SIGURNOSNE PRIJETNJE U SAJBER PROSTORU

Haris Lokvančić

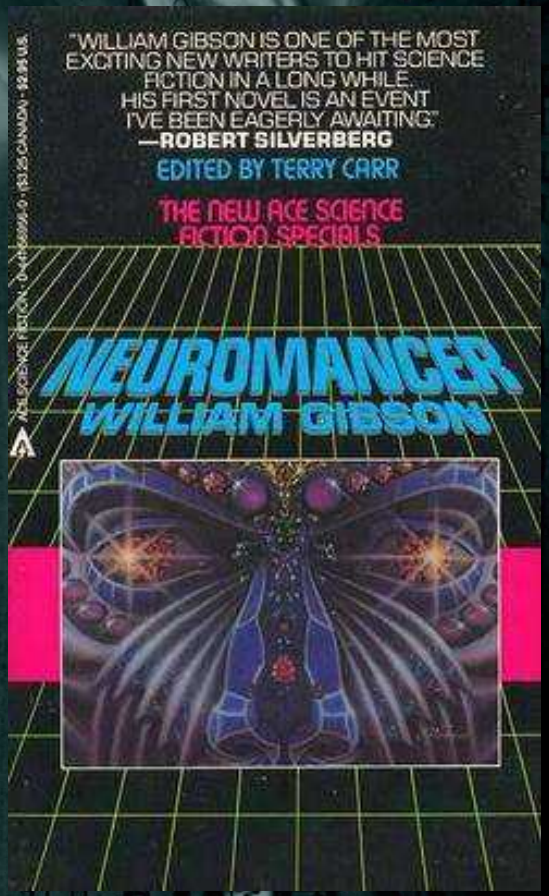
Sarajevo, 25.04.2018.

SAJBER PROSTOR – DEFINICIJA

- *Sajber (eng. cyber): „sve što se odnosi na, ili uključuje, računare ili računarske mreže (kao što je Internet)“ (Merriam-Webster Dict.)*

- *Sajber prostor je više nego Internet, uključuje ne samo hardver, softver i informacione sisteme, već i ljude, društvenu interakciju u okviru ovih mreža*

- *„Sajber okruženje (eng. cyber environment) uključuje korisnike, mreže, uređaje, cjelokupan softver, procese, informacije koje se čuvaju ili komuniciraju, aplikacije, servise i sisteme koji mogu biti direktno ili indirektno povezani sa mrežama“. (ITU)*

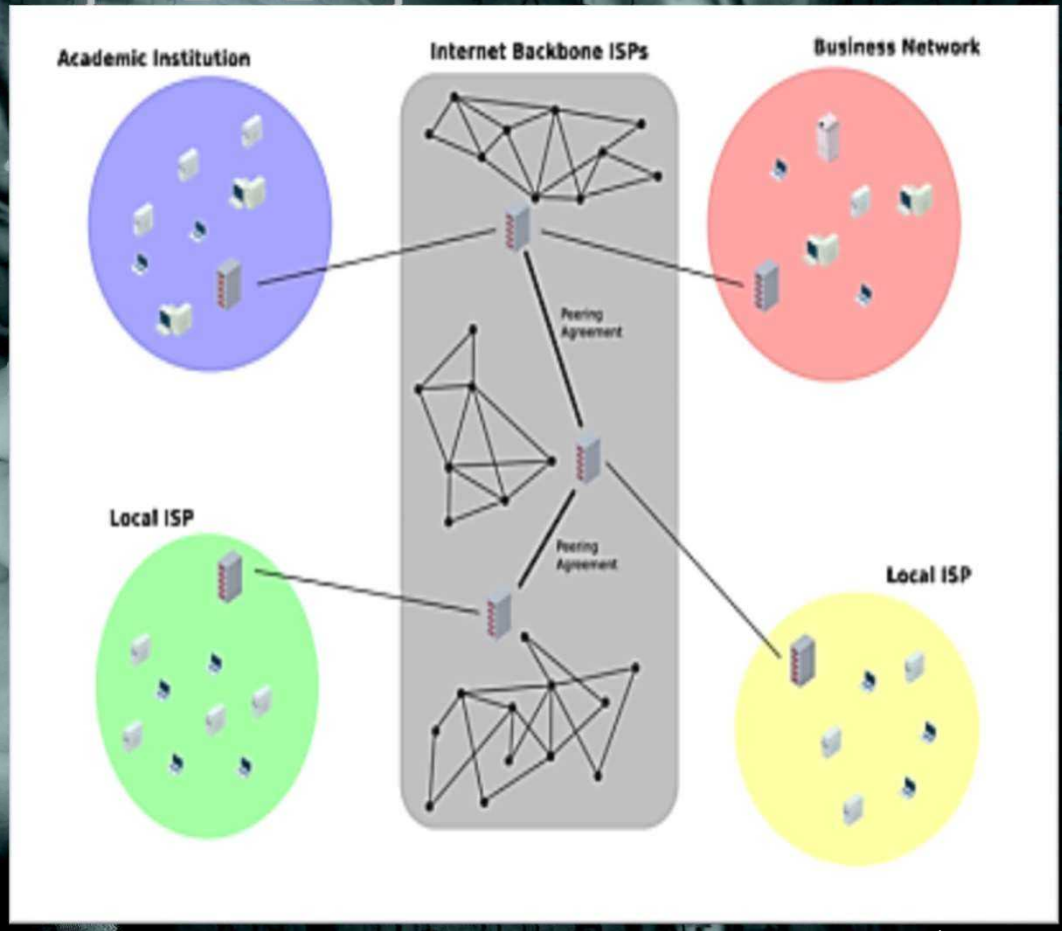


INTERNET I WWW - DEFINICIJE

- Internet : globalni, javno dostupni informacijski sistem međusobno povezanih kompjutera i kompjuterskih mreža koji komuniciraju putem IP grupe protokola (TCP/IP) = **globalna paketna podatkovna mreža („mreža svih mreža“)**

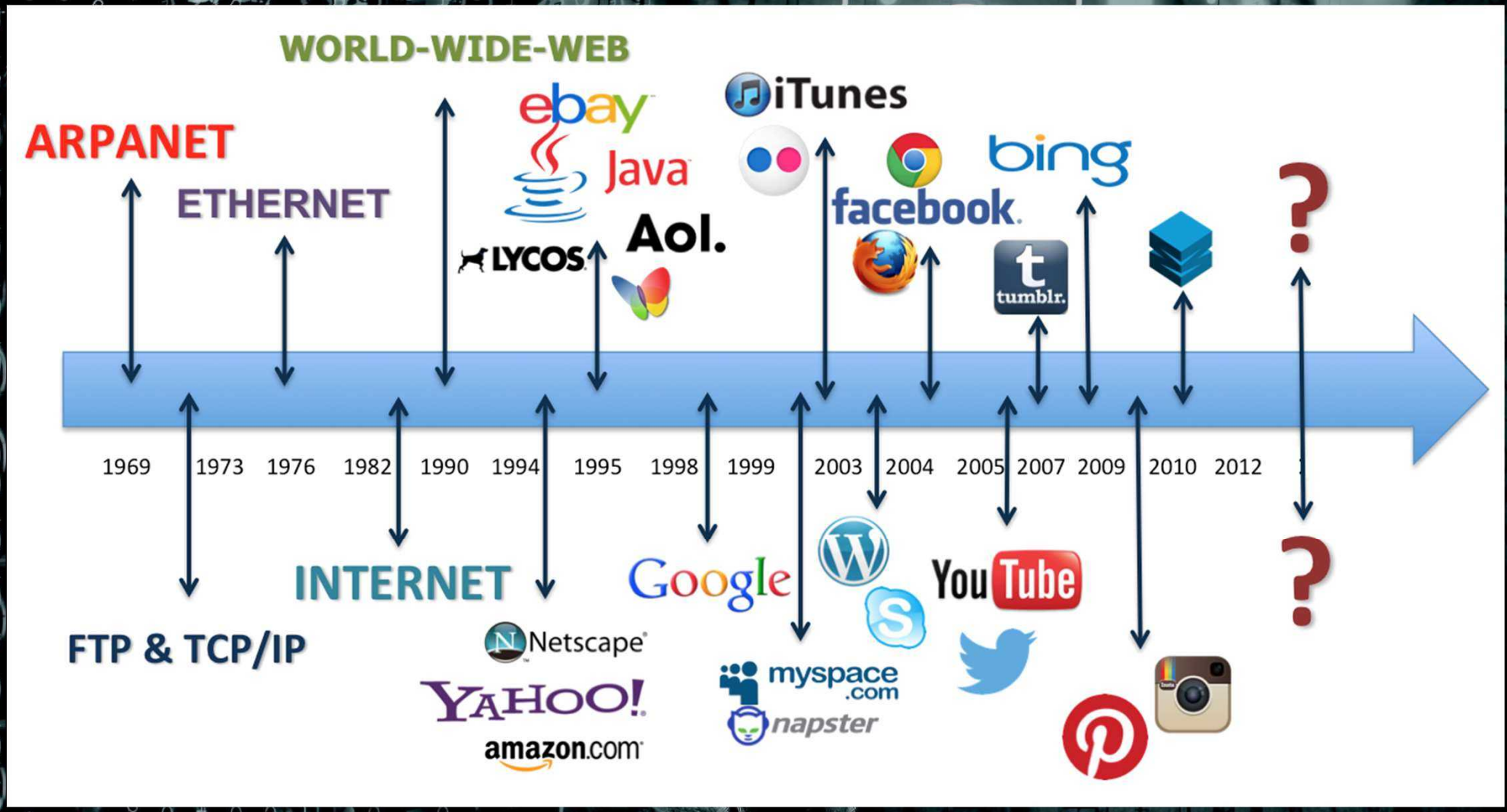
- www ≠ Internet

- World Wide Web (*radna. def.*) : usluga (servis) na Internetu koji, korištenjem posebnog protokola (**HTTP) omogućava** prenos hiperteksta ili multimedijalnih podataka = **omogućava „surfanje“ po Internetu**



Credit UNDOC

RAZVOJ INTERNETA



Credit Global News (adapted)

„STRATIFIKACIJA“ WEBA

Credit Global News (adapted)

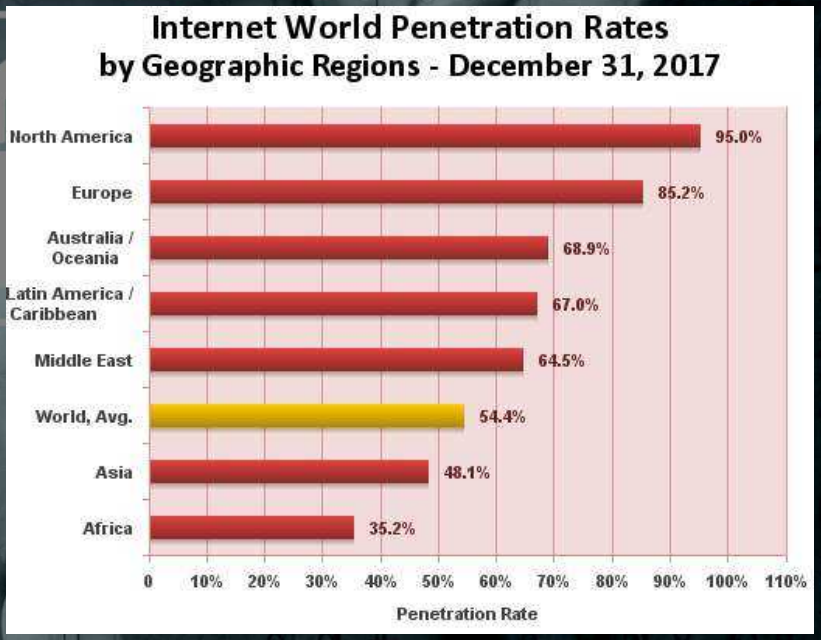
INTERNET– STATISTIKE 2017

- 3,8 milijardi korisnika Interneta – 54% svjetskog stanovništva (2 milijarde u 2015.)
- 4,9 milijardi pojedinačnih korisnika mob. uređaja

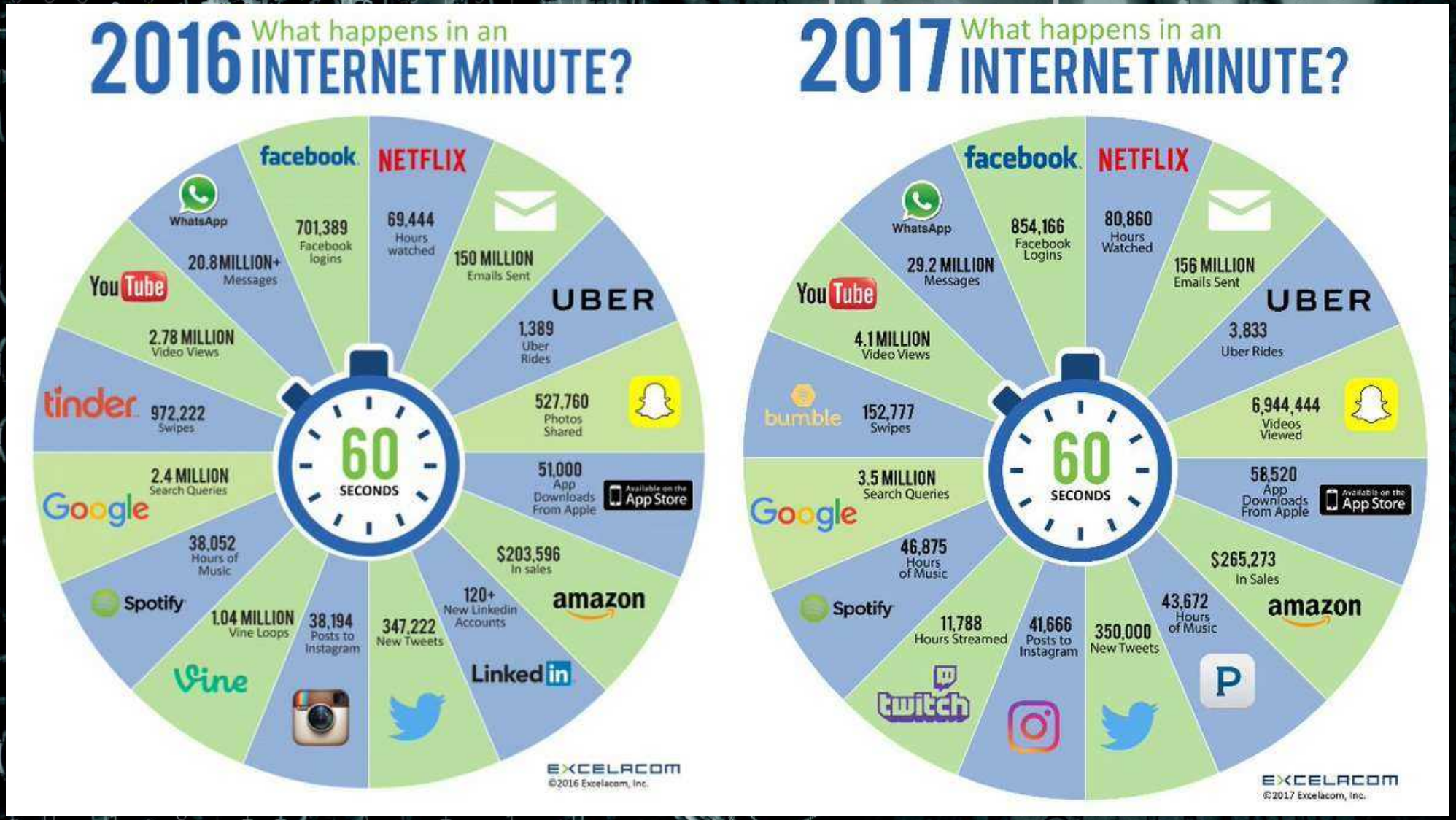
BIH

- 3‘000‘000 korisnika Interneta (700‘578 pretplatnika)
- 70 ISP operatora
- 3‘319‘084 pojedinačnih korisnika mob. uređaja

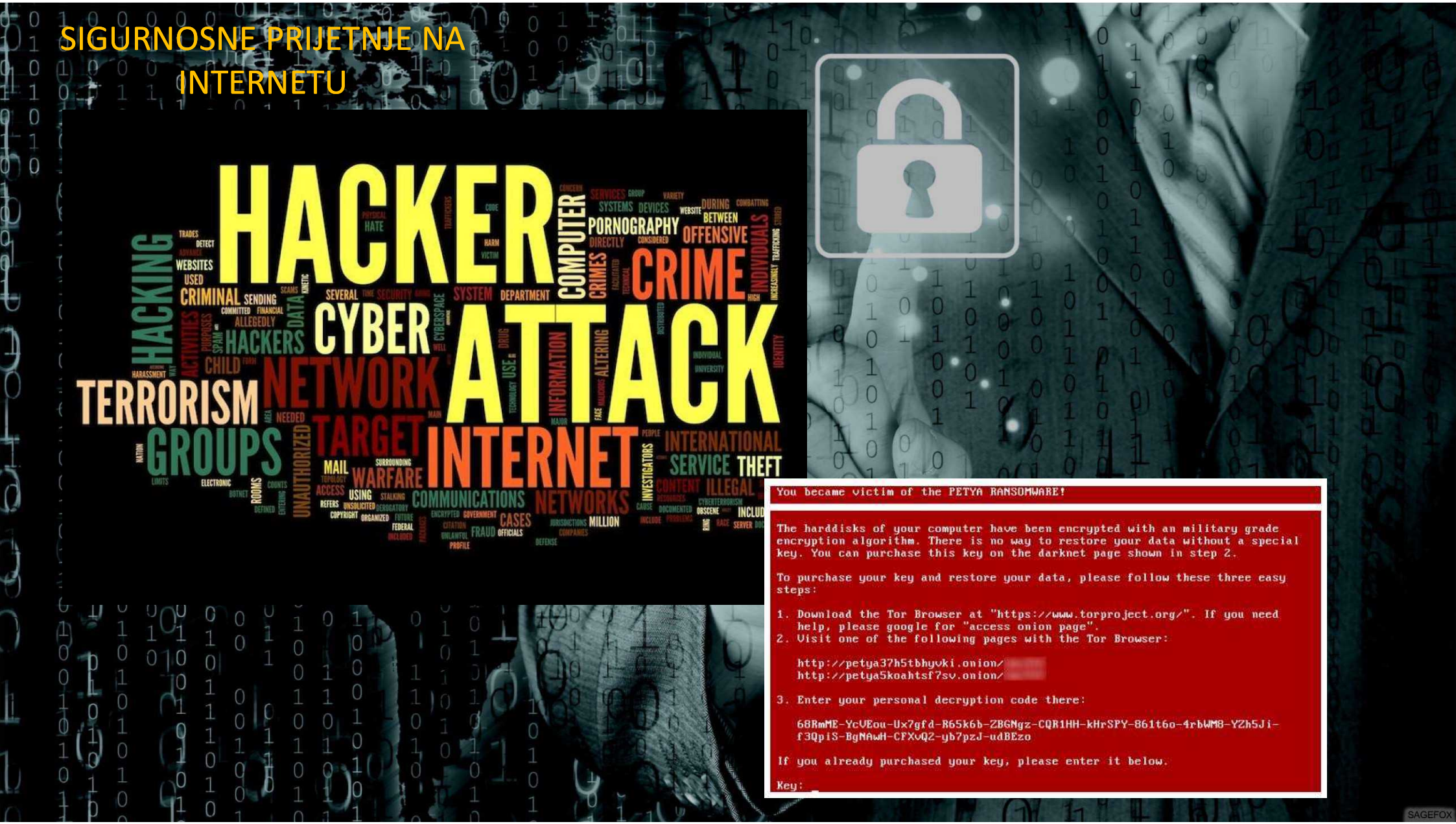
Izvori: Internetworldstats, ITU, UN, RAK BiH



INTERNET U 1 MINUTI



SIGURNOSNE PRIJETNJE NA INTERNETU



SIGURNOSNE PRIJETNJE PREMA MOTIVIMA POČINITELJA

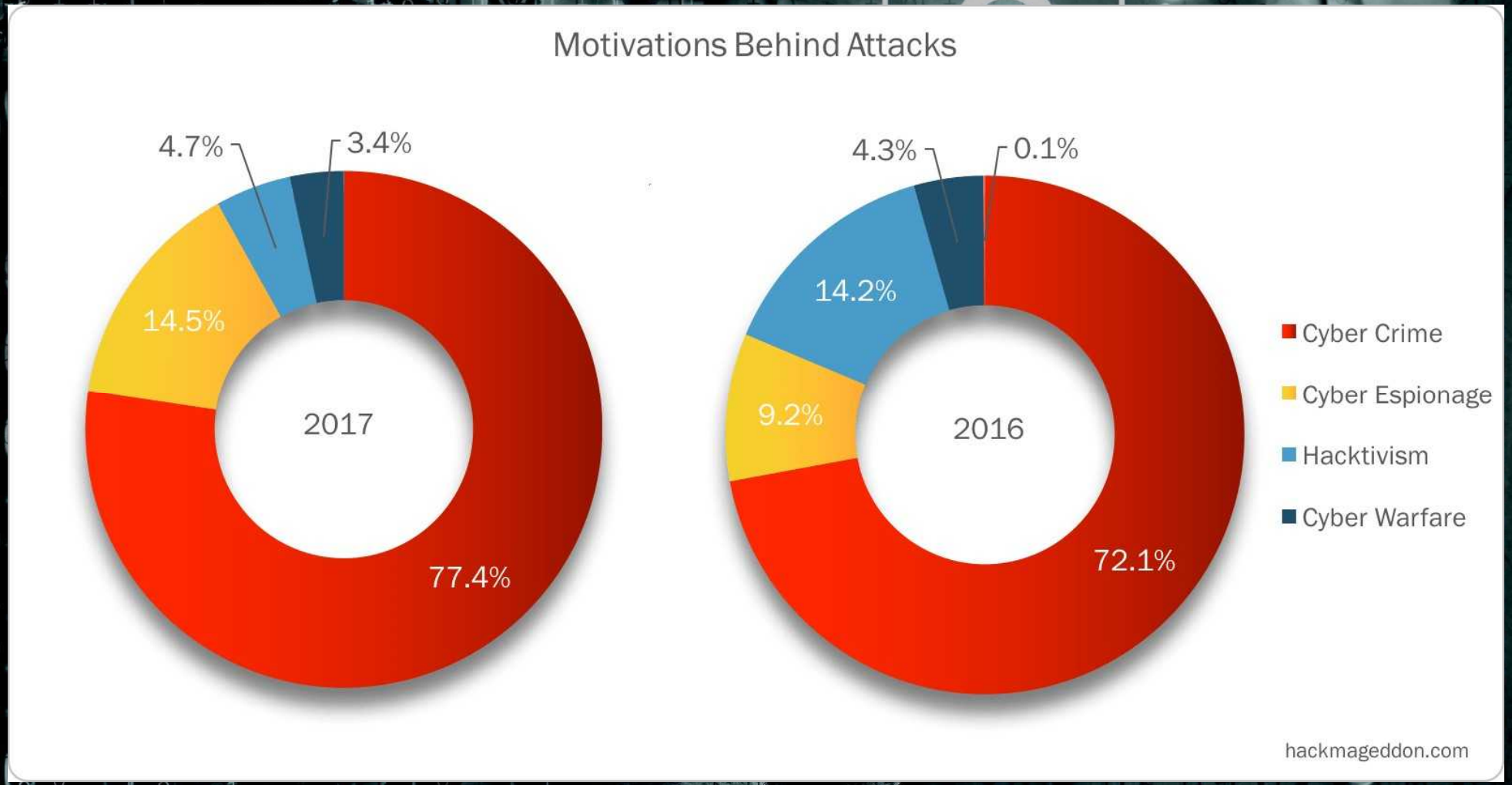
- „Klasični sajber kriminal“ - ekonomski motivi (sajber prevare, haking, krađa internet usluga, piratstvo softvera, mikročipova i baza podataka, sajber industrijska špijunaža, lažne internet aukcije, proizvodnja i distribucija nedozvoljenih i štetnih sadržaja - trgovina, oružjem i drogom, ljudskim organima, dječija pornografija, pedofilija)

- Politički motivi (sajber špijunaža, haking, širenje rasističkih i nacionalističkih ideja i stavova, sekte, sajber sabotaža, sajber terorizam, sajber ratovanje)

- Samodokazivanje (haking radi zabave, prestiža)

- Povreda privatnosti (nadgledanje elektronske pošte, spam, prisluškivanje i snimanje)

STATISTIKE NAPADA NA INTERNETU U 2015. I 2016. (PREMA MOTIVU)



Izvor: hackmaggedon.com (na uzorku od 1061 i 950 napada)

SIGURNOSNE PRIJETNJE PREMA METODU POČINJENJA

- Maliciozni softveri - Malwares (virus, crv, trojanac, ransomware,...)
- Hakovanje („provaljivanje“ u kompjuter ili sistem radi rekonfiguracije ili reprogramira)
- Phishing (pokušaj krađe podataka putem falsifikovane stranice)
- Socijalni inžinjering (proces obmanjivanja, uključujući lažno predstavljanje, kako bi se žrtva navela na davanje zaštićenih informacija)
- Spam (slanje neželjenih masovinh poruka)
- DoS/DDoS (povećanje beskorisnog prometa s ciljem preopterećivanja mreže – uskraćivanje usluga)

SAJBER KRIMINAL - DEFINICIJA

- Sajber kriminal (e-kriminal, VTK): kriminalne aktivnosti u kojima su kompjuteri i slični informatički uređaji i kompjuterska mreža predmet, sredstvo, cilj ili mjesto krivičnog djela

- Konvencija o kibernetičkom kriminalu (CoE, 2001.)

  - Krivična djela protiv povjerljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema (nedozvoljen pristup, nezakonito presretanje, ometanje podataka, ometanje rada sistema, zloupotreba uređaja)
  - Krivična djela u vezi sa kompjuterom (kompjuterska prevara, kompjutersko krivotvorenje)
  - Krivična djela u odnosu na sadržaj (dječija pornografija)
  - Krivična djela koja se odnose na povredu autorskog i srodnih prava

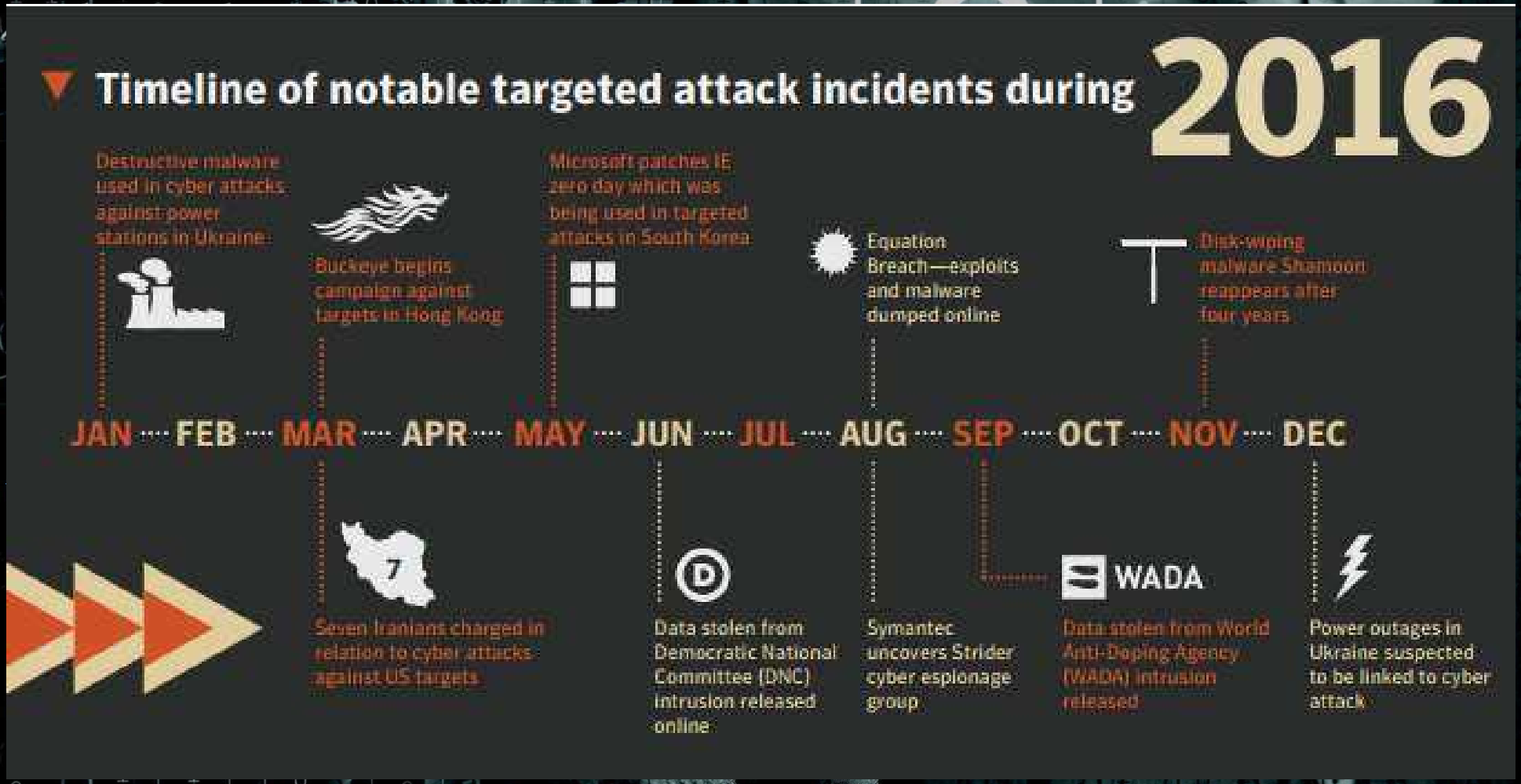
© CoE

INTERNET I SAJBER KRIMINAL – STATISTIKE 2016/2017 I PREDVIĐANJA

- 978 miliona ljudi pogođeno nekogm vrstom sajber kriminala (689,4 miliona u 2016.) – najć. kompromitacija lozinke
- 172 milijarde USD štete za direktno oštećene u 2017. (ca. 142 USD/osobi)
- Napad ransomware-om svakih 40s (očekuje se porast na svakih 19s do 2019.) – povećanje za 36% u odnosu na 2016!
- 1,4 miliona phishing web stranica naprave se mjesečno, 230‘000 novih malware-a proizvede se dnevno
- Do 2021. - preko 3,5 miliona upražnjenih radnih mjesta u domenu sajber sigurnosti

Izvori: Cybersercurty Ventures, Symantec, Microsoft

PREGLED NAJVEĆIH (USMJERENIH) NAPADA NA INTERNETU U 2016.

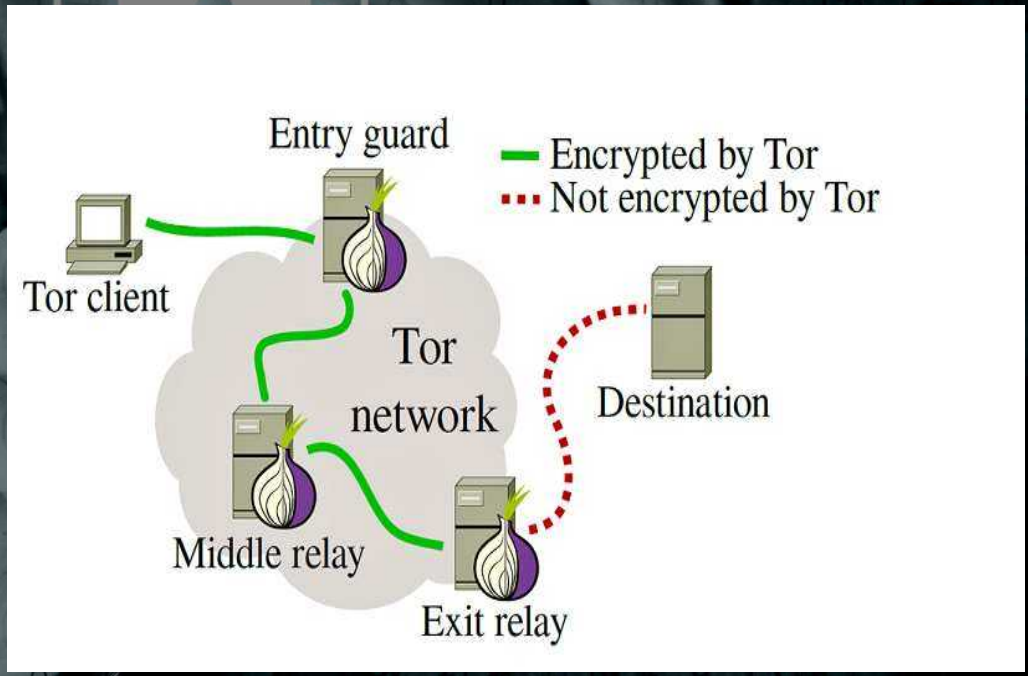


Izvor: Symantec

DARKNET I TOR

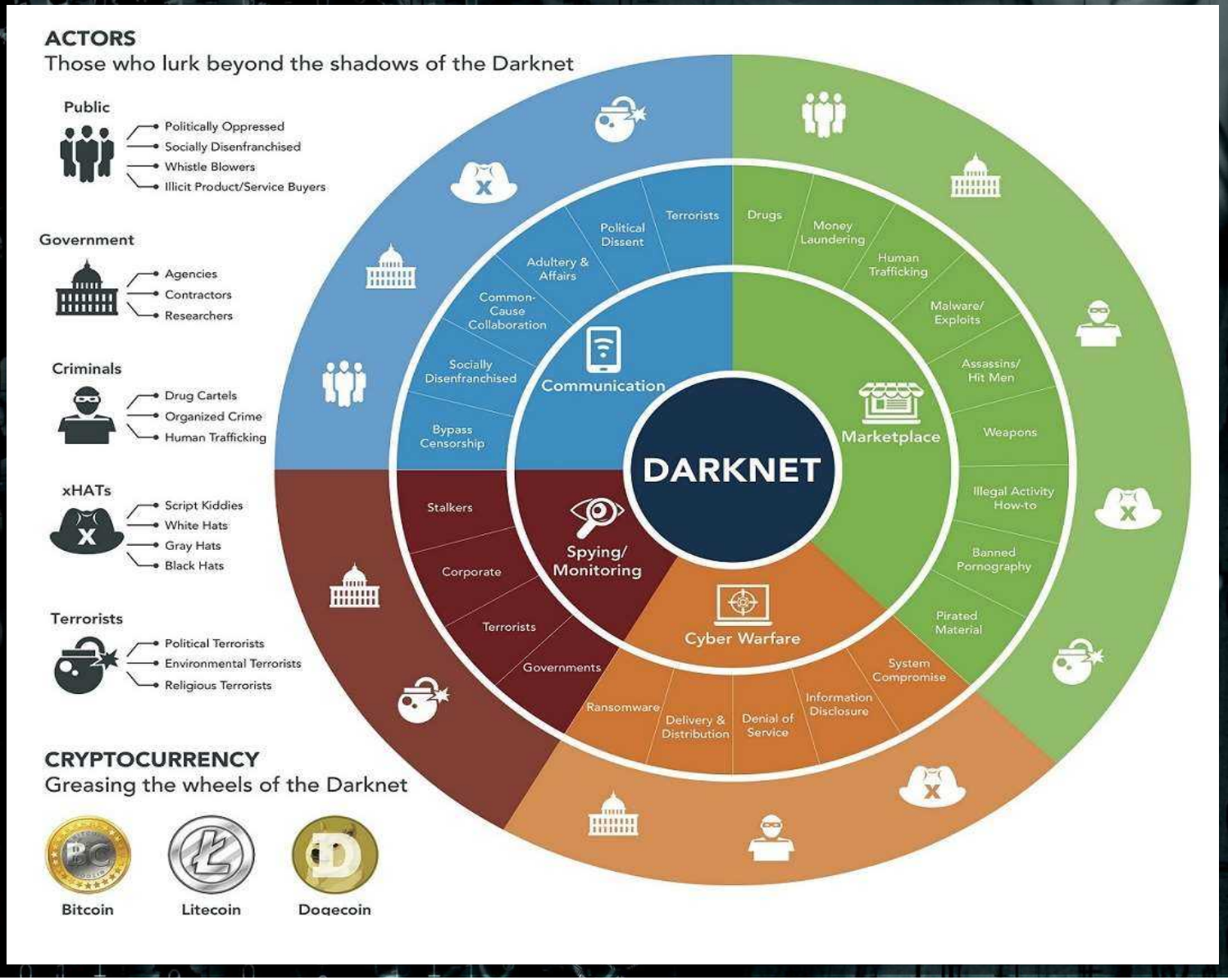
- Darknet (Dark Web) : manji dio Deep Web-a (ca. 6%), sa kriptovanim mrežnim sadržajem koji nije indeksiran (namjerno skriven) i nije mu moguće pristupiti „tradicionalnim“ pretraživačima (IE, Google Chrome, Firefox), već zahtijeva poseban softver (npr. Tor)

- Tor (engl. *The Onion Router*): (besplatni) sofver za omogućavanje anonimne komunikacije na Internetu preusmjeravanjem unutar distribuirane mreže poslužitelja (sakriva stvarnu IP adresu prolazeći kroz mrežu tzv. releja)
  - .onion domena



Credit Tor Project

DARKNET – PODZEMLJE PODZEMLJA

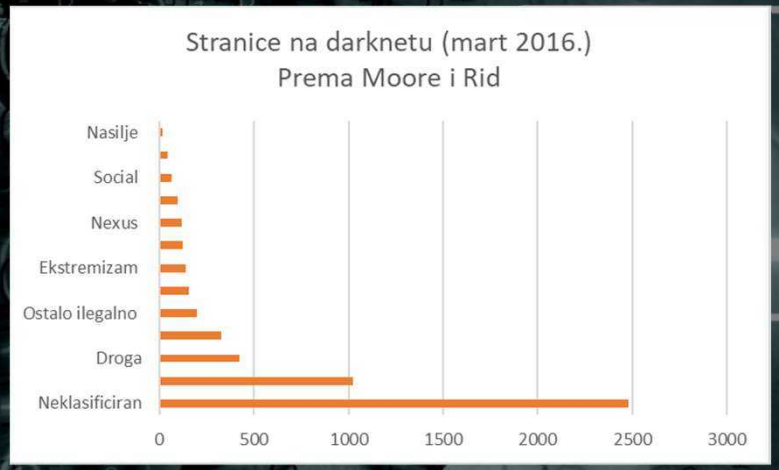


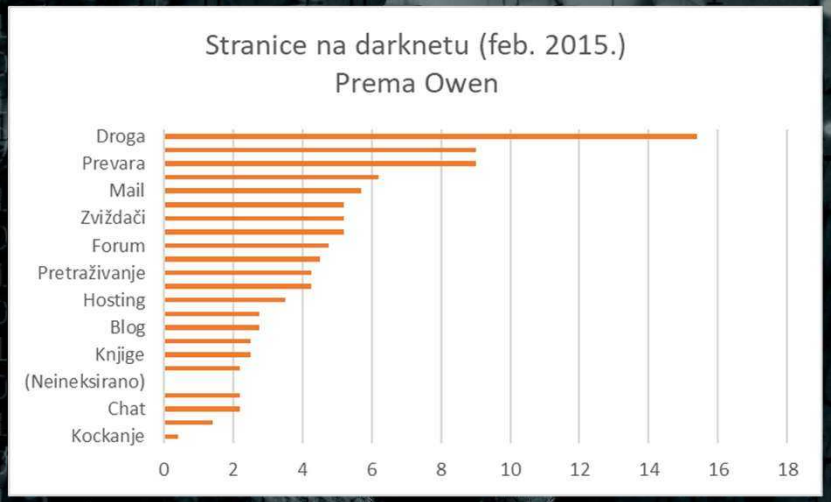
Prema Batblue.com

DARKNET – SADRŽAJ

KATEGORIJA STRANICA	Br.
Neklasificiran	2,482
Ostalo	1,021
Droga	423
Finansije	327
Ostalo ilegalno	198
Nepoznato	155
Ekstremizam	140
Ilegalna pornografija	122
Nexus	118
Hacking	96
Social	64
Oružje	42
Nasilje	17
Ukupno	5,205
Ukupno aktivni	2,723
Ukupno ilegalni	1,547

Prema Moore i Rid 2016.





Prema Owen 2015.

KATEGORIJA STRANICA	%
Kockanje	0.4
Oružje	1.4
Chat	2.2
Novo (Neindeksirano)	2.2
Zlostavljanje	2.2
Knjige	2.5
Direktorij	2.5
Blog	2.75
Pornografija	2.75
Hosting	3.5
Hacking	4.25
Pretraživanje	4.25
Anonimnost	4.5
Forum	4.75
Krivotvorenje	5.2
Zviždači	5.2
Wiki	5.2
Mail	5.7
Bitcoin	6.2
Prevara	9
Crno tržište	9
Droga	15.4

SILKROAD 1.0

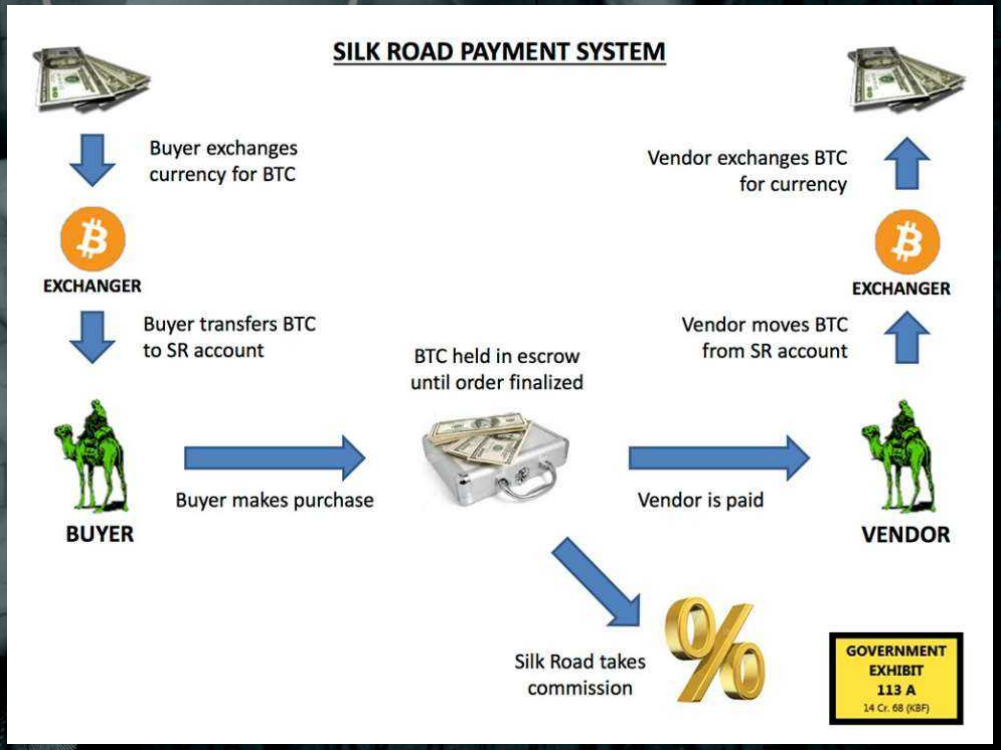
- Silk Road 1.0: platforma za ilegalnu trgovinu online od februara 2011. do oktobra 2013.
- Osnivač: Ross William Ulbricht ("Dread Pirate Roberts“)
  - uhapšen 02.10.2013.
  - pravosnažno osuđen na doživotnu kaznu zatvora 31.05.2017.
- Silk Road 2.0 pokrenut 06.11.2013. i ponovo oboren 06.11.2014. (operacija „Onymus“)
- Silk Road 3.1 : http://silkroad7rnpuhj.onion

Credit freeross.org

SILKROAD 1.0 U BROJKAMA

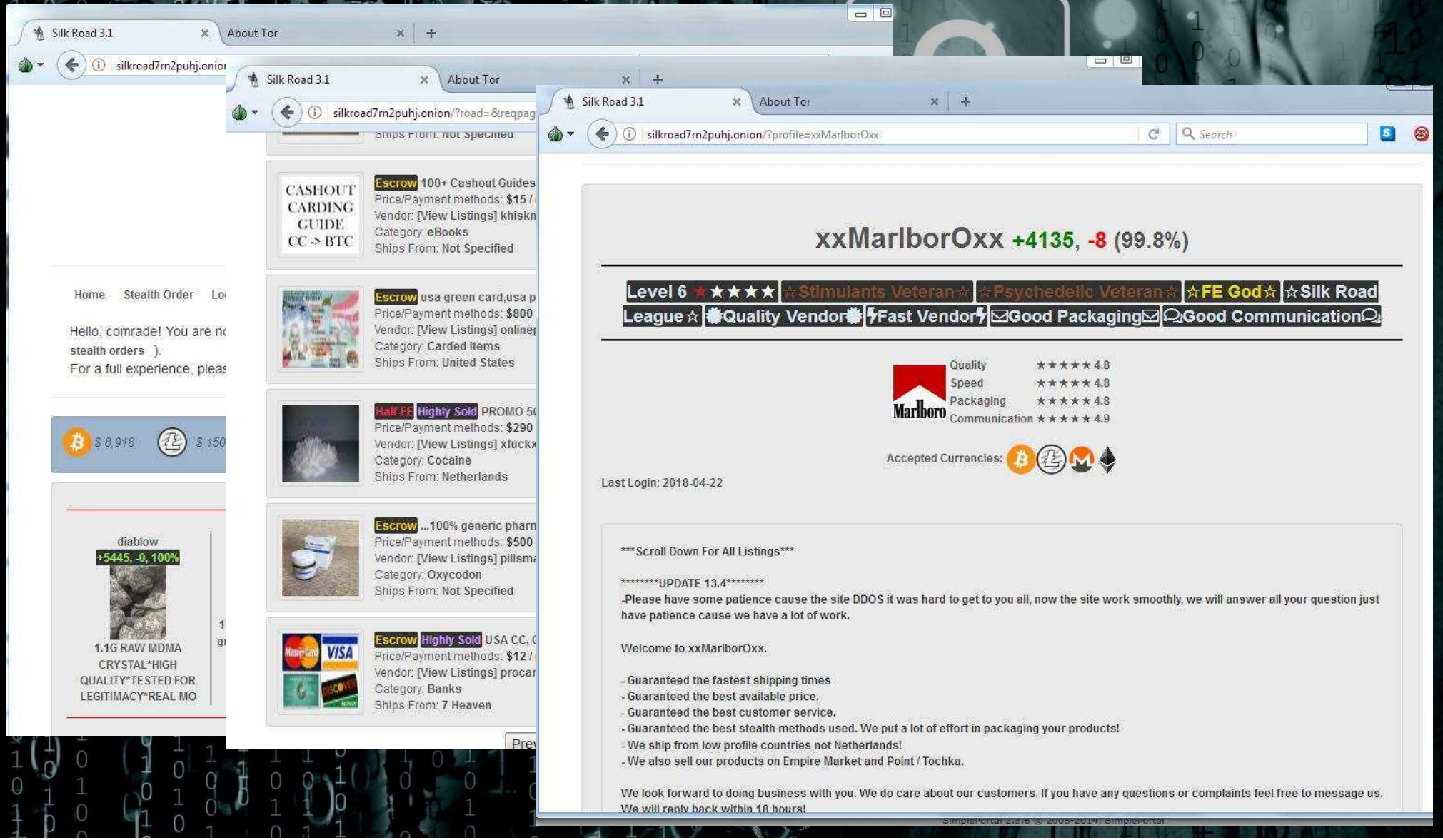
- 146‘946 pojedinačnih korisnika
- 3877 prodavača
- 1,23 miliona transakcija
- Escrow plaćanje
- Ukupan promet u periodu postojanja: 9,3 mio BTC (1,2 milijarde USD)
- Provizija Silk Road: 600‘000 BTC (ca. 78 mio USD)
- 26‘000 BTC u posjedu Ulbricht-a kada je uhapšen

Silk Road
anonymous marketplace



Credit WIKI

DARKNET – PRIMJER 1



DARKNET – PRIMJER 2

Updated: List of Dark Net Mark... | Valhalla

valhallaxmn3fydu.onion/products/96370

valhallaxmn3fydu.onion | All products | My purchases | Messages | Account (0.0 BTC) | Log out

2x Glock 17
Excellent condition, hardly used.

Similar products by other vend

Hard Candy - Hidden Wiki | The Pedophile's Handboo

xnyvcjj6ybauprjx.onion/handbook/main_index.h

Start | Resources | Download | Change log

Freedom
Accessibility
Simplicity
Info

Introduction

VENICEMAN KILLER HITMAN s... | About Tor

yo4jmu6dsfaeekt3.onion

>>Middlemen: read below.

I offer killer services,
I am the only legit killer on tor and I meet personally all my clients who ask, so you can judge me better.
My business is trusted because I put my face in it, and my personal risk.
I offer mainly killings and injuries, also some clients have been asking for damages, fires, finding disappeared people, investigations. I am willing to evaluate other custom services on request.

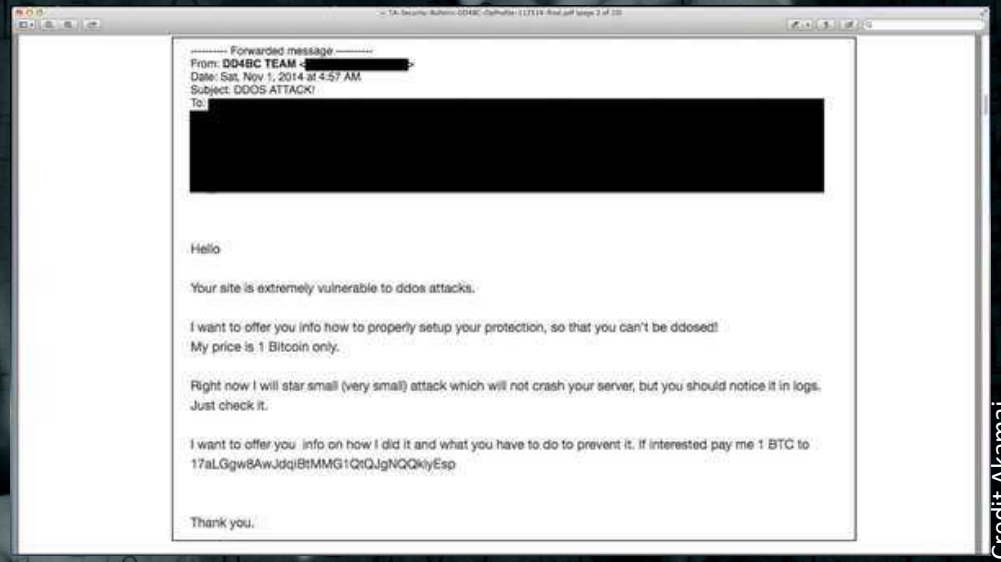
WHERE-WHEN:
Worldwide. Ask anytime availability via email or xmpp chat address.
I can be without delays in Europe, North-South-America, Middle-east, Australia, NZ, South-East-Asia, China, Japan, Africa. Some other countries could take few days/weeks more to arrange the travel visa, but I can operate worldwide.
After I accept the job, I will complete it in a definite time-frame. The usual time frame is one month from the day I arrive in the target country, but custom arrangements are possible.

KILLING:
The mode of execution for killing will be my choice. Gunshots, cuts, hammer, anything, this will be my choice depending on the target situation.
Proofs: deaths are reported in obituary notices for verification. If I can and if you specifically ask, then I will make a photo of the dead body.

PRICES:
Minimum price 70 000 euro plus expenses, depends on target, and depends on country, negotiable.
Expenses comprehend travel, accomodation, transportation, vehicle, new arms, etc. Price and expenses will be evaluated by email/chat after you tell the general info.
Payment currency: cash euro.
Alternative payments: bitcoins, dollars, gold coins (only US-MINT .9999 fine gold

DARKENT I BiH

- Akcija «Koverta» (oktobar 2017.)
- Akcija «Kriptus» (februar 2016.)
- Akcija «Pleiades» (decembar 2015.)
  - Europol, u saradnji sa Austrijom, BiH, Njemačkom, Švicarskom i V. Britanijom
  - podignuta optužnica protiv P.T. (1983.) u martu 2017. (Okružno javno tužilaštvo B. Luka)



---------- Forwarded message ----------
From: **DD4BC TEAM** <[redacted]>
Date: Sat, Nov 1, 2014 at 4:57 AM
Subject: DDOS ATTACK!
To: [redacted]

Hello

Your site is extremely vulnerable to ddos attacks.

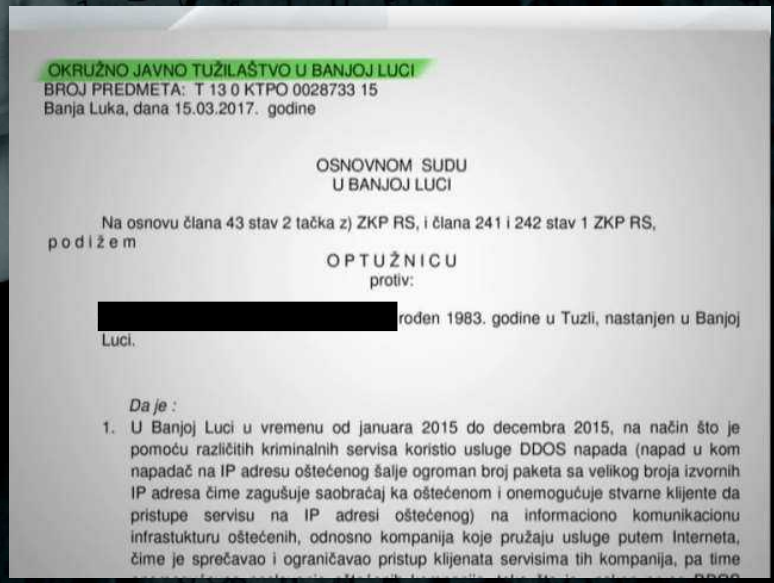
I want to offer you info how to properly setup your protection, so that you can't be ddosed!
My price is 1 Bitcoin only.

Right now I will star small (very small) attack which will not crash your server, but you should notice it in logs.
Just check it.

I want to offer you info on how I did it and what you have to do to prevent it. If interested pay me 1 BTC to 17aLGgw8AwJdqiBtMMG1QtQJgNQQkIyEsp

Thank you.

Credit Akamai



OKRUŽNO JAVNO TUŽILAŠTVO U BANJOJ LUCI
BROJ PREDMETA: T 13 0 KTPO 0028733 15
Banja Luka, dana 15.03.2017. godine

OSNOVNOM SUDU
U BANJOJ LUCI

Na osnovu člana 43 stav 2 tačka z) ZKP RS, i člana 241 i 242 stav 1 ZKP RS,
podižem

O P T U Ž N I C U
protiv:

[redacted] rođen 1983. godine u Tuzli, nastanjen u Banjoj Luci.

Da je :

1. U Banjoj Luci u vremenu od januara 2015 do decembra 2015, na način što je pomoću različitih kriminalnih servisa koristio usluge DDOS napada (napad u kom napadač na IP adresu oštećenog šalje ogroman broj paketa sa velikog broja izvornih IP adresa čime zagušuje saobraćaj ka oštećenom i onemogućuje stvarne klijente da pristupe servisu na IP adresi oštećenog) na informaciono komunikacionu infrastukturu oštećenih, odnosno kompanija koje pružaju usluge putem Interneta, čime je sprečavao i ograničavao pristup klijenata servisima tih kompanija, pa time

SAGEFOX

SAJBER RATOVANJE – DEFINICIJA I KARAKTERISTIKE

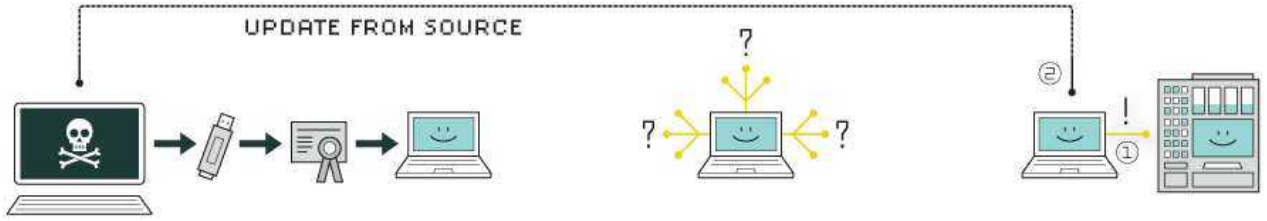
- *„sajber napadi autorizovani od strane državnog učesnika pokrenutI protiv sajber infrastrukture istovremeno sa (odgovarajućom) vladinom kampanjom“* EastWest Institute

- Karakteristike sajber ratovanja:
  - namjerna i organizovana aktivnost primjene sile prema protivniku u cilju nanošenja štete njegovim resursima, vrijednostima, stanju i interesima;
  - ostvaruje se u sajber prostoru i iz sajber prostora, što znači primjenom informacionih sistema i informacija u njima i dejstvom na informacione sisteme i informacije u njima;
  - preduzima se od strane države ili organa u ime države;
  - izvodi se u cilju ostvarivanja vojnih i političkih ciljeva.

Prema Mladenović 2016.

SAJBER RATOVANJE – PRIMJER
STUXNET – „PRVO CYBER ORUŽJE“

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

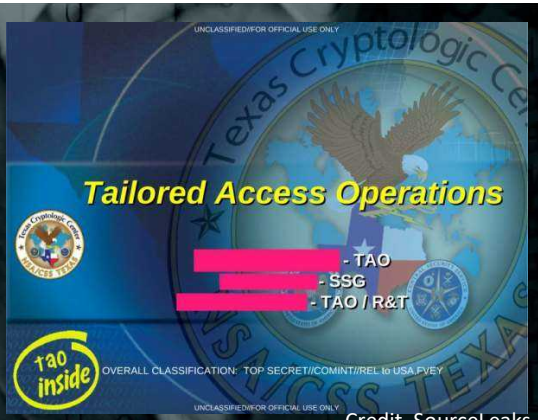
2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.



Credit SourceLeaks


Credit Forbes


Credit President's Office Iran

PITANJA ?

HVALA NA PAŽNJI!

l_haris@hotmail.com; haris.lokvancic@eda.admin.ch