SOPHOS

Poročilo o varnosti poslovnih omrežij 07/08

Rok Jerman

Sophos d.o.o.

Značilnosti groženj v letu 2007

- Razširjanje škodljive kode preko internet strani
- Nove okužene strani vsakih 14 sekund
- Več groženj za uporabnike mobilnih naprav
- Posledice kraje informacij– scammerji s pomočjo teh informacij pripravljajo ciljano elektronsko pošto

Kje nastaja največ škodljive kode?

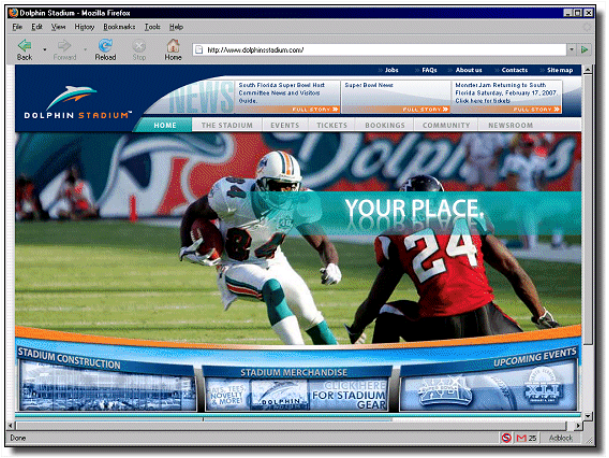
Država	% napisane škodljive kode
Kitajska	21.0%
Brazilija	12.5%
Rusija	9.2%

SOPHOS

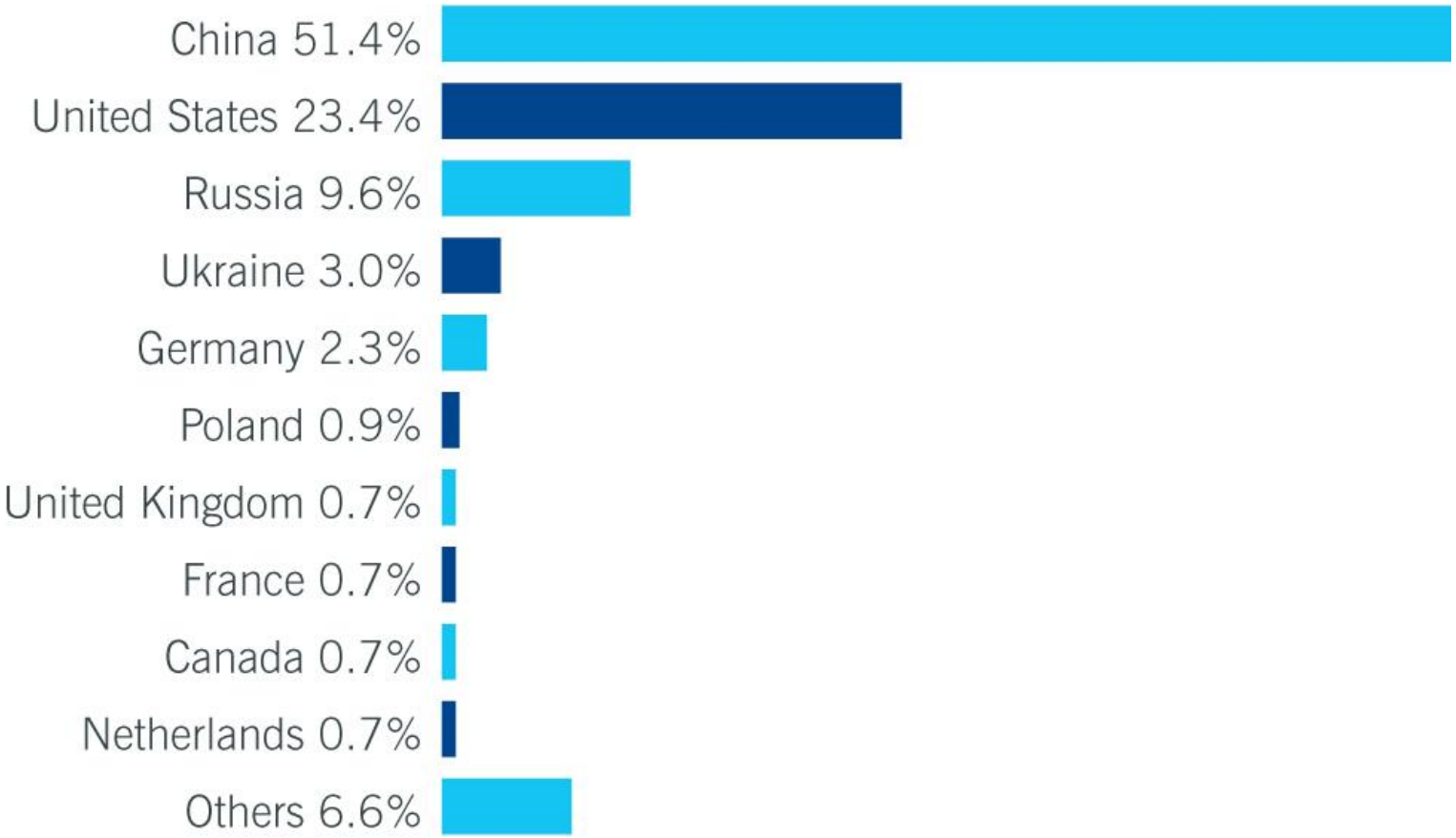
Internetne grožnje – Web zaščita

Internetne grožnje

- Sophos zazna dnevno 6.000 novo okuženih web strani
- 83% teh strani so legalne strani, kamor je bila nameščena škodljiva koda
- Povezave na te strani so največkrat dodane elektronski pošti
- Blokiranje strani glede na vsebino ne zadostuje več



Lestvica držav z okuženimi web stranmi



Priporočila za zaščito web strežnikov

- Ne instalirajte – omogočite nepotrebnih komponent na strežniku
- Preglejte in nameščajte varnostne popravke za vaš sistem
- Uporabljajte posodobljeno anti-virusno zaščito na strežnikih
- Izklopite poročanje o napakah – napake naj se zapisujejo v log datoteke
- Preverite programsko kodo (SQL injection, XSS ..)

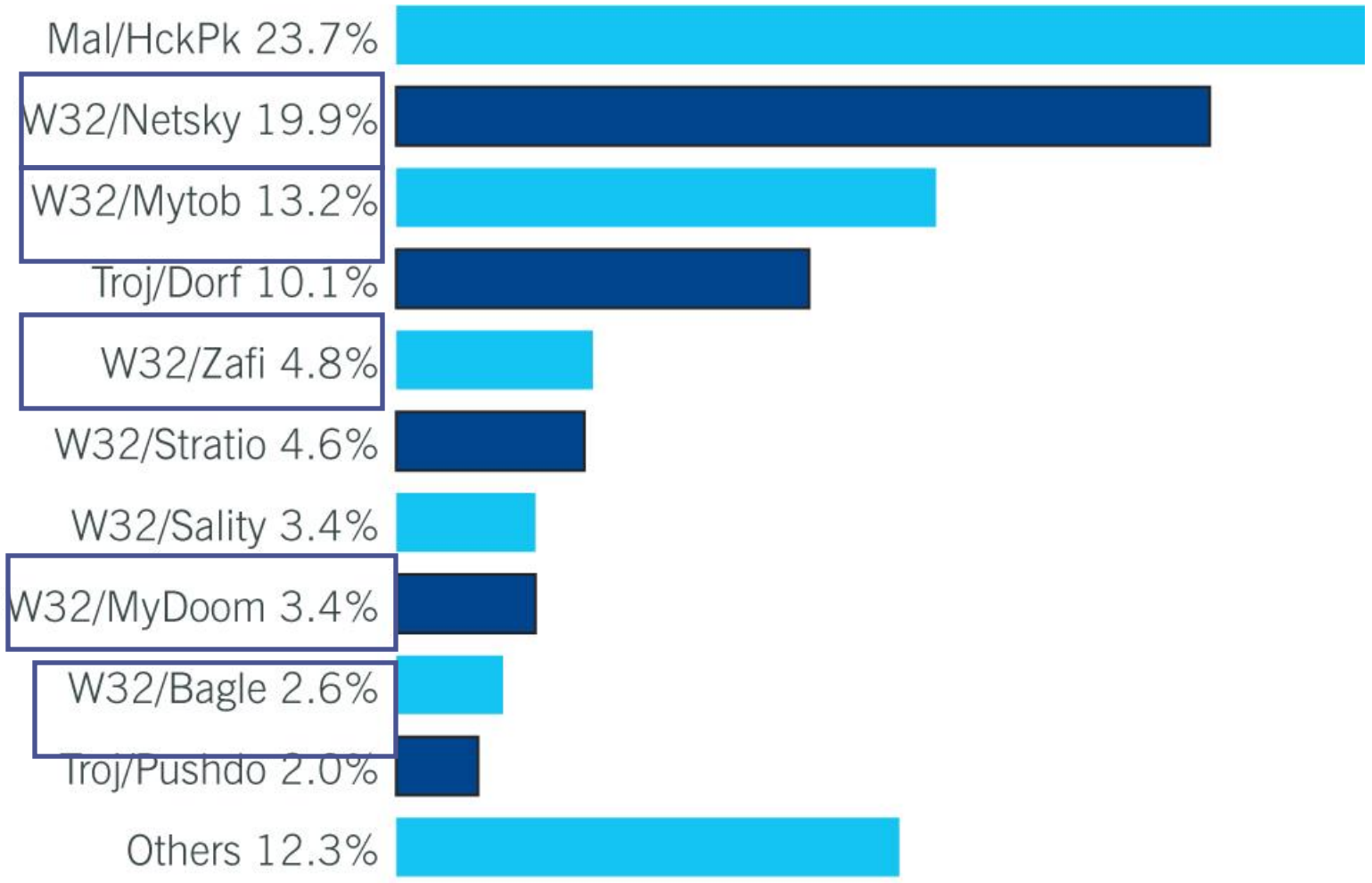
SOPHOS

Elektronska pošta in škodljiva koda

Elektronska pošta in škodljiva koda

Leto	e-pošta s škodljivimi priponkami
2005	1 v 44
2006	1 v 337
2007	1 v 909

Lestvica najpogostejših okužb e-pošte v 2007



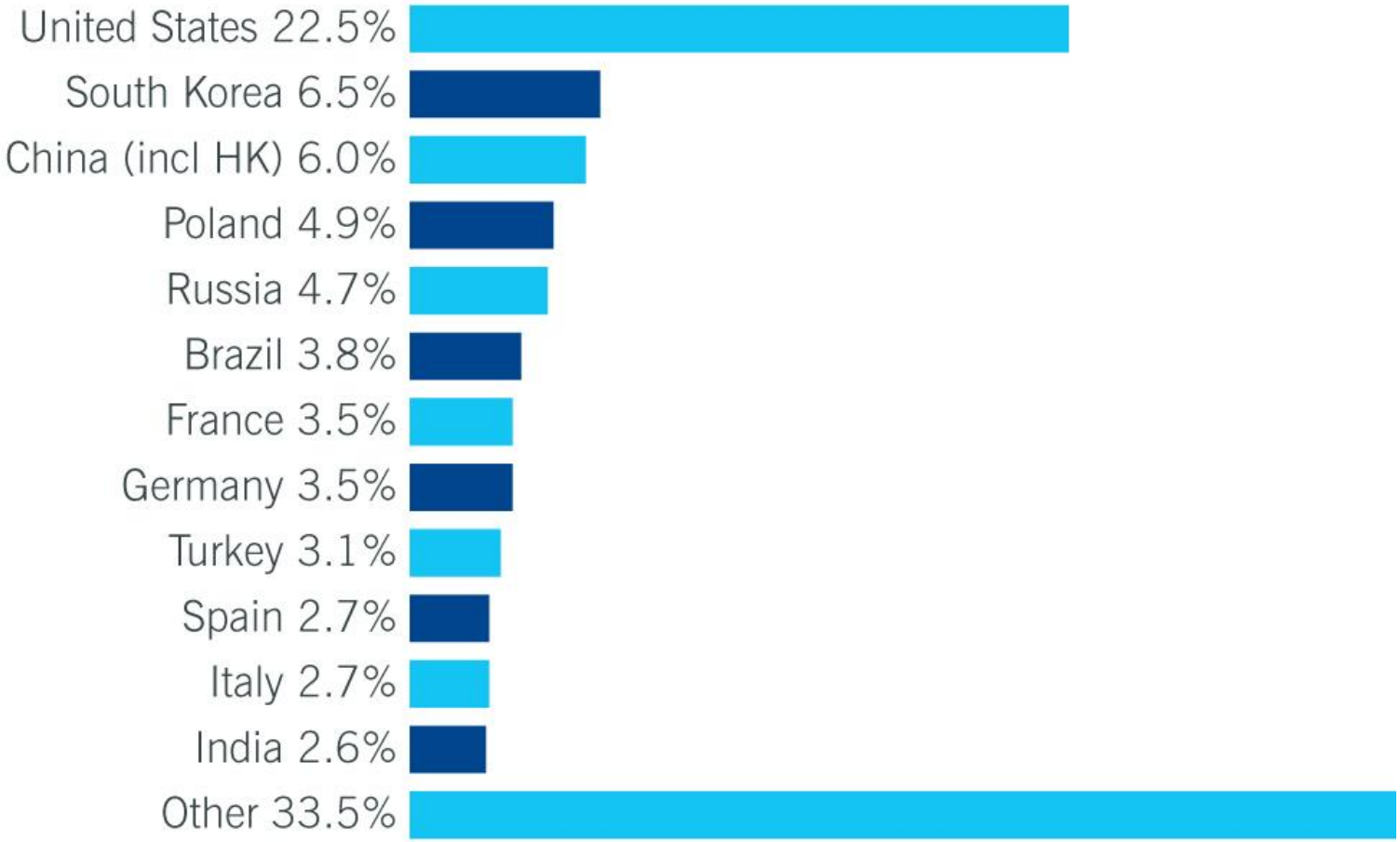
SOPHOS

Nezaželena vsebina - Spam

Spam – naraščujoči problem

- Eden glavnih problemov poslovanja
- 95% vseh elektronskih sporočil je nezaželenih
- Nove tehnike razširjanja

Lestvica držav z največ spam posredniki - 2007



SOPHOS

Mobilne naprave in uporaba brezžičnih naprav

Kaj ogroža mobilne naprave

- Na koncu leta 2007 je bilo prisotnih cca 200 groženj za mobilne naprave (za Windows okolje 300.000)
- Stalna rast groženj
- 64 % poslovnih uporabnikov še ne uporablja nobene zaščite za pametne telefone in dlančnike

Ultra mobilni PC-ji in Wi-Fi naprave

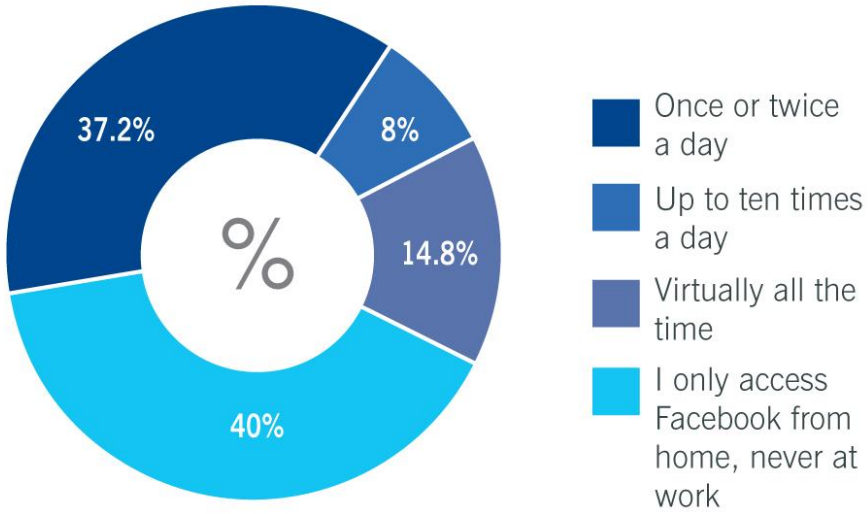
- Naraščajoče število ponudnikov brezžičnega dostopa povečuje uporabo mobilnih brezžičnih naprav
- Zaenkrat ne kaže na strmo naraščanje ogroženosti – ni finančne motivacije
- Poleg Windows okolja najbolj na udaru Apple izdelki: IPod, IPhone, Safari brskalnik

SOPHOS

Socialna omrežja

Socialna omrežja

- Strani kot so Facebook, Bebo, Orkut in Myspace so postale zelo popularne v letu 2007
- Uporablja jih ne samo mladina, ampak tudi odrasli - zaposleni
- Strani so zanimive za kriminalce – vir zasebnih podatkov



SOPHOS

Prihodnost

Prihodnost

- Napovedi so praktično nemogoče, zaradi hitrih sprememb na področju ogrožanja omrežij
- Po mnenju 70% vprašanih v Sophosovi raziskavi bo letošnje leto enako ali slabše kar se tiče ogroženosti poslovnih omrežij
- Število groženj bo še naraslo
- Varovanje in nadzor računalnikov
- Programska oprema za zaščito omrežij se nadgrajuje z novimi funkcionalnostmi

Strategija zaščite

- Začita na nivoju končnega uporabnika – najbolj izpostavljen in ogrožen nivo
- Reaktivna - Proaktivna – Preventivna zaščita
- Network Access Control
- Web Control
- Application Control

Sophos security and control rešitve