PREGLED STANJA SIGURNOSTI U RH IZ PERSPEKTIVE NACIONALNOG CERT-A

Marko Stanec – Nacionalni CERT
CARNet

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Nacionalni CERT

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Osnovni podaci

- Osnovan 2009. godine temeljem ZIS-a
- Odjel unutar CARNeta
- Obrada incidenata na Internetu
- Očuvanje informacijske sigurnosti u RH
- 15 ljudi – 2 tima
  - Služba za obradu incidenata
  - Služba za analitiku i forenziku

Nacionalni CERT

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

NCERT – djelokrug rada – što radimo

- Uklanjanje malicioznog sadržaja s Interneta
- Obrada incidenata na Internetu
- Diseminacija informacija
- Forenzika, analiza malvera, mrežnog prometa, logova...

NCERT – djelokrug rada – što ne radimo

- ✗ Operativno rješavanje problema
- ✗ Briga o sigurnosti pojedinih sustava
- ✗ Kažnjavanje problematičnih korisnika
- ✗ Arbitraža u sporovima
- ✗ Pokretanje krivičnih prijava

Što još NCERT može?

DNS pravilnik

Članak 9.

…

CARNet je ovlašten **privremeno deaktivirati domenu** u slučaju kada osobito opravdani interesi to zahtijevaju…

…

…daljnje korištenje domene moglo bi nanijeti **ozbiljnu i teško nadoknadivu štetu CARNetu ili trećim osobama**.

…

Privremena **deaktivacija traje dok se ne riješe sporna pitanja** ili dok na drugi način njezina daljnja primjena nije više potrebna.

(https://dns.hr/portal/files/HRTLDpravilnik2010hr.pdf)

Suradnja s relevantnim tijelima

- Ured Vijeća za nacionalnu sigurnost – **UVNS**
- Zavod za sigurnost informacijskih sustava – **ZSIS**
- Ministarstvo unutarnjih poslova RH – **MUP RH**
- FIRST
- TI
- CSIRT Network

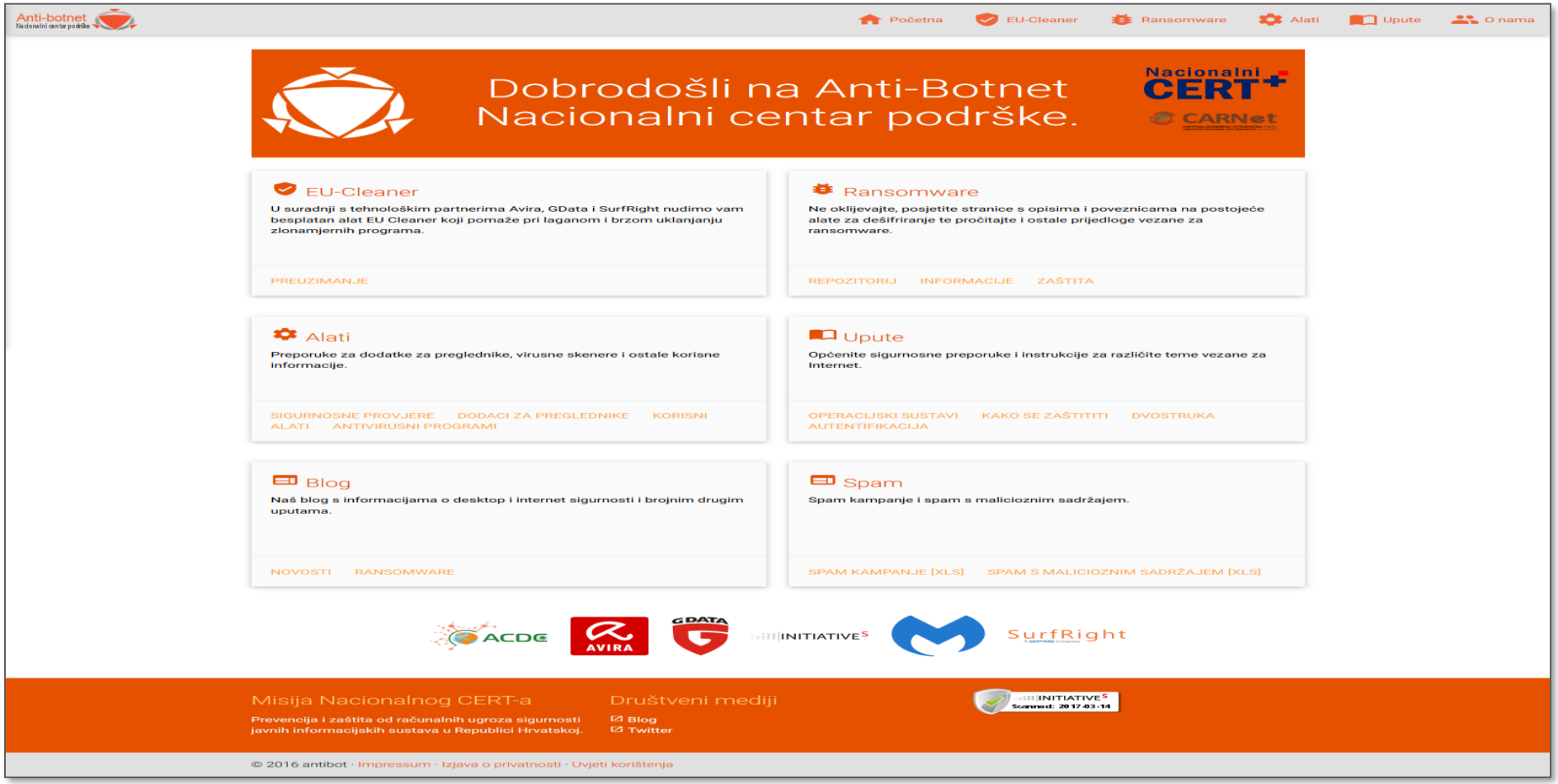
Suradnja unutar i izvan RH

- Nacionalna strategija kibernetičke sigurnosti
- **e-Škole**: Uspostava sustava razvoja digitalno zrelih škola (pilot projekt)
- **GEANT** 4
- **CEKOM**
- **CEF**
- Vježba **Cyber Europe 2016**
- Vježba **Cyber Coalition 2016**

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

www.antibot.hr



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

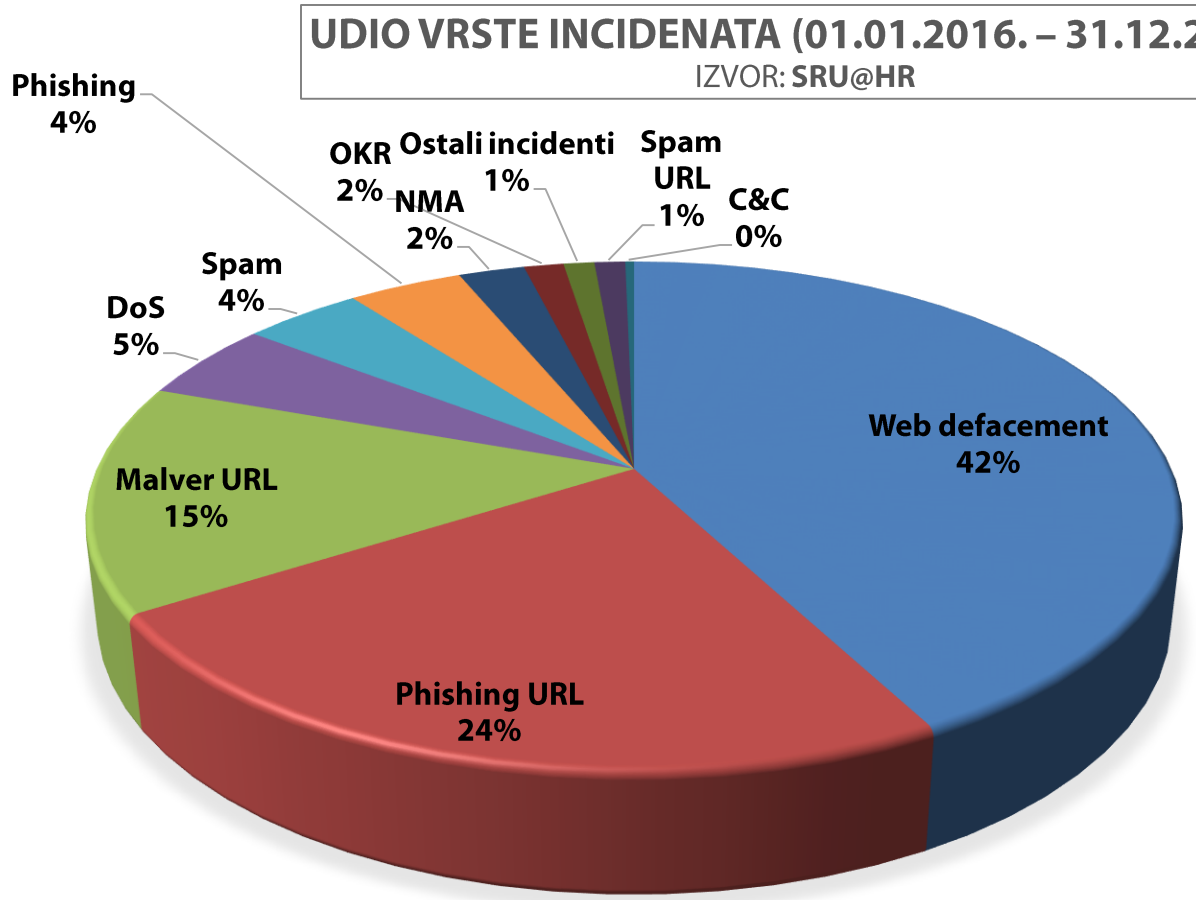
Nacionalni CERT

Pregled incidenata u 2016.

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Pregled incidenata po tipu u 2016.



Tip incidenta	Broj	Trend
Web defacement	271	↑
Phishing URL	152	↓
Malver URL	93	↓
DoS	32	↓
Spam	27	↓
Phishing	26	↓
NMA	15	↑
OKR	9	↑
Ostali incidenti	7	↑
Spam URL	7	↓
C&C	2	↓
Ukupno	**641**	↓

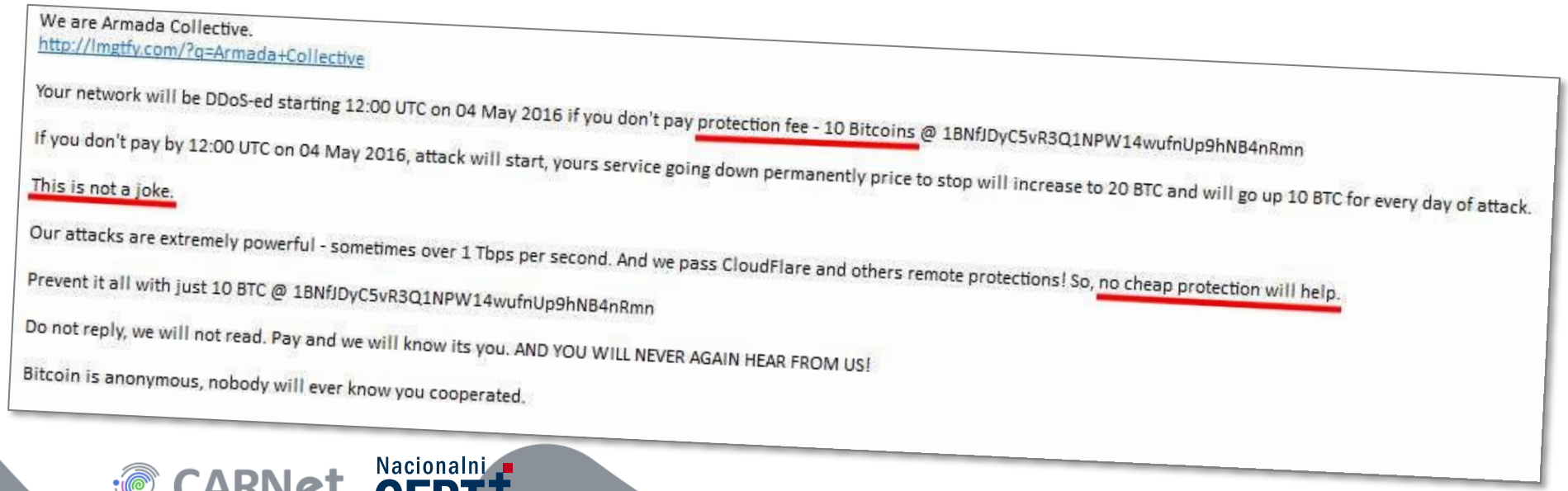
CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

DDoS napadi i prijetnje

- Zabilježen povećan broj DDoS napada

  (TCP SYN flood, UDP flood, NTP amplification, SSDP reflection)
- „e-reketarenja”



We are Armada Collective.
http://lmgtfy.com/?q=Armada+Collective

Your network will be DDoS-ed starting 12:00 UTC on 04 May 2016 if you don't pay protection fee - 10 Bitcoins @ 1BNfJDyC5vR3Q1NPW14wufnUp9hNB4nRmn

If you don't pay by 12:00 UTC on 04 May 2016, attack will start, yours service going down permanently price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per second. And we pass CloudFlare and others remote protections! So, no cheap protection will help.

Prevent it all with just 10 BTC @ 1BNfJDyC5vR3Q1NPW14wufnUp9hNB4nRmn

Do not reply, we will not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

Phishing kampanje

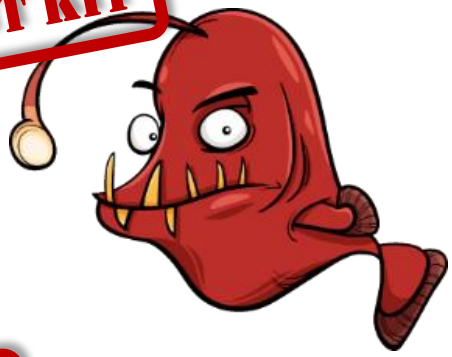
CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Kompromitirani poslužitelji

ANGLER EXPLOIT KIT



NUCLEAR EXPLOIT KIT

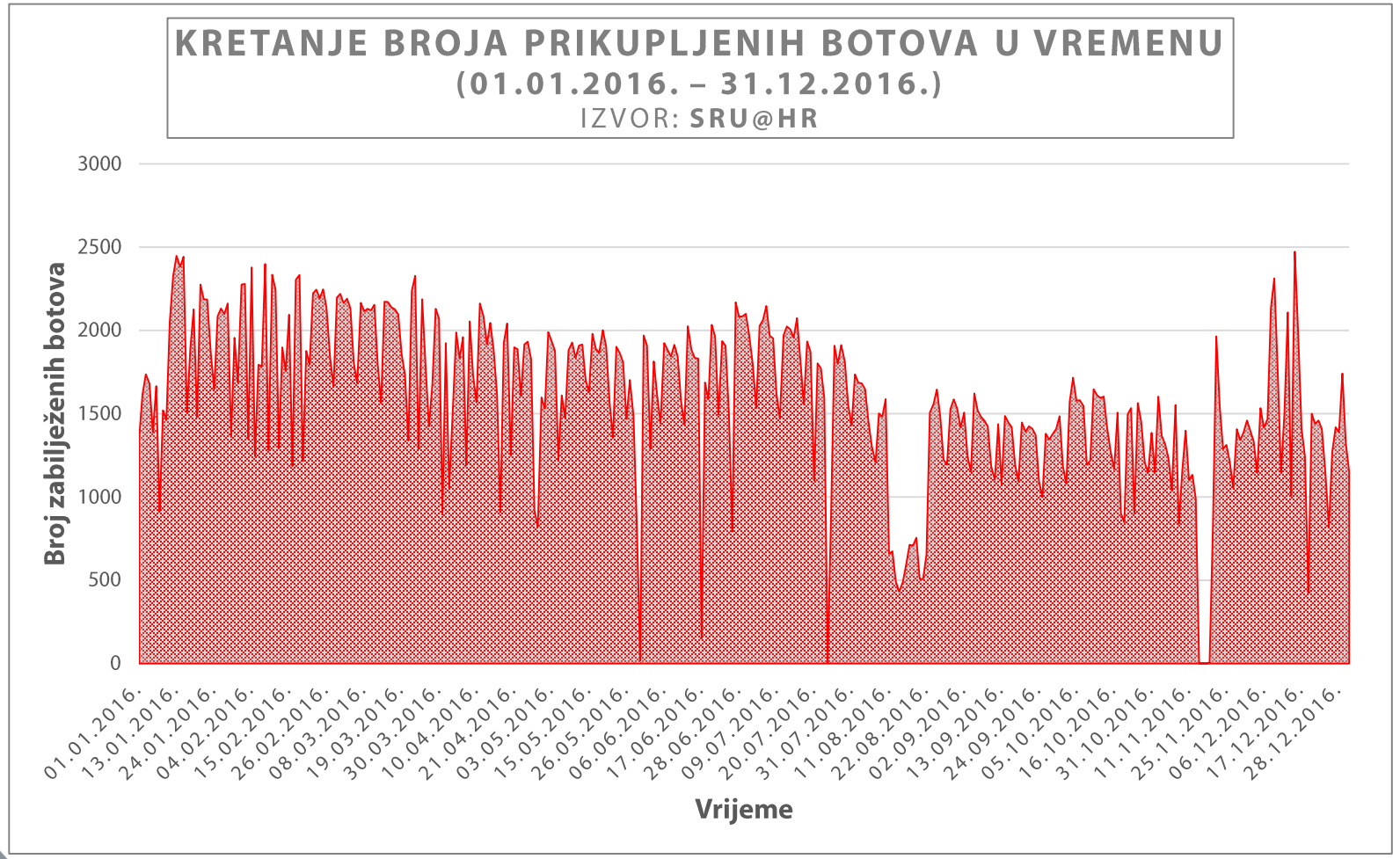
ZEUS C&C

MUMBLEHARD

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Pregled kretanja broja botova u 2016.

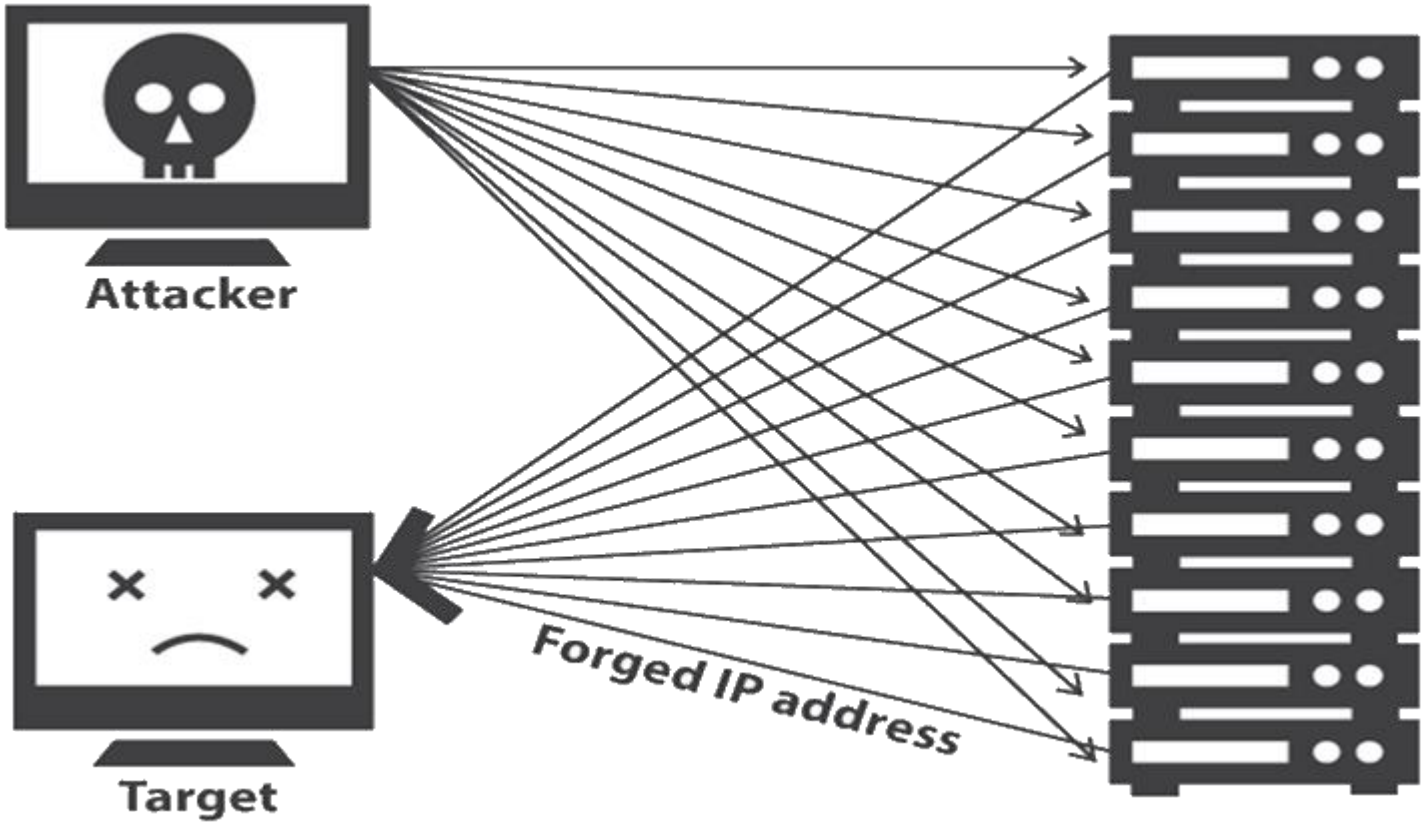


Vrsta malvera	Broj
Conficker	283955
Sality	40872
ZeroAccess	27757
Ponmocup	23334
Nivdort	22038
downadup	19370
Dorkbot	17458
Palevo	16886
Tinba	16049
Mirai	12102

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Javno dostupni servisi

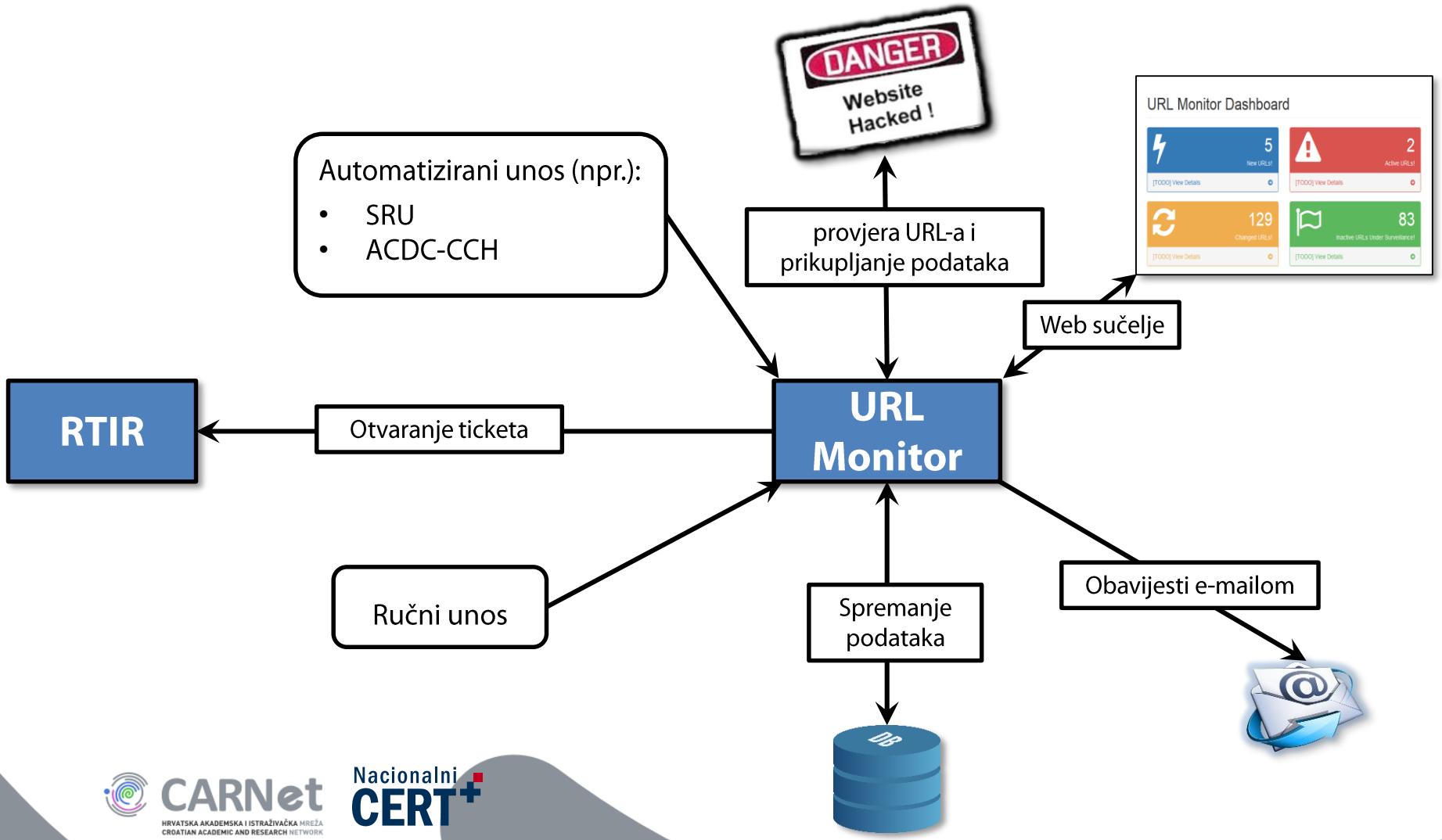


DNS_openresolver
MS-SQL
NTP
Portmapper
SNMP
SSDP

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

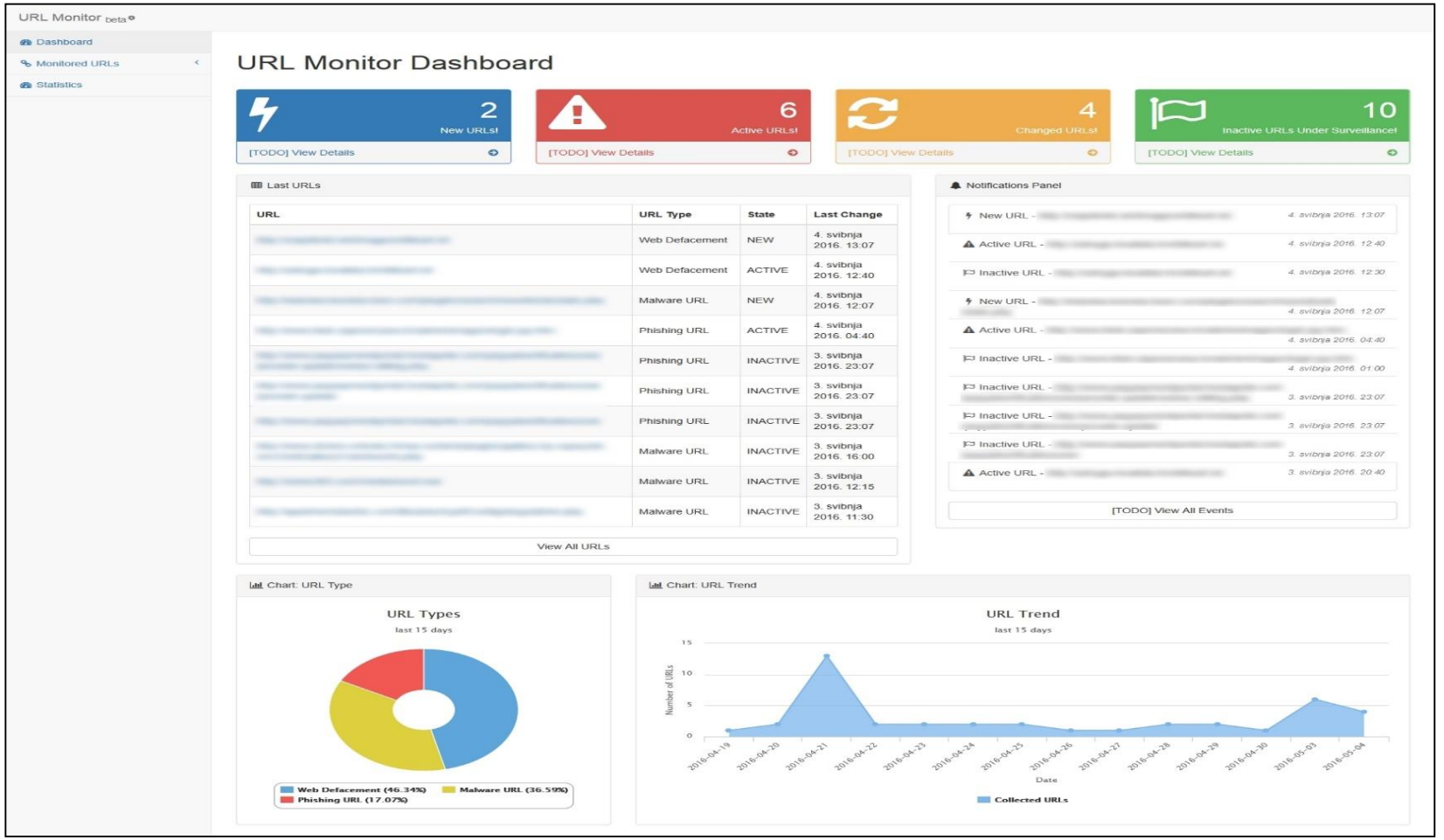
URL Monitor



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

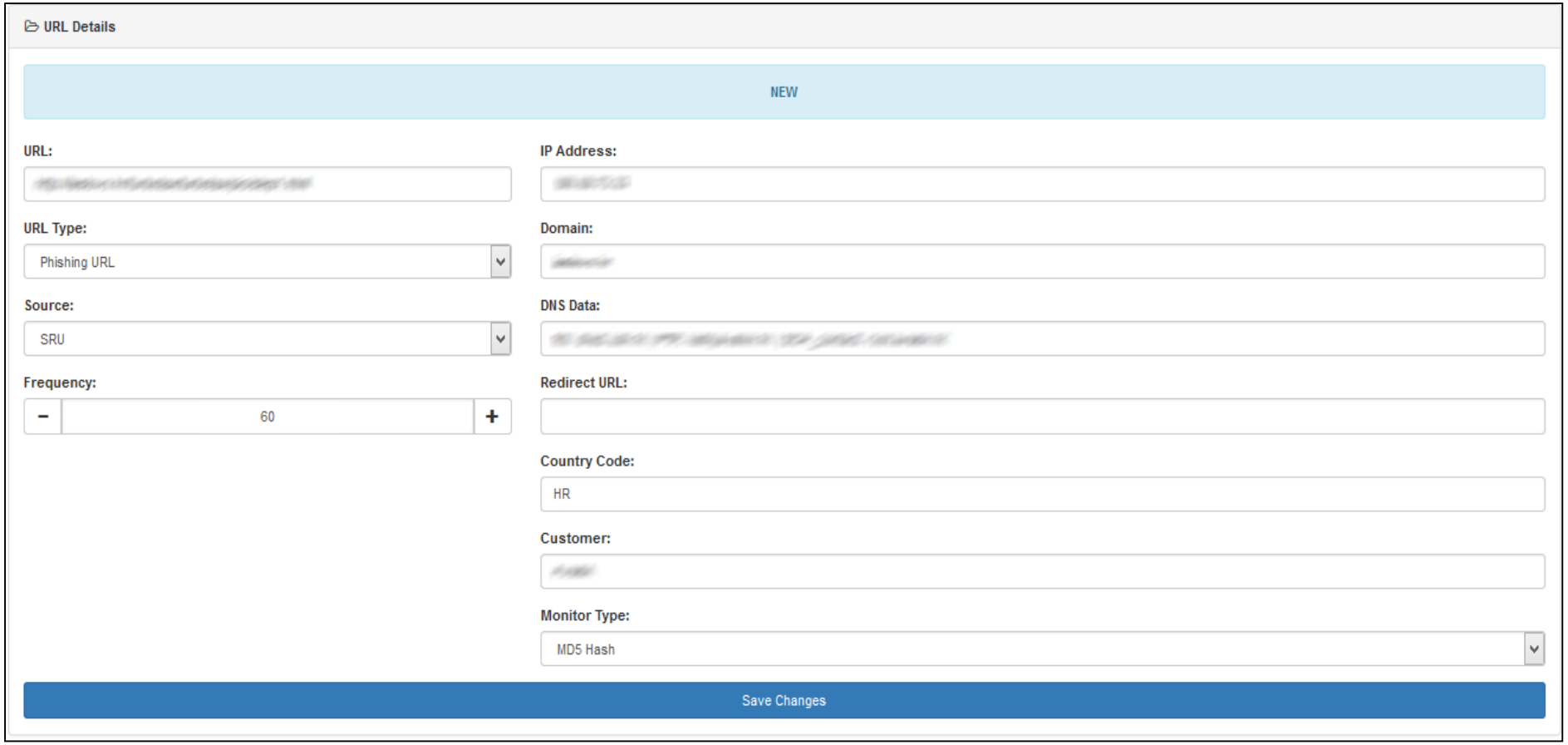
URL Monitor – upravljačka ploča



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

URL Monitor – Informacije



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

URL Monitor – povijest događanja

URL Log

Show 10 entries

Search:

State	Status Code	Screenshot	MD5 Hash	File Type	File	Last change	Actions
changed	200		7aeb47b912a8099048eef1239e74ff73	text/html		11/05/2016 - 00:40	
inactive	Unreachable					10/05/2016 - 20:45	
active	200		7aeb47b912a8099048eef1239e74ff73	text/html		04/05/2016 - 20:40	
inactive	Unreachable					04/05/2016 - 17:30	
active	200		7aeb47b912a8099048eef1239e74ff73	text/html		04/05/2016 - 04:40	
inactive	Unreachable					04/05/2016 - 01:00	
active	200		7aeb47b912a8099048eef1239e74ff73	text/html		03/05/2016 - 08:07	

Showing 1 to 7 of 7 entries

‹ Previous 1 Next ›

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

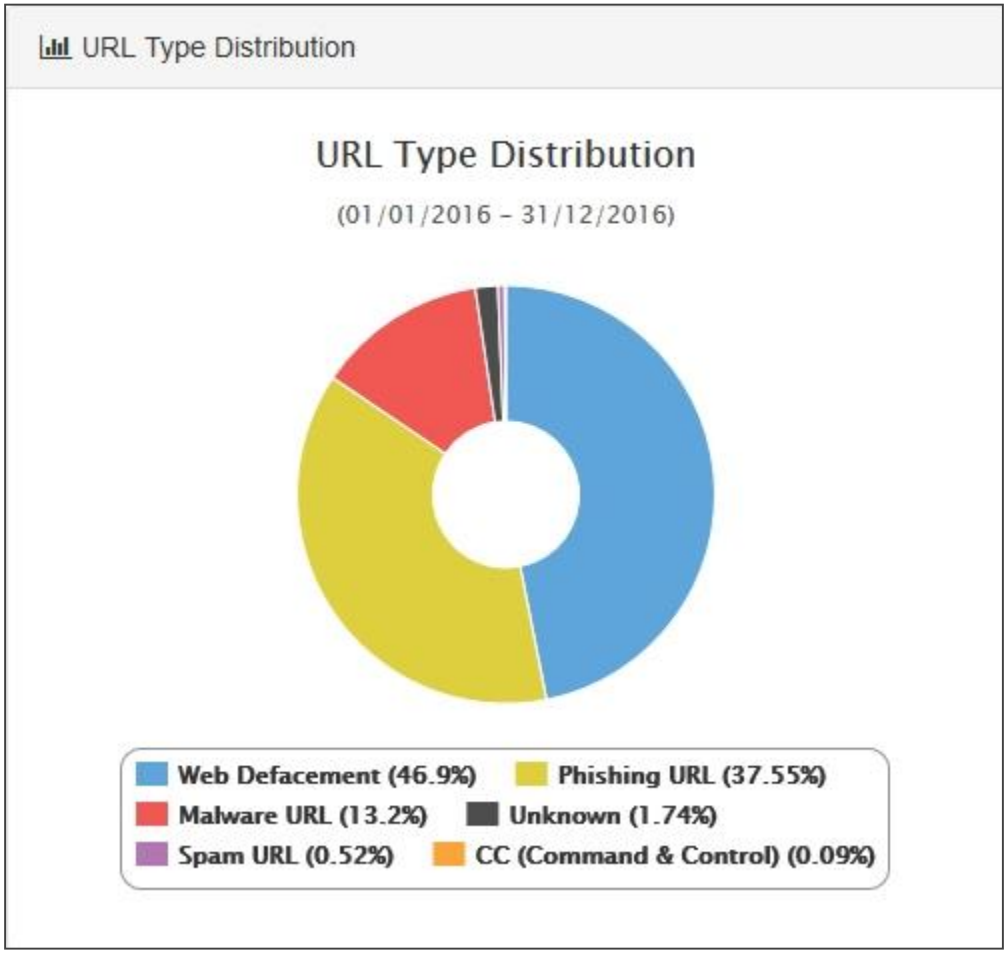
Nacionalni CERT

Izgled kompromitiranih stranica

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

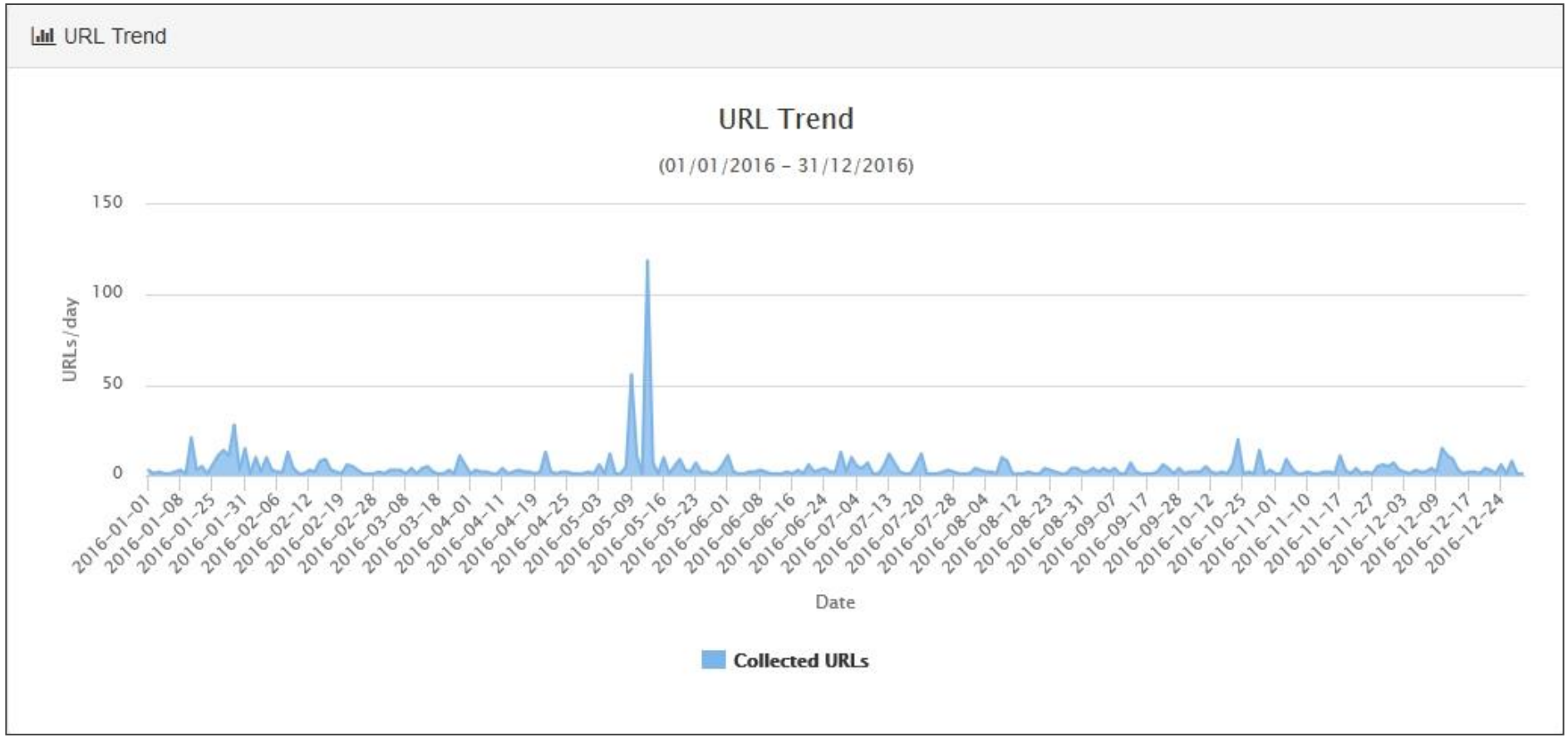
URL Monitor – udio tipa URL-ova



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

URL Monitor – trend kretanja



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Akademska i obrazovna mreža

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

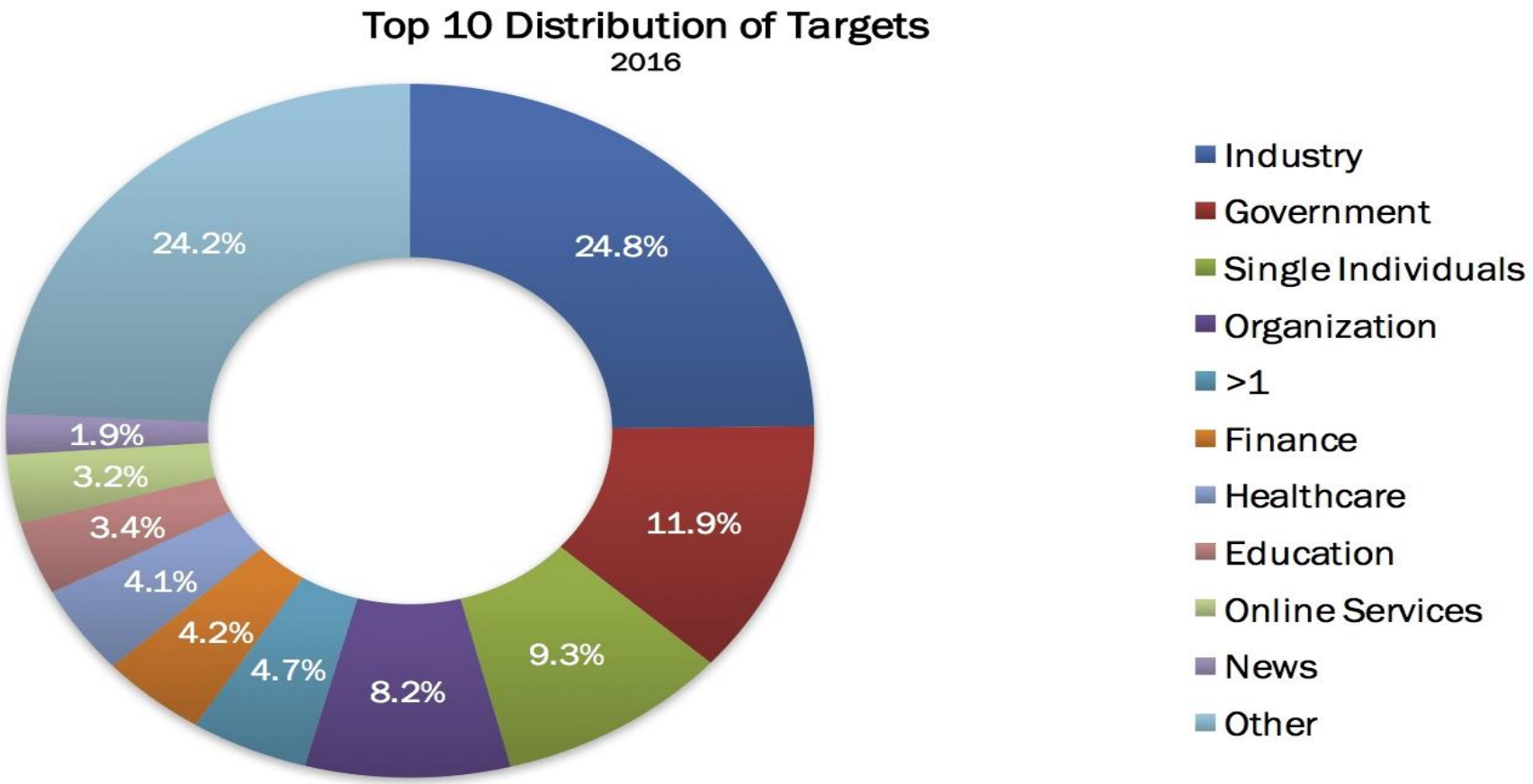
Obilježja akademskih/obrazovnih mreža

- Služi za učenje, podučavanje i istraživanje
- Otvorenost – slabo postavljene sigurnosne mjere
- Veliki broj korisnika – učenici, studenti, nastavno osoblje, vanjski suradnici…
- Napredna računalno-komunikacijska tehnologija
- Veliki kapaciteti linkova

Napadi na akademske/obrazovne mreže

- Jedne od najzanimljivijih meta napada
- Pri samom vrhu prema broju napada na internetu
- Najčešće nisu krajnji cilj
- Izvođenje daljnjih napada

Trendovi napada na internetu

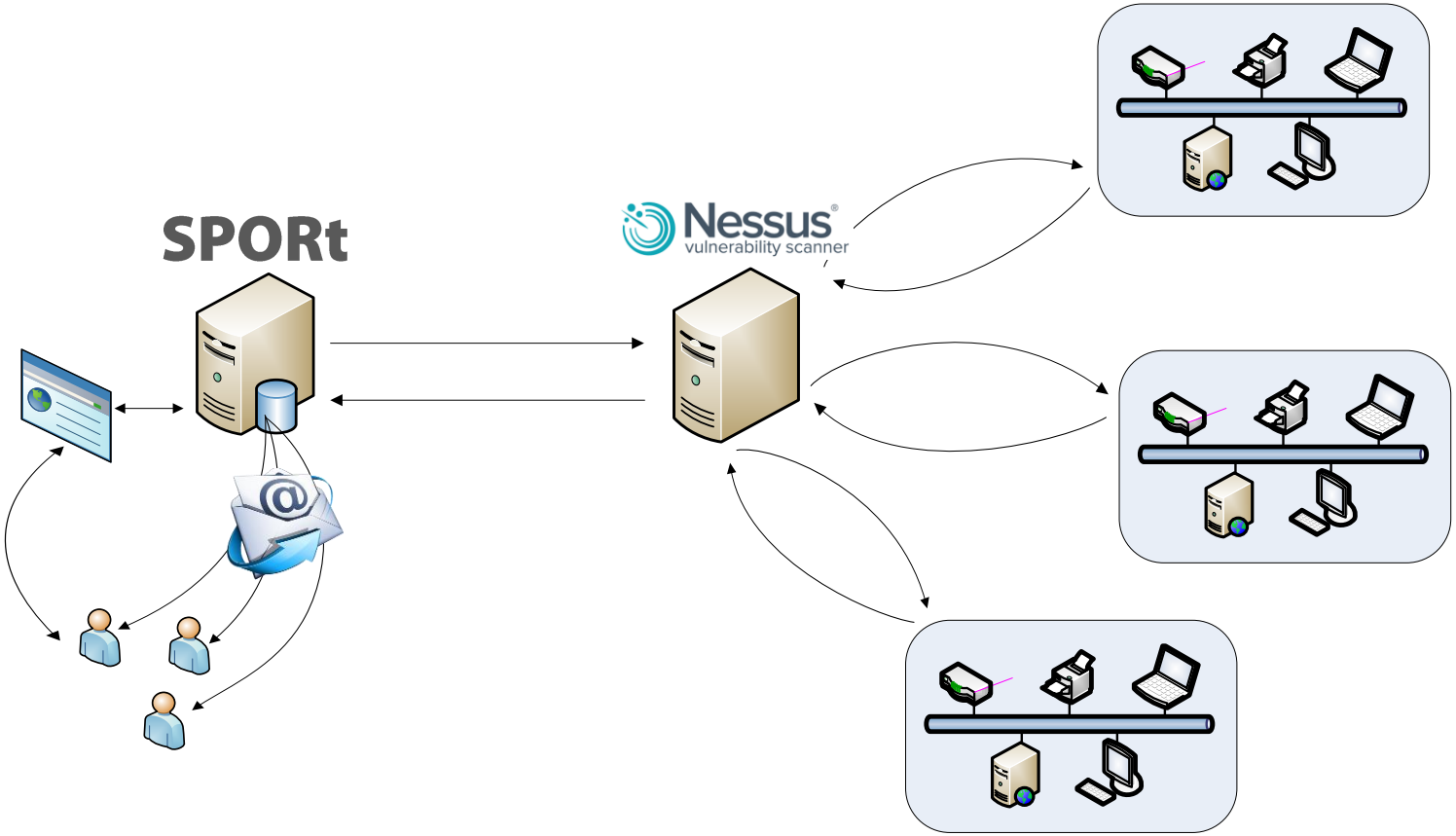


(Izvor: www.hackmageddon.com)

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

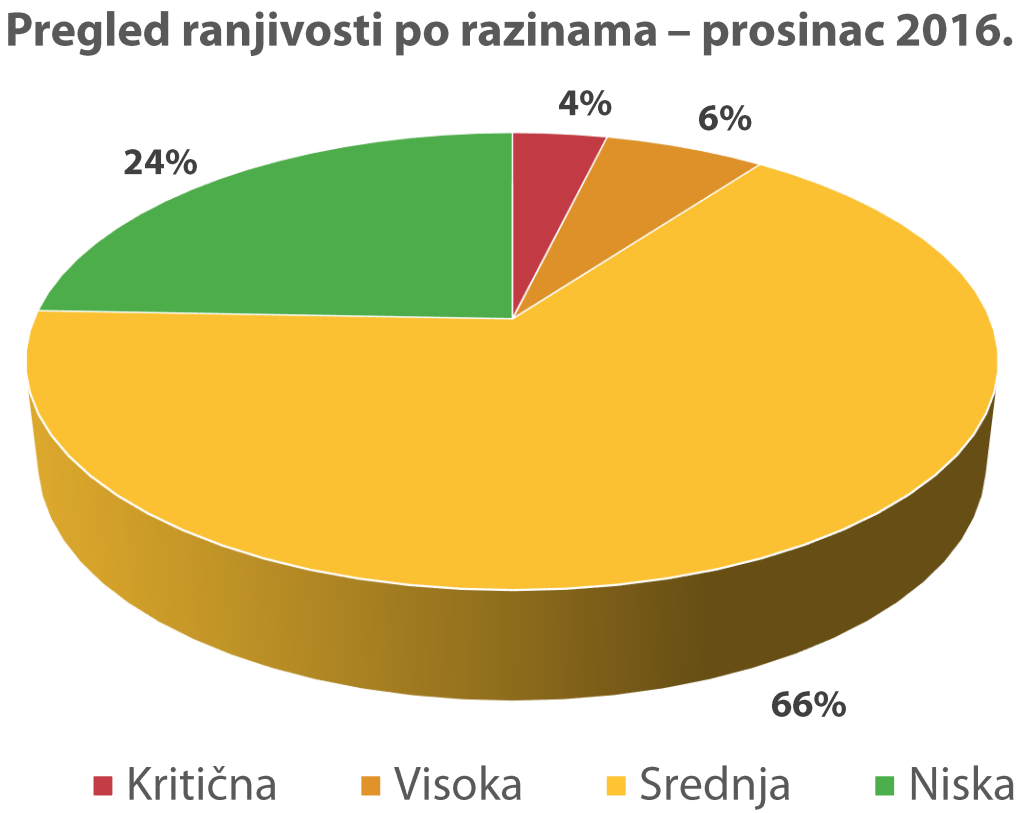
SPORt



CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

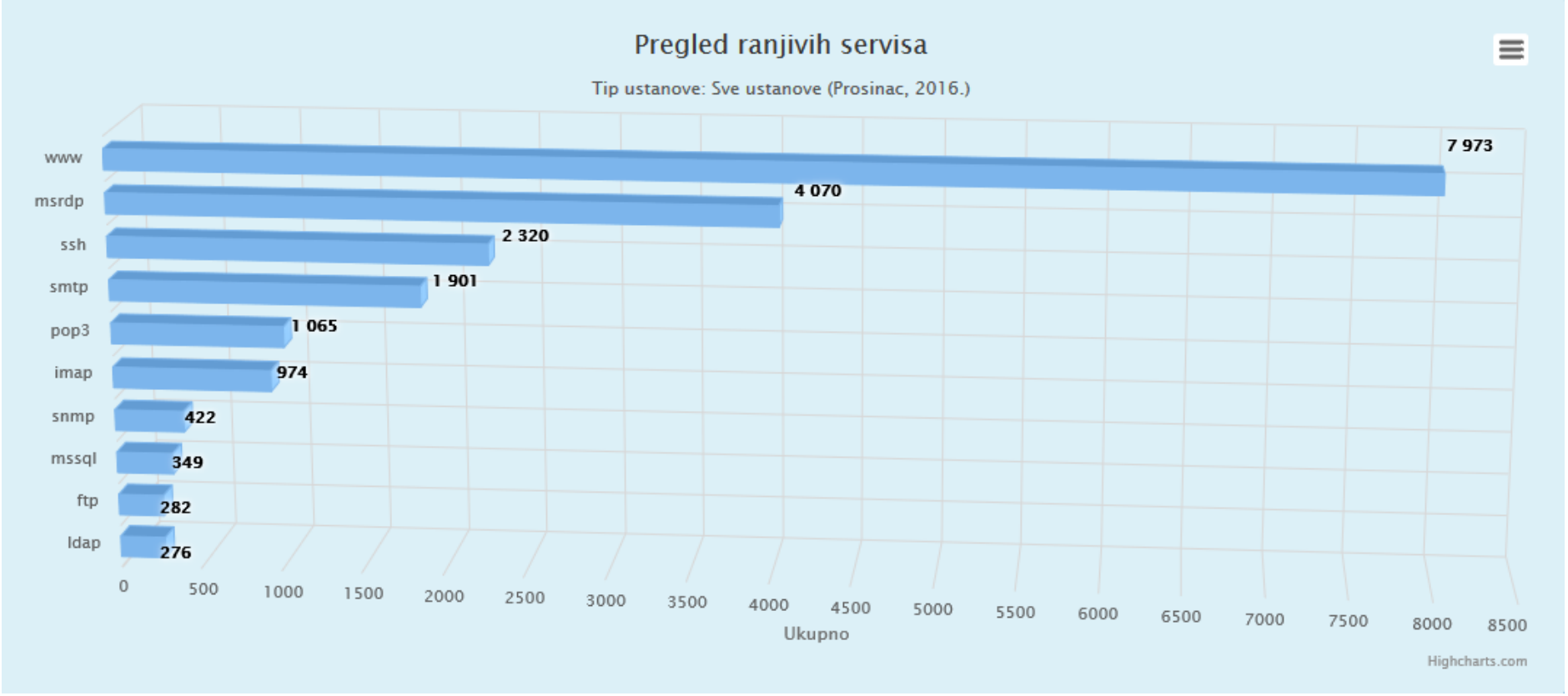
Nacionalni CERT

SPORt – pregled ranjivosti po razinama



Razina	Broj
Kritična	824
Visoka	1400
Srednja	14362
Niska	5355
Ukupno	**21941**

SPORt – ranjivi servisi

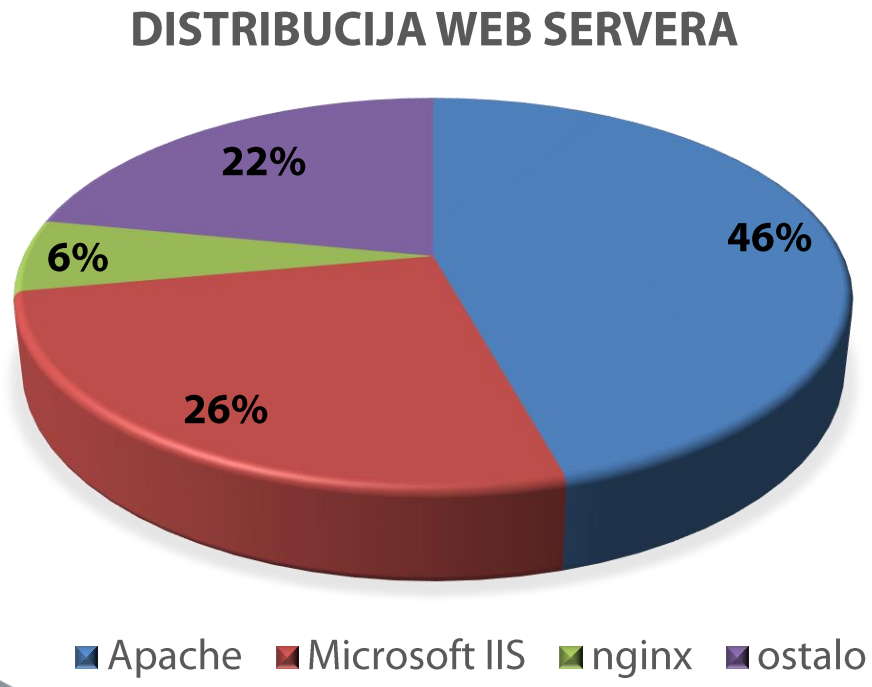


CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

SPORt – distribucija web servera

- 5259 javno dostupnih adresa
- 1387 detektirano kao web server
  - 634 Apache
  - 366 Microsoft IIS
  - 83 nginx



SPORt – najčešće ranjivosti

- Ranjivosti **kritične** razine:
  - OS-ovi sa isteklom podrškom (Windows/Unix)
  - Nepodržani i zastarjeli programski paketi

- Ranjivosti **visoke** razine:
  - Ranjivi servisi i programski paketi (Apache, PHP, OpenSSL, RDP…)
  - msrdp Remote Code Execution

SPORt – najčešće ranjivosti

- Ranjivosti **srednje** razine:
  - korištenje SSL v2/v3 protokola
  - msrdp MITM ranjivosti
  - Problemi sa SSL certifikatima (self-signed/expired)
  - DNS server spoofed request amplification DDoS
- Ranjivosti **niske** razine:
  - Korištenje slabih kriptografskih algoritama
  - Clear Text Authentication (FTP, SMTP, POP3)

„Brand name” ranjivosti

- Shellshock
- Logjam
- BEAST
- Heartbleed
- DROWN
- GHOST
- Bar Mitzvah
- POODLE
- FREAK

Hvala na pažnji

ncert@cert.hr incident@cert.hr

www.cert.hr

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

```
question = (cro_ip_space) ? safe : !safe;
```

„The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.”

- Eugene H. Spafford