KRATKI PREGLED SIGURNOSTI NA INTERNETU U RH (2015/16)

Marko Stanec – Nacionalni CERT
CARNet

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Pitanje koje se postavlja...

question = (to) ? be : !be;

-- Wm. Shakespeare

question = (cro_ip_space) ? safe : !safe;

-- HR-CERT

NCERT – djelokrug rada

- ✓ Uklanjanje malicioznog sadržaja s Interneta
- ✓ Obrada incidenata na Internetu, ako se jedna od strana u incidentu nalazi u RH, osim tijela državne uprave (ZSIS CERT)
- ✓ Diseminacija informacija (vijesti, preporuke, dokumenti, brošure, alati)
- ✓ Forenzika, analiza malvera, mrežnog prometa, logova...
- ✗ operativno rješavanje problema i 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**.

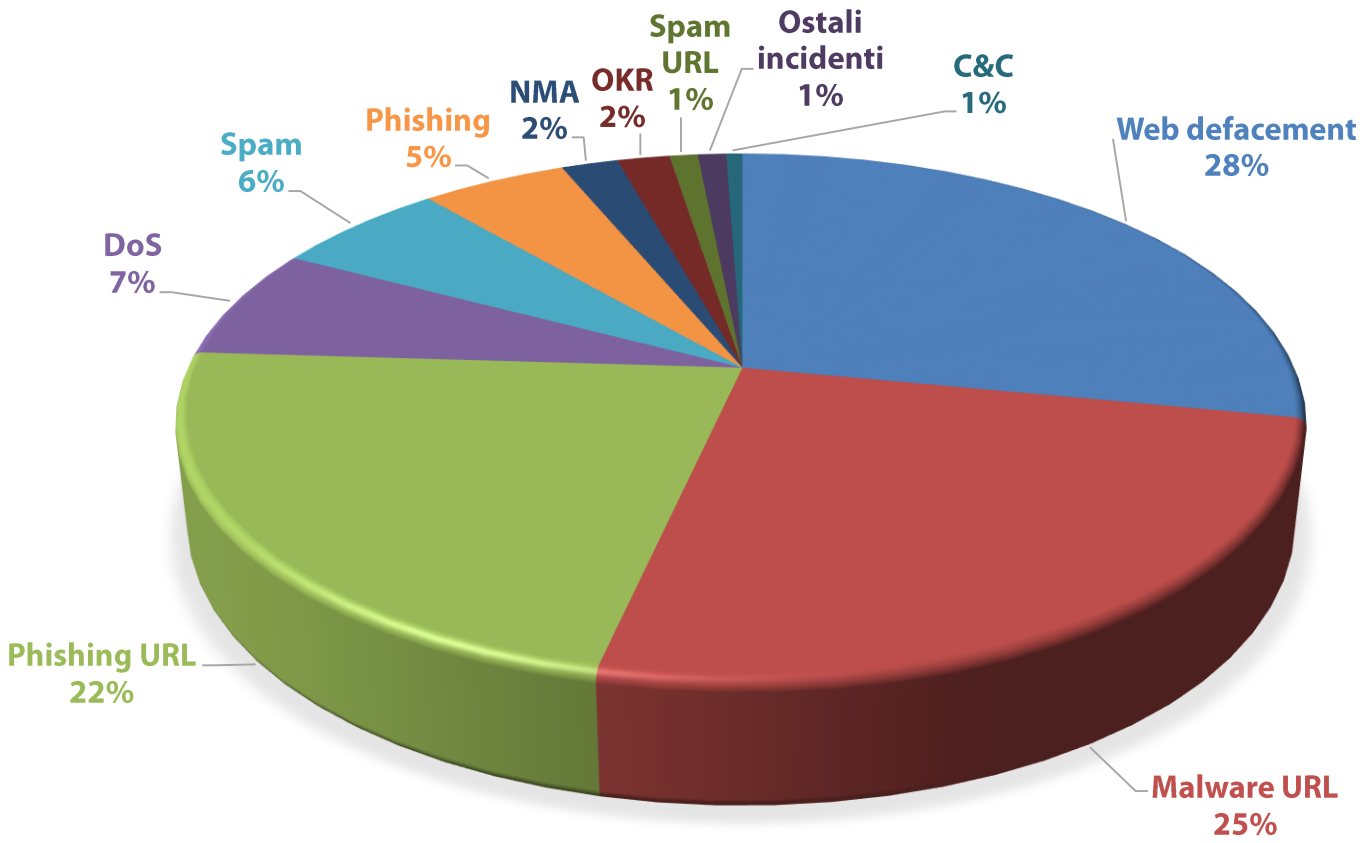
…

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)

Pregled vrste incidenata

UDIO VRSTE INCIDENATA (01.09.2015. - 31.08.2016.)
IZVOR: SRU@HR

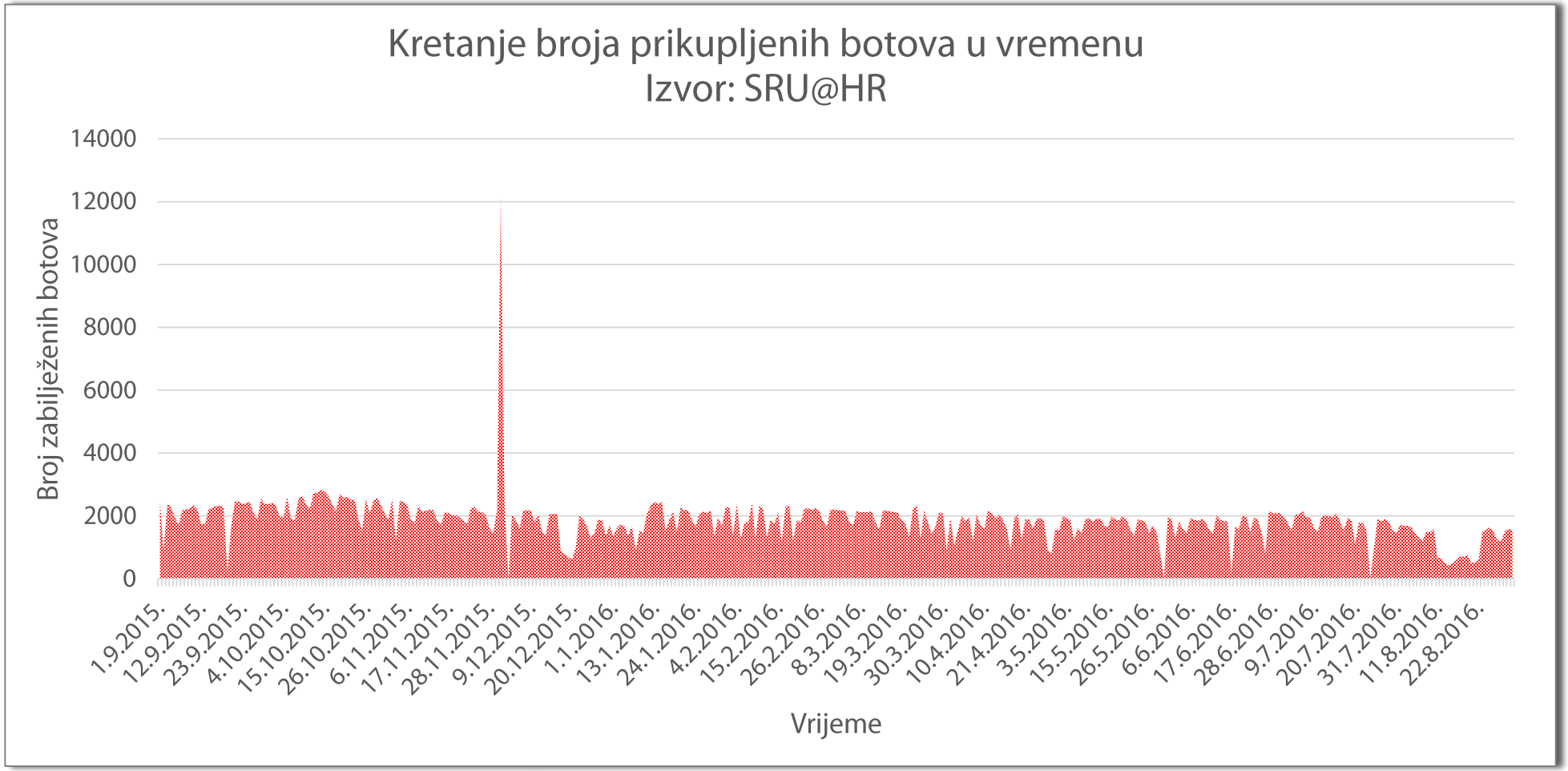


Naziv	Broj	Trend
Web defacement	202	↑
Malware URL	183	↓
Phishing URL	162	↓
DoS	49	↑
Spam	43	↑
Phishing	36	↓
NMA	14	↑
OKR	13	↑
Spam URL	7	↓
Ostali incidenti	7	↓
C&C	4	↓

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Pregled kretanja broja botova



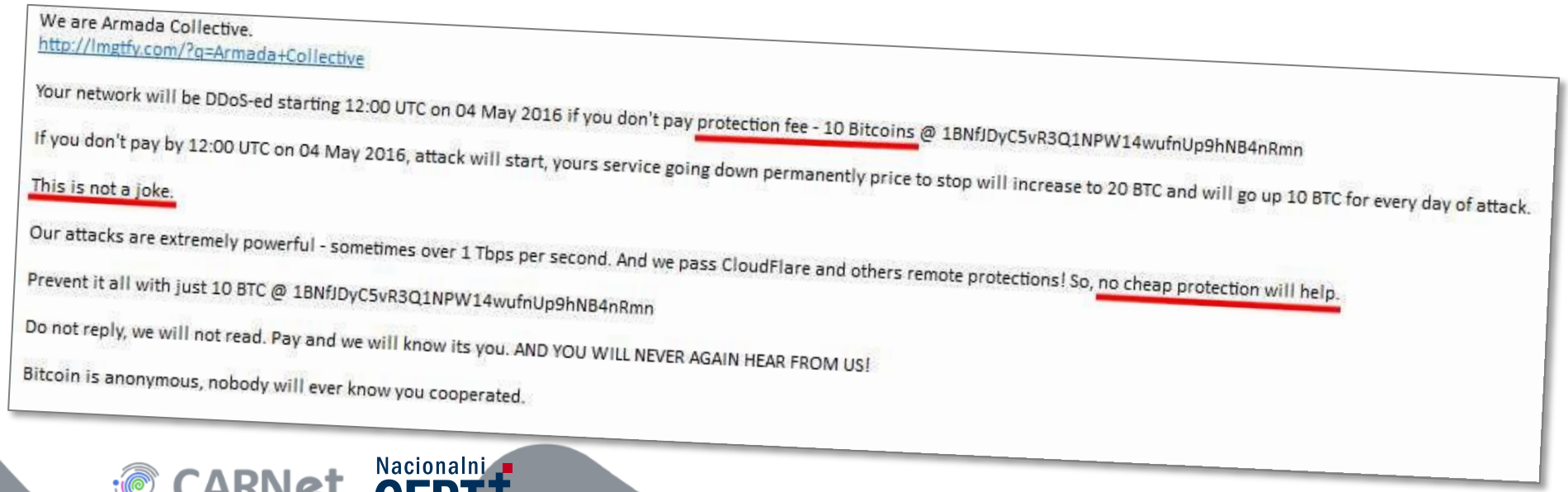
CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

DDoS napadi i prijetnje

- Zabilježen povećan broj DDoS napada

  (TCP SYN flood, UDP flood, NTP amplification, SSDP reflection)
- Zabilježeni slučajevi „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.

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

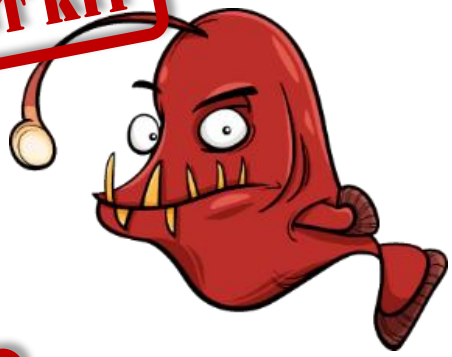
Phishing kampanje

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

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

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

Hvala na pažnji

ncert@cert.hr

www.cert.hr

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT