Croatian National CERT

ACDC project

Darko Perhoc, Head of National CERT
CISSP, CEH, CCNP Security R&S,CCDP

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Croatian National CERT (HR-CERT)

- mission: Promoting and preserving information security of public information systems in Croatia
- staff: 9 employees and 2 external co-worker
- established 2008. in accordance with the Croatian Information security act as an organisational unit within CARNet
- 1996 - 2008, CARNet CERT had the role of national CERT until foundation of HR-CERT

Information security act

V NATIONAL CERT

Article 20

(1) CERT is the national authority competent for prevention and protection from computer threats to public information systems in the Republic of Croatia.

(2) CERT is a separate organizational unit that shall be established within the Croatian Academic and Research Network (hereinafter: CARNet).

(3) CERT shall harmonize procedures in case of security computer incidents in public information systems occurring in the Republic of Croatia or in other countries and organizations when they are related to the Republic of Croatia.

(4) CERT shall harmonize the work of the bodies that are working on the prevention and protection from computer threats to public information systems security in the Republic of Croatia and shall determine the rules and modes of joint performance.

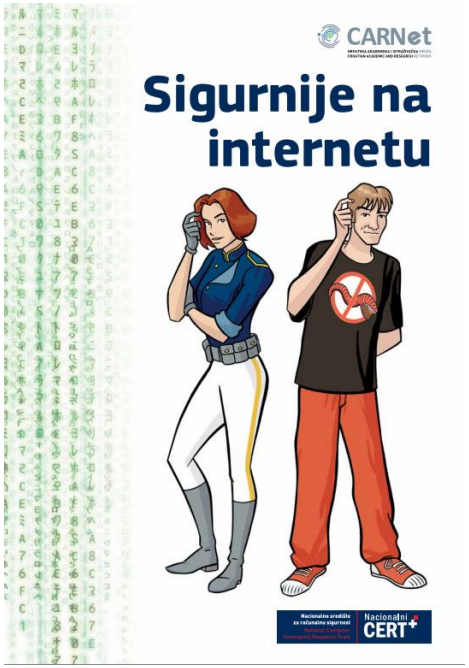
HR-CERT Constituency

- Croatian residents(home end users)
- business subjects (companies, banks etc.)
- ISPs and their Internet abuse services
- Hosting providers
- public institutions and other organizations
- all Internet users in Croatia except:
  - government bodies (→ ZSIS CERT)

HR-CERT proactive measures

- constantly monitoring the computer security field and disseminating information(web news)
- publishing security alerts for discovered software vulnerabilities and patches if available – advisories(mailing list, more than 2000 advisories per year)
- vulnerability scans(CARNet external and internal)
- publishing white papers for various audiences (general public, technical staff, managers)
- publishing brochures about information security on Internet for Internet end users

4 issued brochures about internet security distributed via daily newspapers



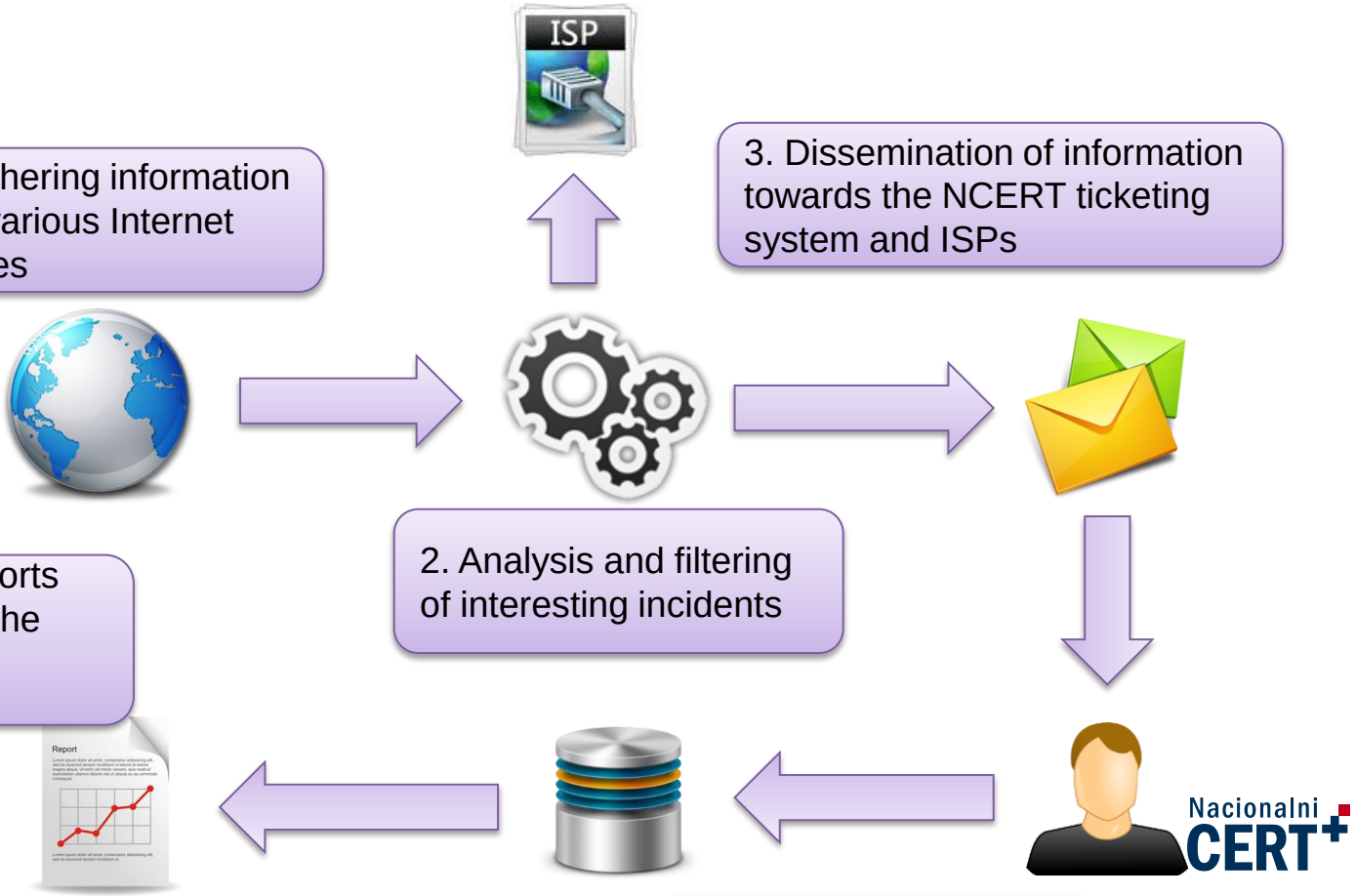
CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

HR-CERT Reactive measures

- Collection and correlation of incident information related to HR-CERT constituency
- Main CERTs task: analysis and removal of malicious content/software from internet(asap)
- coordination of solving major incidents including at least one side from Croatia
- Forensics regarding network, php, javascript, html, logs, malware etc.

Collection of incident data by early detection system(SRU@HR)



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Incident types handeled by National CERT

- attacks against particular services, hosts or entire network infrastructures (DoS,DDoS)
- server compromise (web, mail, ftp, ssh…)
- client compromise (malware analysis)
- unwanted network activities (port and vulnerability scans, brute force attacks)
- network misuse (sending spam etc.)
- phishing and other Internet frauds

Cooperation with other organizations

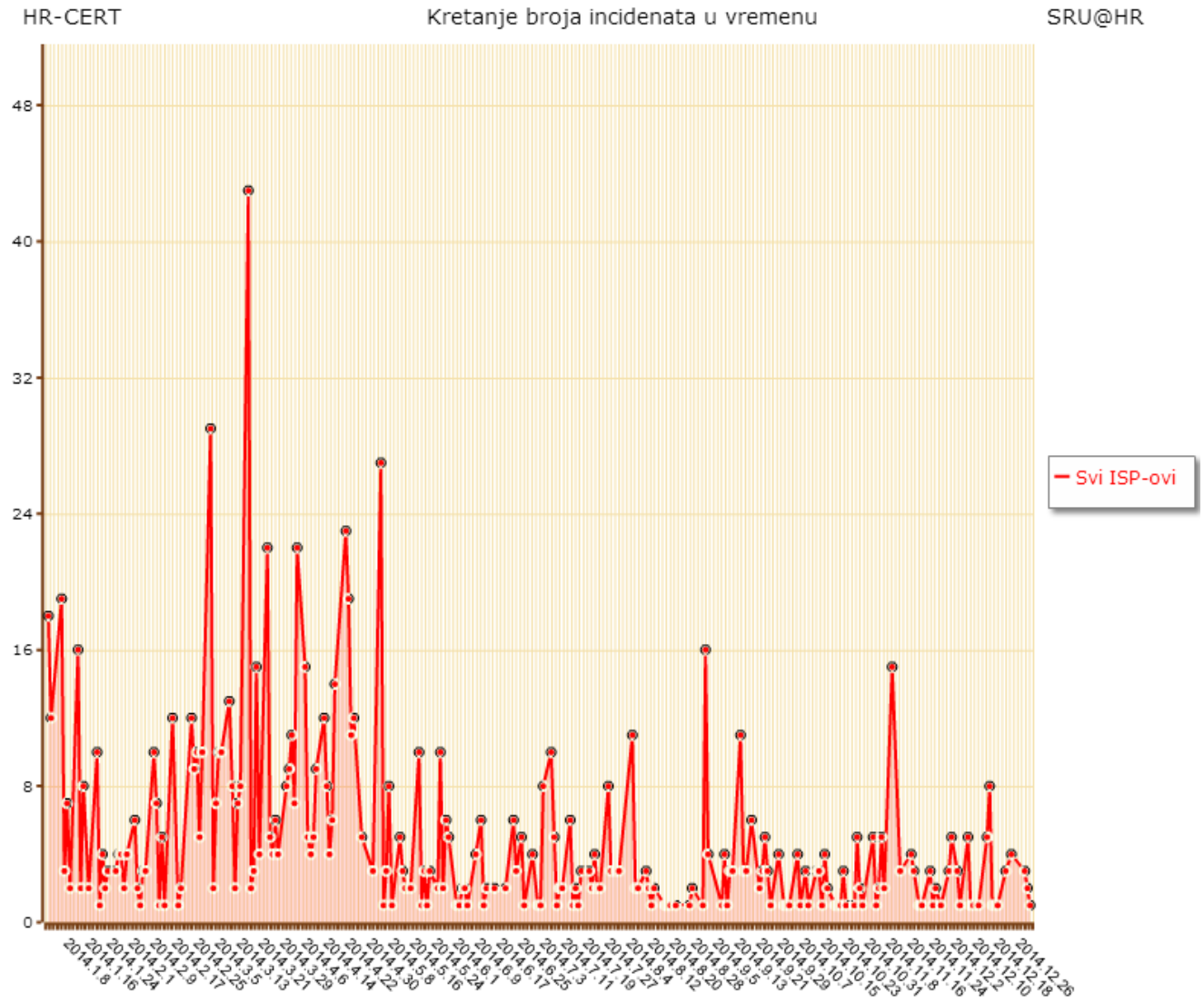
- Relevant authorities in Croatia:
  - Information Systems Security Bureau - ZSIS CERT
  - Office of the National Security Council – UVNS

  Signed MoU with:
  - Ministry of Interior
  - Ministry of defence
- International cooperation with foreign CERTs:
  - Forum of Incident Response and Security Teams (FIRST)
  - TERENA Working Group TF-CSIRT
- Cooperation with ENISA, CERT-EU

SRU@HR Early incident detection system

- based on passive Internet monitoring
- in-house developed system for detecting known incidents on the Internet related to Croatia
- fetches data from 20+ internet feeds about incidents
- daily analysis of over 100.000 incident reports
- provides graphical views of incident occurrences, distribution across ISPs or hosting providers, trends in number of incidents and bots

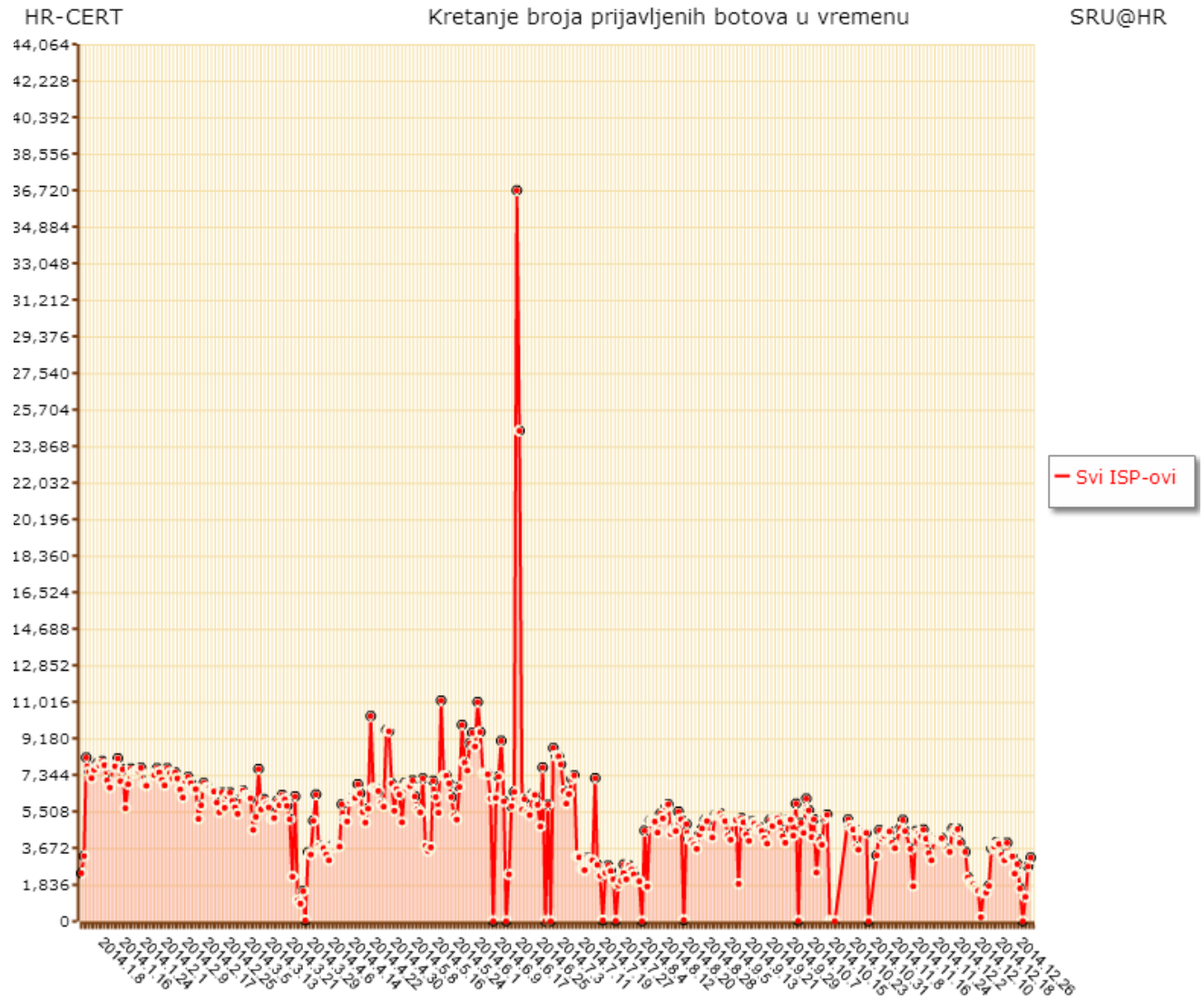
Reported incidents in the year 2014



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

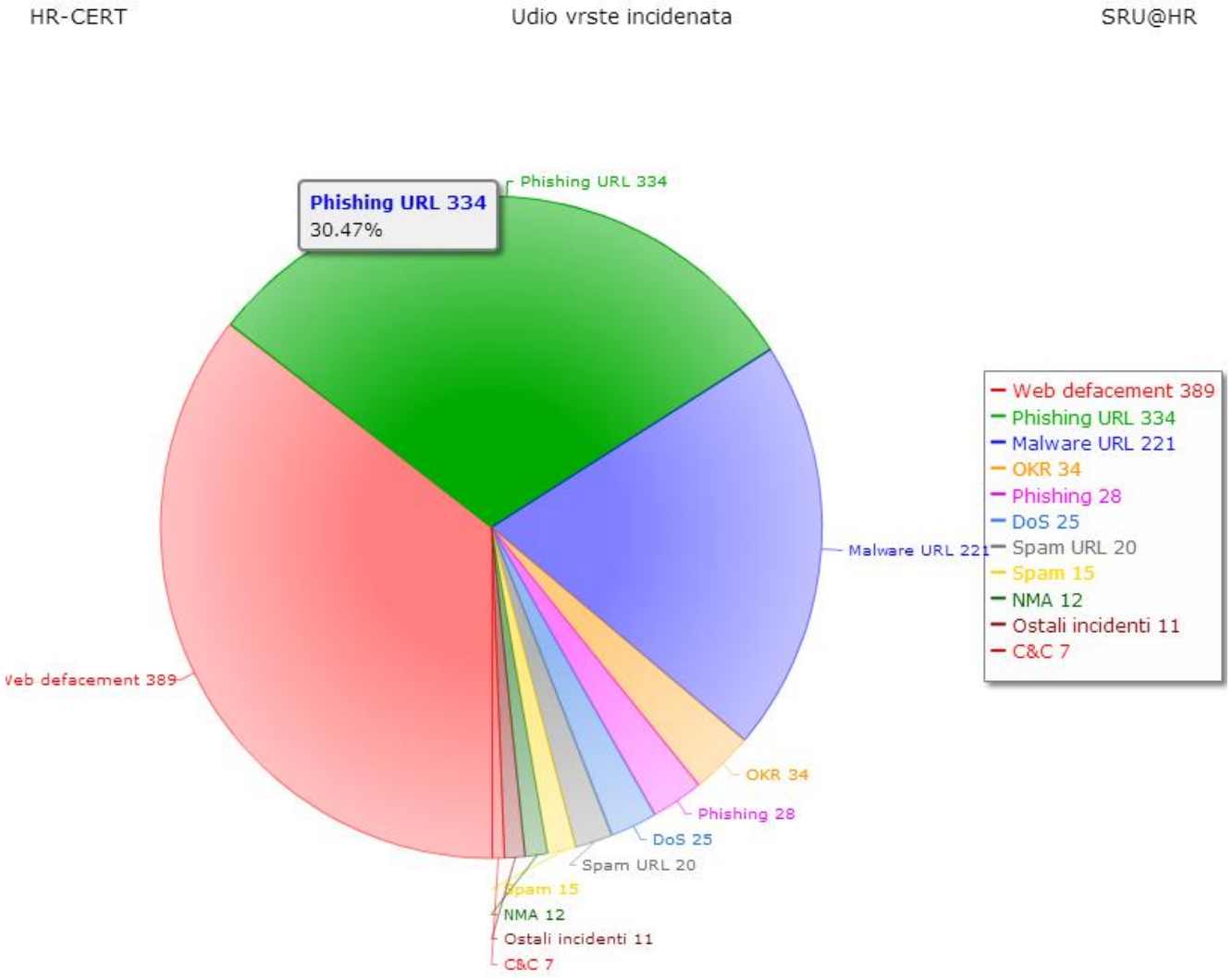
Bot trend in the year 2014



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

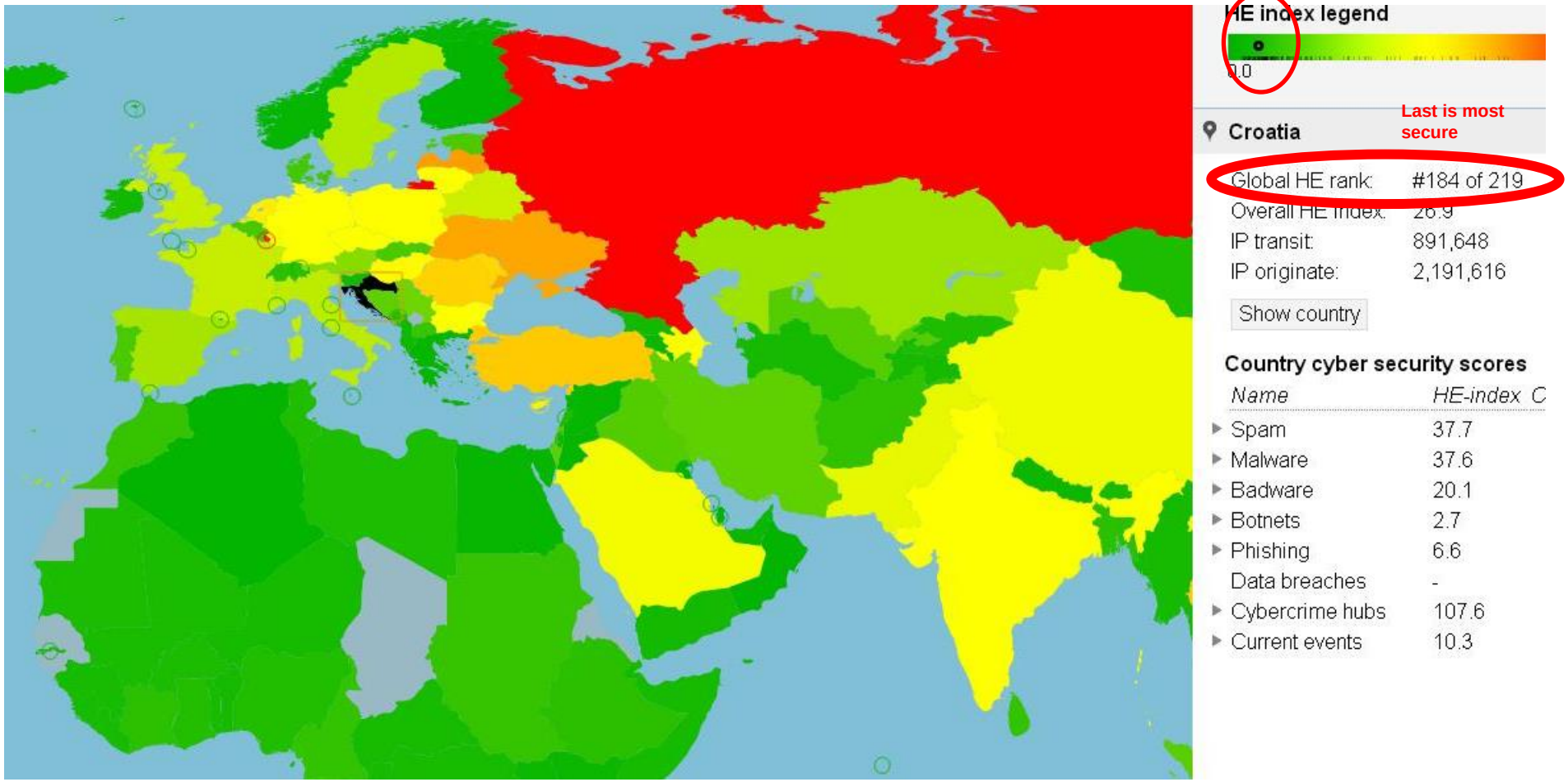
Incident types in the year 2014



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

globalsecuritymap.com



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Current activity-participation in ACDC project

ACDC

the Advanced Cyber Defence Centre
a European project co-funded through the
CIP/PSP programme.

cip competitiveness and innovation framework programme 2007–2013

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

ACDC

ACDC-advanced cyber defence centre I

UNITING A COMMUNITY OF
Internet Service Providers, CERTs, law enforcement agencies, IT providers, National Research and Education Networks (NRENs), Academia and critical infrastructure operators.

28 PARTNERS

14 COUNTRIES DEPLOYING 8 SUPPORT CENTRES

15,5 M€ TOTAL COST

Contact point
Coordinator eco - Association of the German Internet Industry

Web sites
ACDC Botnet Services www.botfree.eu
ACDC www.acdc-project.eu

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT+

ACDC

ACDC-advanced cyber defence centre II

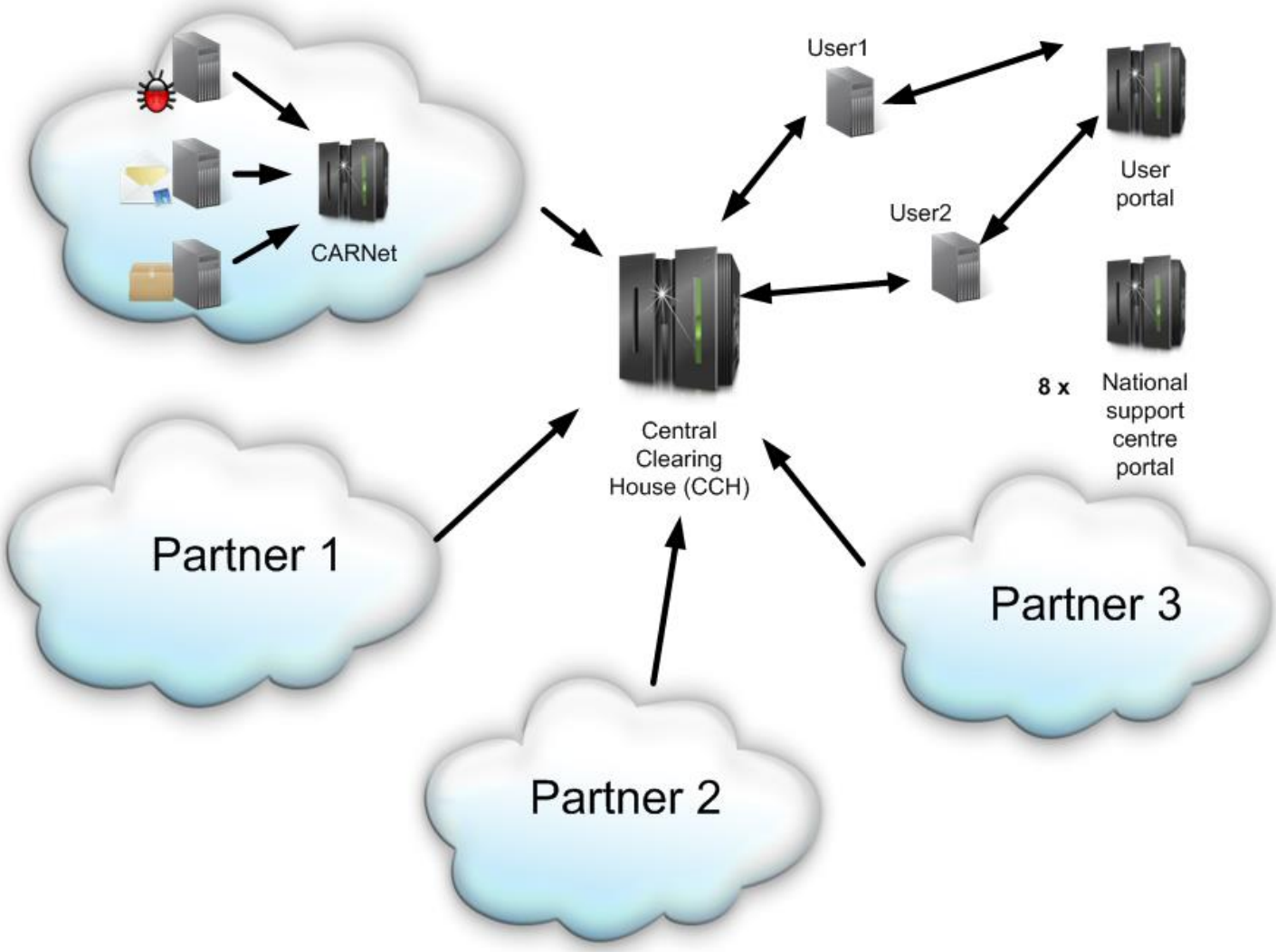
- The goal of the project is to implement EU-wide platform for fighting against botnets
- CARNet with National CERT is the member of ACDC consortium
- CARNet role in ACDC project:
  - development and operations of 3 network sensors
    - spamtrap
    - web honeypot
    - passive DNS
  - Development and operations of ACDC anti-botnet national support centre

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT+

ACDC

ACDC platform architecture

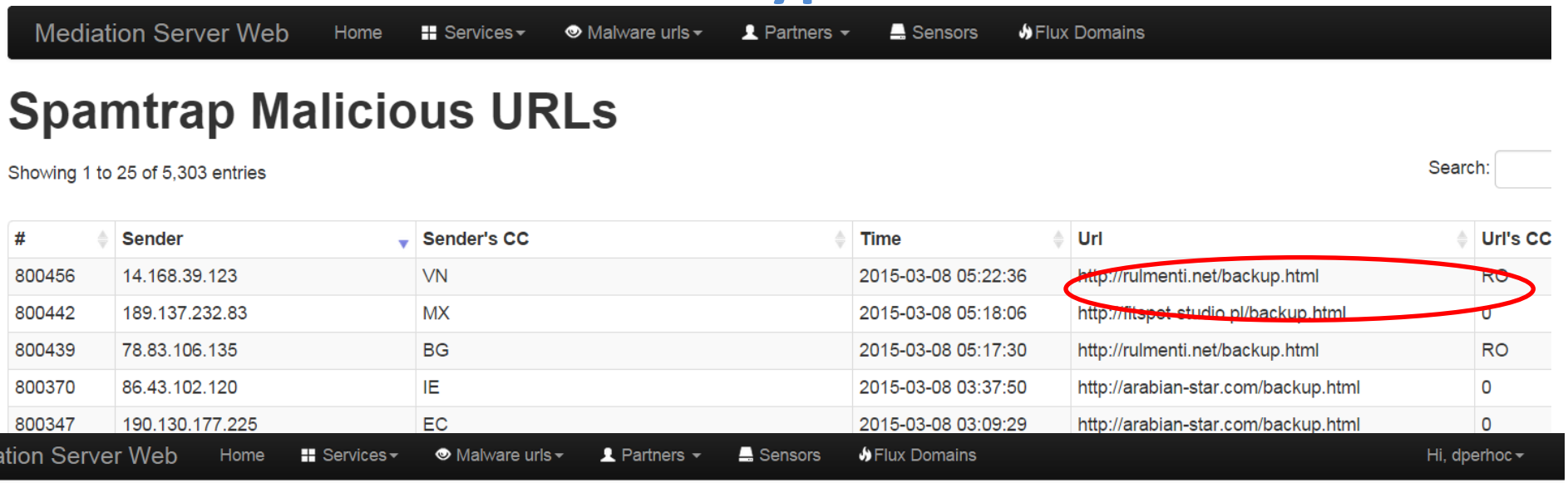


CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

ACDC

Malware URL detected by spamtrap and honeypot



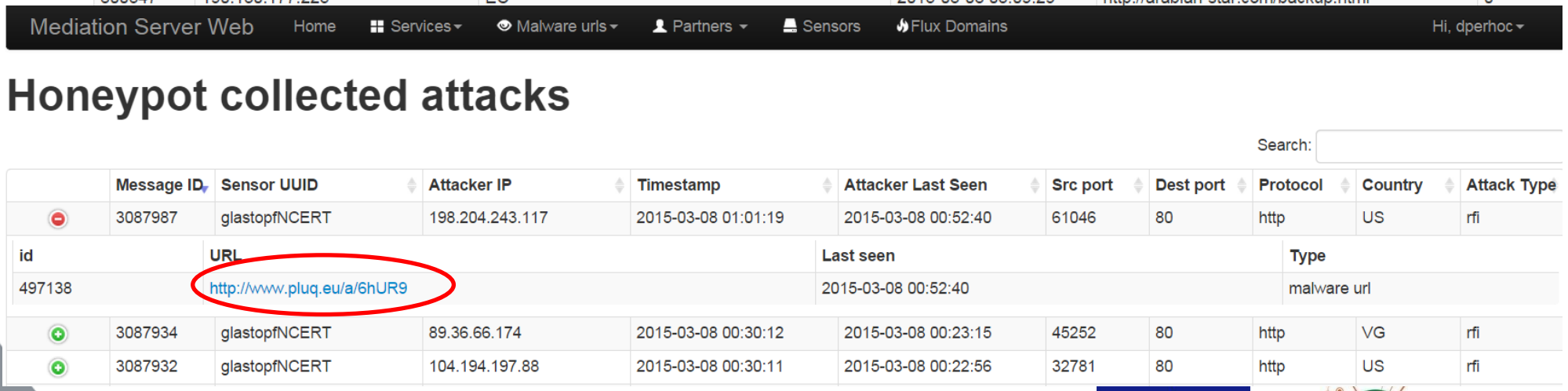
Mediation Server Web | Home | Services | Malware urls | Partners | Sensors | Flux Domains

Spamtrap Malicious URLs

Showing 1 to 25 of 5,303 entries

Search:

#	Sender	Sender's CC	Time	Url	Url's CC
800456	14.168.39.123	VN	2015-03-08 05:22:36	http://rulmenti.net/backup.html	RO
800442	189.137.232.83	MX	2015-03-08 05:18:06	http://fitspot-studio.pl/backup.html	0
800439	78.83.106.135	BG	2015-03-08 05:17:30	http://rulmenti.net/backup.html	RO
800370	86.43.102.120	IE	2015-03-08 03:37:50	http://arabian-star.com/backup.html	0
800347	190.130.177.225	EC	2015-03-08 03:09:29	http://arabian-star.com/backup.html	0



Mediation Server Web | Home | Services | Malware urls | Partners | Sensors | Flux Domains | Hi, dperhoc

Honeypot collected attacks

Search:

	Message ID	Sensor UUID	Attacker IP	Timestamp	Attacker Last Seen	Src port	Dest port	Protocol	Country	Attack Type
⊖	3087987	glastopfNCERT	198.204.243.117	2015-03-08 01:01:19	2015-03-08 00:52:40	61046	80	http	US	rfi

id	URL	Last seen	Type
497138	http://www.pluq.eu/a/6hUR9	2015-03-08 00:52:40	malware url

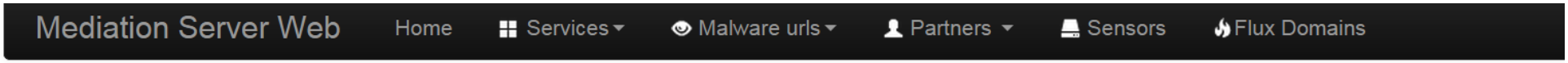
⊕	3087934	glastopfNCERT	89.36.66.174	2015-03-08 00:30:12	2015-03-08 00:23:15	45252	80	http	VG	rfi
⊕	3087932	glastopfNCERT	104.194.197.88	2015-03-08 00:30:11	2015-03-08 00:22:56	32781	80	http	US	rfi

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

ACDC

Detected fast-flux domains



Collected Fast Flux Domains

Showing 1 to 30 of 560 entries

Search:

#	Name	First Seen	Last Seen	Detected
826	firehordersg.com	2015-02-16 11:13:36	2015-02-26 12:40:54	2015-02-24 10:00:01
825	toyootacrusernow.net	2015-02-08 04:27:59	2015-02-08 04:27:59	2015-02-15 10:00:02
823	ronaldogo.ru	2015-02-06 07:38:24	2015-02-20 07:13:38	2015-02-13 10:00:01
824	bandcump.com	2015-02-05 20:17:17	2015-02-05 20:17:17	2015-02-13 10:00:01
822	hxqbvhgjihsk.xyz	2015-01-29 22:38:57	2015-01-29 22:38:57	2015-02-06 10:00:01
820	vaihers.ru	2015-01-24 03:32:58	2015-01-24 11:48:34	2015-01-31 10:00:02
821	gefomm.ru	2015-01-24 03:32:57	2015-01-24 11:00:32	2015-01-31 10:00:02
819	luposer.su	2015-01-23 20:17:54	2015-02-18 14:28:55	2015-01-31 10:00:02
818	ns1.brikebrak.ru	2015-01-16 08:53:41	2015-01-17 21:05:02	2015-01-23 10:00:01
817	ns1.salthashdns.ru	2015-01-15 20:48:09	2015-01-16 05:44:17	2015-01-23 10:00:01

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK
Nacionalni CERT
ACDC

National support centre portal for ACDC

www.antibot.hr

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

ACDC

Contact information and portals

- address: Jurišićeva 3, 10000 Zagreb, Croatia
- phone: +385 1 6661 650
- web: www.cert.hr
- e-mail: cert@cert.hr

- ACDC NSC: www.antibot.hr

questions?

Thank You!