Dinko Korunić, InfoMAR

OBLICI RAČUNALNOG KRIMINALITETA

O predavaču

- certifikati: LPIC 1/2/3, SUSE Tech Spec, Novell CLA
- BUG, SRCE, CARNet, InfoMAR, Crossvallia
- FER, FSB, VSS, FPZ, HGI-CGS, ...
- Ured predsjednika RH, Vijetnamska vlada, Ministarstvo financija, Vlada republike Hrvatske, IGH, Hrvatska narodna banka, 24 sata, Netgen, Sense consulting, Algebra, T-mobile, VB Leasing, ...
- R&D manager - non-mainstream sadržaj i Alexa top 200 sajtovi
- 17 godina Linux/Unix security iskustva

Napomene

- predavanje
  - ne smije biti suhoparno i dosadno
  - ako što nije jasno, pitajte
  - ako želite nešto komentirati, komentirajte
- materijala ima i previše
  - u 2 sata je skoro nemoguće pokriti sve
    - pokriveno površno, nedovoljno tehničkih činjenica
  - fokusirajmo se na bitno
  - izvori su brojni (sigurnosne liste, sigurnosne Web stranice, AV/firewall/itd. proizvođači)

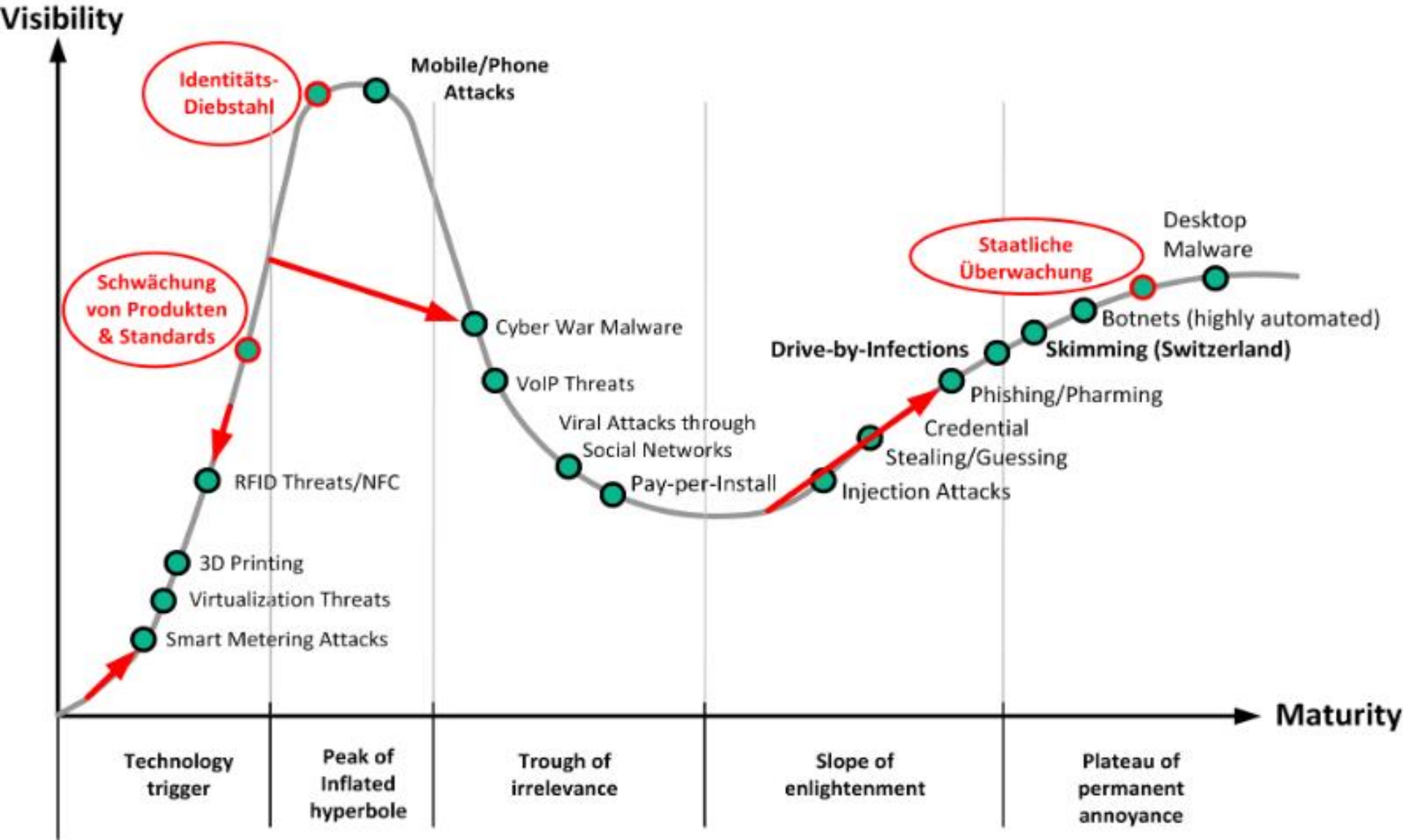
Tipovi

- računalo kao objekt napada:
  - virusi
  - DoS napadi
  - maligni kod - malware
- računalne mreže ili uređaji kao objekt:
  - stalking
  - prevara i krađa identiteta - phishing/scam
  - informacijski rat - cyber-warfare/espionage
  - spam

Tipovi (2)

- phishing/scam
  - krađa lozinki, kreditnih kartica, korisničkih imena i ostalih podataka radi koristi
  - lažni e-mail, IM poruke
  - zlonamjerni WiFi, manipulacija URL-ovima
- krađa identiteta
  - kriminalna, financijska, kloniranje identiteta, medicinska, itd.
  - ilegalna imigracija, terorizam, phishing, špijuniranje, krađa kreditnih kartica, dizanje kredita, itd.

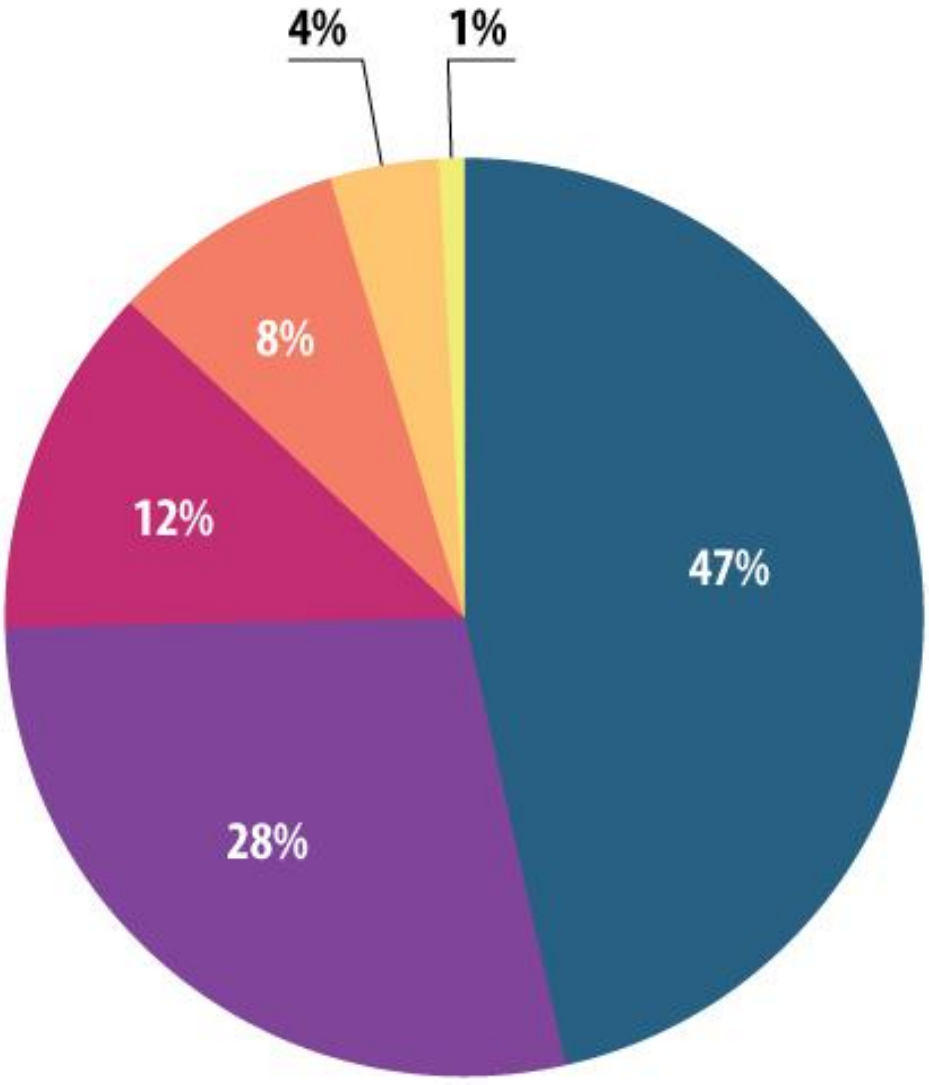
Krivulja opasnosti



Juice jacking

Juice jacking - USB condom

Online ranjivosti

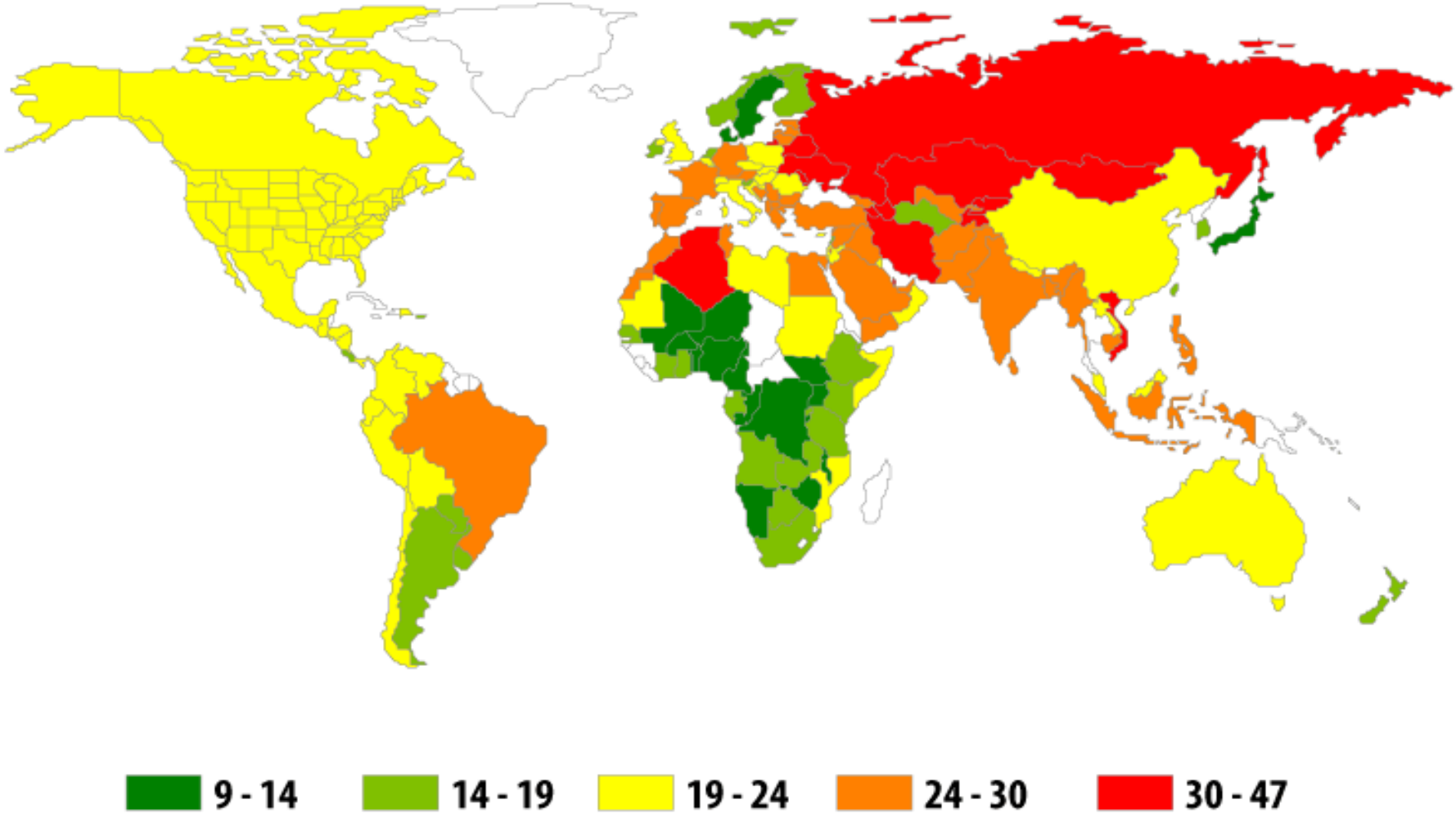


- 47% svih ranjivosti je u Web preglednicima
- skoro svaki paket ranjivosti i za Internet Explorer
- Java ranjivosti na drugom mjestu
- Adobe Reader na trećem mjestu

Online ranjivosti

- Q3 2014 čak 26.641.747 jedinstvenih zlonamjernih objekata
- top 3 opasnih:
  - zlonamjerni URL: 59.83%
  - adware: 14.46%
  - trojan: 13.13%
- top 5 izvorišta:
  - USA 33.12%
  - Nizozemska 17.74%
  - Njemačka 13.48%
  - Rusija 9.12%
  - Ukranija 4%

Online ranjivosti – geo raspodjela opasnosti



Mobilne ranjivosti

- napadaju se uređaji (operativni sustav) i aplikacije
- razlog:
  - prikupljanje korisničkih podataka
  - bankovni/financijski podaci
  - SMS trojani
  - špijuniranje razgovora, nadzor, itd.
- vektor napada:
  - infekcija Web stranica
  - ukradene aplikacije (alternativni app store)
  - tekstualne poruke sa infektivnim adresama
  - sistemske ranjivosti (Android)
- 10.000.000 jedinstvenih zaraznih objekata u 2013

Mobilne ranjivosti – izvori

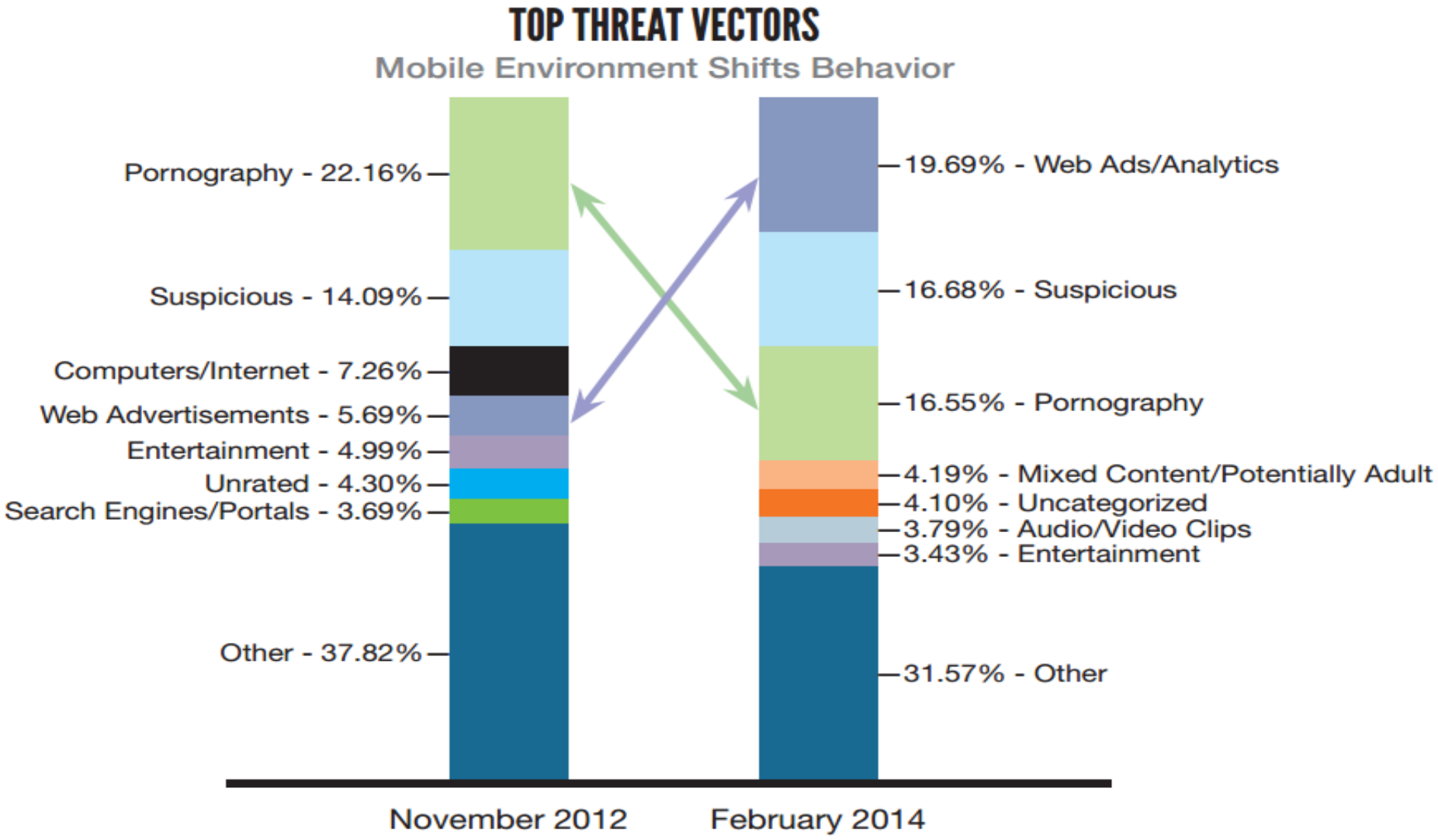
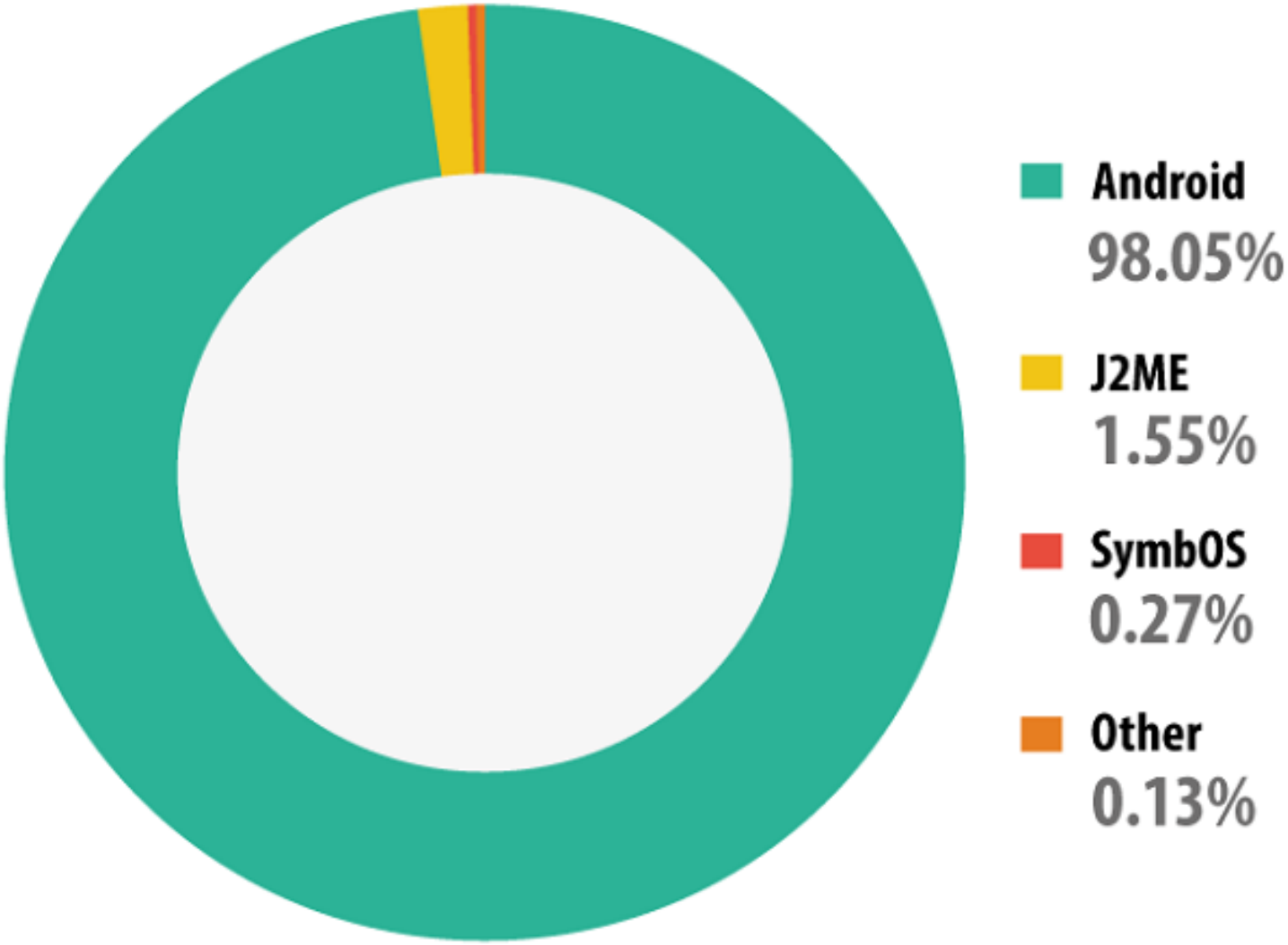
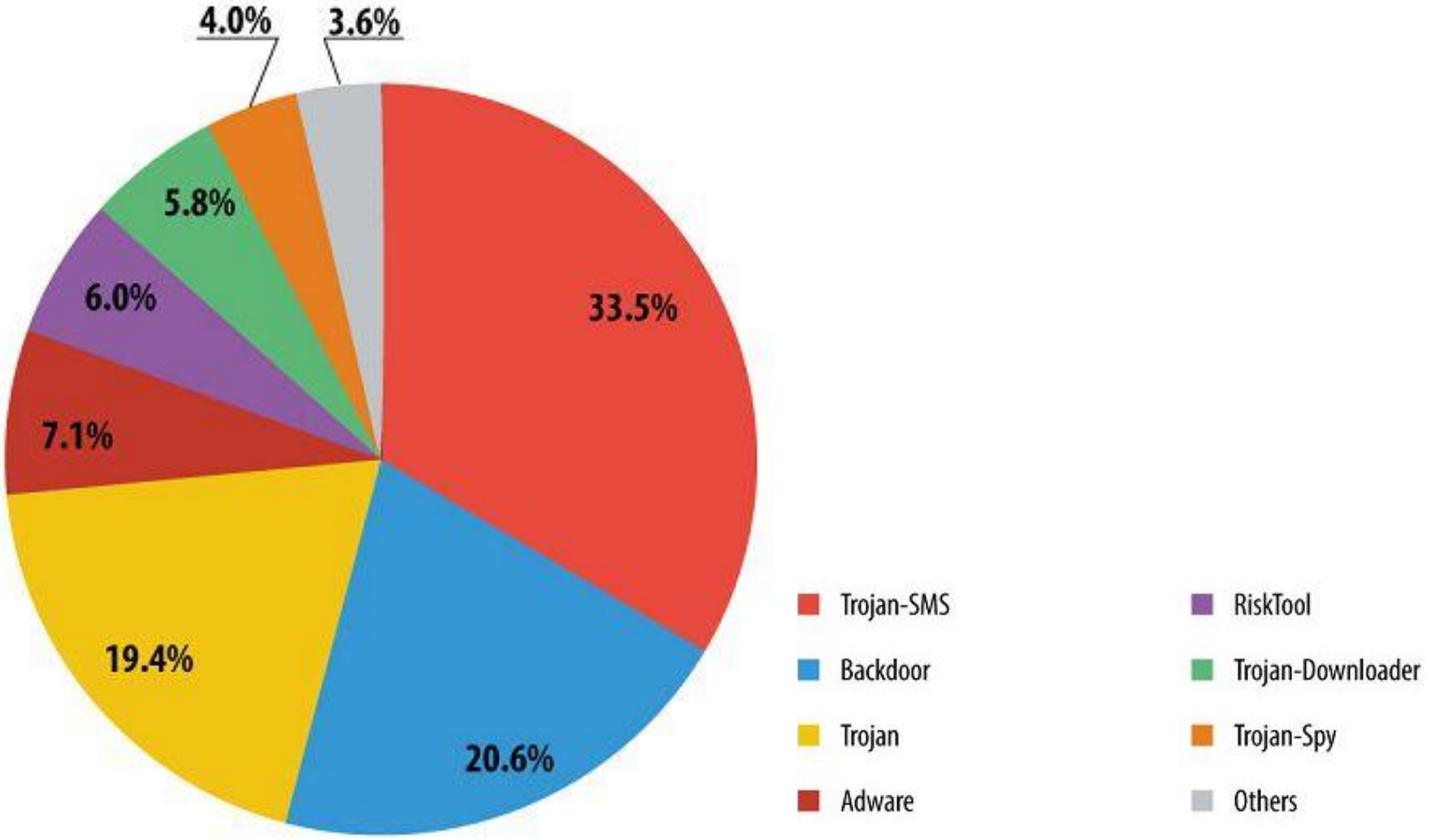


Figure 3: Shift in behavior for mobile users

Mobilne ranjivosti – raspodjela operativnih sustava



Mobilne ranjivosti – raspodjela tipova opasnosti



Mobilne ranjivosti – Svpeng

- krađa novca sa bankovnog računa
- širi se kroz SMS spam
- Trojan imitira Adobe Flash Player
- karakteristike:
  - skuplja informacije: IMEI, zemlja, provider, OS i jezik
  - krade SMS poruke i podatke o glasovnim pozivima – radi identifikacije banaka
  - krade novac sa računa (SMS) za direktno povezane brojeve
  - krade korisničke podatke za online banking

Mobilne ranjivosti – Svpeng (2)

- krade podatke o kreditnim karticama: broj, exp datum, CVV2/CVC2
- ucjenjuje korisnika da će blokirati telefon i traži novac
- sakriva tragove (sakriva SMS poruke i pozive od i prema banci)
- dobiva Administratorske ovlasti na uređaju da bi se zaštitio od brisanja

- slične aplikacije
  - Perkele - presreće mTAN
  - Wroba - briše i zamjenjuje postojeće banking aplikacije
- banking malware – trend 2013 i 2014
  - trenutan fokus Rusija

Krađa identiteta / provale

- breach – ciljane provale (velikih) kompanija
- ukupno +62% više u 2013
  - 253 velike provale u 2013 vs 156 u 2012
  - 552m identiteta u 2013 vs 93m u 2012
- top tipovi ukradenih informacija:
  - stvarno ime i prezime
  - datum rođenja
  - social security, broj osobne, itd.
  - kućna adresa, medicinska dokumentacija, telefonski brojevi, financijski podaci, e-mail adrese, korisnička imena i lozinke, osiguranje
- https://haveibeenpwned.com/

Krađa identiteta

152,445,165	Adobe accounts	
4,821,262	mail.ru Dump accounts	
4,789,599	Bitcoin Security Forum Gmail Dump accounts	
4,609,615	Snapchat accounts	
1,247,574	Gawker accounts	
1,186,564	Yandex Dump accounts	
1,057,819	Forbes accounts	
859,777	Stratfor accounts	
855,249	Manga Traders accounts	
530,270	Battlefield Heroes accounts	
453,427	Yahoo accounts	
227,746	Cannabis.com accounts	
202,683	Win7Vista Forum accounts	
191,540	hackforums.net accounts	
180,468	AhaShare.com accounts	
158,093	Boxee accounts	
148,366	WPT Amateur Poker League accounts	
116,465	Pokemon Creed accounts	
104,097	Insanelyi accounts	
56,021	Vodafone accounts	
55,622	Spirol accounts	
45,018	Lounge Board accounts	
38,108	Pixel Federation accounts	
37,784	Muslim Directory accounts	
37,103	Sony accounts	
36,789	BigMoneyJobs accounts	
35,368	Fridae accounts	
28,641	hemmelig.com accounts	
26,596	Business Acumen Magazine accounts	
20,902	Bell accounts	
16,919	Verified accounts	
5,788	Astropid accounts	
3,200	UN Internet Governance Forum accounts	
2,239	Tesco accounts	

Neželjeni e-mail / spam

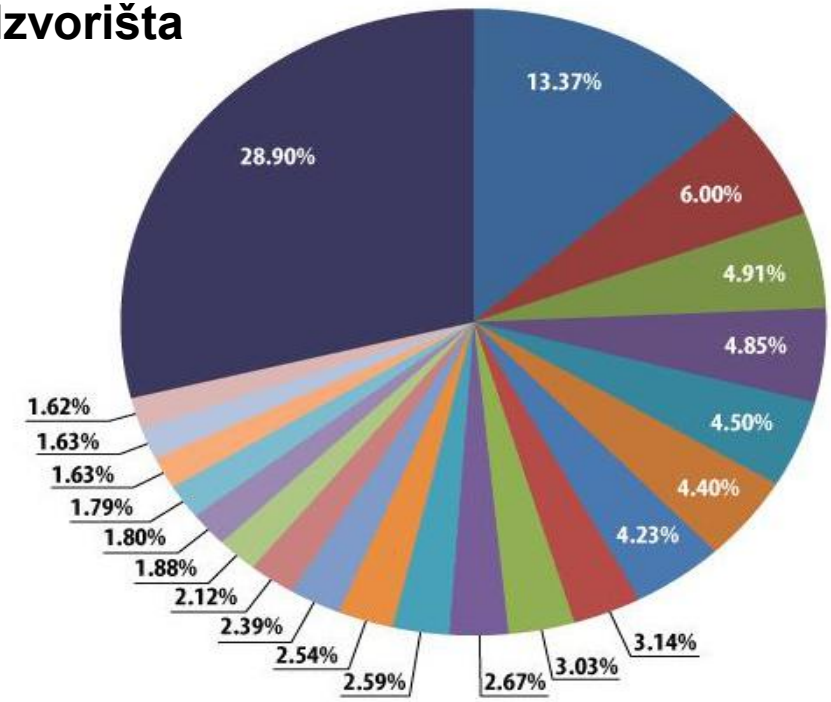
- prodaja, malware, phishing, krađa e-mailova
- prodaja postojećih e-emailova sa Weba, foruma, provali itd.
- oko 80% spama do 1KB veličine
- vektor - spam botnetovi:
  - 2.3m računala u 2013 vs 3.4m u 2012
  - ZeroAccess botnet – 1.9m računala
- 66% e-emaila je spam u 2013 vs 69% u 2012
- 29b spama dnevno u 2013 vs 30b u 2012
  - farmaceutski spam: 18% u 2013 vs 21%
  - adult/sex spam: 70% u 2013 vs 55% u 2012
  - 1 virus u 196, 1 phishing u 392 e-maila

Neželjeni e-mail / spam (2)

- tehnike:
  - slike – image spam: OCR nije uvijek moguć
  - prazan – blank spam: greška u slanju
  - povratni – backscatter: napad refleksijom
- sadržaj skoro uvijek “izmjenjen”:
  - V1gra, Via’gra, Vi”graa, vi*gra, \iagra, ...
- open mail relays, proxy servers
- različite tehnike provjere e-maila:
  - DNSBL (Spamhaus, SORBS, SPEWS, MAPS RBL), SMTP AUTH, Sender Policy Framework, greylisting, spamtraps, Bayesian, CRM114, ...

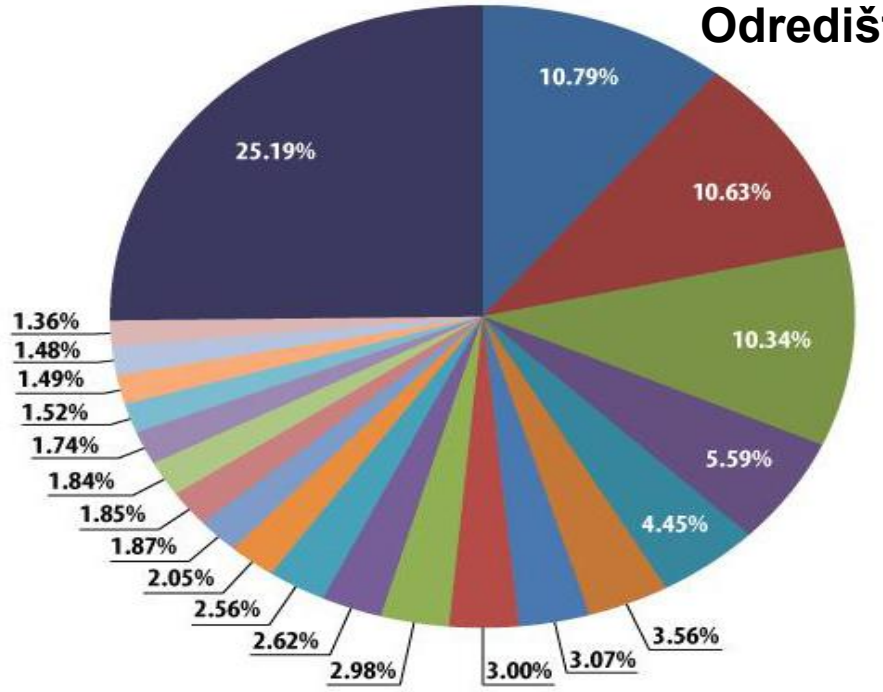
Neželjeni e-mail / spam (3)

Izvorišta



- USA
- Russia
- Vietnam
- Argentina
- China
- Spain
- Germany
- Italy
- Ukraine
- Brazil
- India
- France
- Iran
- Great Britain
- Belarus
- Romania
- Colombia
- Mexico
- Israel
- Taiwan
- Other

Odredišta



- Great Britain
- Germany
- USA
- India
- Brazil
- Italy
- France
- Vietnam
- Hong Kong
- Australia
- UAE
- Turkey
- Malaysia
- Japan
- Canada
- Austria
- Taiwan
- Colombia
- Russia
- Bangladesh
- Other

Neželjeni e-mail / spam (4)

From: Sweepstakechoices [redacted]
To:
Cc:
Subject: Qualify and GET an iPhone6!

Qualify and GET an iPhone6!

How to Snag- an Iphone-6

Start and Begin-Here Today

Get a **brand new** iPhone 6*!

Enter your ZIP for availability:

GO >>

From: Purchase SMS [redacted]@gmail.com>
To:
Cc:
Subject: Stay In Touch With Your Clients With SMS. Call [redacted]

Click here to unsubscribe

Phishing

- “pecanje” žrtava
  - osjetljive informacije: korisnička imena, lozinke, kreditne kartice
  - novac
- komunikacija iz lažiranih izvorišta
  - banke, IT odjel, država, ministarstva, policija, ...
- vektor napada
  - IM (Skype, MSN, AIM), e-mail spoofing
  - manipulacija URL-ovima, lažne Web stranice
  - socijalni mediji (Facebook, Twitter, Myspace)
- edukacija, SSL i SNI, browseri i crne liste
- 2-faktor autentikacija, OTP

Phishing (2)

From: PayPal Review Department <mgrp@mgrp.org.kw>
To:
Cc:
Subject: Your PayPal account has been suspended

PayPal

Warning Notification

Dear PayPal Costumer,

It has come to our attention that your PayPal® account information needs to be updated as part of our continuing commitment to protect your account and to reduce the instance of fraud on our website. If you could please take 5-10 minutes out of your online experience and update your personal records you will not run into any future problems with the online service.

However, failure to update your records will result in account suspension. Please update your records before OCT 1, 2014.

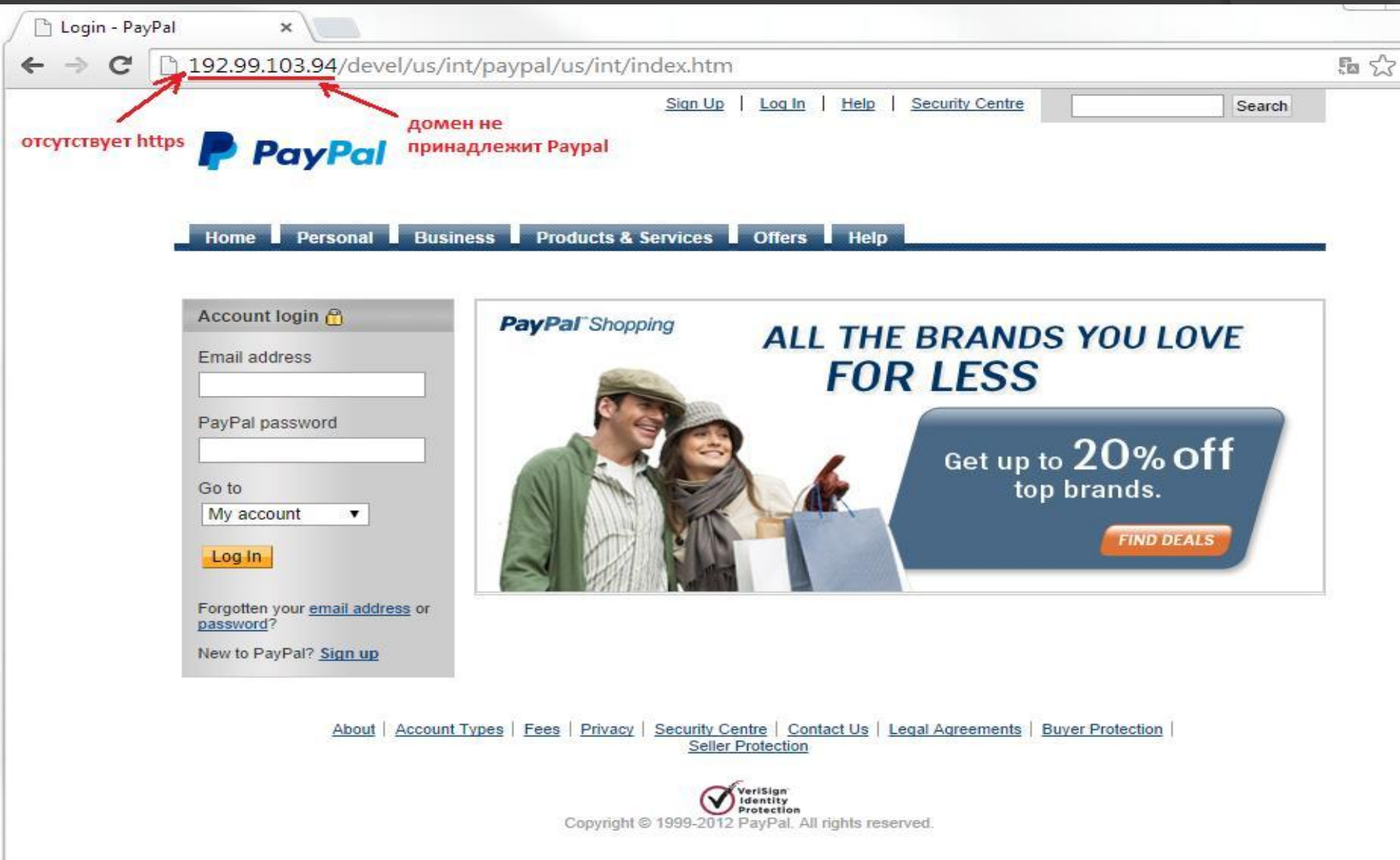
Once you have updated your account records, your PayPal® account activity will not be interrupted and will continue as normal.

Click here to update your PayPal account information

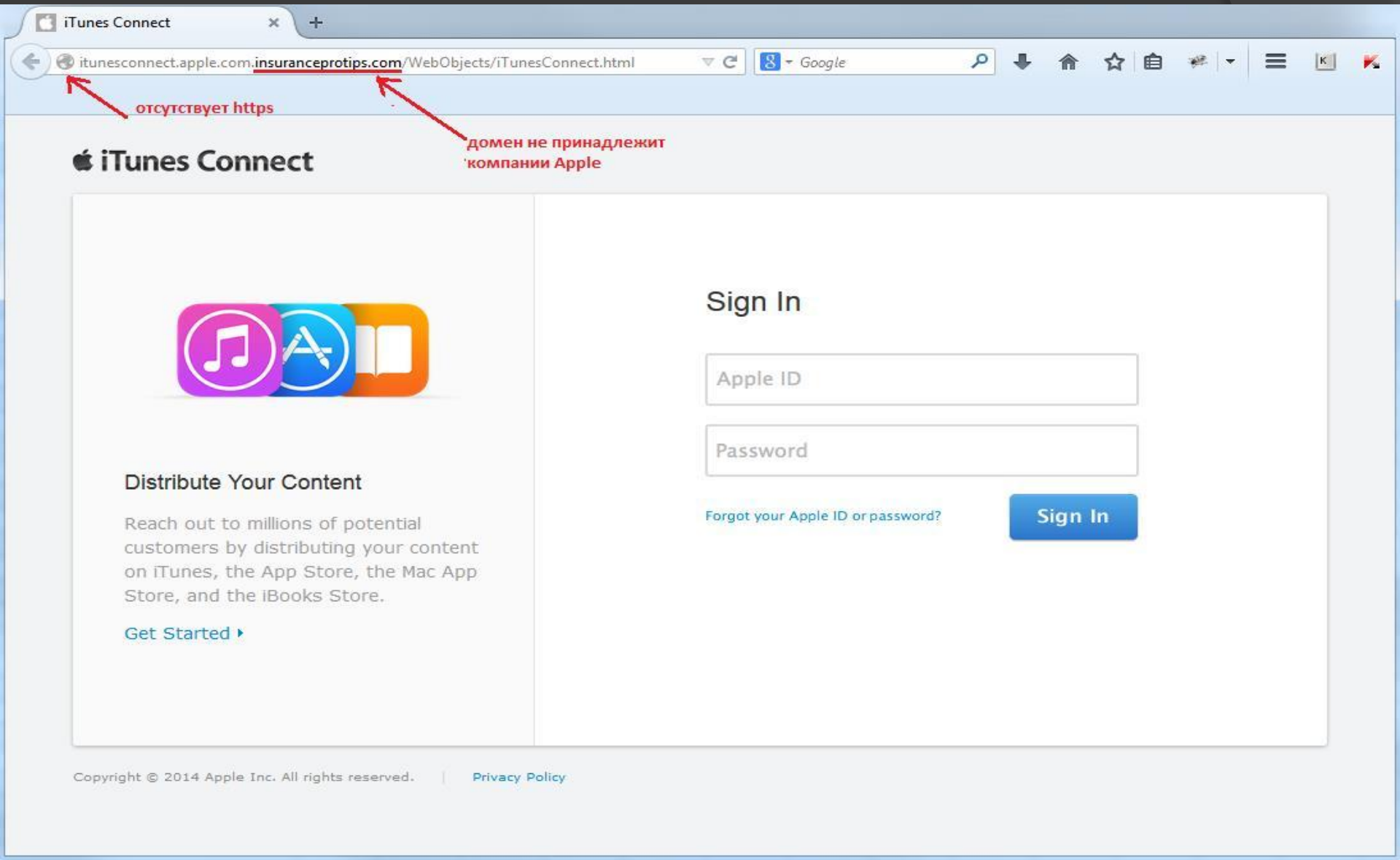
Information about FDIC pass-through insurance

Username: ufologistx Password: d13a8b1e5125 Hostname: ftp.firedrive.com

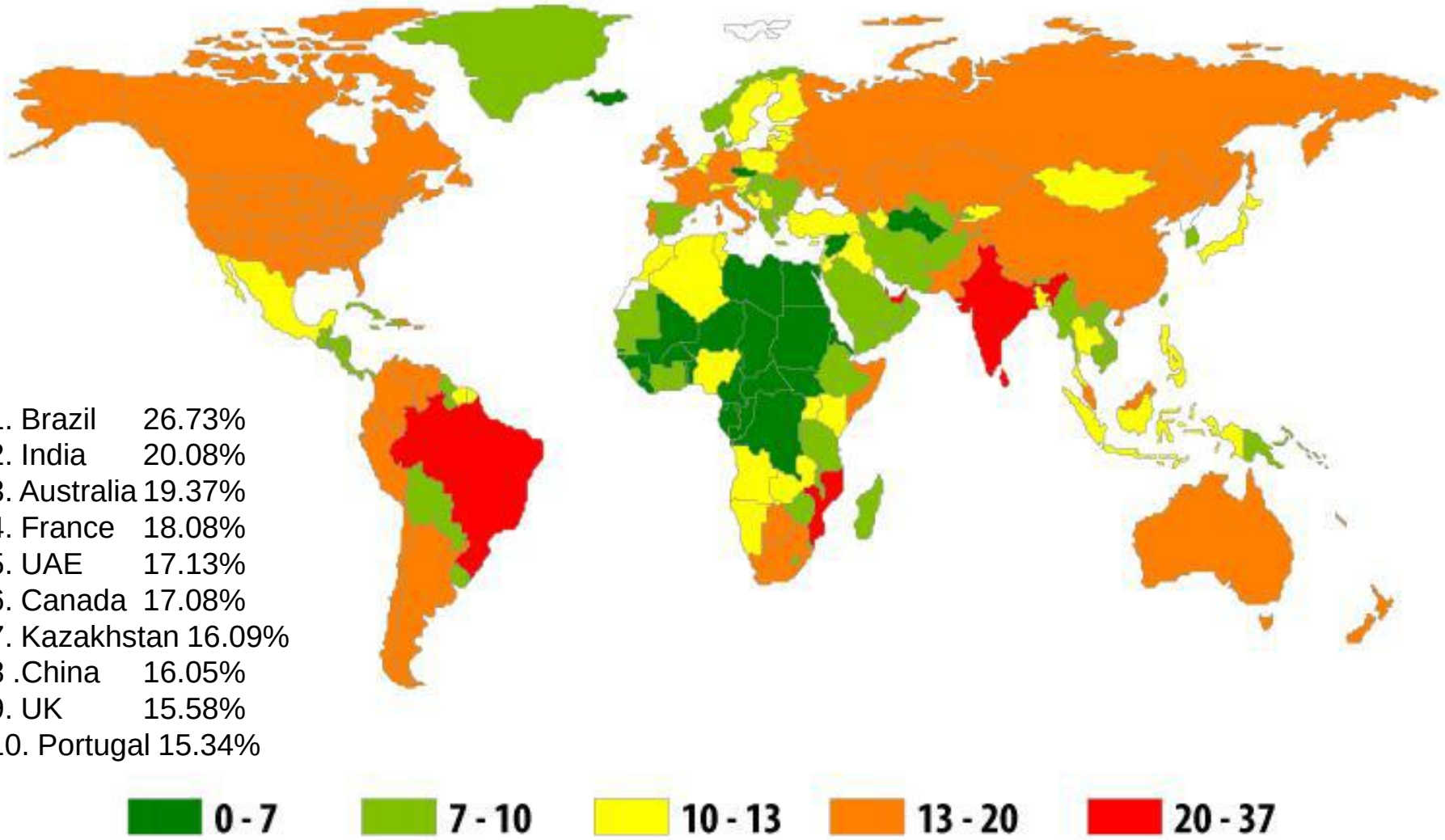
Phishing (3)


Login - PayPal
192.99.103.94/devel/us/int/paypal/us/int/index.htm
отсутствует https
домен не принадлежит Paypal
Sign Up | Log In | Help | Security Centre
Search
PayPal
Home
Personal
Business
Products & Services
Offers
Help
Account login
Email address
PayPal password
Go to
My account
Log In
Forgotten your email address or password?
New to PayPal? Sign up
PayPal Shopping
ALL THE BRANDS YOU LOVE FOR LESS
Get up to 20% off top brands.
FIND DEALS
About | Account Types | Fees | Privacy | Security Centre | Contact Us | Legal Agreements | Buyer Protection | Seller Protection
VeriSign Identity Protection
Copyright © 1999-2012 PayPal. All rights reserved.

Phishing (4)

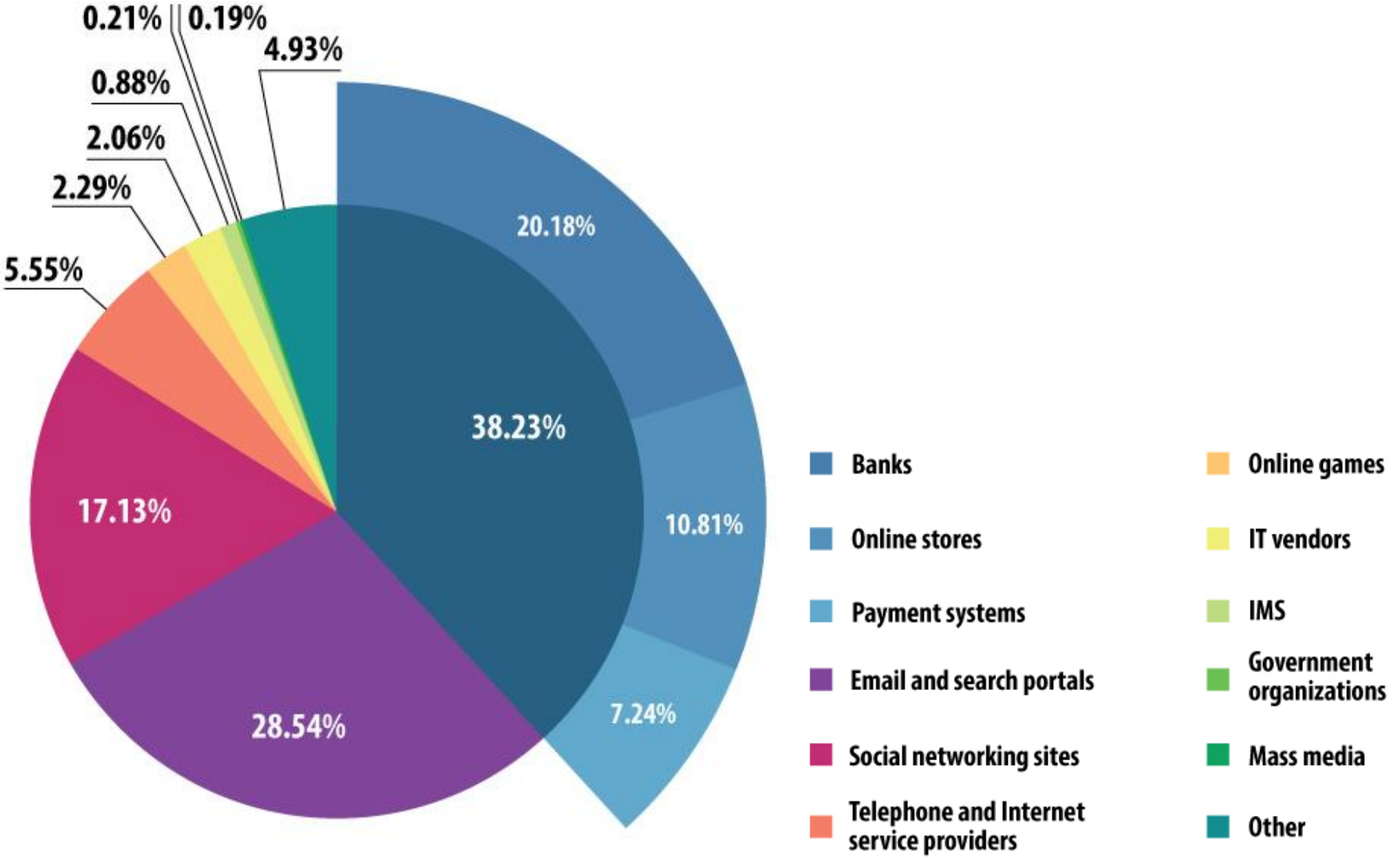

iTunes Connect
itunesconnect.apple.com.insuranceprotips.com/WebObjects/iTunesConnect.html
Google
отсутствует https
домен не принадлежит компании Apple
iTunes Connect
Distribute Your Content
Reach out to millions of potential customers by distributing your content on iTunes, the App Store, the Mac App Store, and the iBooks Store.
Get Started
Sign In
Apple ID
Password
Forgot your Apple ID or password?
Sign In
Copyright © 2014 Apple Inc. All rights reserved.
Privacy Policy

Phishing (5) – zemlje odredišta

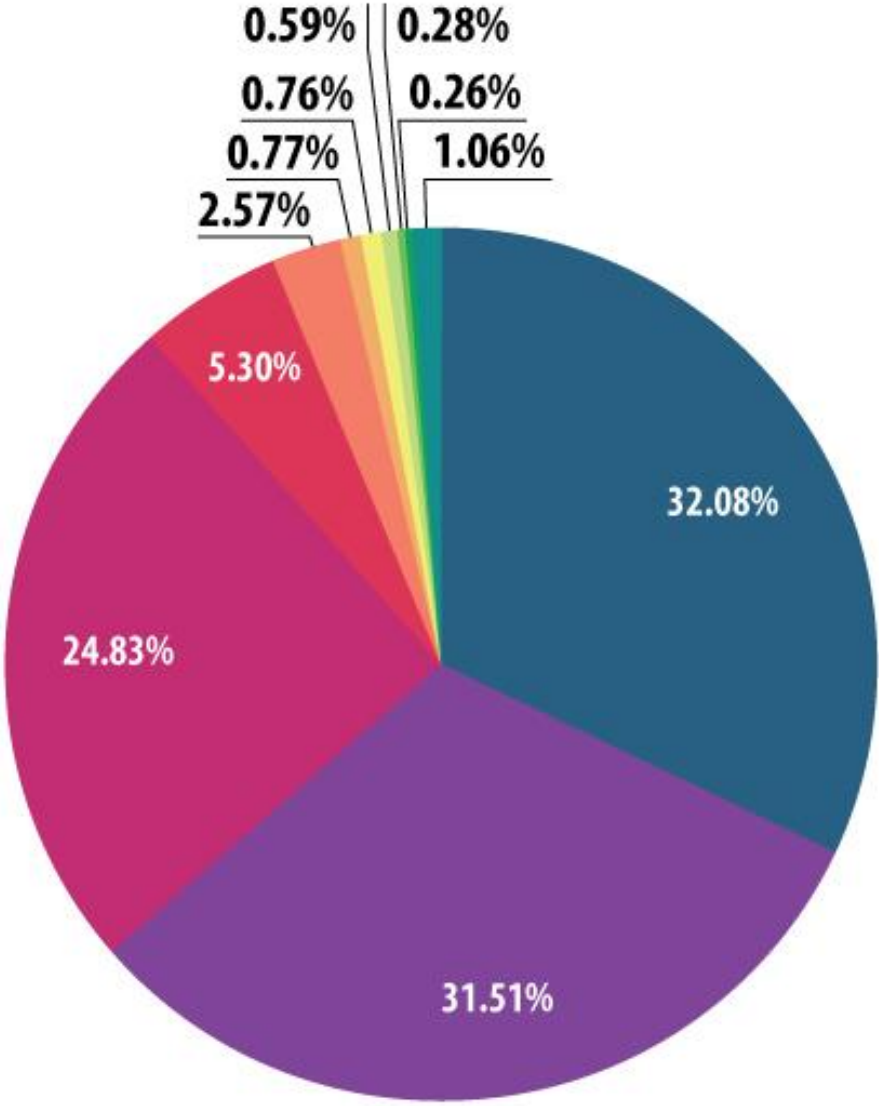


1. Brazil 26.73%
2. India 20.08%
3. Australia 19.37%
4. France 18.08%
5. UAE 17.13%
6. Canada 17.08%
7. Kazakhstan 16.09%
8 .China 16.05%
9. UK 15.58%
10. Portugal 15.34%

Phishing (6) – tip odredišta



Phishing (7) – napadnute banke



top 3 napadnute organizacije:

1. Google	10.34%
2. Facebook	10.21%
3. Yahoo!	6.36%

- PayPal
- Visa Inc.
- American Express
- MasterCard International
- Skrill Ltd.
- Payoneer
- Cielo S.A.
- Western Union
- Epoch
- MoneyGram
- Other

Cyber warfare/espionage

- politički motivirano
  - vojni razlozi, terorizam, civilni sustavi (Internet), privatni sektor
- iznimni resursi
  - ljudstvo, novac, vrijeme
- primjeri
  - Stuxnet (NSA, CIA, IDF), Regin (GCHQ, NSA), Turla (Rusija?)
  - prisluškivanje, redirekcija prometa itd.
  - DoS napadi, uništenje podmorskih kablova

Stuxnet

- computer worm – okriven 2010, jedan od najsloženijih ikad, funkcionalan 1+ godinu
  - oko 100 tisuća zaraženih računala
  - oko 3280 različitih uzoraka
- cilj napada
  - Iranski industrijski sustavi, automatizacija separacije nuklearnog materijala (obogaćivanje urana)
  - Windows + Siemens Step7: oštećenja nuklearnih centrifuga, ~20% nuklearnog programa (1000 centrifugi)
- način
  - 0-day exploits, Windows rootkit, PLC rootkit, AV evasion, process injection/hooking, network infection, P2P communication, C&C interface

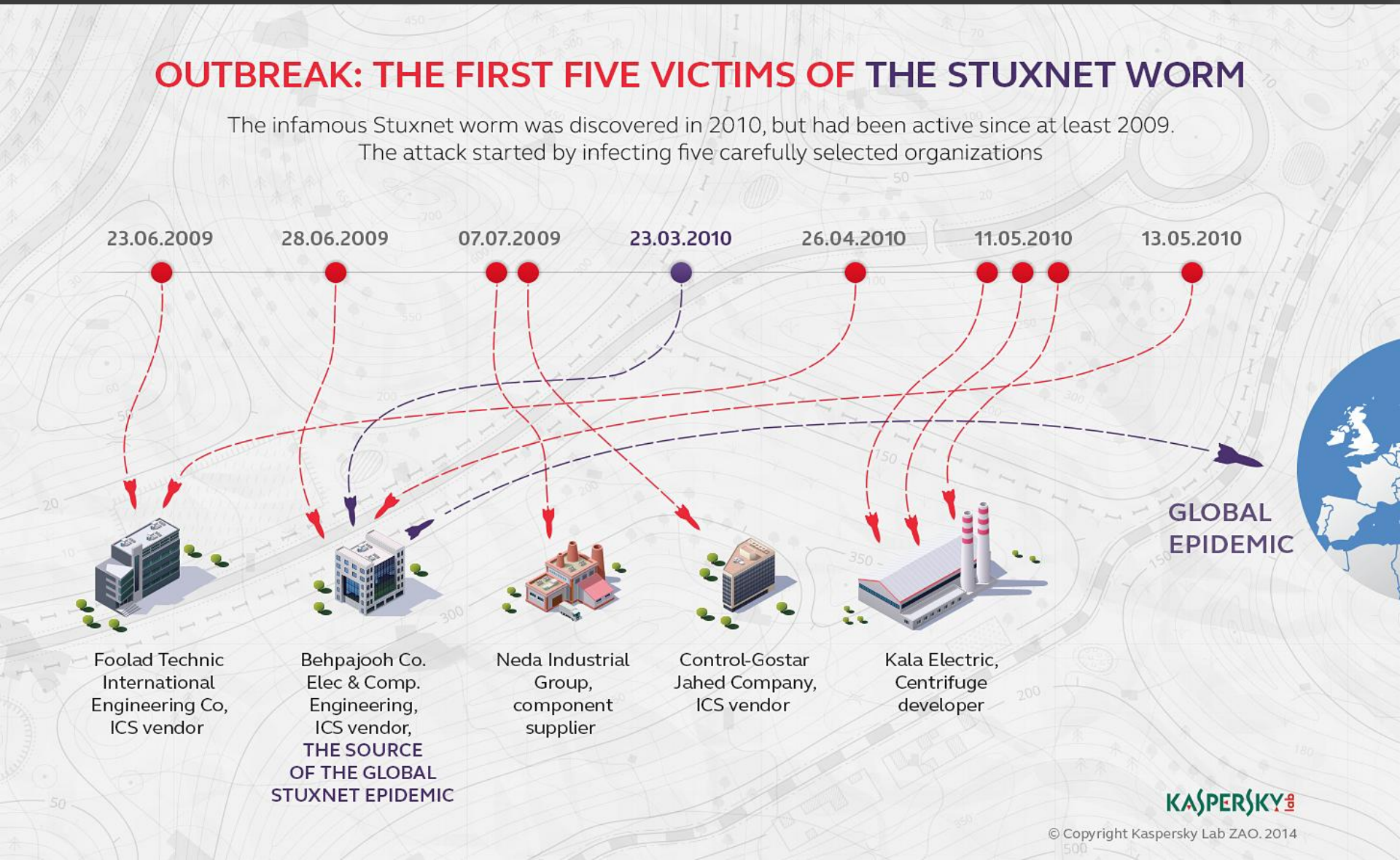
Stuxnet (2)

- karakteristike
  - inicijalni vektor: samo-replikacija kroz USB/HDD uređaje i samo-izvršavanje (LNK, PIF datoteke)
  - širenje kroz LAN (Windows Print Spooler ranjivosti, SMB ranjivosti, WinCC/SCADA ranjivosti) koristeći ranjivosti i SMB dijeljene resurse
  - zadobiva sistemske ovlasti
  - instalacija u Step7 projekte
  - P2P nadogradnja među replikama
  - C&C komunikacija prema centru, samo-nadogradnje
  - sakriva vlastite datoteke od sustava i AV proizvoda
  - prepoznaje PLC i ICS
  - sabotira Siemens PLC-ove modificirajući PLC kod te sakriva taj modificirani kod

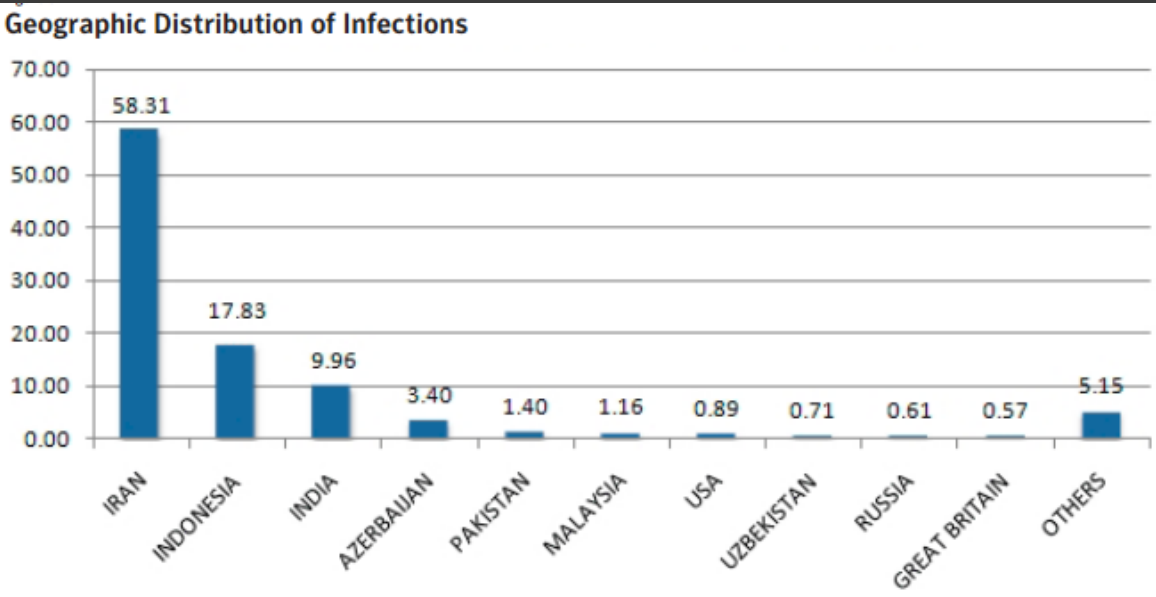
Stuxnet (3)

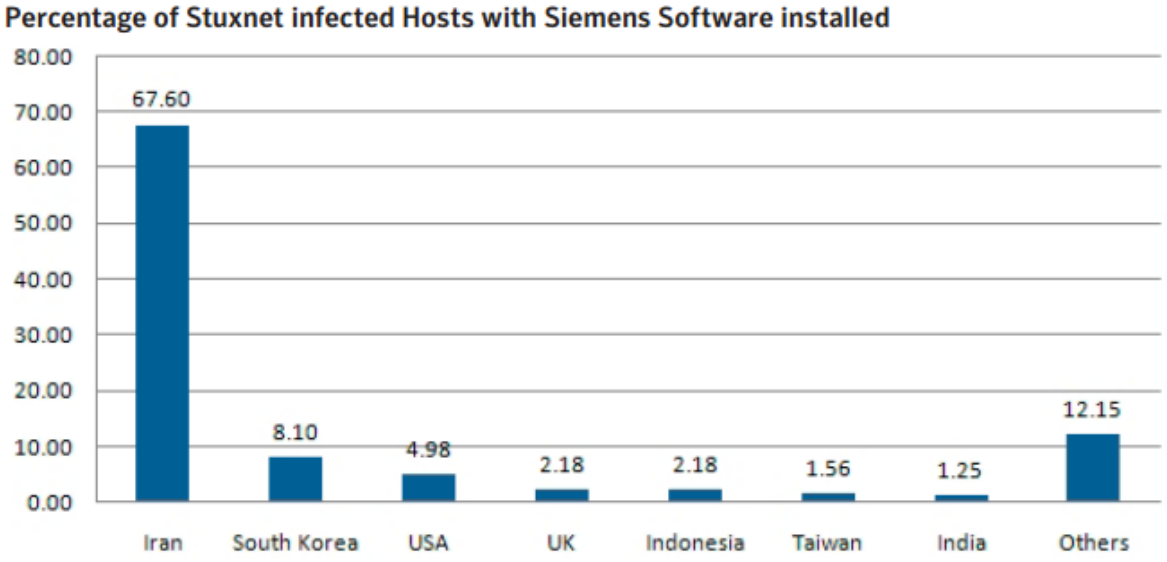
- daljnje karakteristike:
  - inertan ako nema PLC i Step7
  - širi se na max 3 računala
  - EOL 24.6.2012
  - digitalni potpis drivera: JMicron i Realtek
  - specifično dizajniran da gađa određeni PLC i hardversku konfiguraciju

Stuxnet – patient zero

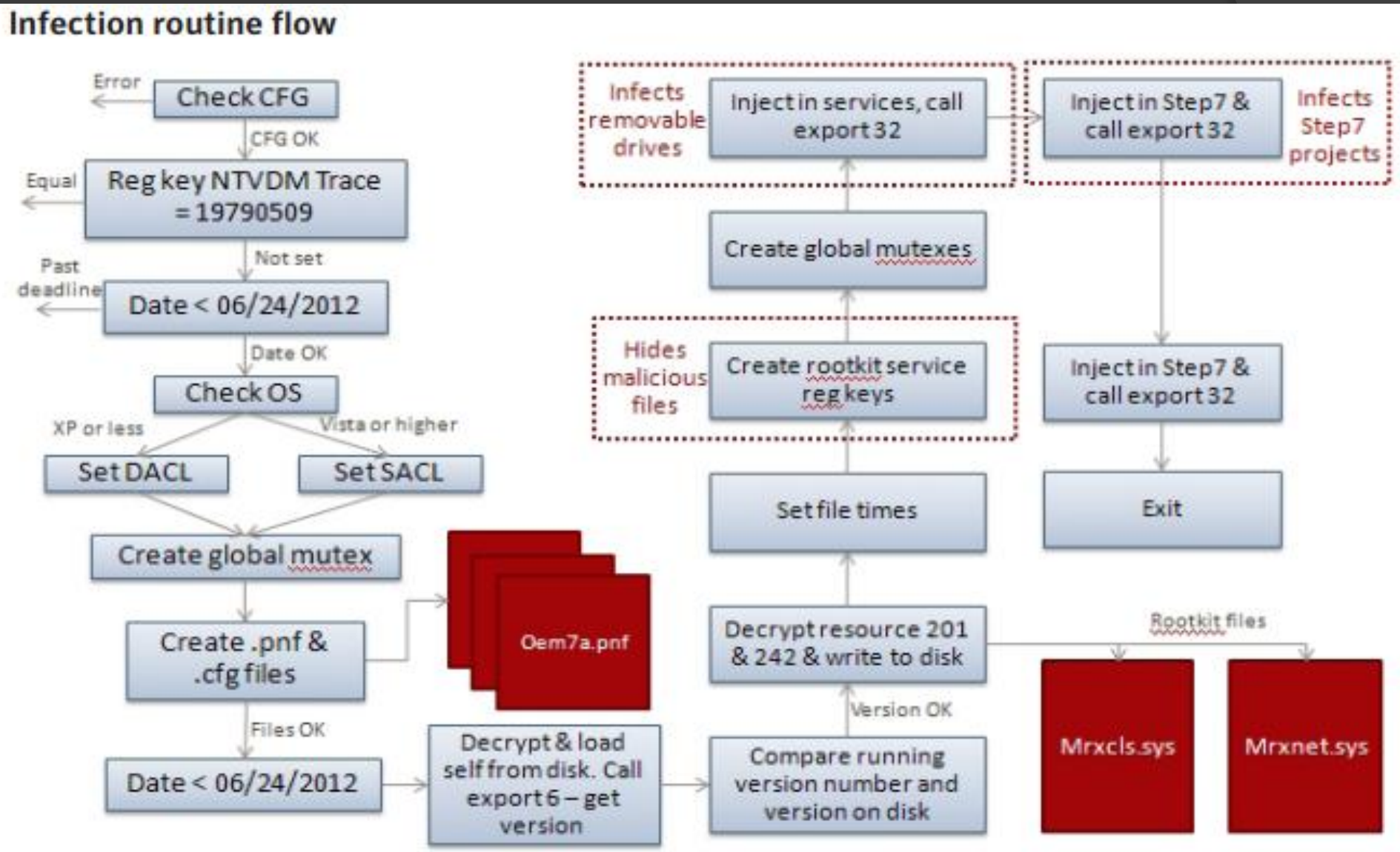


Stuxnet – odredišta zaraze





Stuxnet – shema zaraze



Stuxnet – post mortem

- vremenska linija
  - otkriven 06.2010.
  - 29.11.2010. Iranski predsjednik Mahmoud Ahmadinejad javno potvrdio
  - 01.2010. auto-bomba na Teheranskog profesora nuklearne fizike
  - istog dana dva napada auto-bombom na Iranske nuklearne fizičare (jedan ubijen, drugi teško ranjen)
  - 01.2012. ubijen direktor Natanz-a auto bombom
- Izrael
  - Gabi Ashkenazi, bivši šef IDF-a potvrdio angažman u Stuxnetu
- USA
  - anti-iranski program počeo tijekom Busha i nastavio za Obamom
  - WikiLeaks – potvrdio angažman protivno iračkom nuklearnom programu
  - United States Cyber-Consequences Unit program za napad centrifuga
  - 2011. iranska vlada potvrdila da istraga nedvojbeno ukazuje na USA i Izrael – CIA i IDF
  - Wikileaks dokumenti ukazuju na Stratfor kao izvorište
  - 06.2013. NSA prebjeg Edward Snowden potvrdio
- daljni razvoj: Duqu, Flame

Turla

- vrijeme: 2012-2014, izvorni tragovi i ranije
- cilj napada - vlade i ambasade istočnog bloka
  - ambasade u Franckuskoj, Ukraniji, Belgiji, Kini, Jordanu, Grčkoj, Kazahstanu, Armeniji, Poljskoj, Njemačkoj
  - kasnije vojni kompleksi, državne institucije, istraživački centri, farmaceutske kompanije, ...
- sustav infekcije
  - spear phishing, waterholing
  - zarazni payload Trojan.Wipbot, Tavdig
  - 0-day infekcija: Adobe Reader, Windows XP i 2003
    - CVE-2013-5065 - Privilege escalation vulnerability in Windows XP and Windows 2003
    - CVE-2013-3346 - Arbitrary code-execution vulnerability in Adobe Reader

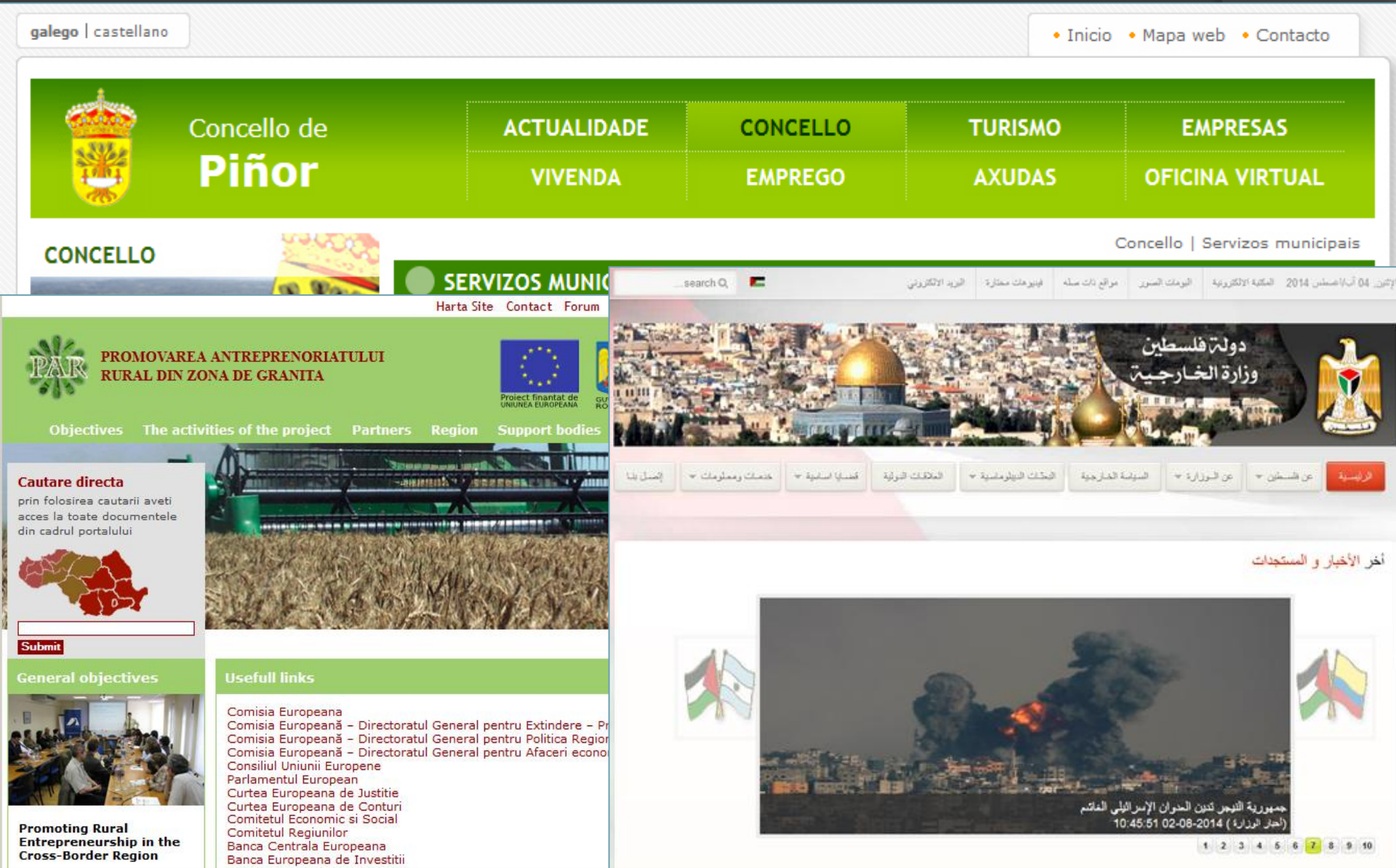
Turla (2)

- Epic Turla – kampanja zaraze
  - spearphishing e-mails - Adobe PDF exploits
  - socijalni inženjering - malware u ".SCR" datotekama
  - watering hole attacks - Java exploits, Adobe Flash exploits, Internet Explorer 6/7/8 exploits, lažni "Flash Player" malware – stotine Web sjedišta
- trajni nadzor i špijuniranje
  - Trojan.Turla, Carbon/Cobra sustav
  - rootkit – trajno skrivanje, administrativne privilegije
  - otvara trajni backdoor prema C&C poslužiteljima: kopiranje datoteka, brisanje, prijenos, nadograđivanje, itd.
  - enkriptirana komunikacija povrh HTTP upita
  - nadogradnja u Turlu samo za zanimljive sustave

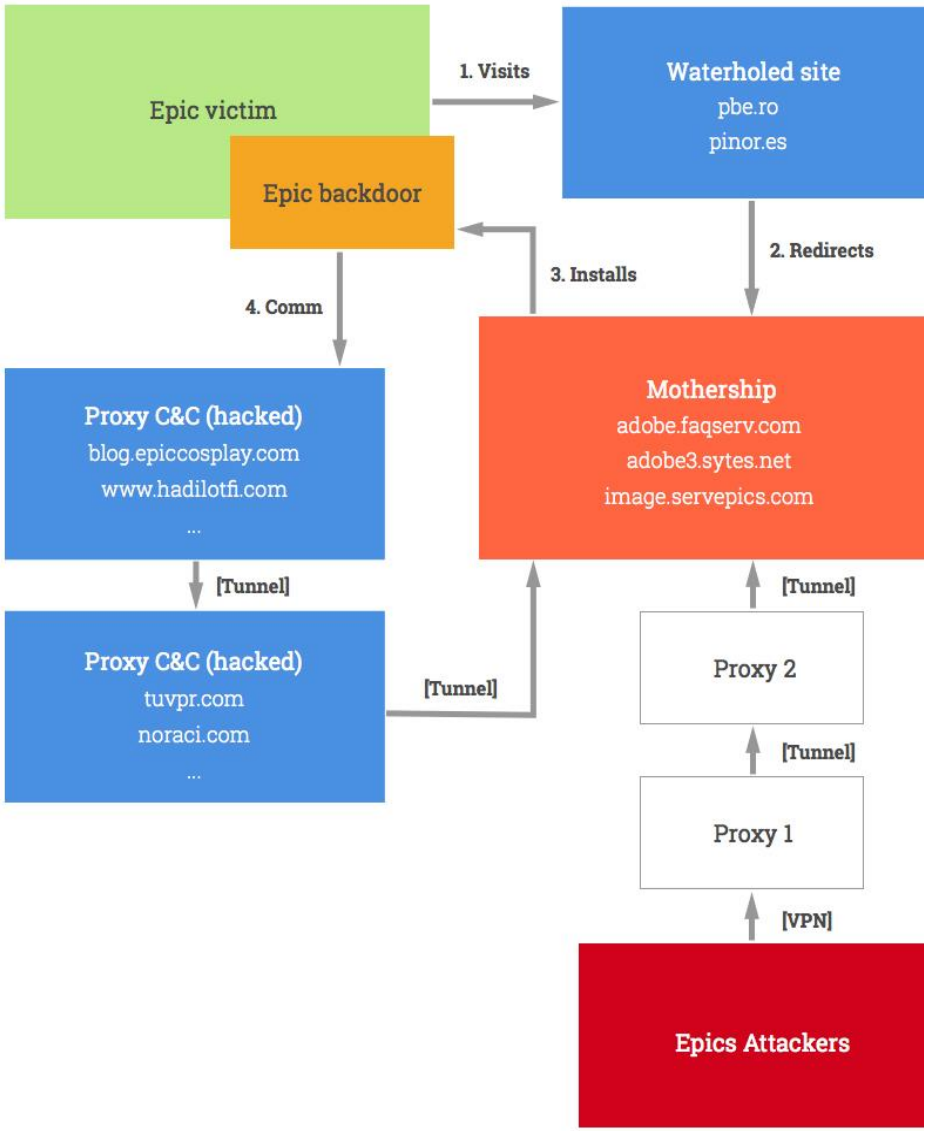
Turla – SCR malware

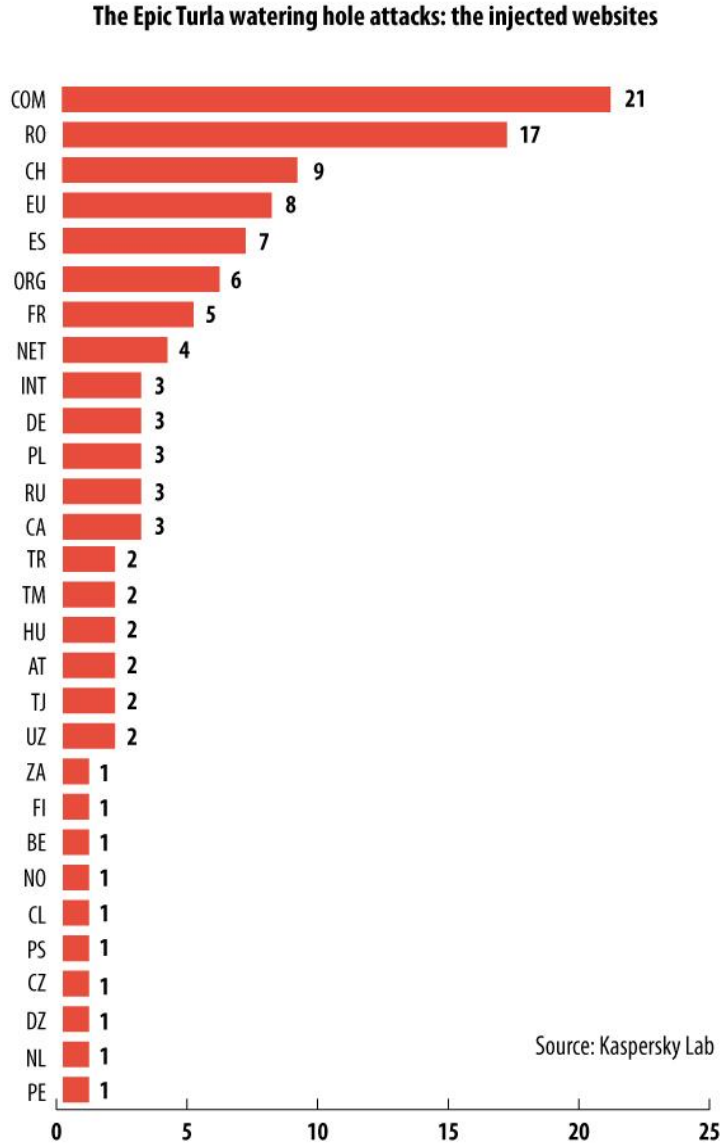
- primjeri SCR datoteka:
  - .مؤتمر جنيفrar (Arapski: “Geneva conference.rar”)
  - NATO position on Syria.scr
  - Note_№107-41D.pdf
  - Talking Points.scr
  - border_security_protocol.rar
  - Security protocol.scr
  - Program.scr

Turla – water hole attacks



Turla – životni ciklus





Turla – shematski prikaz

The Epic Snake: Unraveling the mysteries of the Turla cyber-espionage campaign

Ongoing cyber-espionage campaign

Epic Turla: The early-stage infection mechanism

Mission: Attackers inject the Epic backdoor into the high-profile victim's PC to validate the identity thereof

Infection vectors:

Watering hole attacks

>100 injected websites

Direct spearphishing emails

Hundreds of victim IPs
>45 countries

Targets:

- Government bodies
- Embassies
- Military
- Research and education organizations
- Pharmaceutical companies

Cobra system and Snake malware platform

Cobra Carbon system/ Pfinet (+others):
Intermediary upgrades and communication plugins.

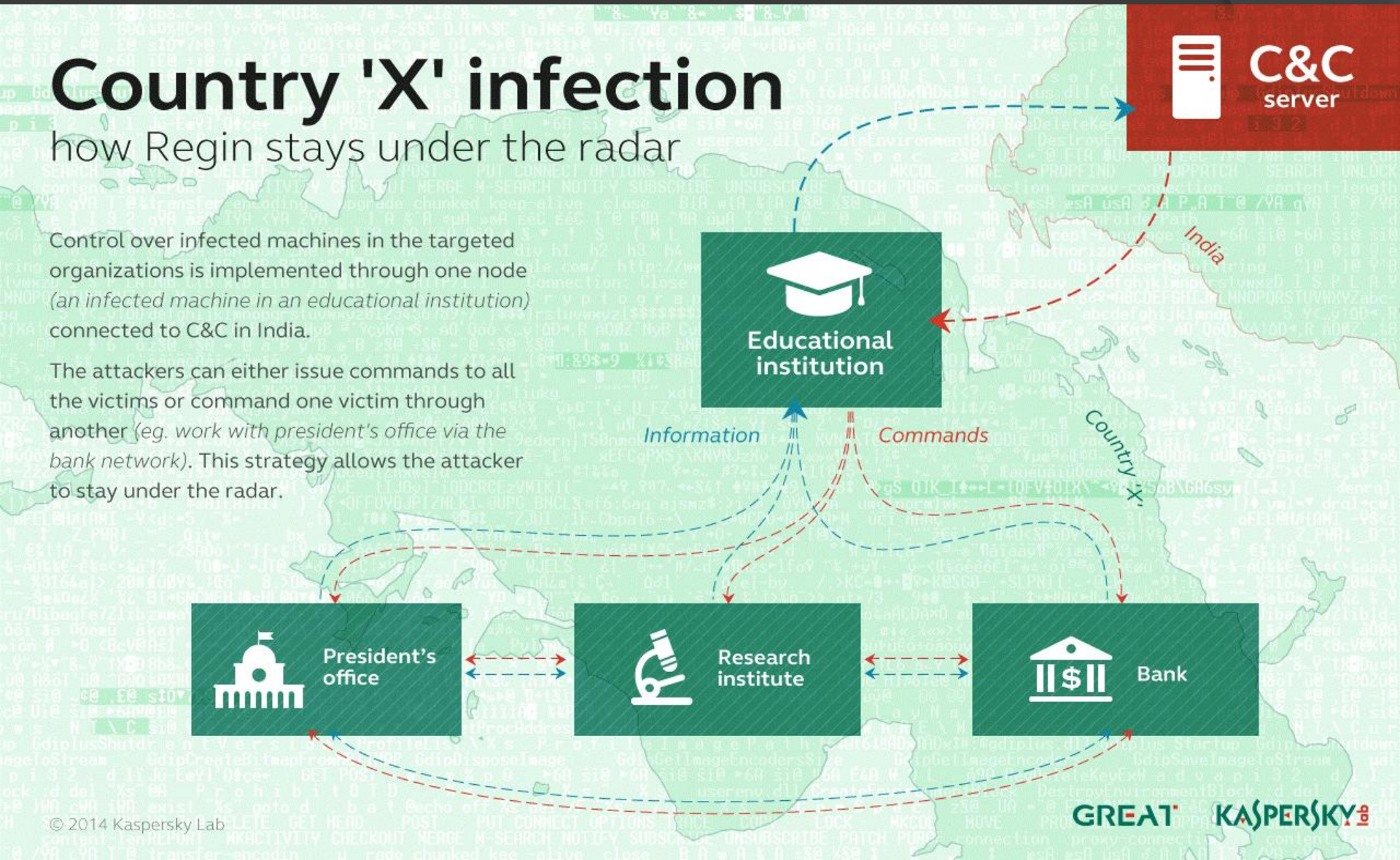
Snake/Uroburos:
High-grade malware platform that includes a rootkit and virtual file systems

KASPERSKY lab

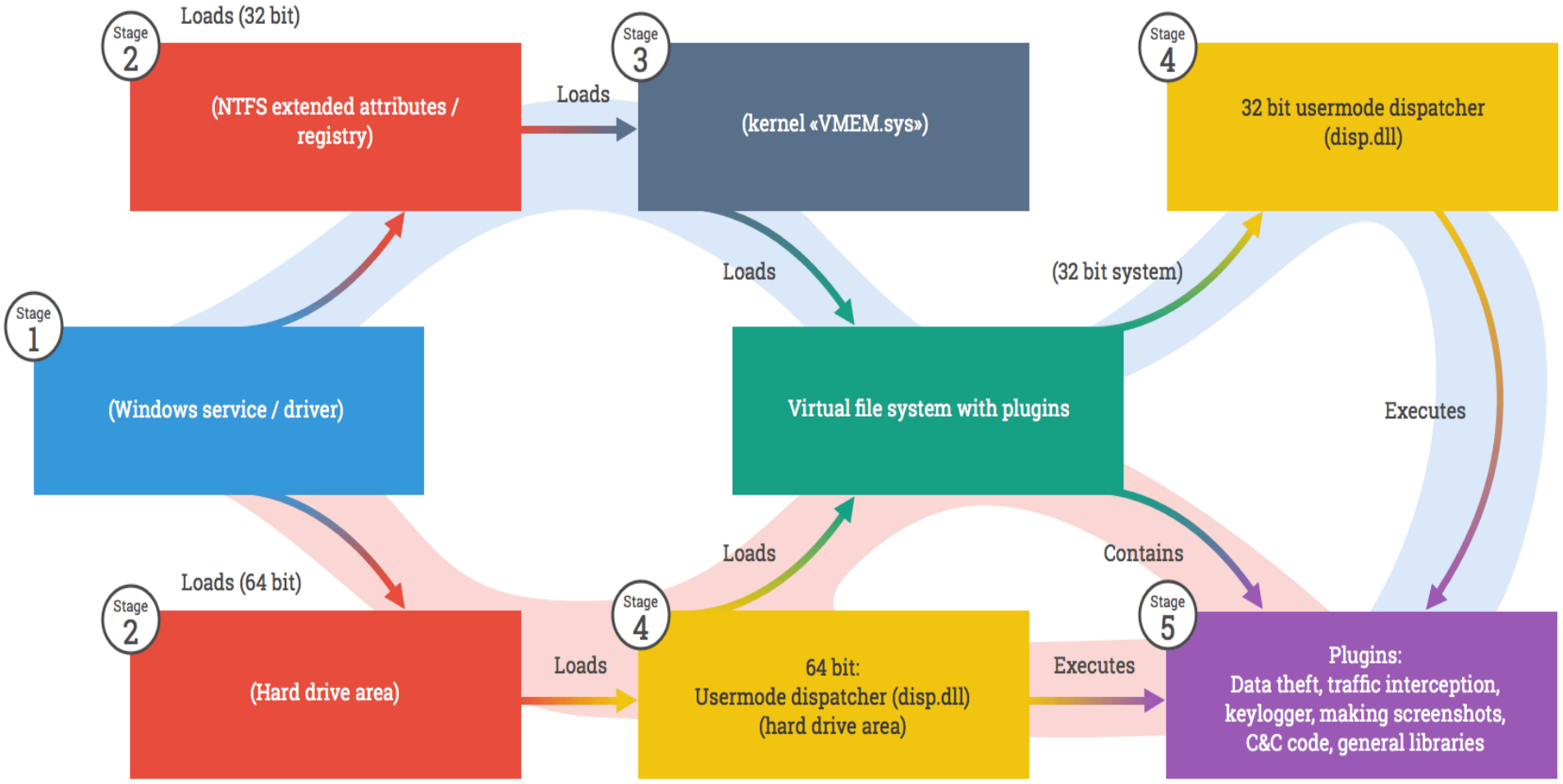
Regin

- prvi cyber-attack platform
  - prvi uzorci iz 2003, intenzivno od proljeća 2012
  - provaljuje i prisluškuje GSM mreže uz standardne tipove napada
  - modularni, izmjenjivi dizajn
- meta:
  - telekomi, vladine institucije, multinacionalna politička tijela, financijske institucije, istraživački centri, individualni kriptografski i matematički eksperti
- cilj:
  - skupljanje informacija (emailovi, dokumenti)
  - usluge novih tipova napada
  - udaljena kontrola na različitim nivoima

Regin – C&C mreža i tuneli



Regin – modularan dizajn

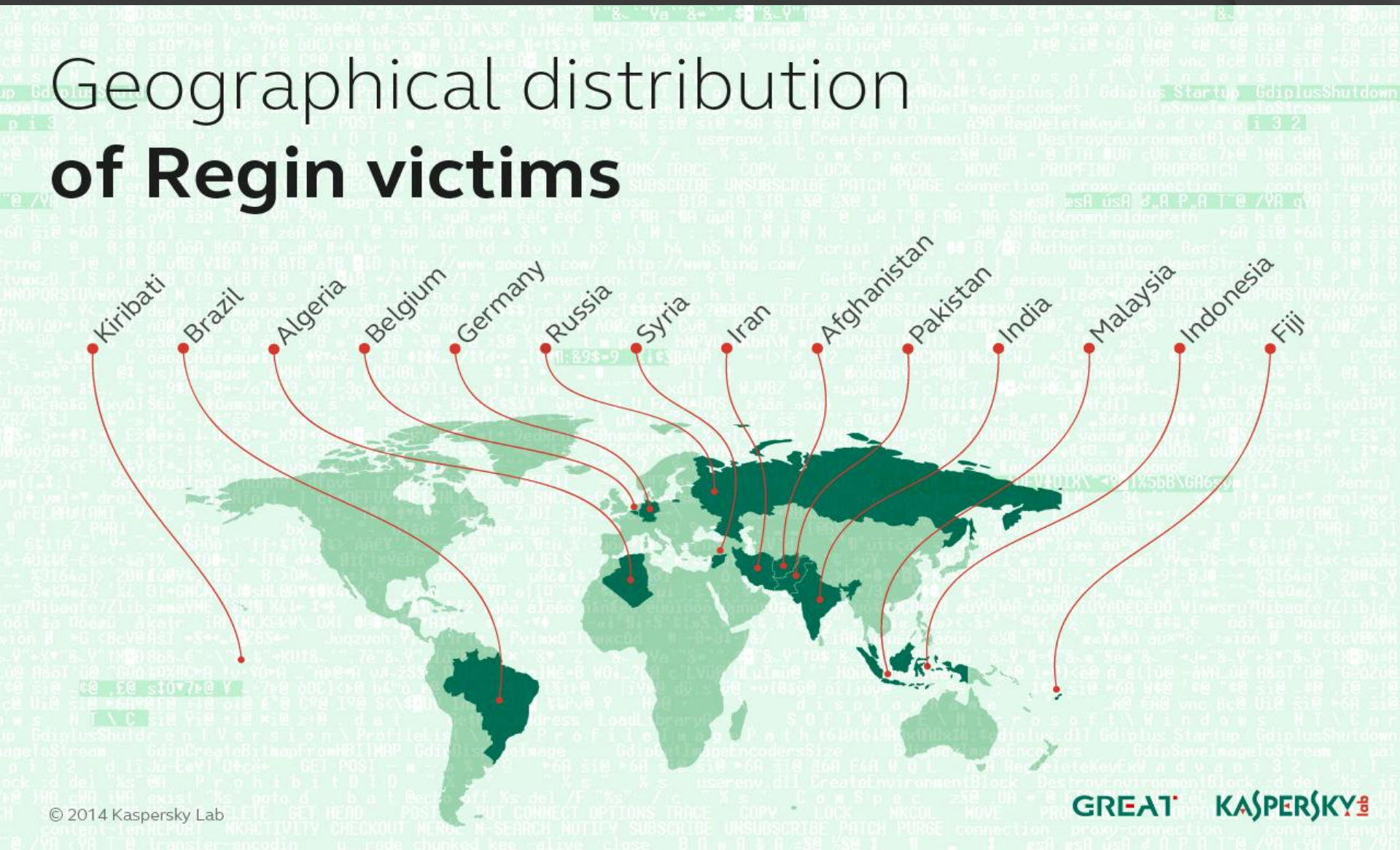


GREAT KASPERSKY lab

Regin – daljnje karakteristike

- karakteristike
  - self-encrypted, vlastiti VFS
  - mreža dronova u mreži žrtve
  - interna skrivena kriptirana mreža kroz različite protokole (ICMP, Winsock, HTTP, HTTPS, SMB/pipes), zaobilazi mrežne filtre
- jedan od ciljeva
  - napad GSM bazne stanice tijekom 2008 i prikupljanje informacija o ćelijama i sa ćelija
- C&C centri:
  - Tajvan (Taichung, kineska provincija), Indija (Chetput, Thane), Belgija (Brisel)
  - P2P mreža u srednjeistočnoj zemlji (ured predsjednika, istraživački centri, edukacijska mreža, banka)

Regin – geografski raspored



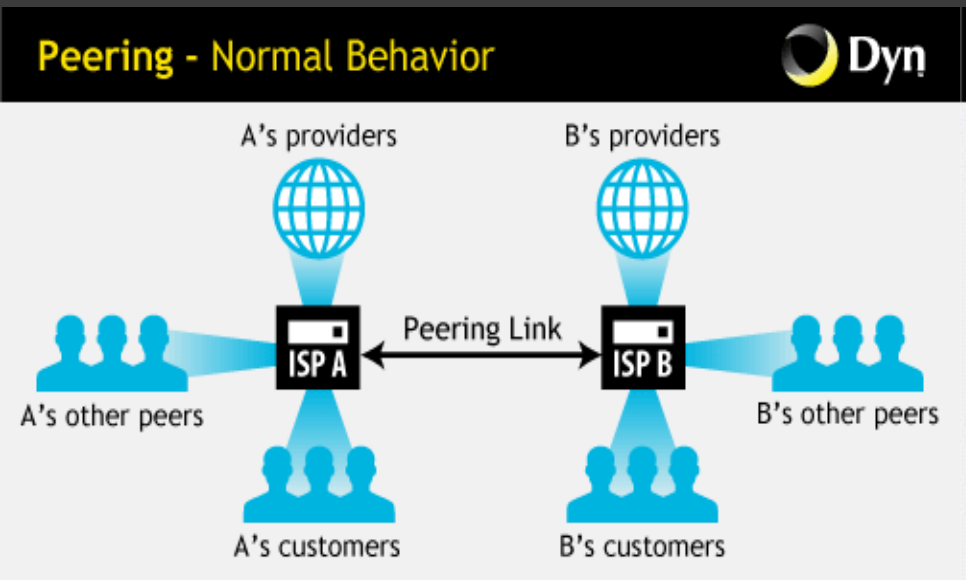
Regin - zaključak

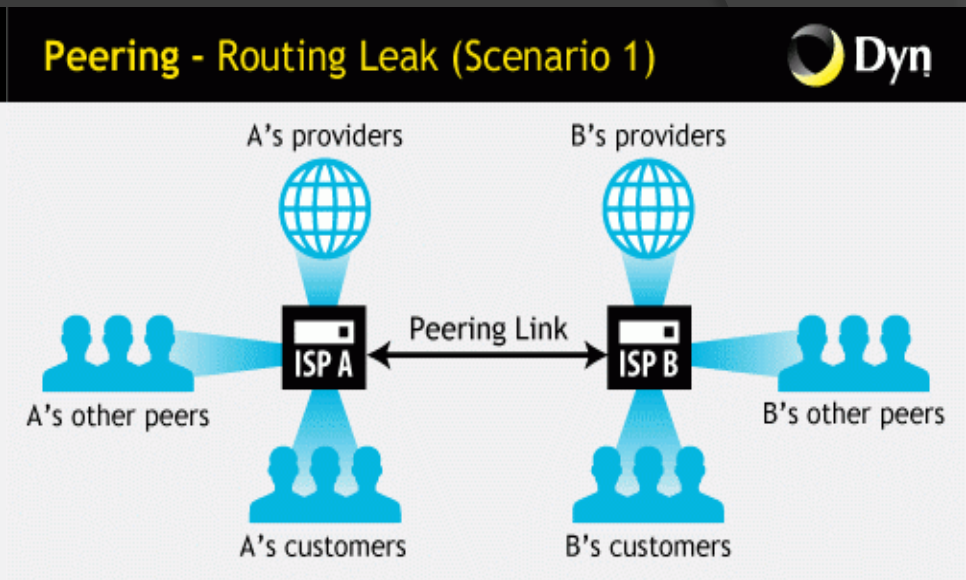
- ultimativni cilj:
  - Belgacom (telefonija, Internet)
  - NSA prebjeg Snowden ukazuje da je to NSA/GCHQ projekt prisluškivanja Europske unije, Europskog parlamenta itd.
  - Operation Socialist – 2010. GCHQ (Government Communications Headquarters) hackirao Belgacom kroz lažne LinkedIn stranice – početak daljnjih napada

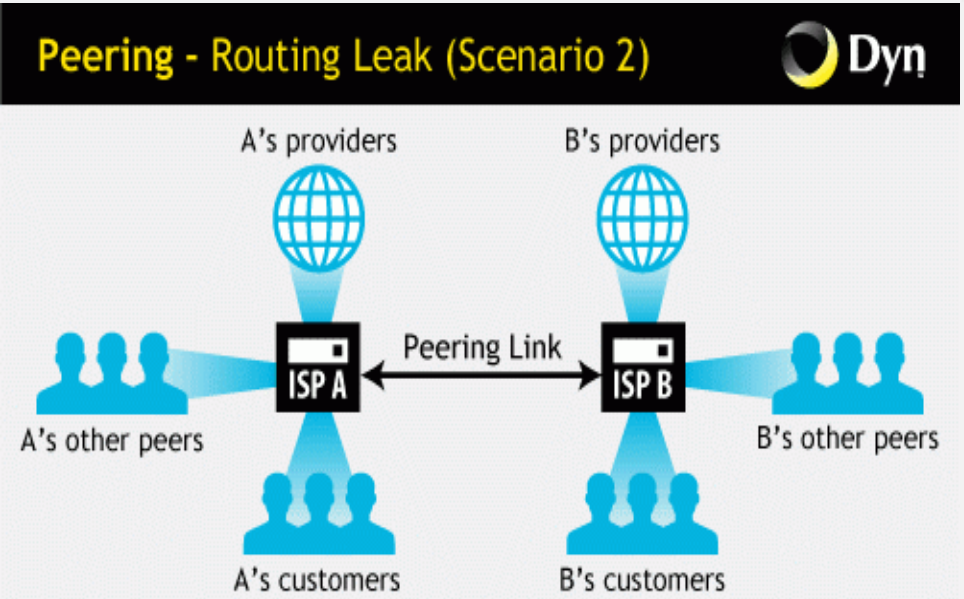
Kinesko “otimanje” Interneta

- autonomni sustavi
  - oglašavanje prefiksa IP adresa
  - tablice usmjeravanja
  - BGP kao protokol za razmjenu
- moguća zlouporaba:
  - AS oglašava prefiks koji nije njegov
  - AS oglašava više specifičan prefiks nego što oglašava “pravi” AS
  - AS oglašava da može usmjeravati promet prema nekom drugom AS-u sa kraćom rutom (neovisno da li je to istina ili ne)
  - BGP filtriranje – nije uvijek aktivno i efikasno

Kinesko “otimanje” Interneta (2)



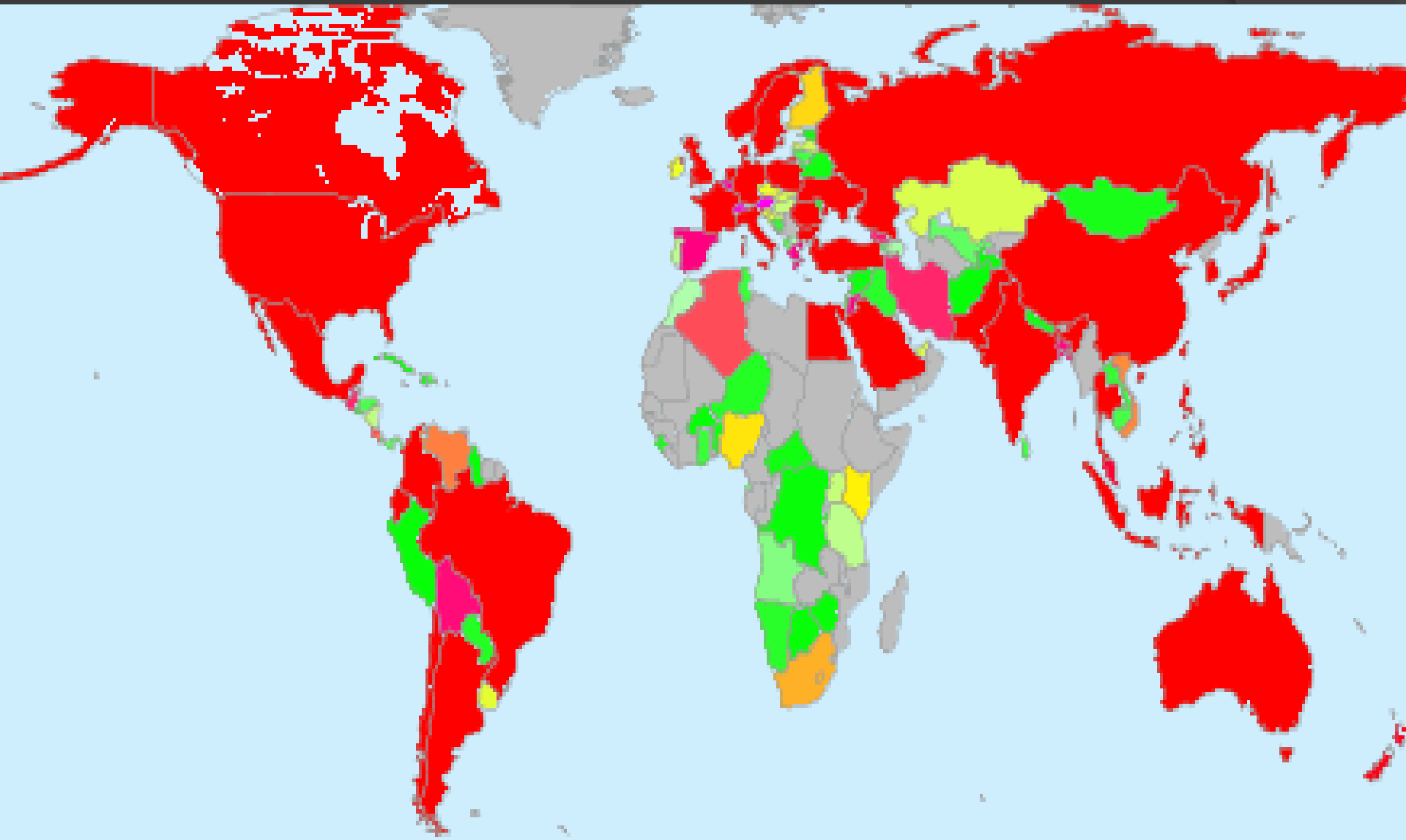




Kinesko “otimanje” Interneta (3)

- 15 minuta “Kineske tišine”
  - “ukradeno” 11% Interneta (?)
- vremenski slijed:
  - 08.04.2010. AS23724 (China Telecom) umjesto 40ak prefiksa oglasio 37000 jedinstvenih prefiksa
  - oko 11% prefiksa iscurilo izvan kineske mreže: dell.com, cnn.com, www.amazon.de, www.rapishare.com, www.geocities.jp, mnogo najpoznatijih kineskih sajtova, neki .mil sajtovi, .gov sajtovi, itd.

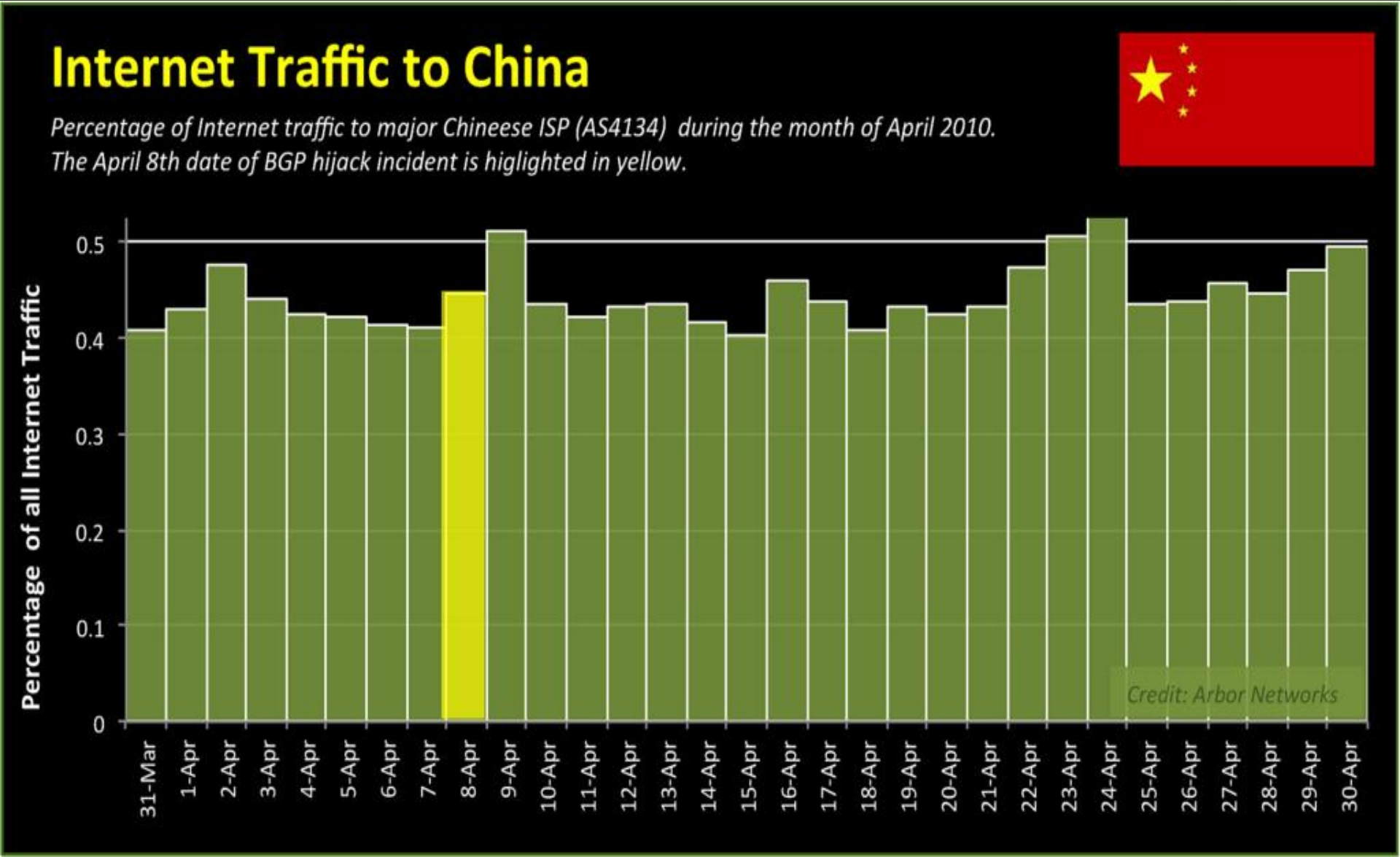
Kinesko “otimanje” Interneta (4)



Kinesko “otimanje” Interneta (5)

- ukradenih prefiksa:
  - US => 10547
    CN => 10298
    KR => 2857
    AU => 1650
    MX => 885
    IN => 719
    JP => 604
    BR => 592
    FR => 508
    RU => 471
  - CA => 425
    TH => 372
    ID => 369
    IT => 338
    CO => 328
    GB => 322
    CL => 302
    SE => 281
    HK => 276
    EC => 272
    DE => 227

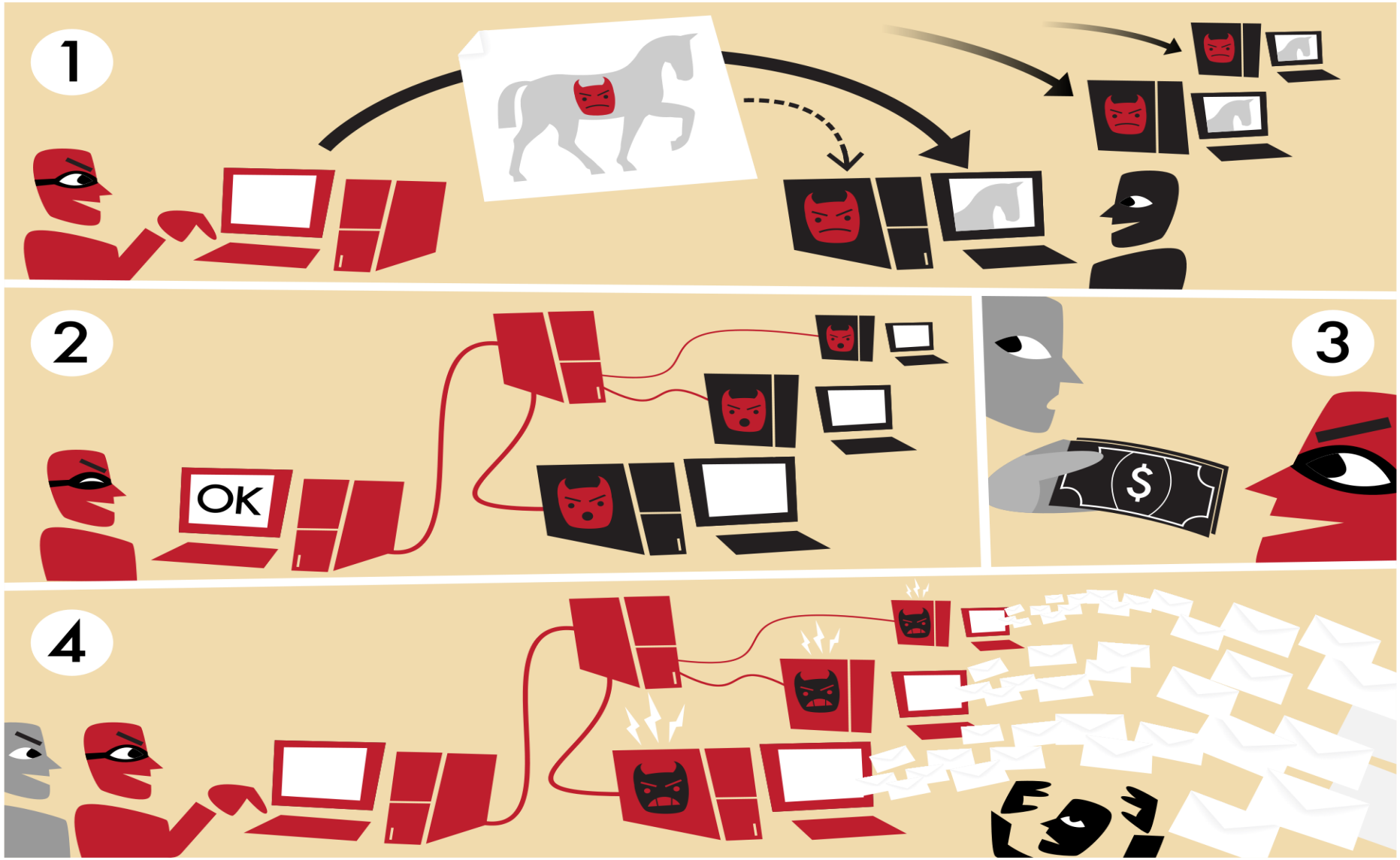
Kinesko “otimanje” Interneta (6)



Botnet

- botnet = robot + network
  - mreža povezanih programa
  - IRC, C&C
- vektor
  - ranjivosti (preglednici, e-mail, itd.), trojanci, ...
- tipično redundantni
  - veliki broj
  - nekoliko kontrolera
  - P2P komunikacija, višerazinska hijerarhija i složenije topologije

Botnet – shematski prikaz



Botnet

- namjena:
  - DDoS napadi – veliki broj upita prema jednom računalu/servisu, često se koristi refleksija
  - SMTP spam
  - bitcoin mining
  - krađa (kreditne kartice, korisnička imena...)
  - click fraud – pay per click varanje
  - spamdexing – Black-Hat SEO

Botnet - statistike

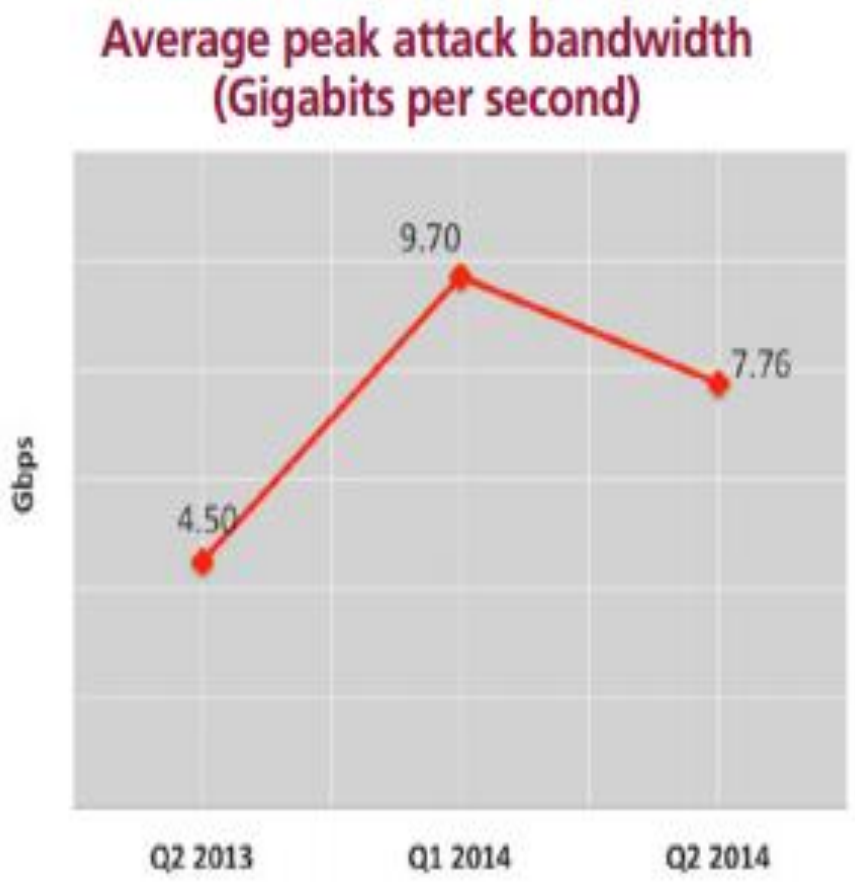


Figure 1: Average peak attack bandwidth soared during Q1 and Q2, and remains near Q1 2014's record setting levels

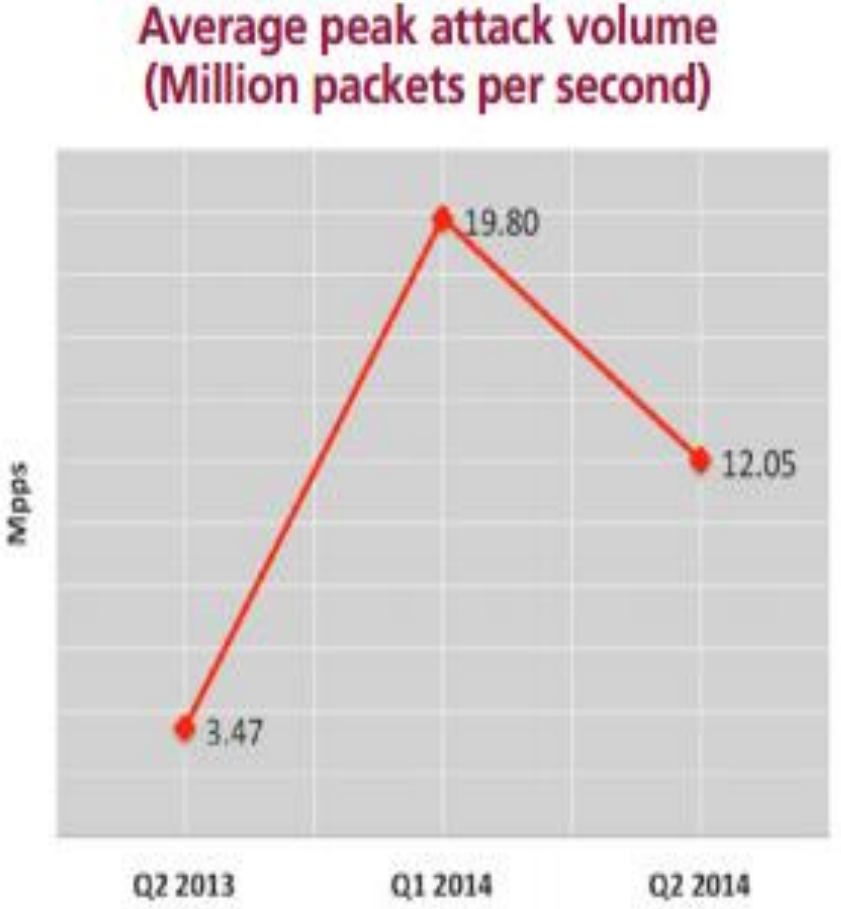


Figure 2: Average peak attack volume has more than tripled year-over-year and remains near Q1 2014's high

Botnet - DDoS

- izvorišta:
  - lažirana i stvarna
- tip napada:
  - 90% infrastrukturni: modifikacija paketa, refleksije, itd. – preopterećenje fizičkih resursa (propusnost, CPU, RAM)
  - 10% aplikativni: zlouporaba protokola (rušenje i/ili preopterećenje servisa)
- zombie/drone:
  - postaju nenadograđena, neodržavana računala

Botnet – protokoli

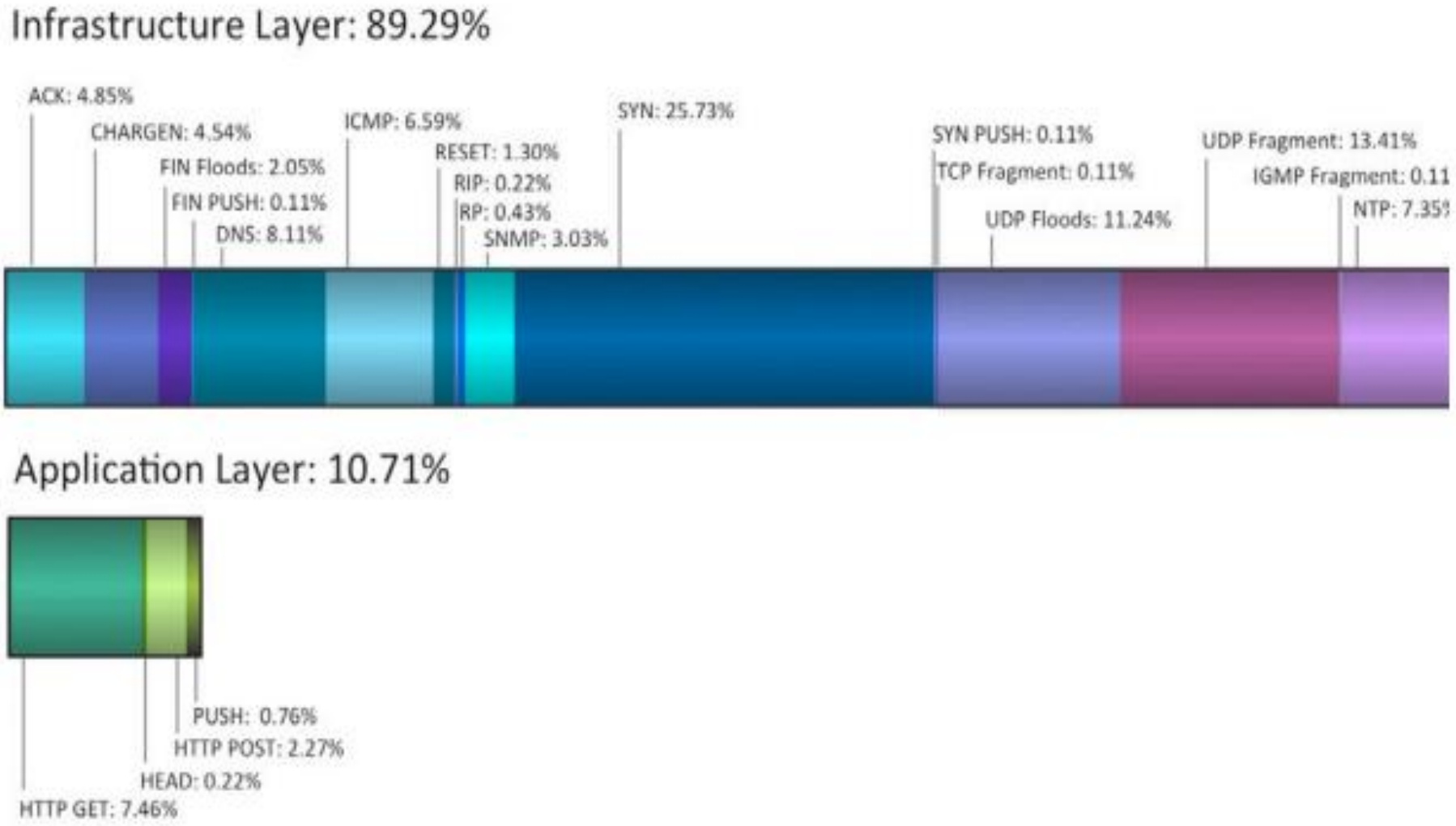


Figure 3: Types of DDoS attacks and their relative distribution in Q2 2014

Botnet – napadnuti

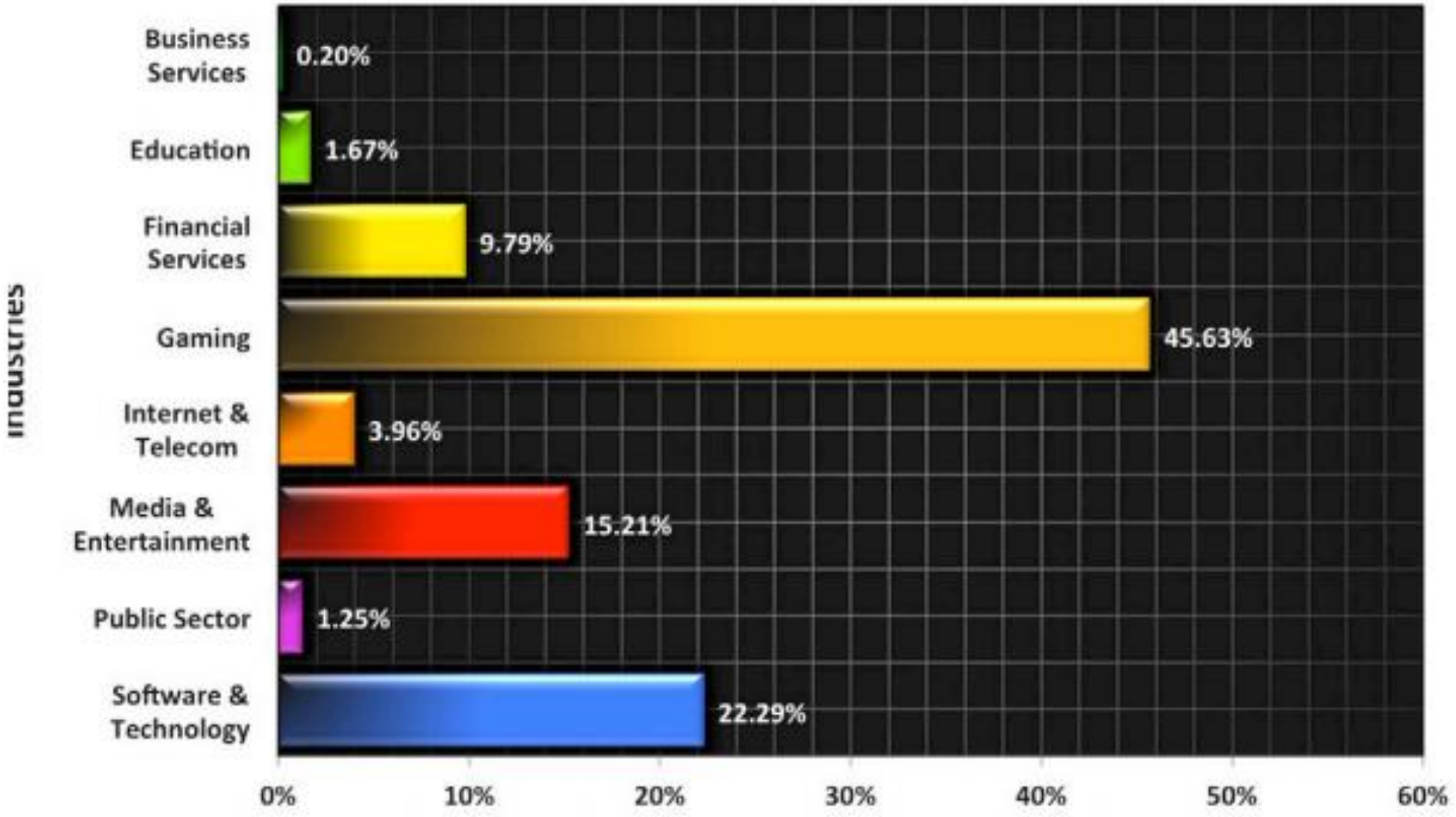


Figure 5: Industries most frequently targeted by DDoS attacks in Q2 2014

Botnet – izvorišta

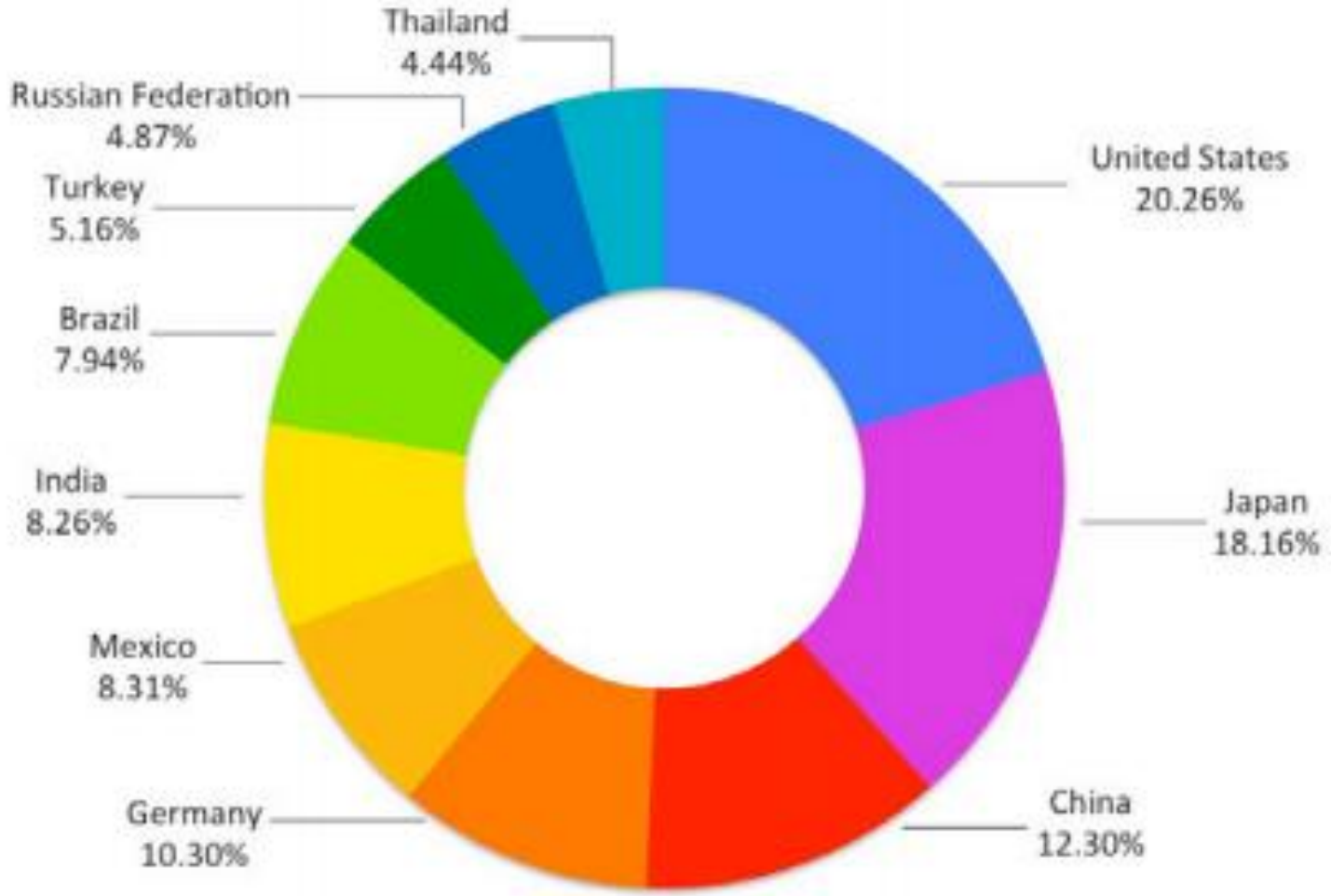


Figure 6: Top 10 source countries for DDoS attacks in Q2 2014

Botnet – SYN* na Akamai DNS

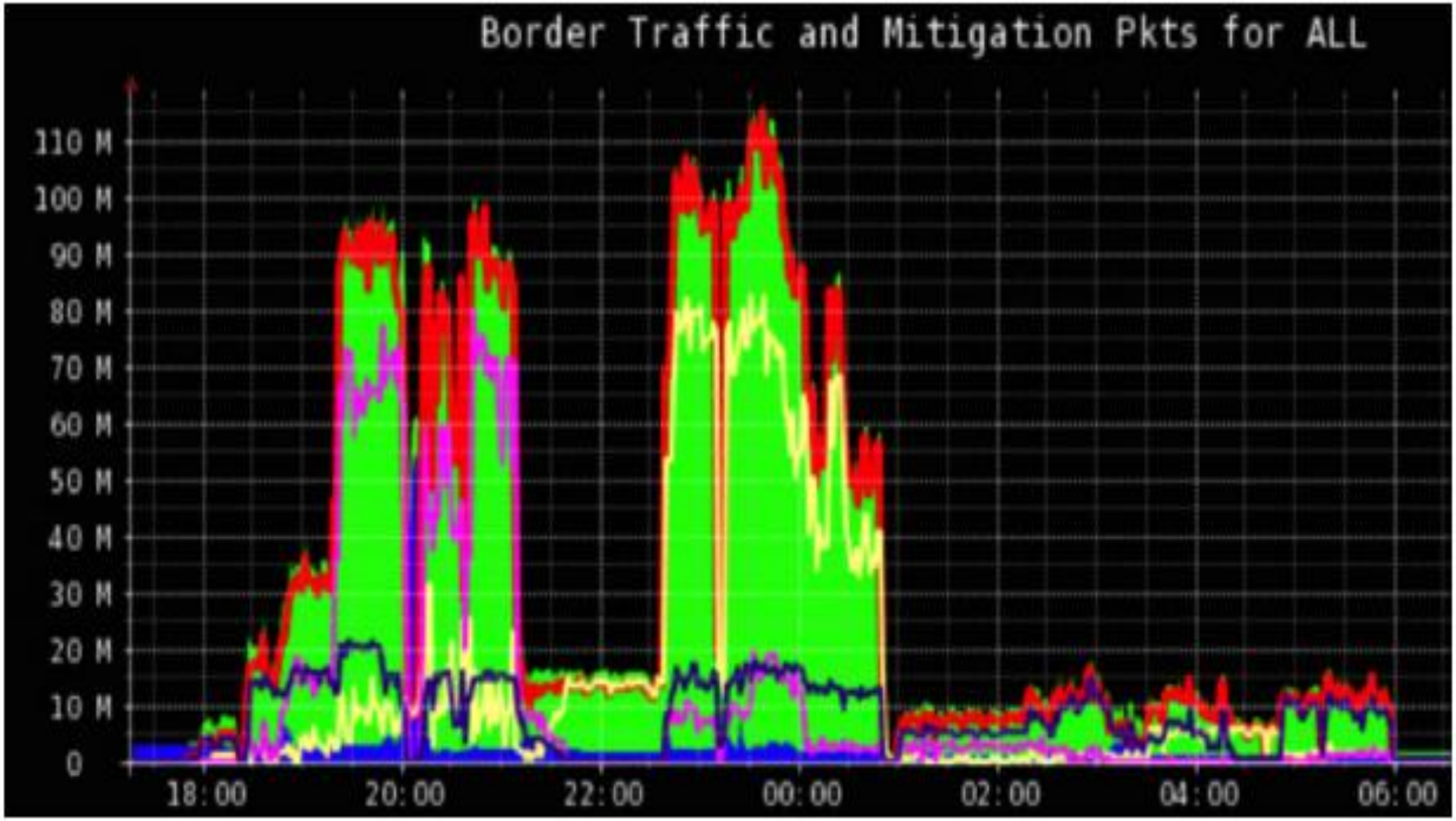
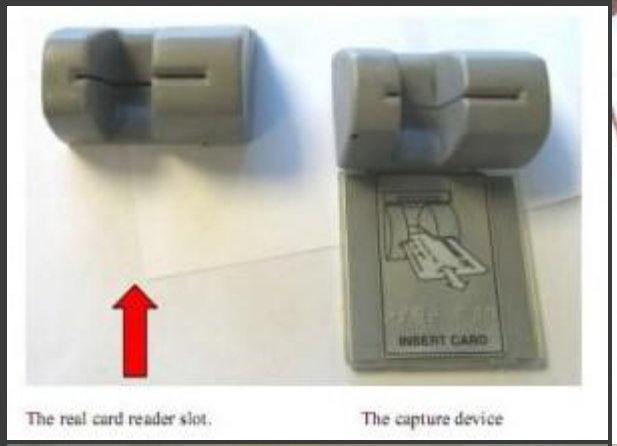
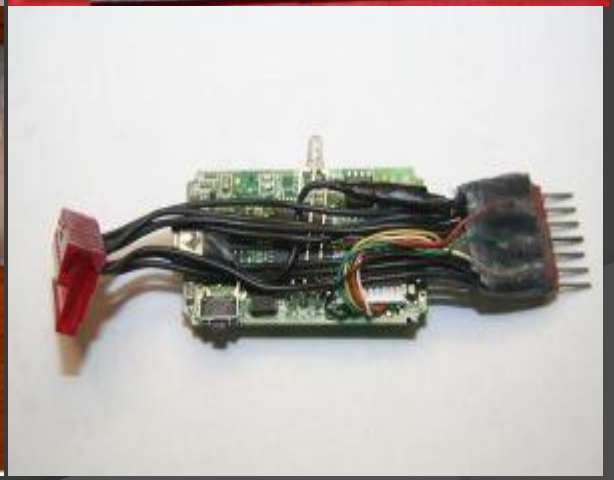


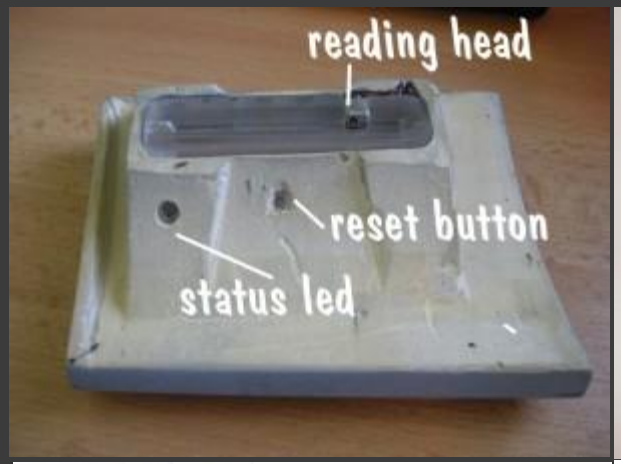
Figure 20: Border traffic and packet-per-second volume for the May 30 attack

Skimming

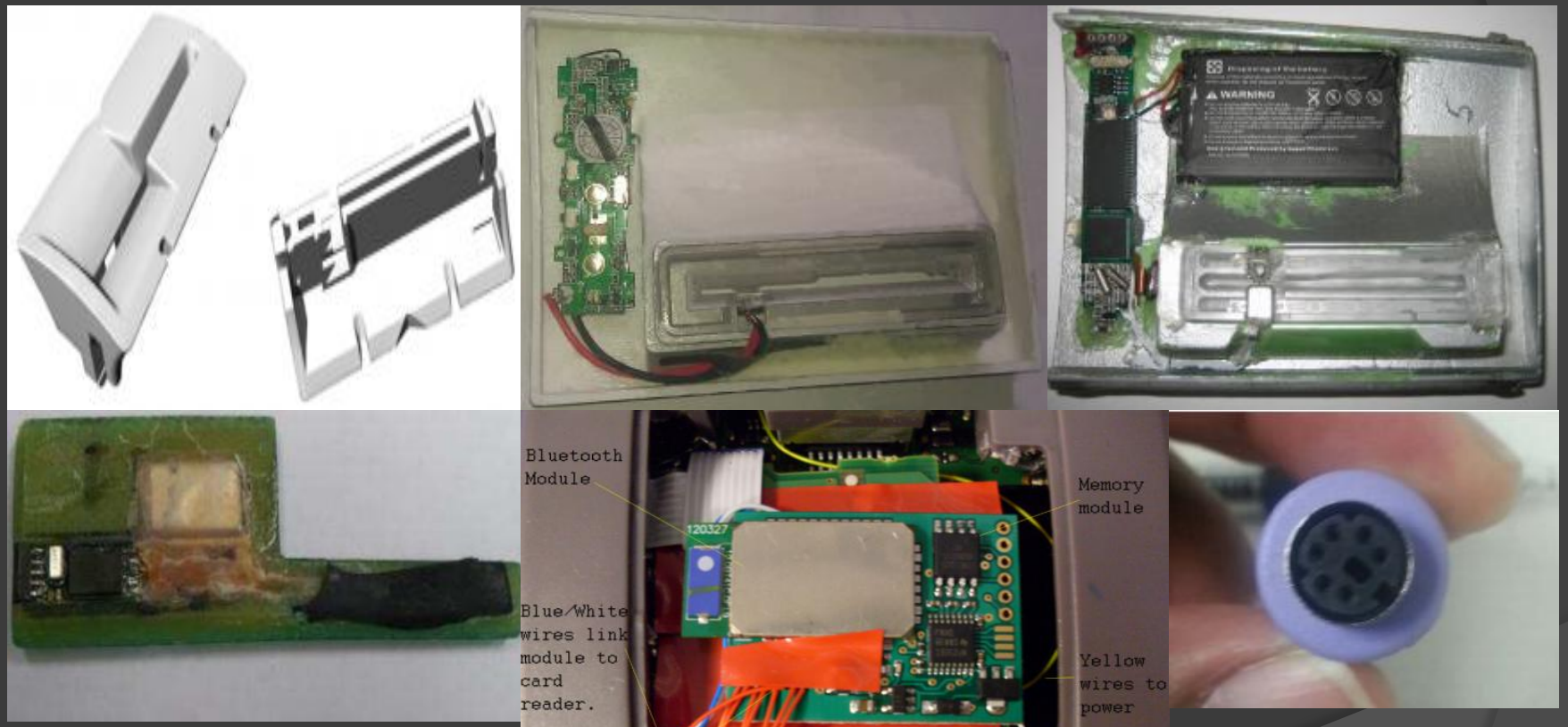




Skimming (2)



Skimming (3)


Bluetooth Module
Memory module
Blue/White wires link module to card reader.
Yellow wires to power
Orange wires connect to PIN pad.