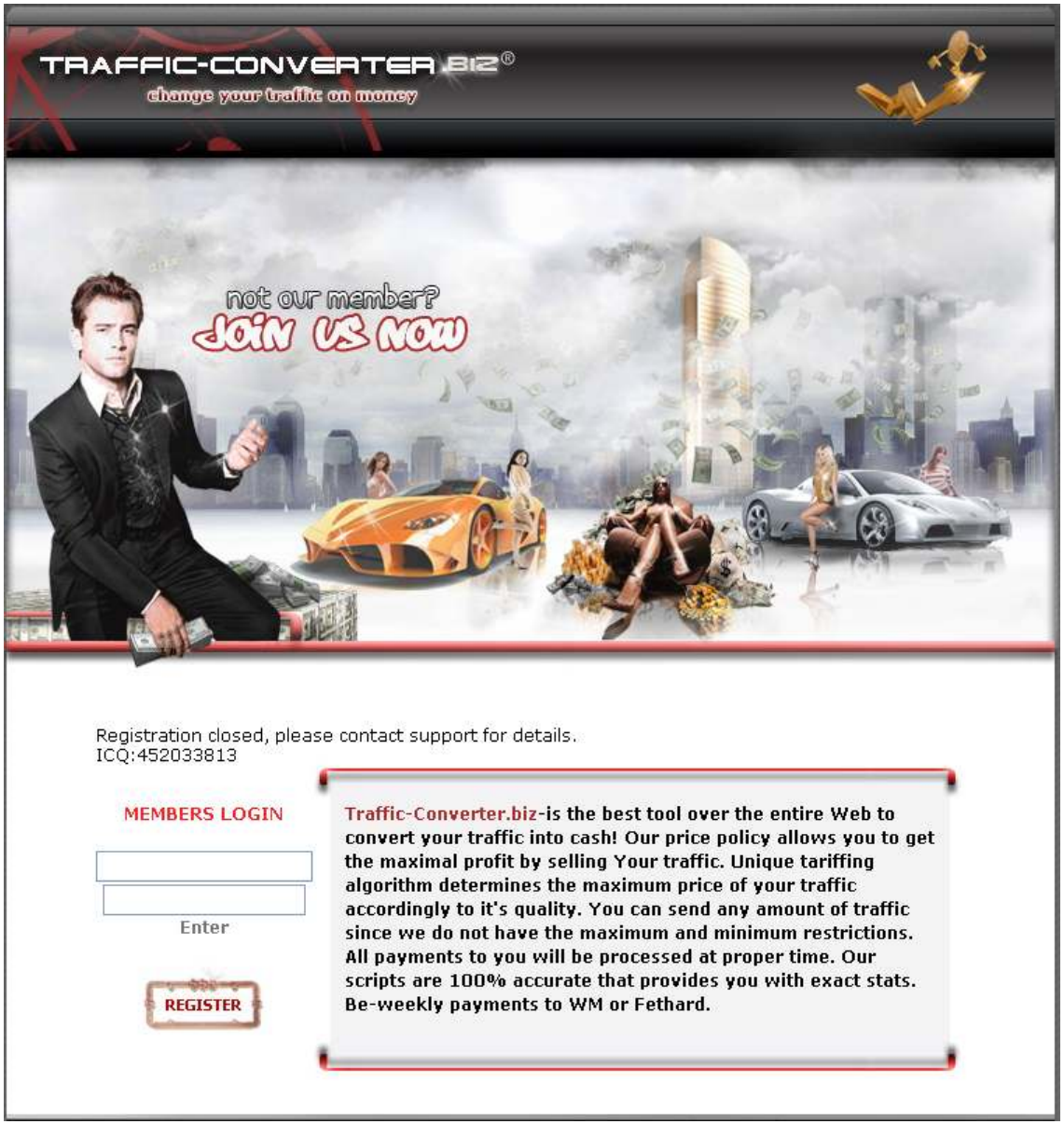


The Business of Cybercrime

The Business of Cybercrime

The Business of Cybercrime

The Business of Cybercrime



The Business of Cybercrime

The Business of Cybercrime

Underground Shopping Cart

Underground Shopping Cart

– Web Attack Toolkits

- **MPack**
  - – US$700
  - – DreamDownloader + US$300
  - – Adding new exploit + US$50-150
  - – Avoid AV detection + US$20-30
- **IcePack**
  - – Lite: US$30
  - – Platinum: US$400
- **FirePack**
  - – US$3,000
- **Traffic Pro**
  - – US$40
- **Ecore**
  - – Bundle US$590 (for a domain / ip with ecore installed).
  - – Domain / additional ip US$490
  - – Help for the installation US$15

Underground Shopping Cart

– Malware

- **Keylogger Teller 2.0**
  - Typical keylogger; it uses stealth techniques and is quite complete: US$40
- **Webmoney Trojan**
  - It captures Webmoney accounts: US$500 (the first 100 will obtain it for US$400!)
- **WMT-spy:**
  - Another Trojan to obtain WebMoney accounts, but cheaper than the previous one
  - Trojan US$5
  - Updates US$5
  - Builder US$10
- **SNATCH TROJAN:**
  - It steals passwords and has rootkit functionalities: US$600
- **Limbo:**
  - Banking Trojan, keylogger, etc. US$1,000
- **Pinch:**
  - Very complete Trojan. US$30
  - Update: US$5

Underground Shopping Cart

- Joiner and encryption

  - **Polaris**
    - Polymorphic encryption for your executables — US$20
  - **Freejoiner**
    - Hides your executables joining them with other files — US$30 + US$5 per update
  - **My joiner**
    - Other joiner belonging to the creator of Pinch — US$10
  - **Pity Joiner**
    - Just another joiner — US$7

Underground Shopping Cart

- Other Tools

  - **FTP checker**
    - Program to validate stolen FTP accounts. — US$15
  - **Dream Bot Builder**
    - Floods servers — US$500 + US$25 per update

Underground Shopping Cart

– Spam

- Spam Hosting: US$200
- Dedicated spam server US$500
- +10,000,000 Mails per day US$600
- SMS spam (per message) US$0.2
- ICQ (1,000,000) US$150

Mailing lists for spam: (US$)

ACCOUNTS	USA	GERMANY	RUSSIA	UKRANIA
1,000,000	100	100	100	100
3,000,000	200	200	200	200
5,000,000	300	300	300	-
8,000,000	500	500	500	-
16,000,000	900	-	-	-
32,000,000	1500	-	-	-

Underground Shopping Cart

– Accounts

- **FTP accounts:**
  - US$1 per account
- **Icq numbers:**
  - From US$1 to US$10 (depending on the ICQ number)
- **RapidShare premium accounts:**
  - 1 month - US$5
  - 2 months - US$8
  - 3 months - US$12
  - 6 months - US$18
  - 1 year - US$28
- **Online Shop accounts**
  - (megashop.ru, bolero.ru, cup.ru, etc. ALL RUSSIAN): - US$50 each
- **50MB of Limbo Trojan logs**
  - US$30 (contains email accounts, bank account numbers, credit card numbers, etc. A percentage is guaranteed)

Underground Shopping Cart

- Already finished?

  - **Credit Cards**
    - VISA / MASTERCARD
      - 1 - 10 cards — US$2 (per card)
      - 10 - 100 cards — US$1.5 (per card)
    - AMEX
      - 1 - 10 cards — US$2.5 (per card)
      - 10 - 100 cards — US$2 (per card)

  - **Passports:**
    - Black and white: US$2
    - Color: US$5

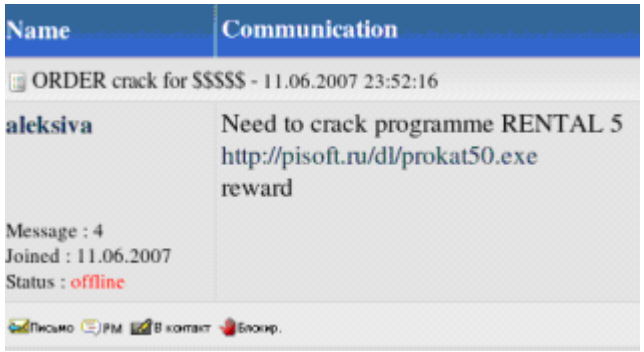
Where to buy?

- отображение размера логов
- поиск по логам
- архивация логов
- фильтрация по стране
- возможность посылки логов на email
- статистику по зараженим
- просмотр сграбленных emails
- дачу заметок выбранным пользователям
- время последнего захода
- отображение в постраничном виде (скажем по 200 записей на страницу)
- возможность грабить все в один файл (по желанию)
- сортировка логов по разным критериям
- удаление всех логов

Данные команды скачиваются с хостинга через определенный интервал времени и выполняются; в админке можно видеть статус команды для определенного пользователя - скачана\скачана но не выполнена\выполнена.

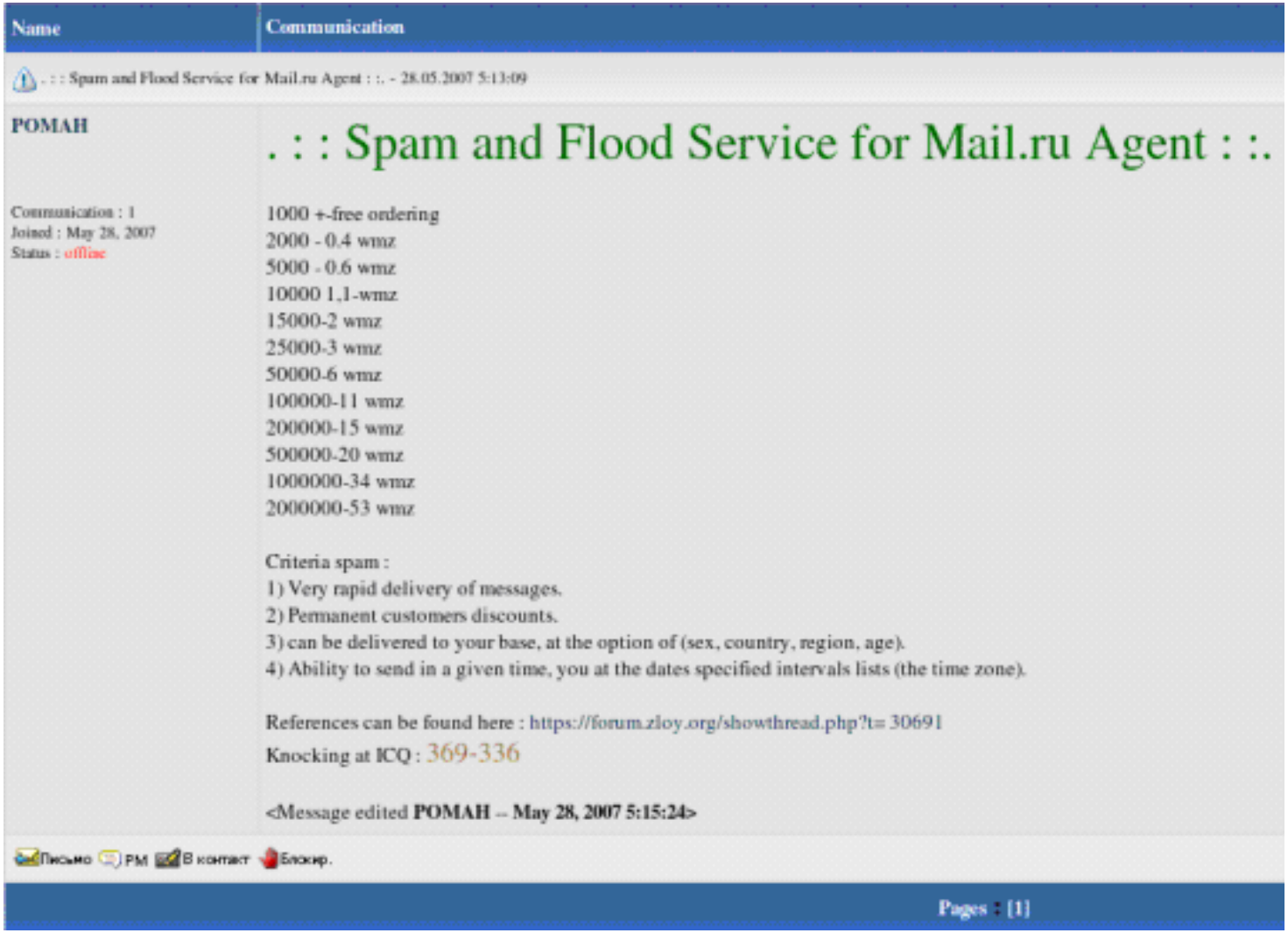
Билд - 500 wmz
ICQ [redacted]
Кому интересно, могу дать посмотреть тестовую админку.

The Business of Cybercrime



Name	Communication
ORDER crack for $$$$$ - 11.06.2007 23:52:16	
aleksiva Message : 4 Joined : 11.06.2007 Status : offline	Need to crack programme RENTAL 5 http://pisoft.ru/dl/prokat50.exe reward
Письмо ICQ В контакт Блокир.	

The Business of Cybercrime

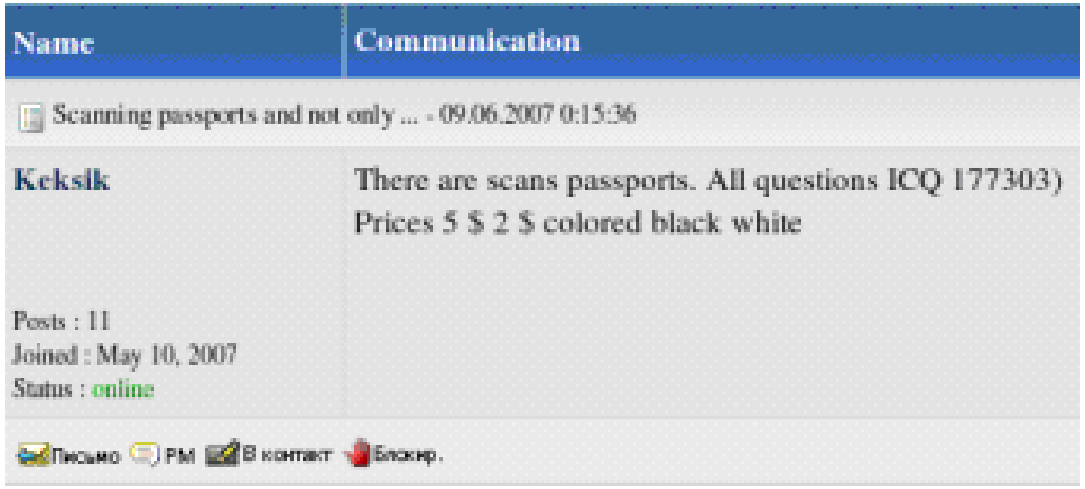


Name	Communication
. : : Spam and Flood Service for Mail.ru Agent : :. - 28.05.2007 5:13:09	
POMAH Communication : 1 Joined : May 28, 2007 Status : offline	. : : Spam and Flood Service for Mail.ru Agent : :. 1000 +-free ordering 2000 - 0.4 wmz 5000 - 0.6 wmz 10000 1,1-wmz 15000-2 wmz 25000-3 wmz 50000-6 wmz 100000-11 wmz 200000-15 wmz 500000-20 wmz 1000000-34 wmz 2000000-53 wmz Criteria spam : 1) Very rapid delivery of messages. 2) Permanent customers discounts. 3) can be delivered to your base, at the option of (sex, country, region, age). 4) Ability to send in a given time, you at the dates specified intervals lists (the time zone). References can be found here : https://forum.zloy.org/showthread.php?t= 30691 Knocking at ICQ : 369-336 <Message edited **POMAH -- May 28, 2007 5:15:24**>
Письмо PM В контакт Блокир.	
	Pages : [1]

The Business of Cybercrime

Name	Communication
Service sales CC! ! ! - 09.06.2007 20:53:51	
fektih Communication : 1 Joined : 09.06.2007 Status : offline	Service sales CC! ! ! I wish to invite you to board with cvv2 Usa, (Walid - 90-95%). there VISA - MC PRICE : 1-10 cards - $ 2 (per unit) 10-100 cards - $ 1.5 (each) DISCOVER-AMEX 1-10 cards - $ 2.5 (each) 10-100 cards - $ 2 (per unit) Nevalid change within 3 days! STANDING POKUPATELYAM DISCOUNTS! ! ! We guarantee the sale only in one hand and a high validity. if we can make a selection in the state, bin etc.! ! ! pounding in ICQ : 498-007-015 Write to OFF-line. Answer
Письмо PM В контакт Блокир.	

The Business of Cybercrime



Name	Communication
Scanning passports and not only ... - 09.06.2007 0:15:36	
Keksik Posts : 11 Joined : May 10, 2007 Status : online	There are scans passports. All questions ICQ 177303) Prices 5 $ 2 $ colored black white
Письмо PM В контакт Блокир.	

The Business of Cybercrime

Name	Communication
Selling scans paspartov ... - 03.04.2007 1:42:46	
PosTerminal Message : 7 Joined : 03.04.2007 Status : offline	There paspartov scans are available : USA, Russia, Ukraine, England, Australia Zealand, Nigeria, Shvedtsii, China, Kazak --- Added some countries Drive license : Australia Germany Lithuania Norway Russia Thailand Ukraine England USA Estonia Sweden

70 Mage 70 Warrior 70 Shaman 70 Warlock all full epic

Seller of this item? Sign in for your status

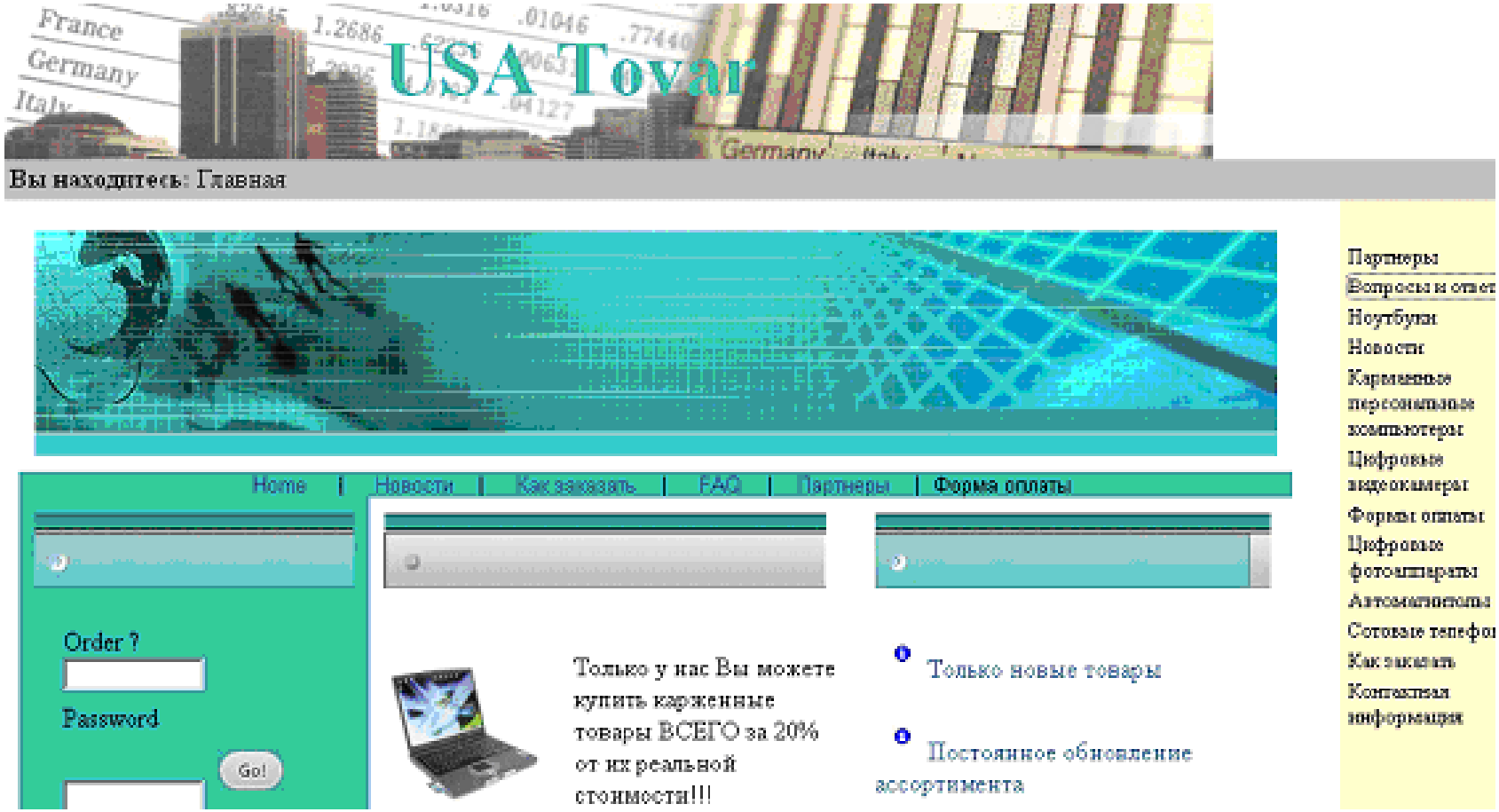
1 of 4

View larger picture

Starting bid:	US $27,000.00
	PayPal account required
Your maximum bid:	US $ [ ] Place Bid >
	(Enter US $27,000.00 or more)
	Get $10 back on this item Apply
End time:	2 hours 40 mins (Feb-18-08 07:54:44 PST)
Shipping costs:	Free Other (see description) Service to United States
Ships to:	United States
Item location:	McKeesport, PA, United States
History:	0 bids
You can also:	Watch This Item
	Get mobile or IM alerts | Email to a friend

Listing and payment details: Show

The Business of Cybercrime



PANDA SECURITY | One step ahead.

Thanks!

Luis Corrons

luis.corrons@pandasecurity.com

PandaLabs Blog:

http://www.pandalabs.com