



PREGLED STANJA SIGURNOSTI U RH IZ PERSPEKTIVE NACIONALNOG CERT-A

Marko Stanec – Nacionalni CERT
CARNet

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



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**



www.antibot.hr

Anti-botnet
Nacionalni centar podrške

Početna EU-Cleaner Ransomware Alati Upute O nama

Dobrodošli na Anti-Botnet Nacionalni centar podrške.

Nacionalni CERT+
CARNET

EU-Cleaner
U suradnji s tehnološkim partnerima Avira, GData i SurfRight nudimo vam besplatan alat EU Cleaner koji pomaže pri laganom i brzom uklanjanju zlonamjernih programa.

[PREUZIMANJE](#)

Alati
Preporuke za dodatke za preglednike, virusne skenere i ostale korisne informacije.

SIGURNOSNE PROVJERE DODACI ZA PREGLEDNIKE KORISNI ALATI ANTIVIRUSNI PROGRAMI

Ransomware
Ne oklijevajte, posjetite stranice s opisima i poveznicama na postojeće alate za dešifriranje te pročitajte i ostale prijedloge vezane za ransomware.

REPOZITORIJ INFORMACIJE ZAŠTITA

Upute
Općenite sigurnosne preporuke i instrukcije za različite teme vezane za Internet.

OPERACIJSKI SUSTAVI KAKO SE ZAŠTITITI DVOSTRUKA AUTENTIFIKACIJA

Blog
Naš blog s informacijama o desktop i internet sigurnosti i brojnim drugim uputama.

NOVOSTI RANSOMWARE

Spam
Spam kampanje i spam s malicioznim sadržajem.

SPAM KAMPANJE [XLS] SPAM S MALICIOZNIM SADRŽAJEM [XLS]

GACDE AVIRA GDATA INITIATIVES SurfRight

Misija Nacionalnog CERT-a
Prevencija i zaštita od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj.

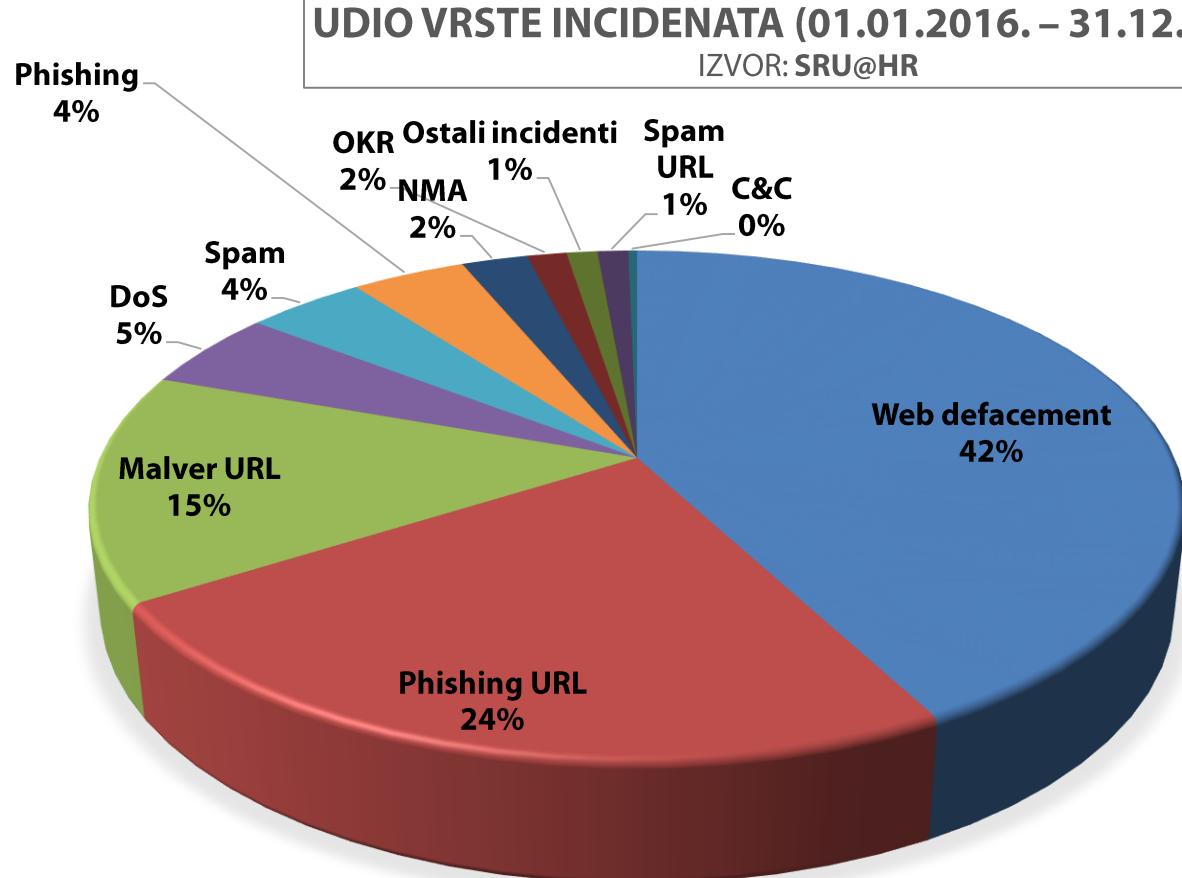
Društveni mediji
[Blog](#) [Twitter](#)

Scanned: 2017-03-14

© 2016 antibot · Impressum · Izjava o privatnosti · Uvjeti korištenja

Pregled incidenata u 2016.

Pregled incidenata po tipu u 2016.



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://Imgfyy.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



NO MORE RANSOM!

★ English ▾

Crypto Sheriff Ransomware: Q&A Prevention Advice Decryption Tools Report a Crime Partners About the Project

NEED HELP unlocking your digital life
without paying your attackers*?

YES NO

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

GOOD NEWS

Prevention is possible. Following simple cyber security advice can help you to avoid becoming a victim of ransomware.

BAD NEWS

Unfortunately, in many cases, once the ransomware has been released into your device there is little you can do unless you have a backup or security software in place.

GOOD NEWS

Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted files or locked systems, without having to pay. We have created a repository of keys and applications that can decrypt data locked by different types of ransomware.

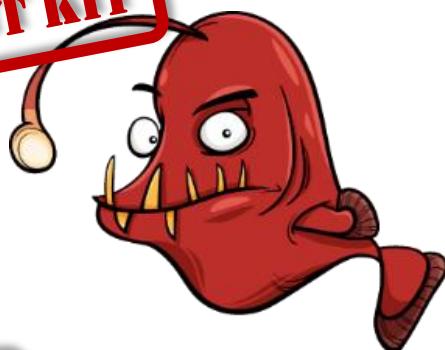
At the moment, not every type of ransomware has a solution. Keep checking this website as new keys and applications are added when available.

CERI

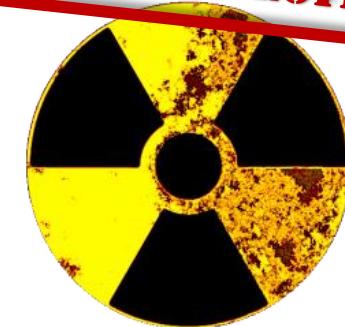
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Kompromitirani poslužitelji

ANGER EXPLOIT KIT



NUCLEAR EXPLOIT KIT



ZEUS C&C

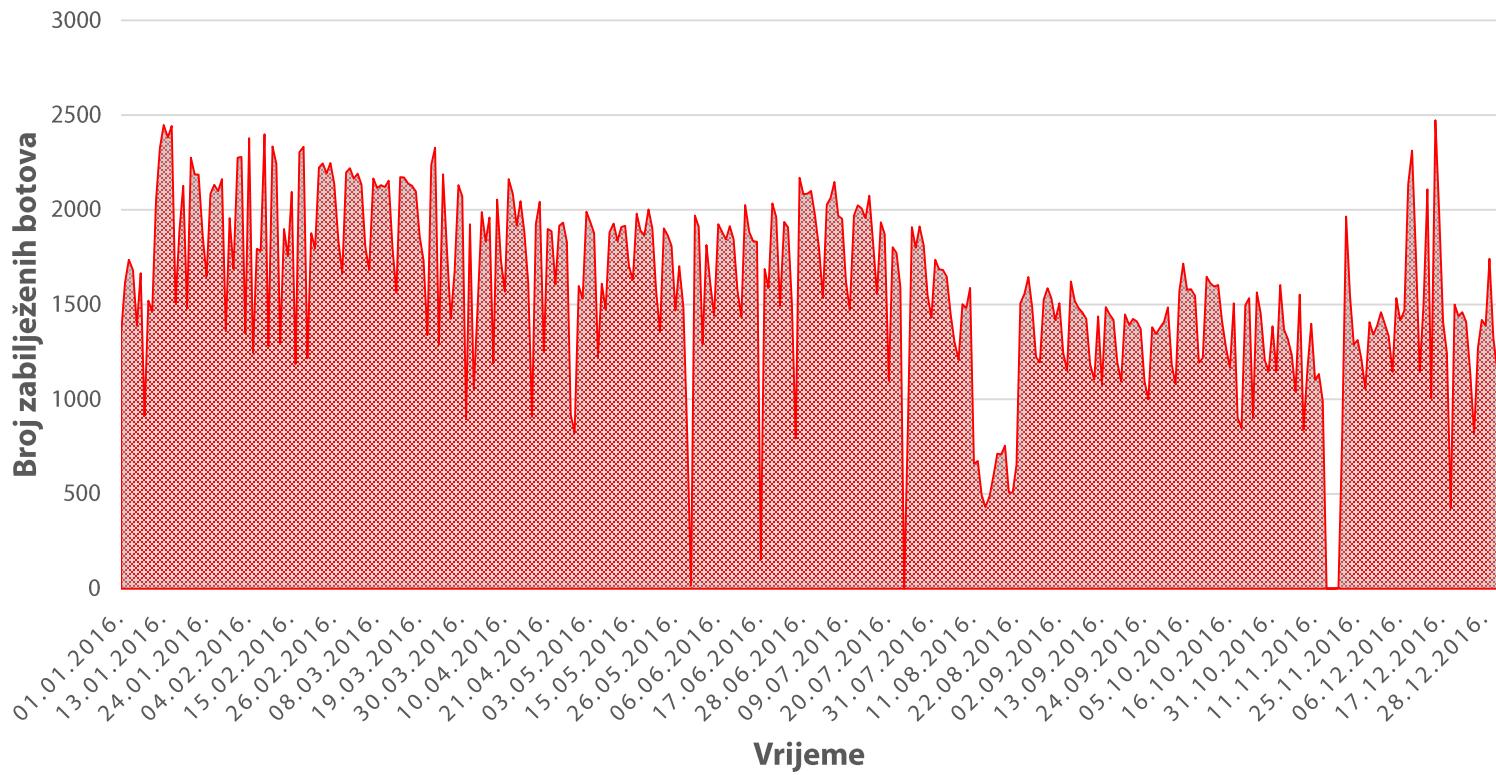


MUMBLEHARD



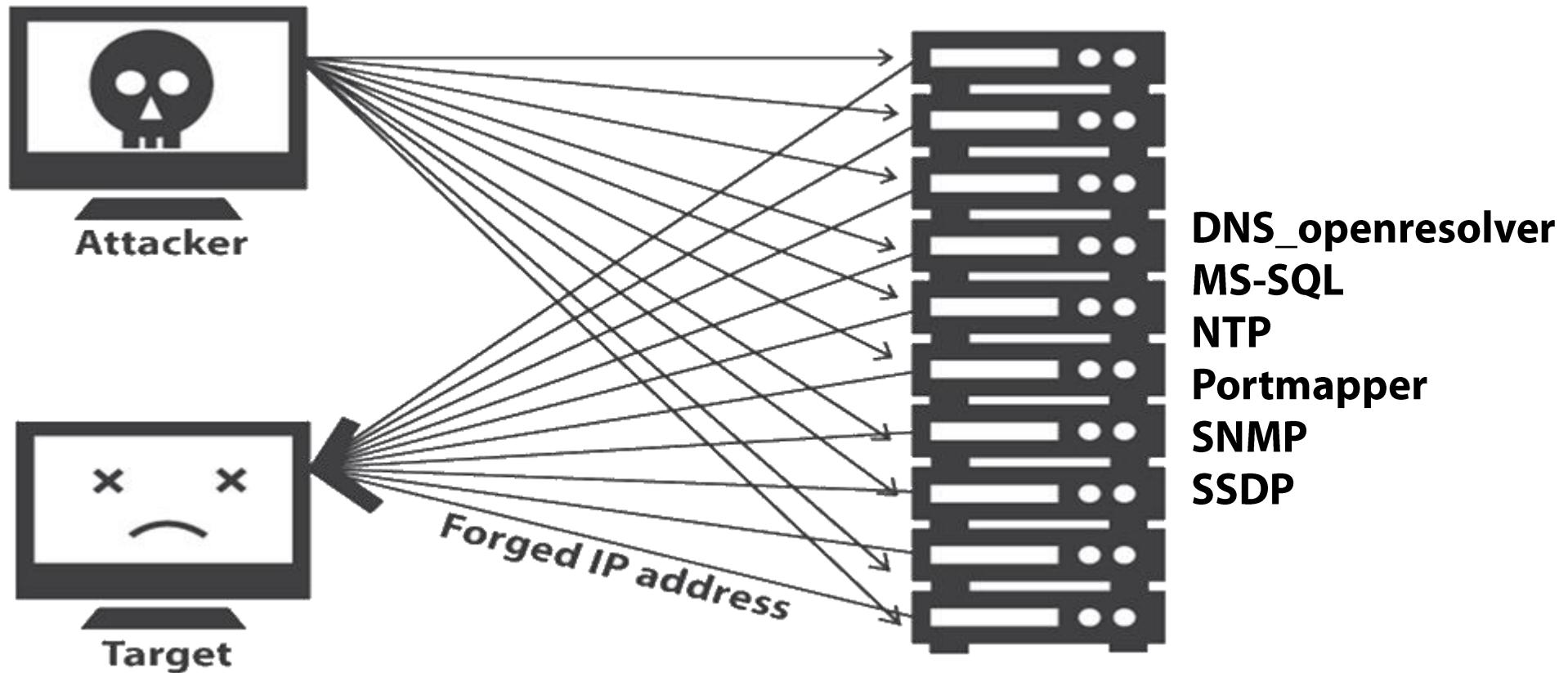
Pregled kretanja broja botova u 2016.

KRETANJE BROJA PRIKUPLJENIH BOTOVA U VREMENU
(01.01.2016. – 31.12.2016.)
IZVOR: SRU@HR

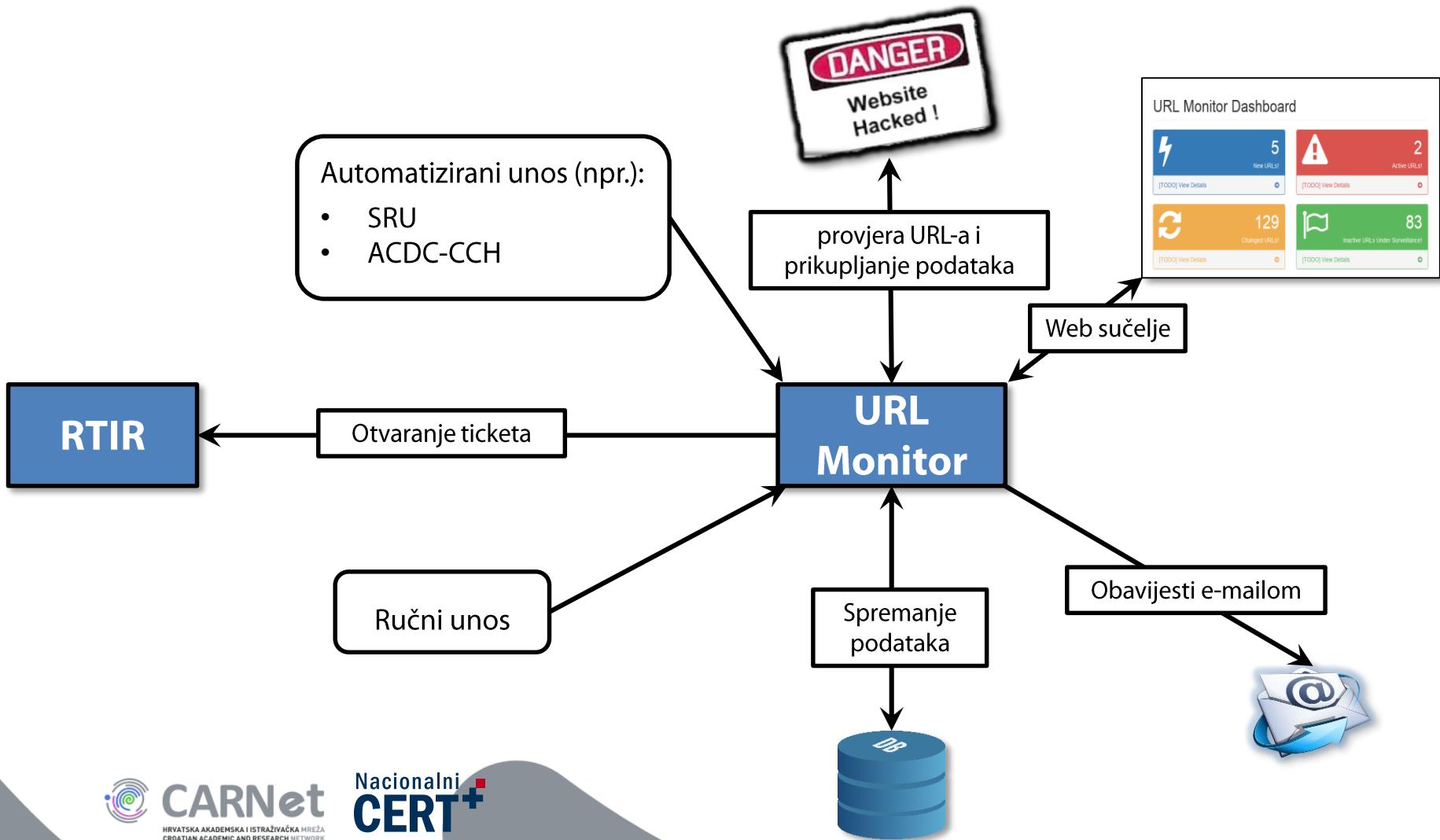


Vrsta malvera	Broj
Conficker	283955
Sality	40872
ZeroAccess	27757
Ponmocup	23334
Nivdort	22038
downadup	19370
Dorkbot	17458
Palevo	16886
Tinba	16049
Mirai	12102

Javno dostupni servisi



URL Monitor



URL Monitor – upravljačka ploča

URL Monitor beta®

- Dashboard
- Monitored URLs
- Statistics

URL Monitor Dashboard

New URLs: 2 [TODO] View Details

Active URLs: 6 [TODO] View Details

Changed URLs: 4 [TODO] View Details

Inactive URLs Under Surveillance: 10 [TODO] View Details

URL	URL Type	State	Last Change
[REDACTED]	Web Defacement	NEW	4. svibnja 2016. 13:07
[REDACTED]	Web Defacement	ACTIVE	4. svibnja 2016. 12:40
[REDACTED]	Malware URL	NEW	4. svibnja 2016. 12:07
[REDACTED]	Phishing URL	ACTIVE	4. svibnja 2016. 04:40
[REDACTED]	Phishing URL	INACTIVE	3. svibnja 2016. 23:07
[REDACTED]	Phishing URL	INACTIVE	3. svibnja 2016. 23:07
[REDACTED]	Phishing URL	INACTIVE	3. svibnja 2016. 23:07
[REDACTED]	Malware URL	INACTIVE	3. svibnja 2016. 16:00
[REDACTED]	Malware URL	INACTIVE	3. svibnja 2016. 12:15
[REDACTED]	Malware URL	INACTIVE	3. svibnja 2016. 11:30

[View All URLs](#)

Notifications Panel

⚡ New URL - [REDACTED]	4. svibnja 2016. 12:07
⚠ Active URL - [REDACTED]	4. svibnja 2016. 12:40
⚠ Inactive URL - [REDACTED]	4. svibnja 2016. 12:30
⚡ New URL - [REDACTED]	4. svibnja 2016. 12:07
⚠ Active URL - [REDACTED]	4. svibnja 2016. 04:40
⚠ Inactive URL - [REDACTED]	4. svibnja 2016. 01:00
⚠ Inactive URL - [REDACTED]	3. svibnja 2016. 23:07
⚠ Inactive URL - [REDACTED]	3. svibnja 2016. 23:07
⚠ Active URL - [REDACTED]	3. svibnja 2016. 23:07
[TODO] View All Events	

Chart: URL Type

last 15 days

Type	Percentage
Web Defacement	46.34%
Malware URL	36.59%
Phishing URL	17.07%

Chart: URL Trend

last 15 days

Date	Number of URLs
2016-04-19	~2
2016-04-20	~2
2016-04-21	~12
2016-04-22	~2
2016-04-23	~2
2016-04-24	~2
2016-04-25	~2
2016-04-26	~2
2016-04-27	~2
2016-04-28	~3
2016-04-29	~3
2016-04-30	~3
2016-05-01	~5
2016-05-02	~5
2016-05-03	~5
2016-05-04	~5

URL Monitor – Informacije

URL Details

NEW

URL:	IP Address:
<input type="text" value="http://www.virusshare.com/phishing-test"/>	<input type="text" value="192.168.1.100"/>
URL Type:	Domain:
<input type="text" value="Phishing URL"/>	<input type="text" value="virusshare.com"/>
Source:	DNS Data:
<input type="text" value="SRU"/>	<input type="text" value="NS1.DNS.CLOUD.CLOUDS.COM."/>
Frequency:	Redirect URL:
<input type="button" value="-"/> 60 <input type="button" value="+"/>	<input type="text"/>
Country Code:	Customer:
<input type="text" value="HR"/>	<input type="text" value=""/>
Monitor Type:	
<input type="text" value="MD5 Hash"/>	<input type="button" value="▼"/>

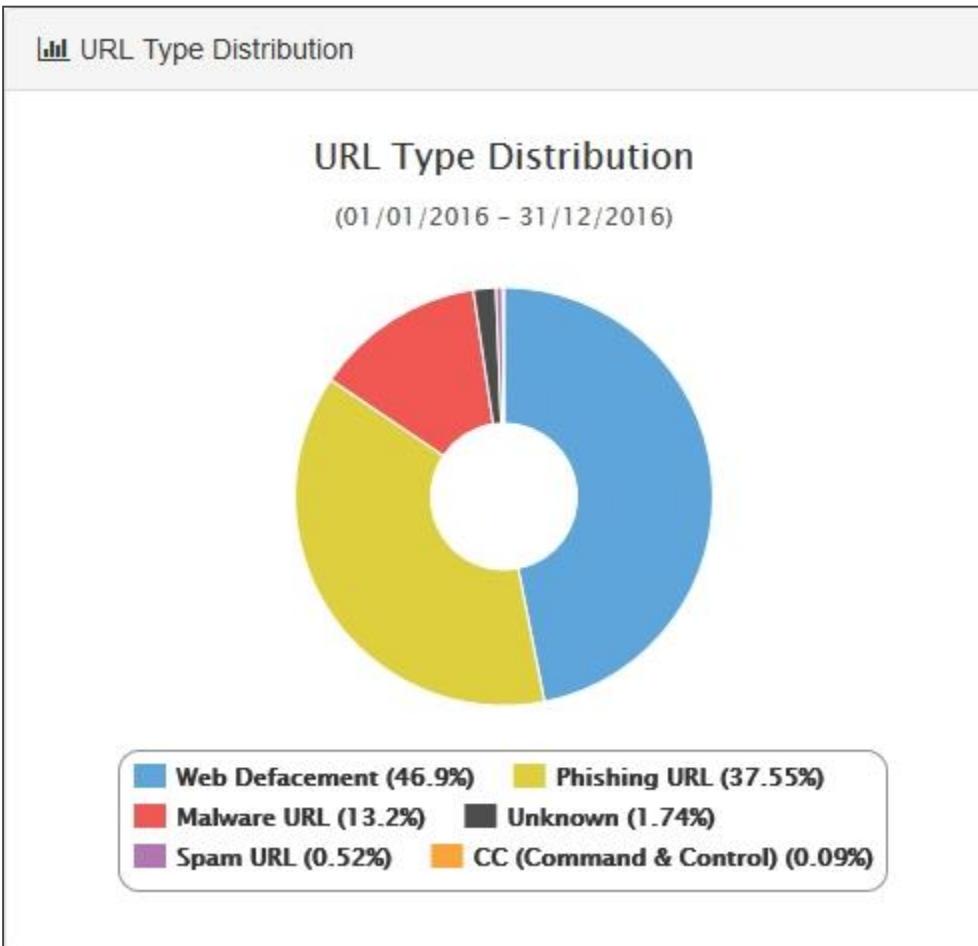
URL Monitor – povijest događanja

URL Log							
Show 10 entries				Search: <input type="text"/>			
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 >	

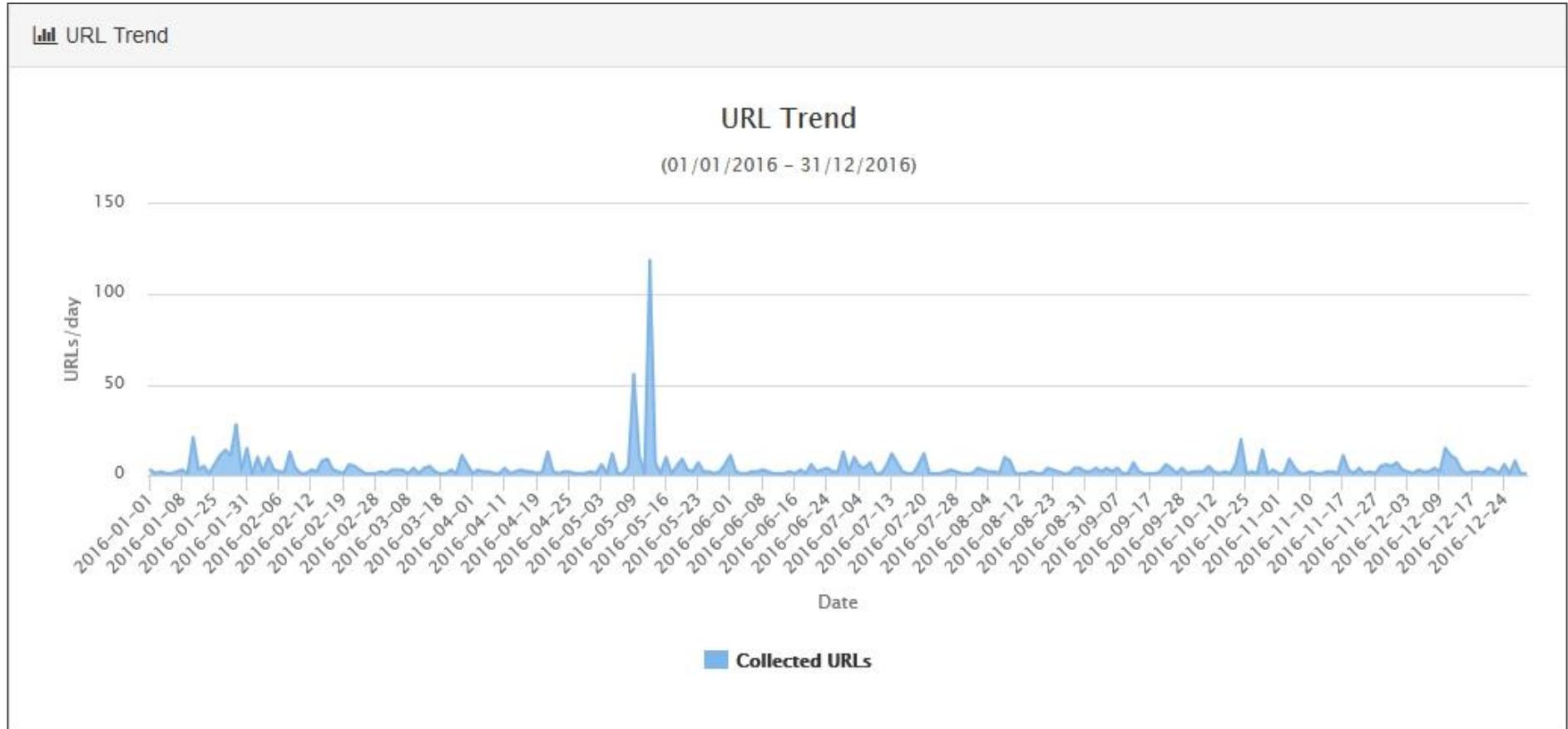
Izgled kompromitiranih stranica



URL Monitor – udio tipa URL-ova



URL Monitor – trend kretanja



Akadembska i obrazovna mreža

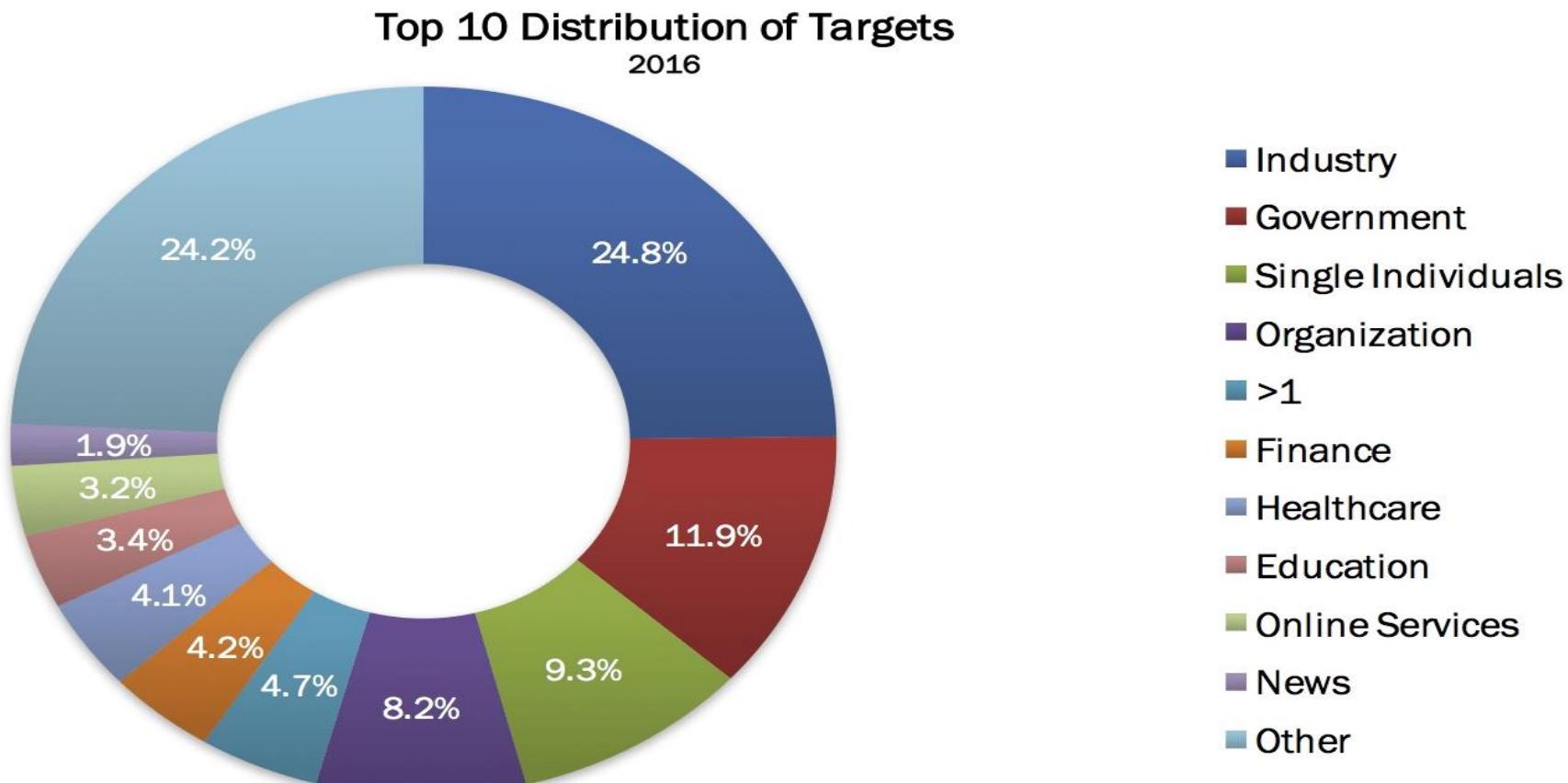
Obilježja akademskih/obrazovnih mreža

- 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

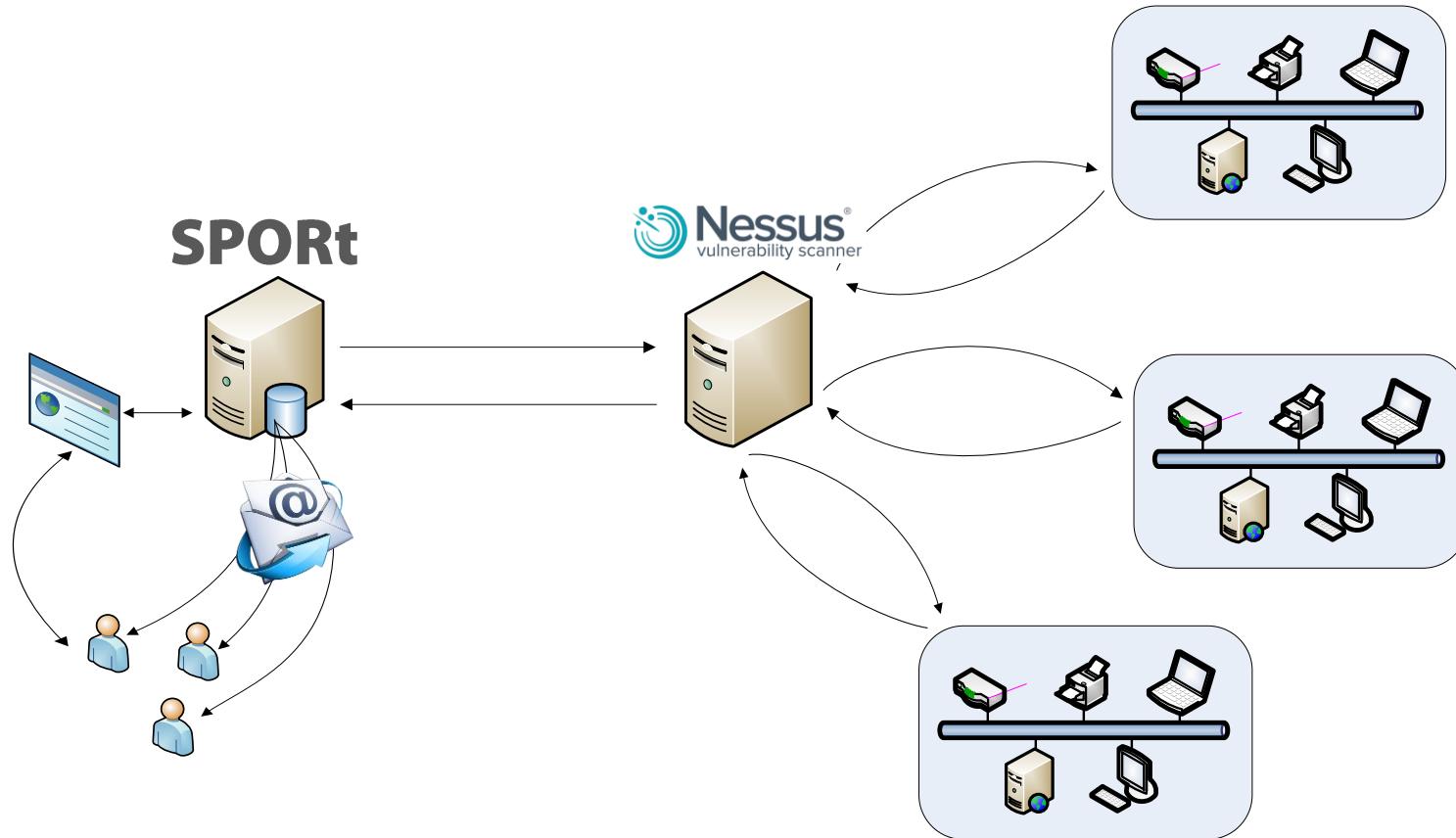
- Jedne od najzanimljivijih meta napada
- Pri samom vrhu prema broju napada na internetu
- Najčešće nisu krajnji cilj
- Izvođenje dalnjih napada

Trendovi napada na internetu



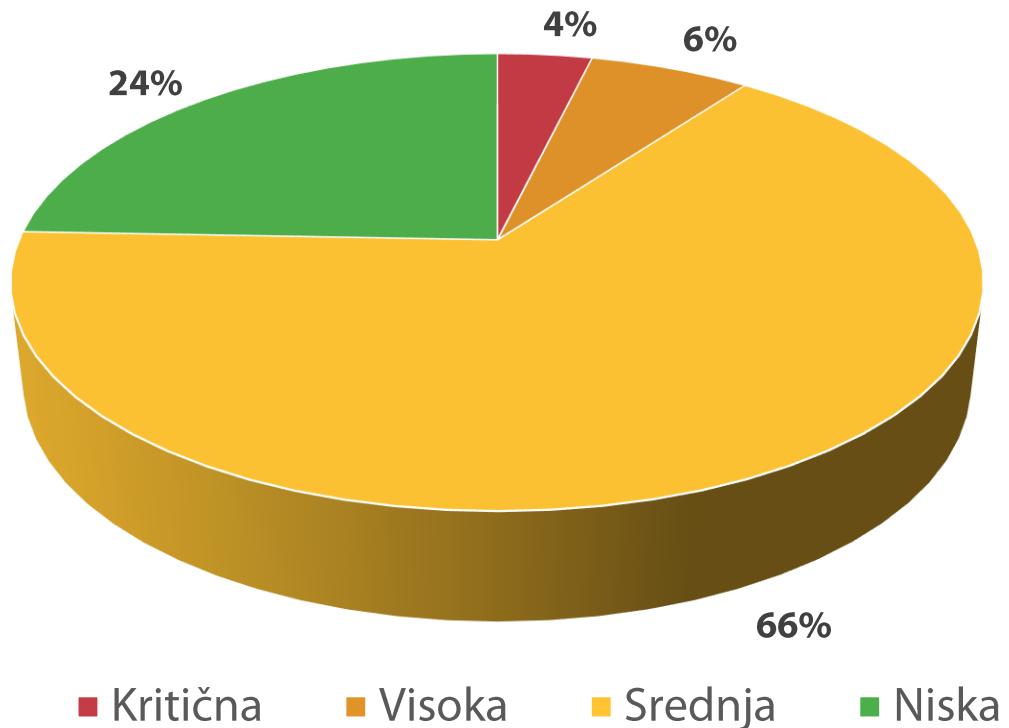
(Izvor: www.hackmageddon.com)

SPORt

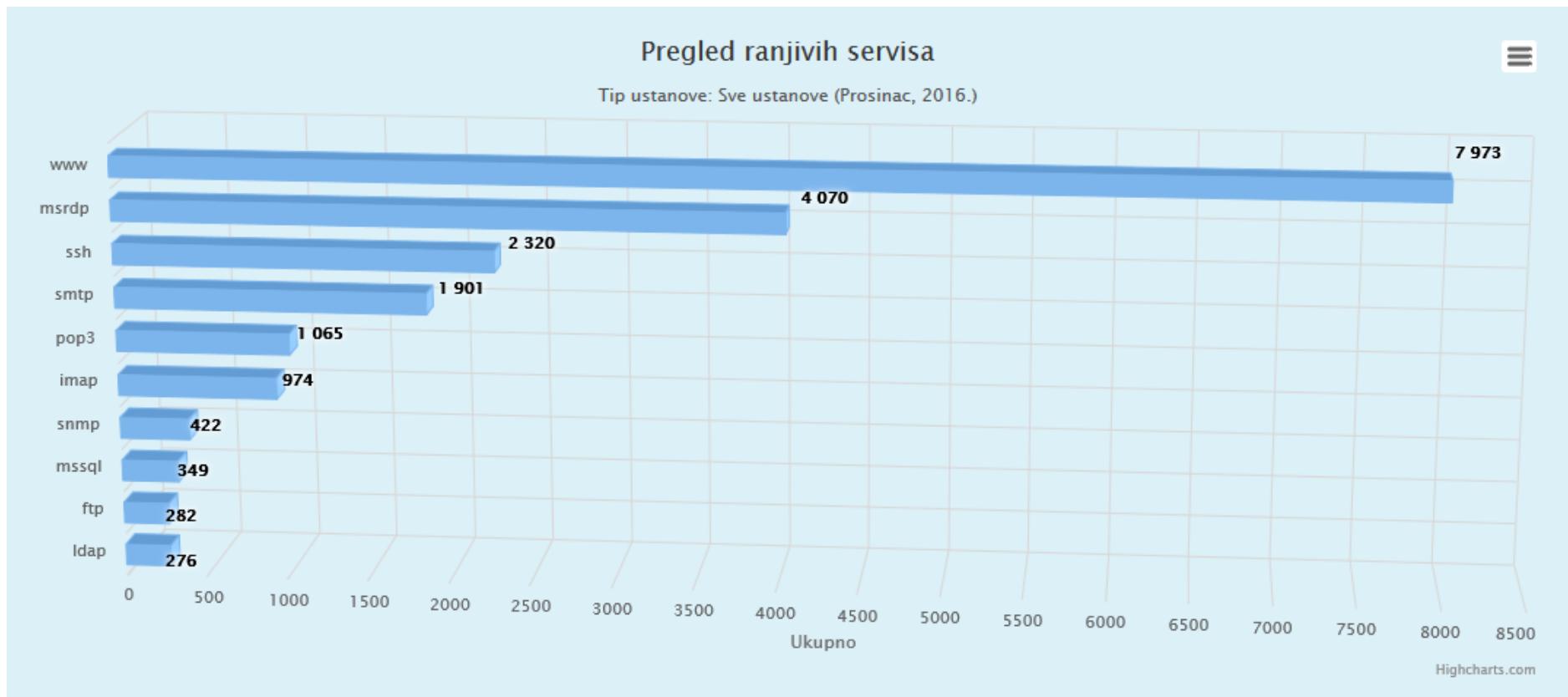


SPORt – pregled ranjivosti po razinama

Pregled ranjivosti po razinama – prosinac 2016.

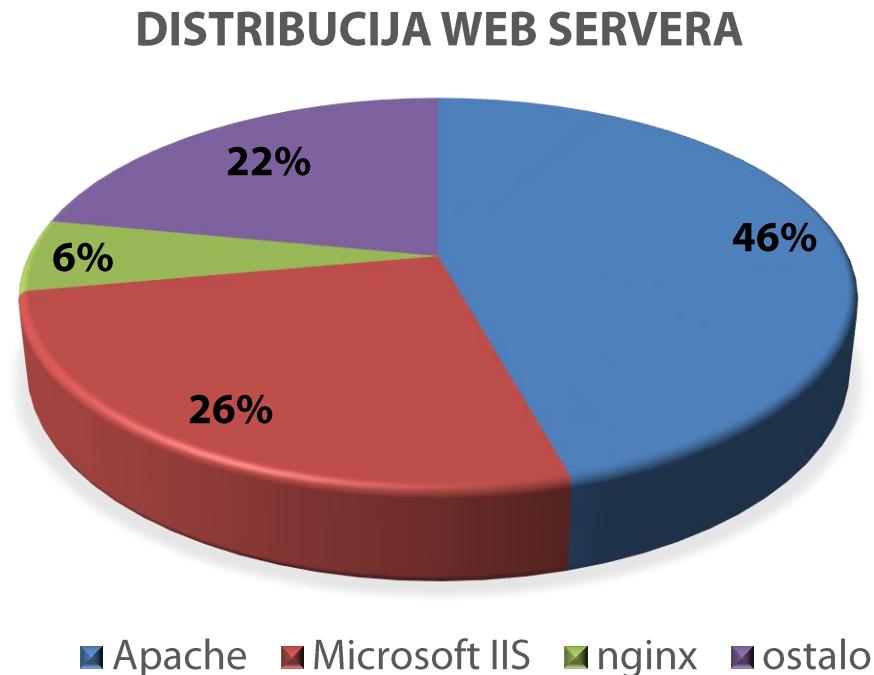


SPORt – ranjivi servisi



SPORt – distribucija web servera

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



SPORt – najčešće ranjivosti

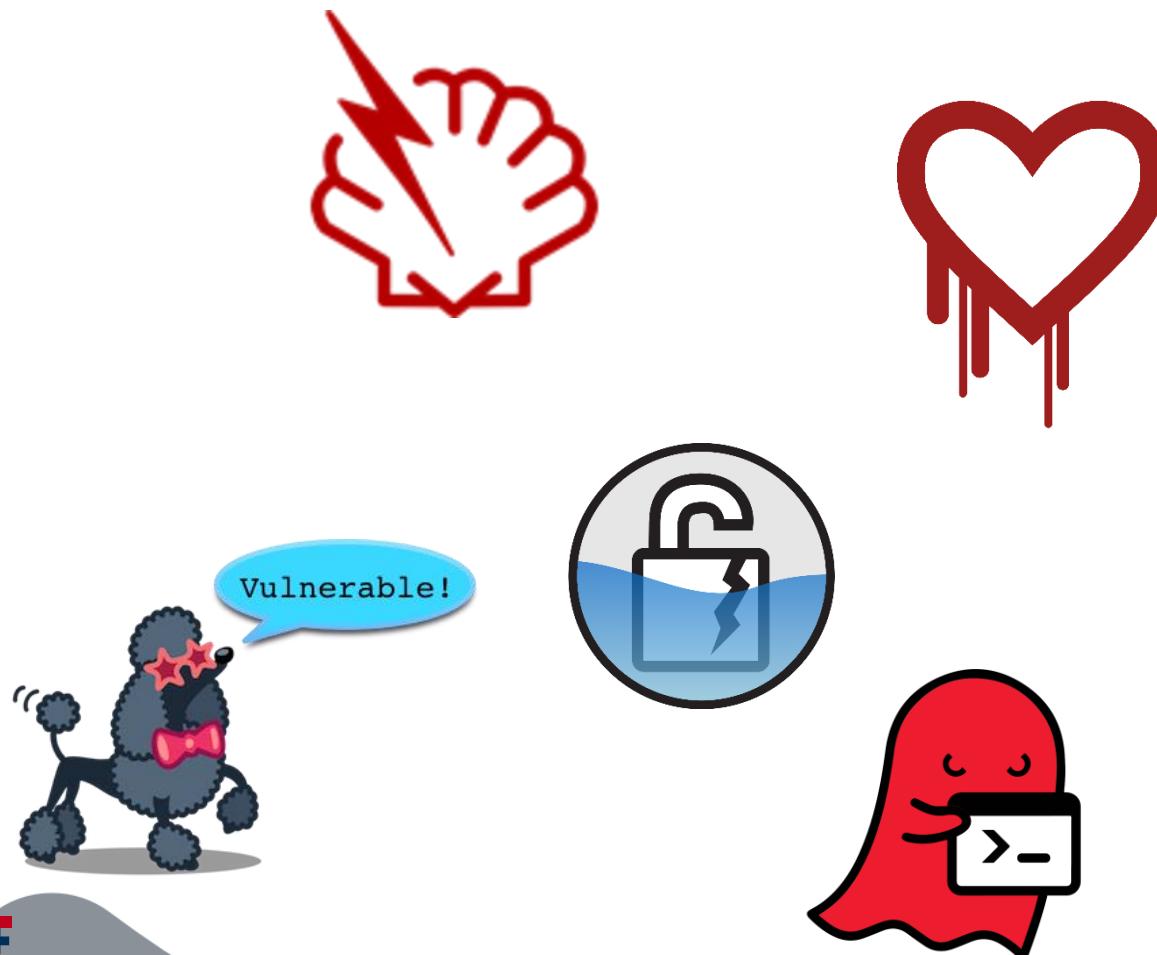
- Ranjivosti **kritične** razine:
 - OS-ovi sa isteklom podrškom (Windows/Unix)
 - Nepodržani i zastarjeli programski paketi
- Ranjivosti **visoke** razine:
 - Ranjivi servisi i programski paketi (Apache, PHP, OpenSSL, RDP...)
 - msrdp Remote Code Execution

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

```
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