

KIBERNETINIS SAUGUMAS:

iššūkliai, atakų tipai bei telekomunikacijų
operatoriaus vaidmuo

Vytautas Bučinskas, Rizikų valdymo skyriaus direktorius

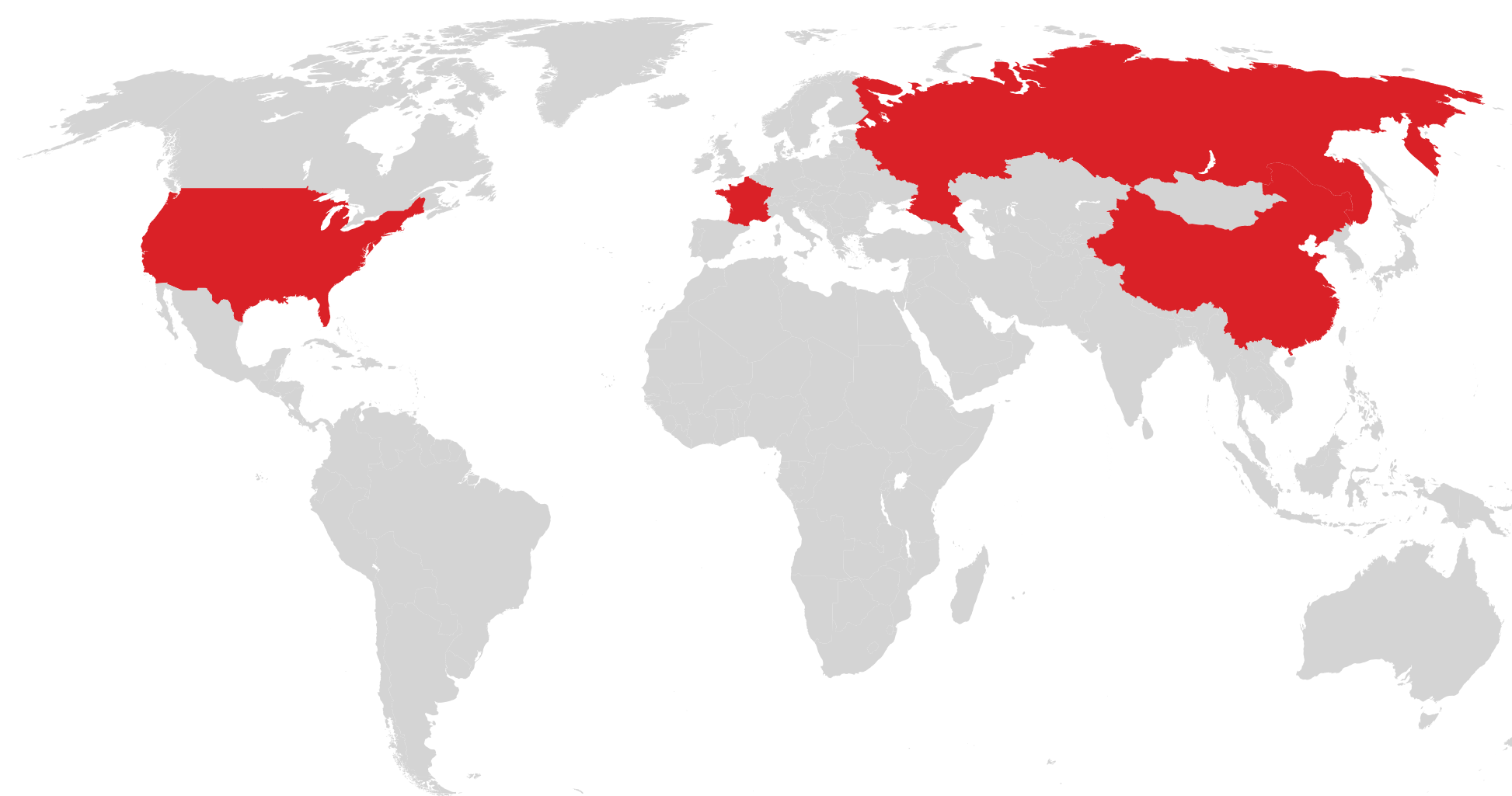
GEOPOLITINĖ APLINKA



PAGRINDINIAI ŽAIDĖJAI KIBERNETINĖJE SFEROJE:

- **VALSTYBĖS**

- JAV,
- Rusija,
- Kinija,
- Prancūzija



GEOPOLITINĖ APLINKA (2)

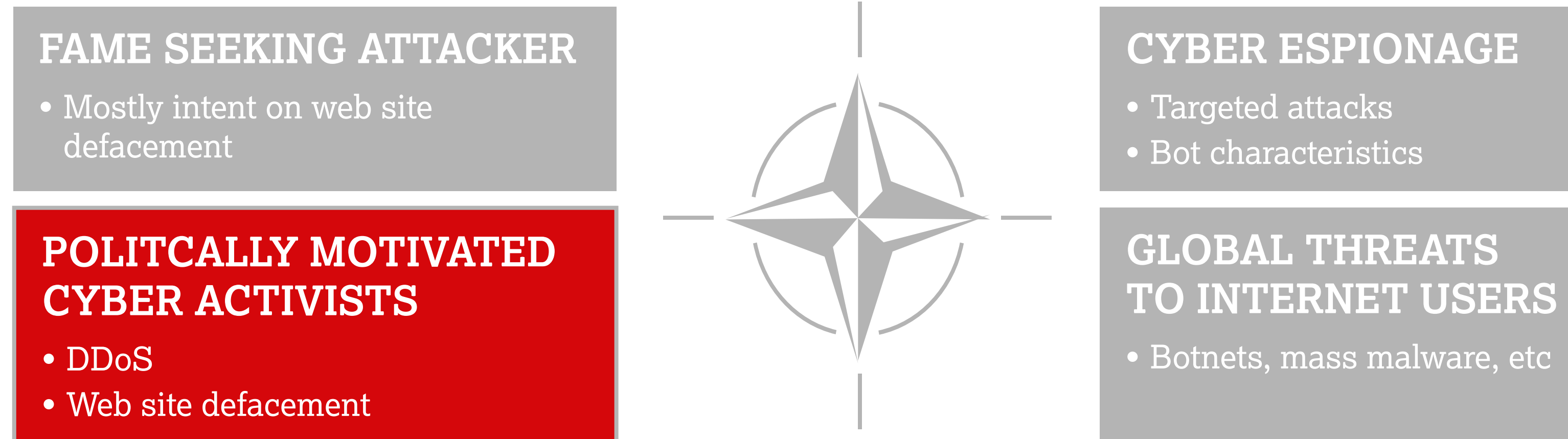


PAGRINDINIAI ŽAIDĖJAI KIBERNETINĖJE SFEROJE:

- **NEVALSTYBINĖS ORGANIZACIJOS**
 - **ORGANIZUOTAS** nusikaltamumas
 - pvz., RBN – „Russian Business Network“
 - **HAKERIAI** ir (arba) kibernetiniai teroristai
 - Estijos, Gruzijos kibernetiniai karai, „Anonymous“ grupė



GRĖSMIŲ KATEGORIJOS PAGAL NATO



- **OPERATORIUI** didžiausias vaidmuo tenka DDoS rizikai valdyti
- **MANOME**, kad be operatoriaus įsikišimo jokia institucija nebus pajėgi susidoroti su šiuolaikine gerai organizuota DDoS ataka

DDOS ATAKOS PASAULYJE

ARBOR SKELBIAMA STATISTIKA

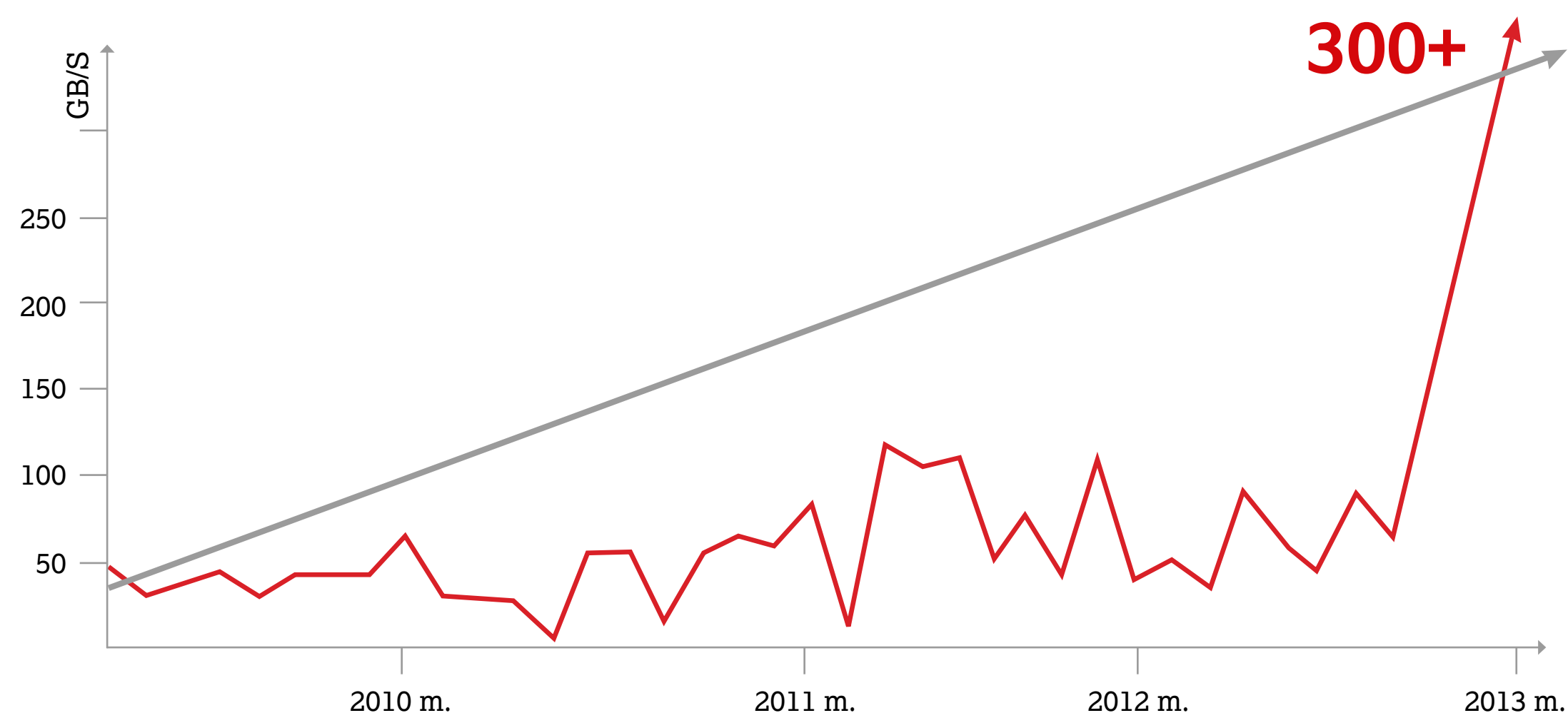
- Užfiksuota atakų, kurioms vykstant viršytas 100 Gb/s greitis tinkle

TAIP BUVO APIE 10 METŲ IKI 2013 M. KOVO 27 D., KAI BUVO ATAKUOJAMAS „SPAMHAUS“

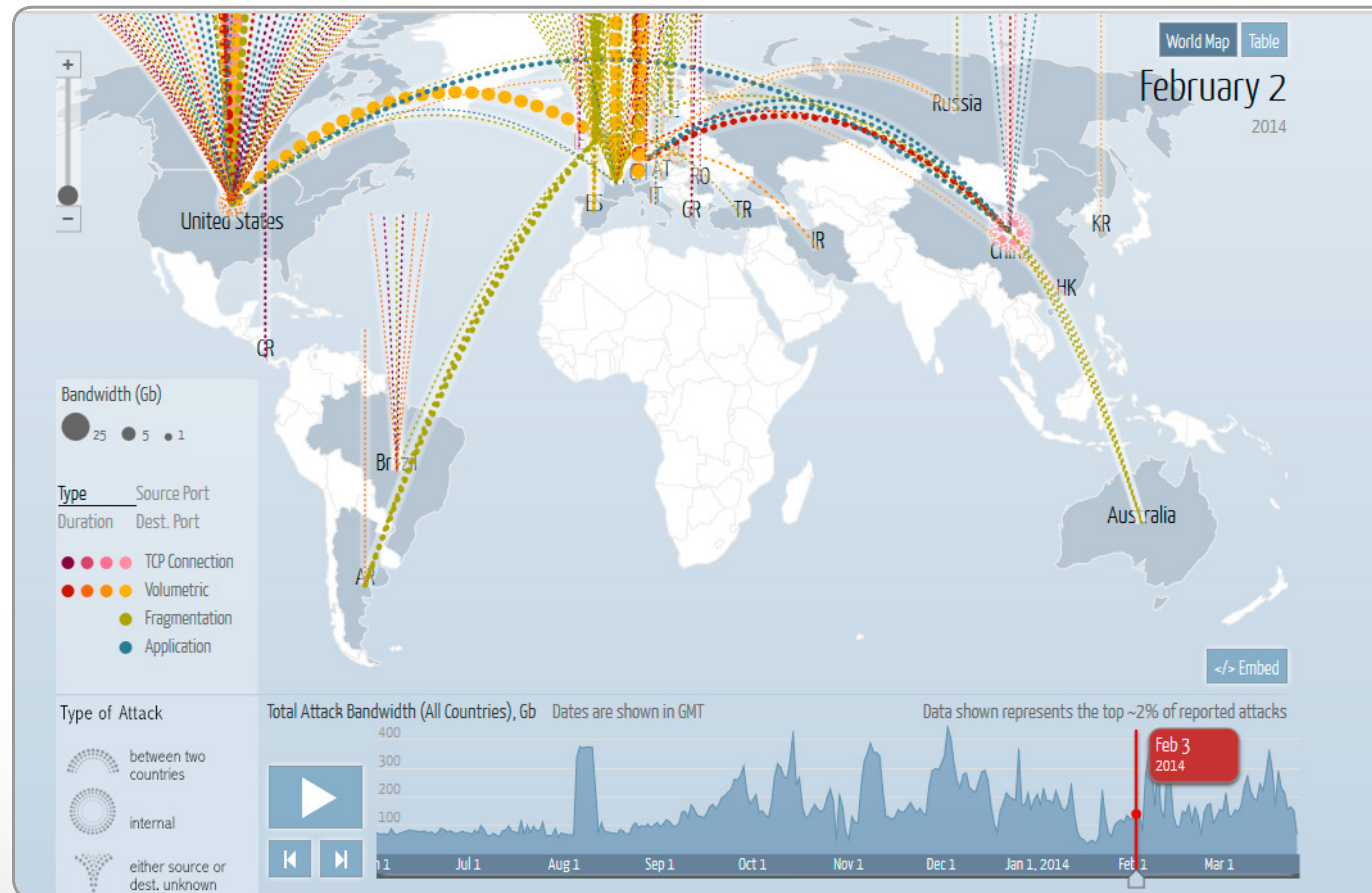
- Atakos srautas pasiekė iki 300 Gb/s spartą
- Priemonės „Botnet“, „Open DNS“, „Spoofed IP“
- Atakos metu pakeista atakos kryptis, nukreipiant srautą į vieną iš „Internet Exchange“ taškų
- Klaida IX konfigūracijoje lėmė tai, kad kai kuriose Europos šalyse buvo interneto sutrikimų

2014 M. „CLOUDFLARE“ PASKELBĖ APIE JUOS PASIEKUSIĄ 400 GB/S ATAKĄ

DDOS ATAKŲ APIMTYS



EILINĖ DIENA PASAULIO ATAKŲ ŽEMĖLAPYJE



Šaltinis – <http://www.digitalattackmap.com/>

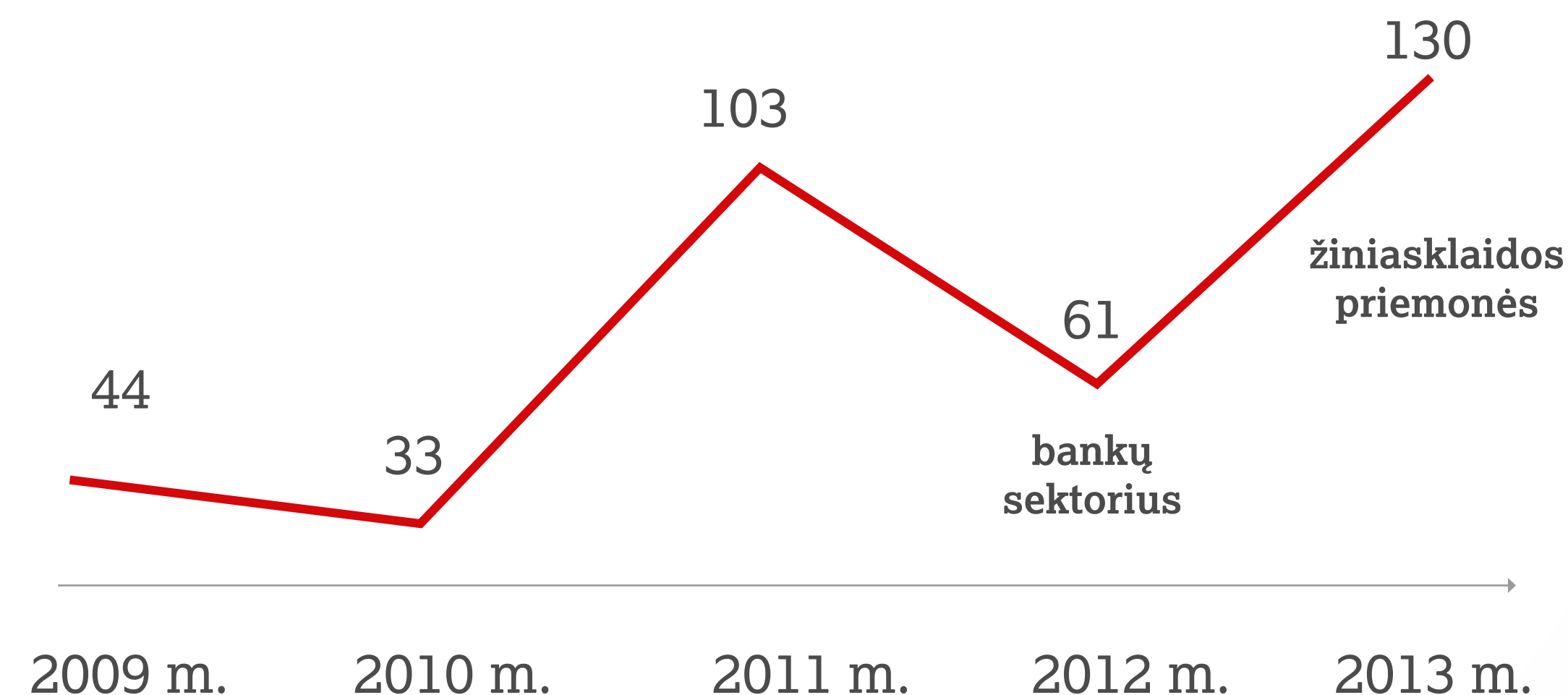
DDOS ATAKOS LIETUVOJE

CERT-LT SKELBIAMA STATISTIKA

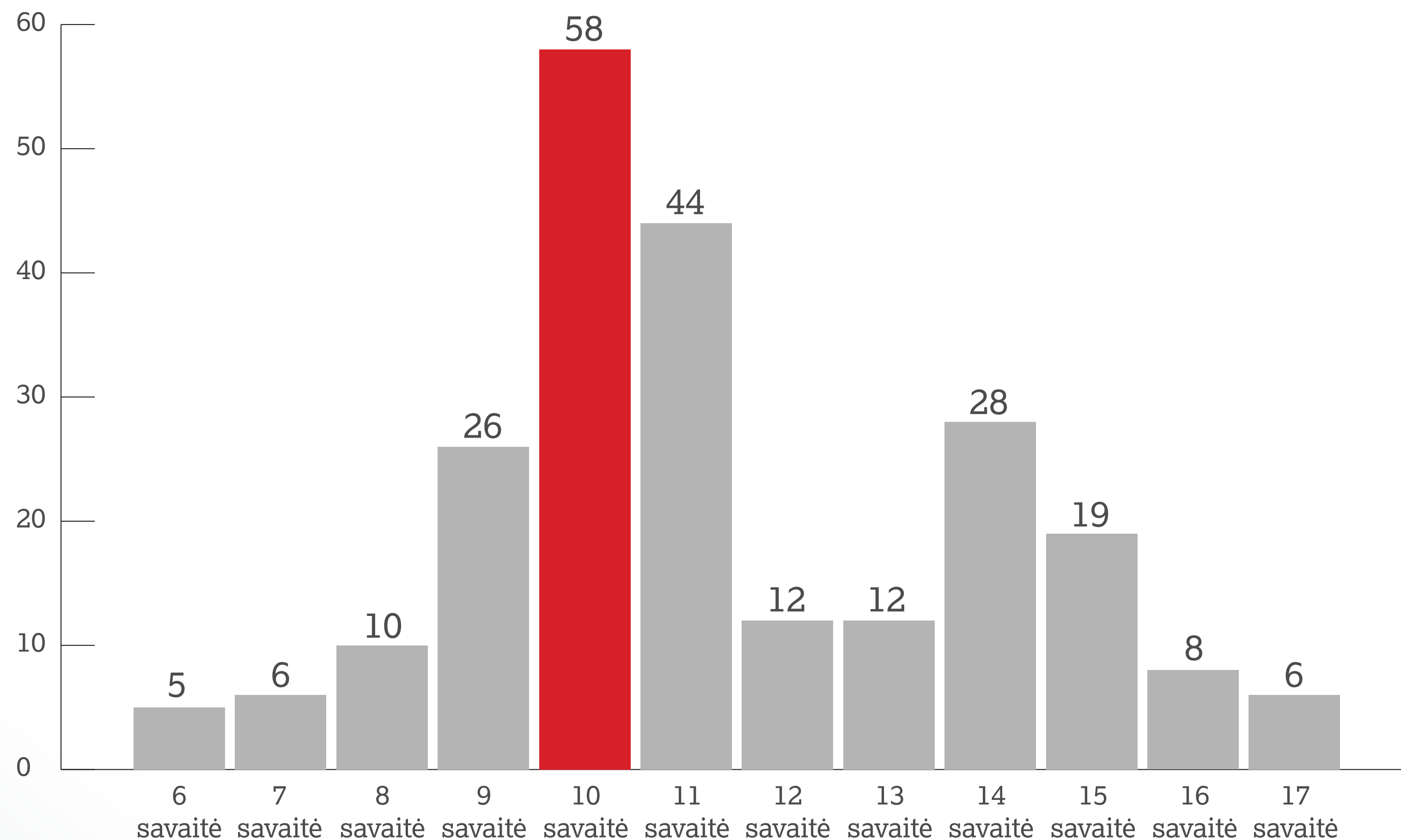
- Apie 7 tūkst. kompiuterių „zombių“ Lietuvoje dalyvauja *botnet* veiklose kas dieną
- 2013-09-09 neutralizuotas Lietuvoje veikęs *botnet* serveris, kuris galėjo valdyti 5400 kompiuterių visame pasaulyje. Iš tuo metu veikiančių 600 „zombių“ 75 buvo iš Lietuvos.
- 2013 m. CERT-LT ištyrė 130 pranešimų apie elektronines paslaugos trikdymo (DDoS) atakas

KAS BUS 2014 M.?

DDOS ATAKŲ SKAIČIUS LIETUVOJE



REALIŲ ATAKŲ Į TEO TINKLĄ APIMTYS 2014 M., GB/S*



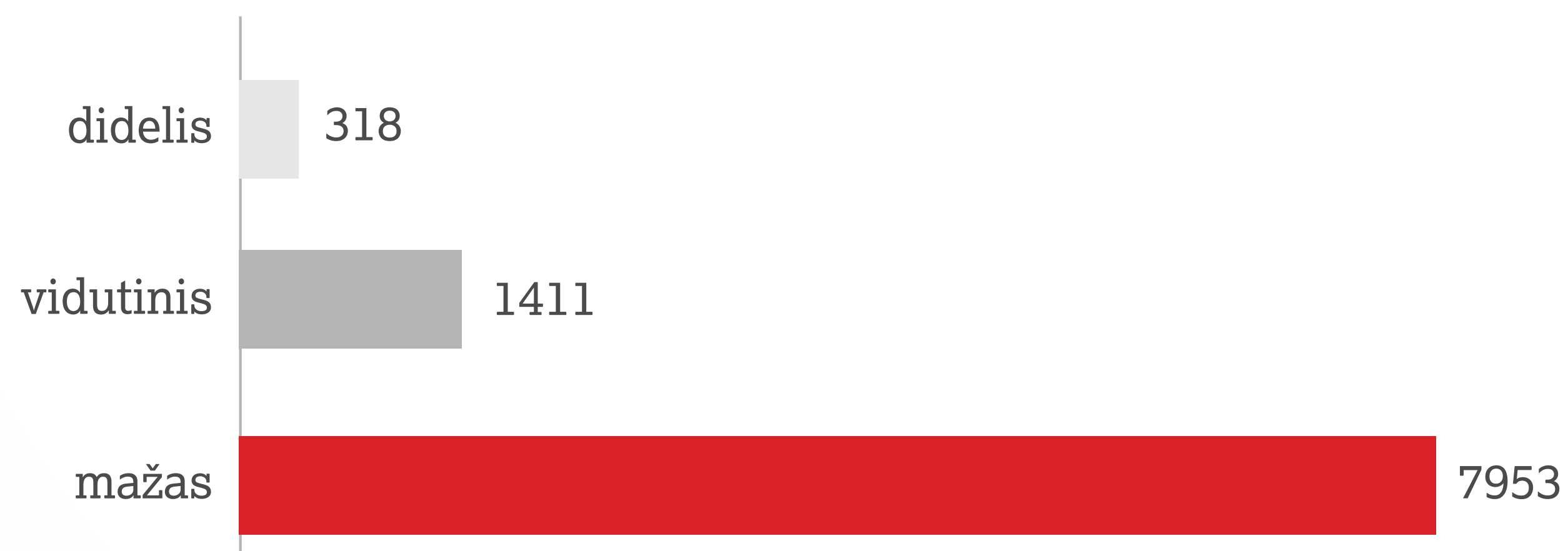
* - pagal TeliaSoneros Arbor ataskaitas, didžiausios atakos apimtis Gbps nurodytą savaitę

2014-04-30

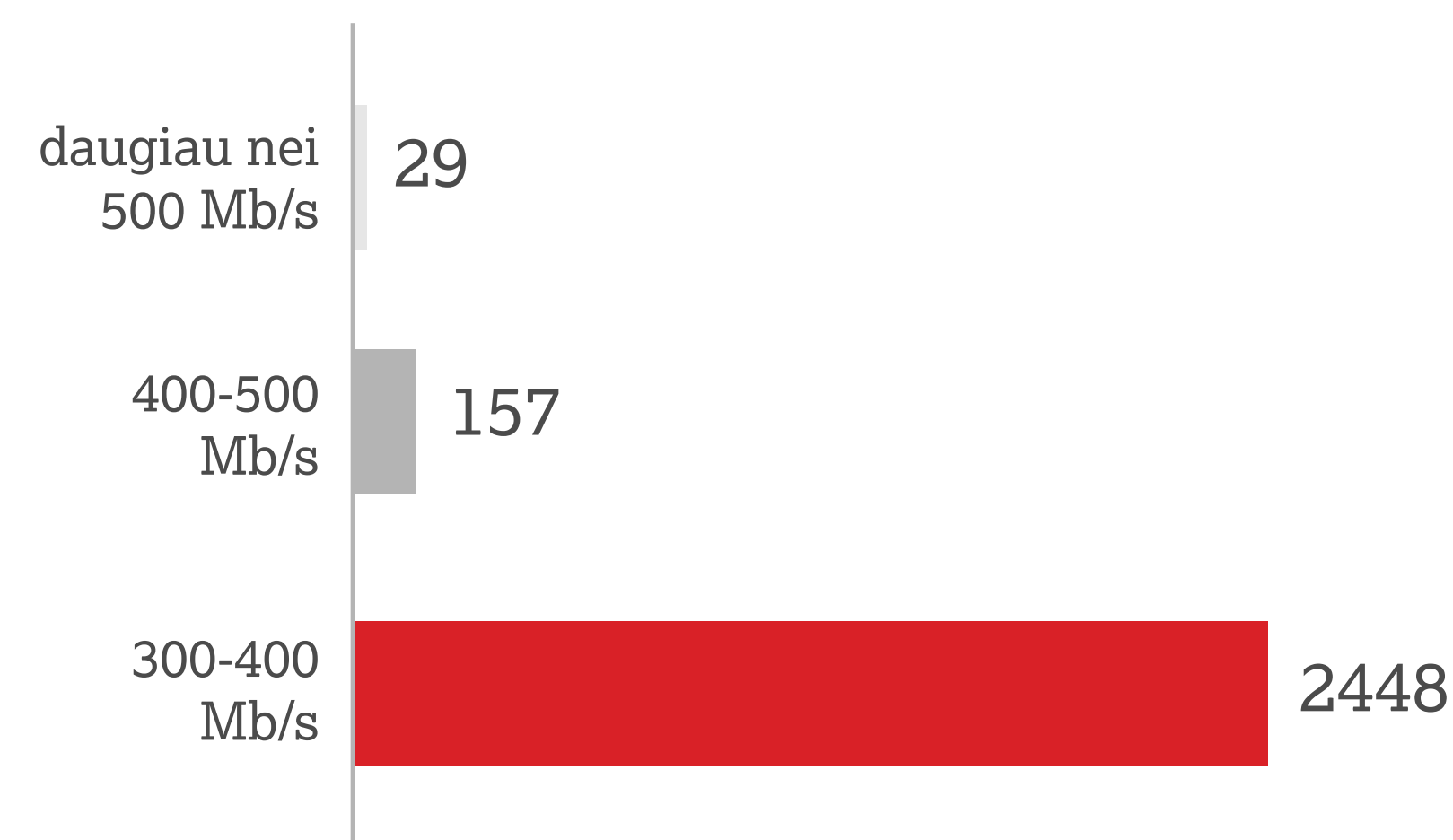
DDOS ATAKŲ KIEKIAI TEO TINKLE



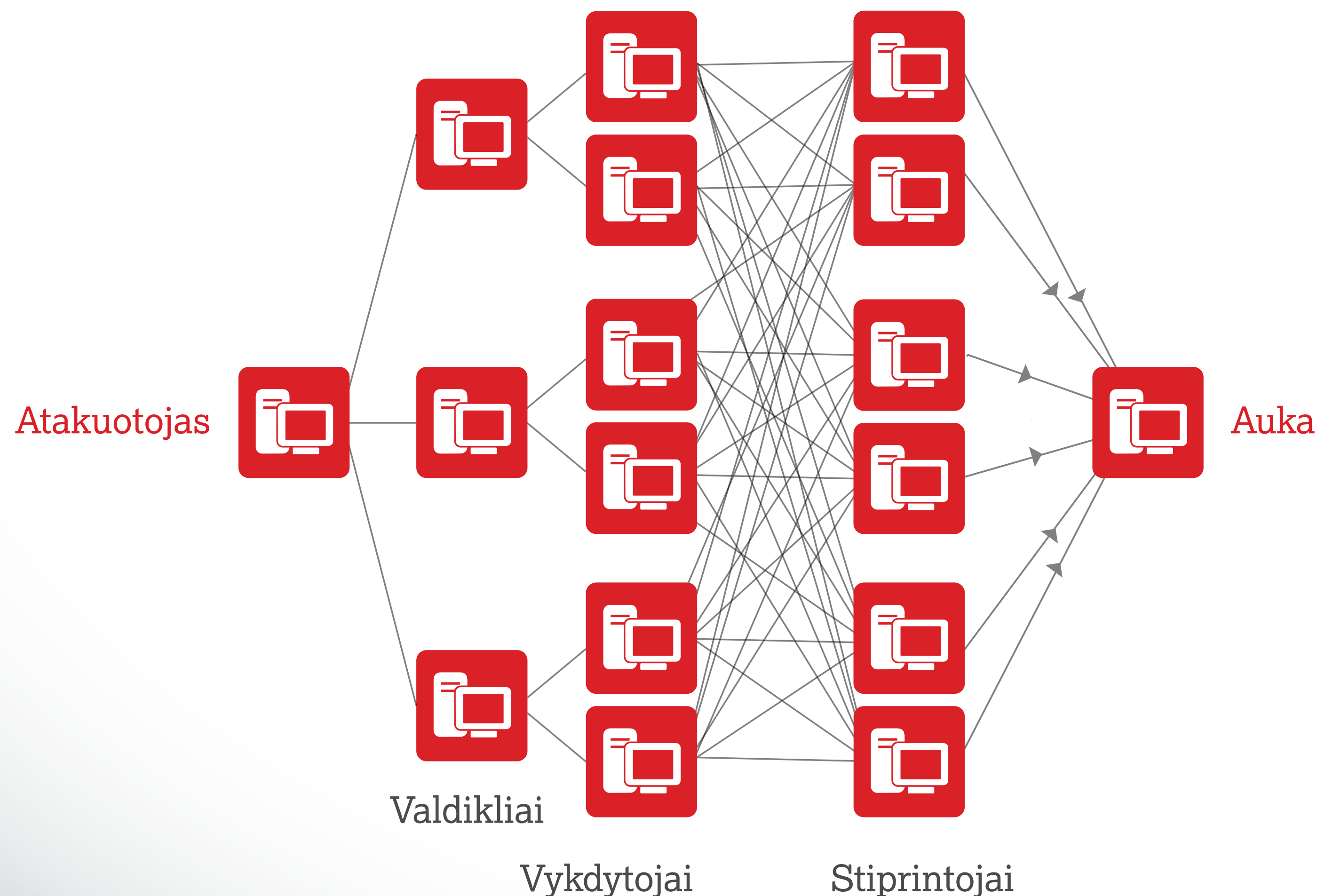
ATAKŲ PAVOJAUS LYGIS IR SKAIČIUS



ATAKŲ APIMTIS IR SKAIČIUS



KO REIKIA ATAKAI?



ATAKUOTOJO

VALDIKLIŲ

(kompiuteriai „zombiai“)

VYKDYTOJŲ

(daug kompiuterių „zombių“)

STIPRINTOJŲ (pvz. atviri DNS)

„NESAUGIŲ“ ISP

(nepakankama autentifikacija)

AUKOS

AR SUNKU RASTI UŽKRĖSTŲ KOMPIUTERIŲ?



Top 10 Booters

#1: Divine Stresser - <http://Divinestresser.com> (120GB/seconds)(Skype Resolver)(Stop Button)(Cheapest)(Strongest Ever)(Admin's Choice)

#2: Minecraft Stresser - <http://Minecraftstresser.com> (80GB/seconds)(Skype Resolver)(Good Staff)(Powerful)

#3: Dark Booter - <http://darkbooter.com> (Up for 2 years)(Good Price)(Great Support)

#4: IP Stresser - <http://ipstresstest.com> (Powerful)(Up for 3 years)

#5: Power Stresser - <http://powerstresser.com> (Strong Power)

#6: Titanium Stresser - <http://titaniumstresser.net>

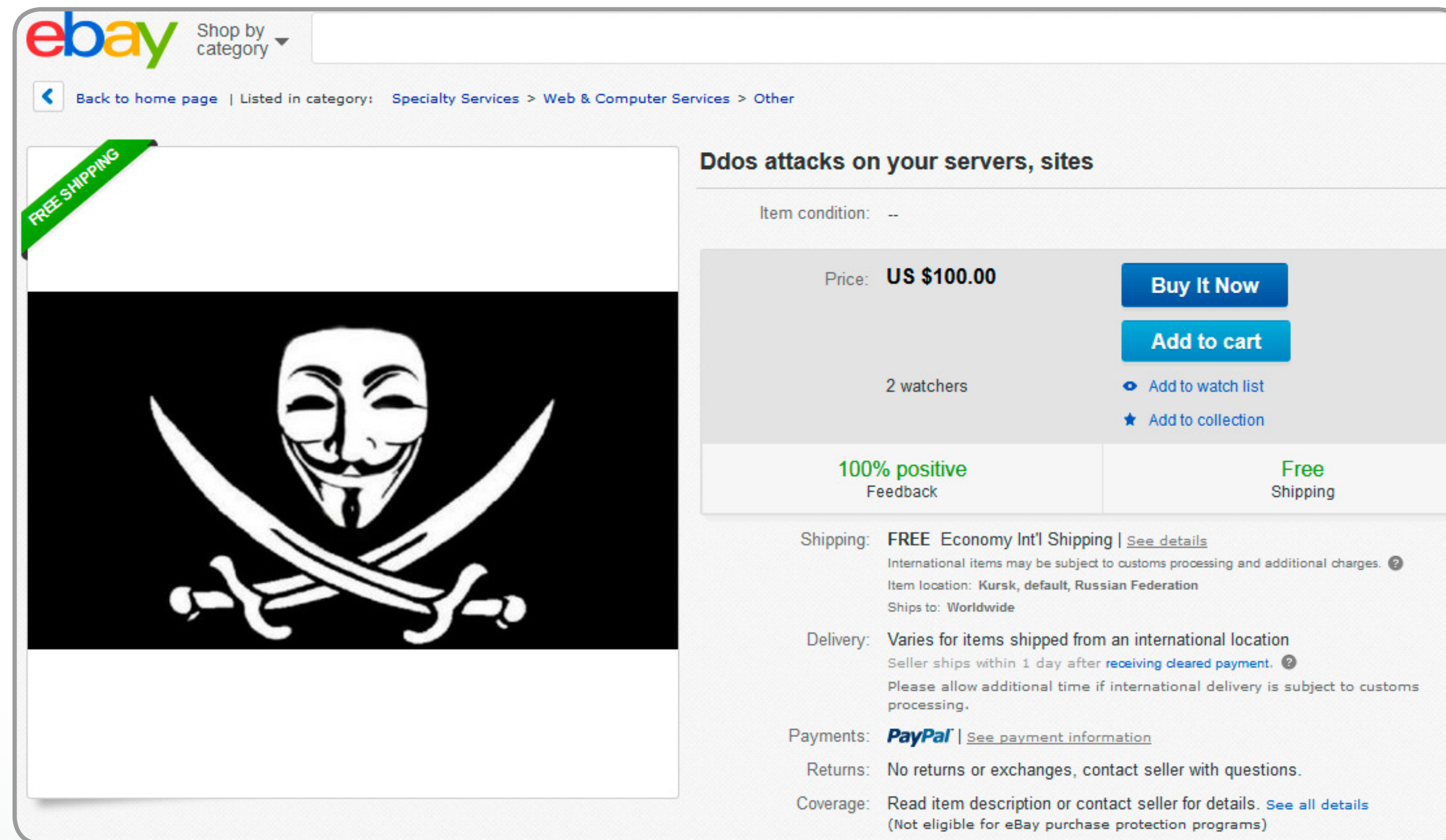
#7: DejaBooter Stresser - <http://www.dejabooter.com/> (Max Time)

#8: Legion Booter - <http://legion.cm/> (Strong)

#9: Masterboot - <http://www.masterboot.net/> (Hard Hitting)

#10: Avenge Stresser - www.avengestresser.com/ (Great Price)

AR DAUG KAINUOJA JŲ ĮSIGYTI?



- 1 VAL. – 10 JAV DOLERIŲ
- 24 VAL. – NUO 100 JAV DOLERIŲ
- SAVAITĖ – NUO 600 JAV DOLERIŲ
- MĖNUO – NUO 2 000 JAV DOLERIŲ

AR LENGVA RASTI ATAKOS STIPRINTOJŲ?



INTERNETE ESANTYS ATAKOS STIPRINTOJAI:

- atviri DNS resolveriai (~28 mln. visame pasaulyje)
- atviri, pažeidžiami NTP servais
- atviri SNMP servais
- atviri nebenaudojami „legacy” servais (pvz. chargen)

ATAKOS SRAUTĄ PADIDINA:

8 kartus

iki 200 kartų

650 kartų

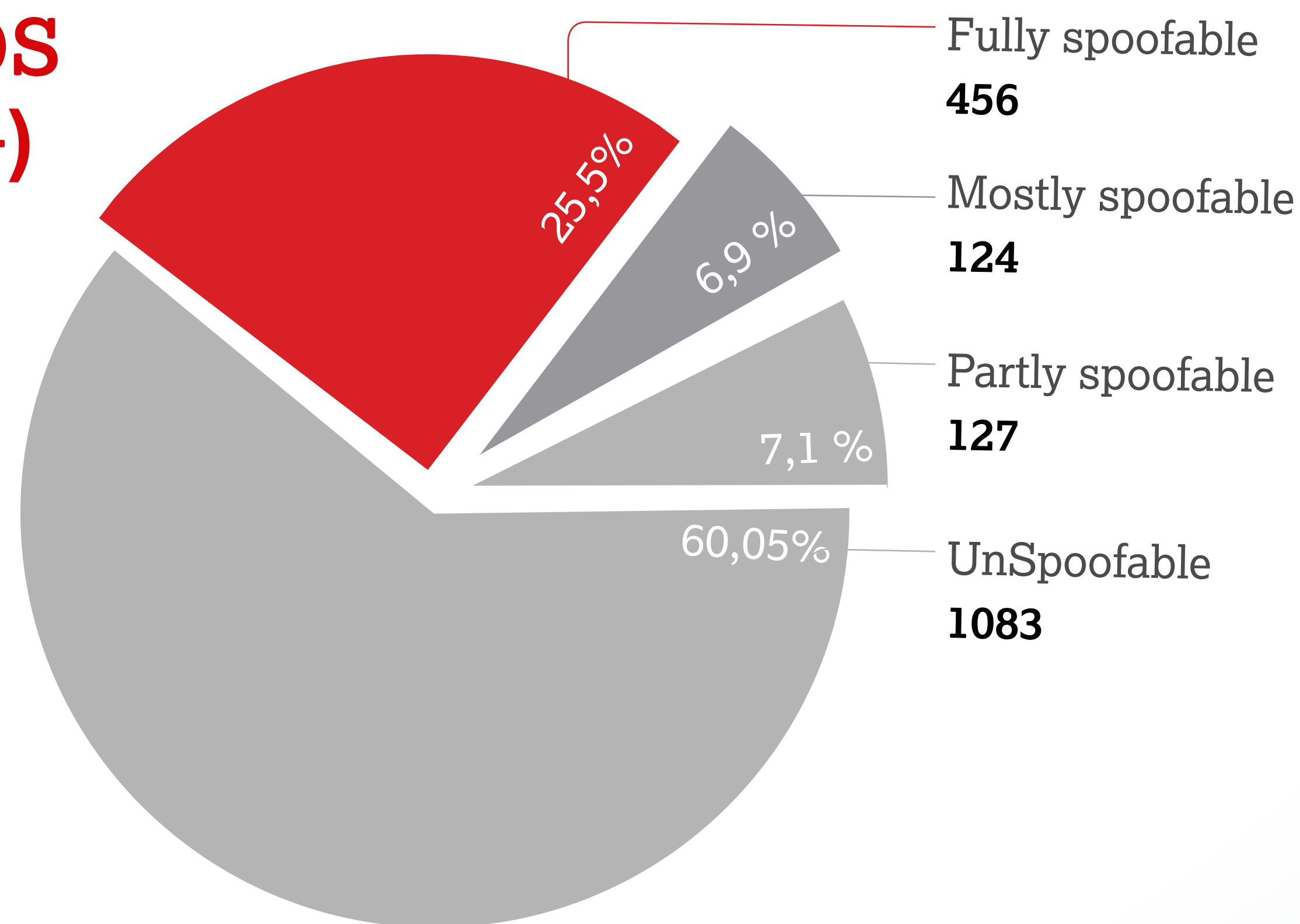
200-1000 kartų

AR DAUG TINKLŲ LEIDŽIA IMITUOTI IP ADRESUS?

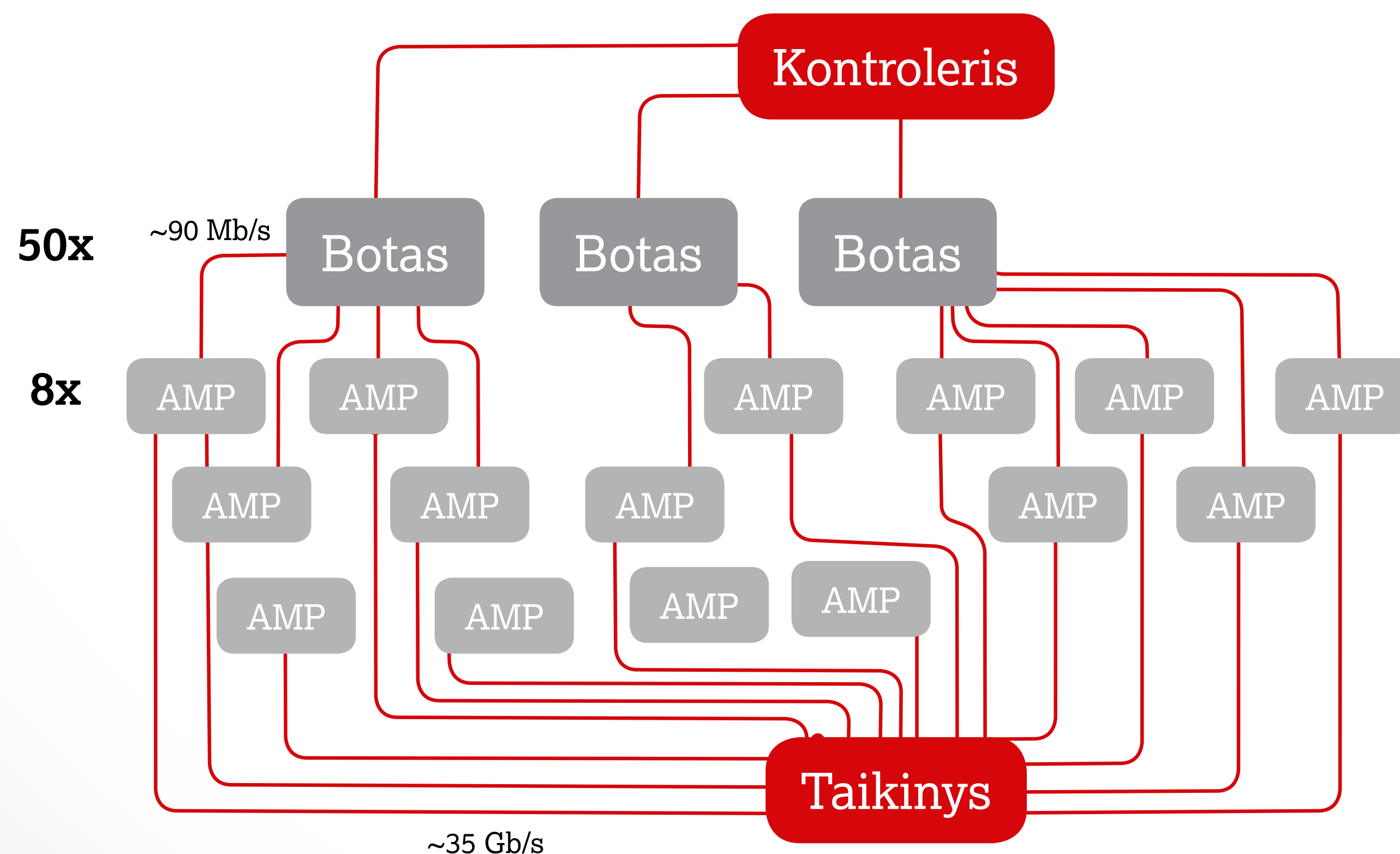


SOURCE IP AUTENTIFIKACIJOS NEBUVIMAS (ANTI-SPOOFING)

- 25% tinklų pasaulyje netaiko *anti-spoofingo*

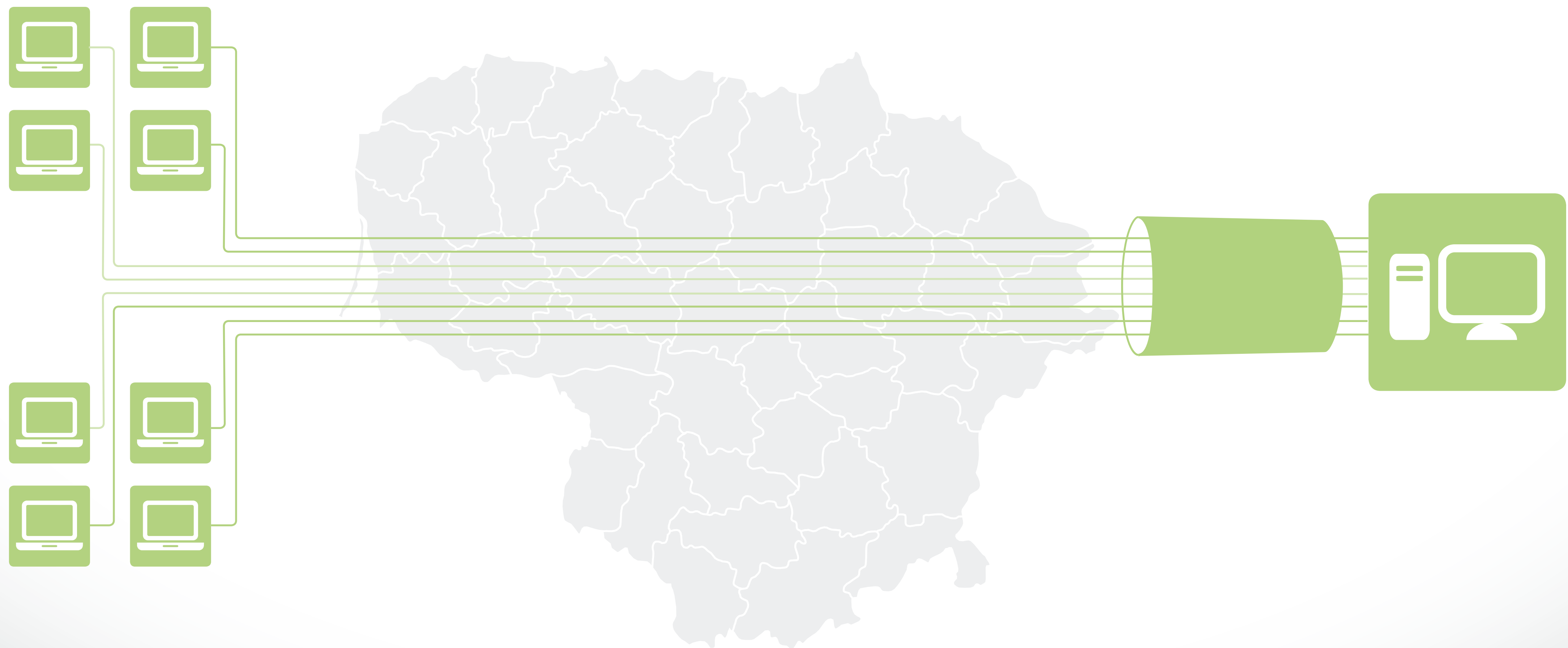


KĄ SU VISU TUO GALIMA PADARYTI?

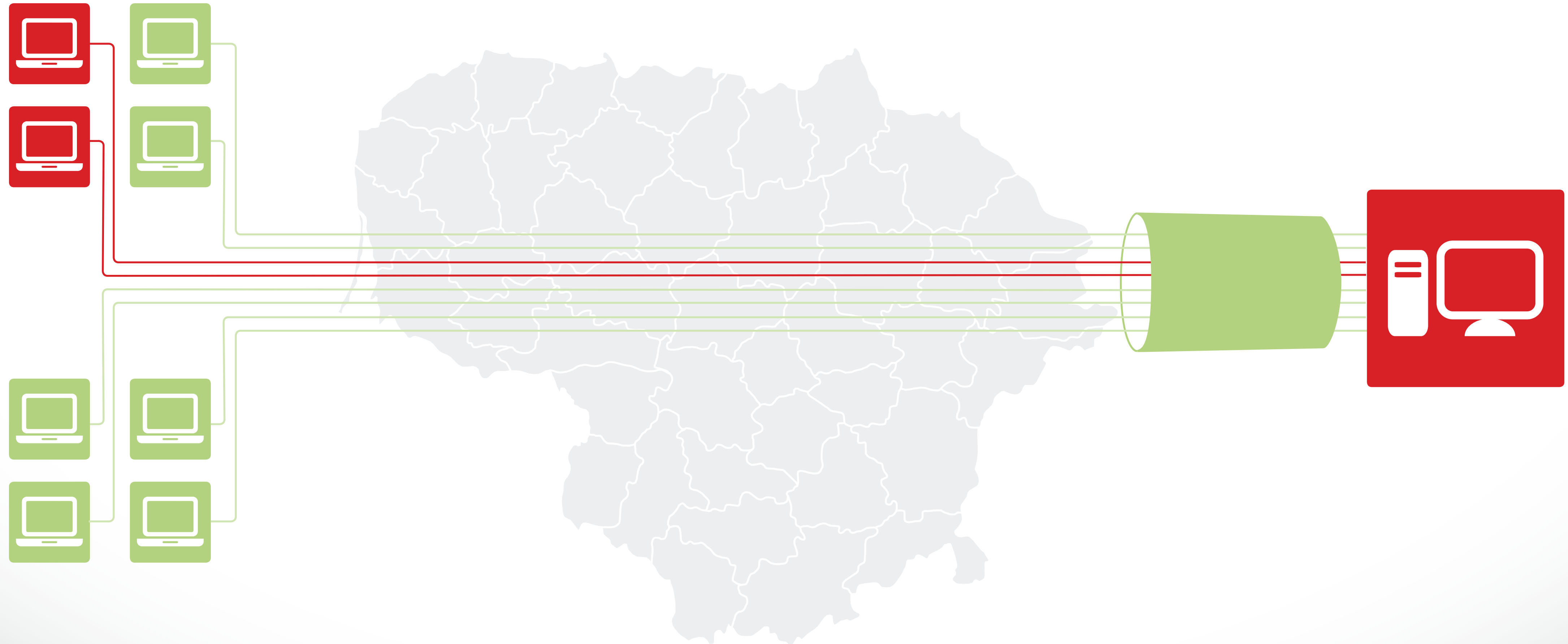


- **50 UŽVALDYTŲ** kompiuterių (*botų*) turinčių gerą ryšį (100 Mb/s)
- **VISI UŽVALDYTI** kompiuteriai (*botai*) nesaugiamame, netaikančiame antispoofig'o interneto paslaugų teikėjo (ISP) tinkle
- **4,5 GB/S** DNS užklausų į 1000 atvirų DNS *resolverių* visame pasaulyje
- **REZULTATAS** – daugiau kaip 30 Gb/s DDoS ataka

ATAKA, KAI AUKA BE APSAUGOS NUO ATAKOS



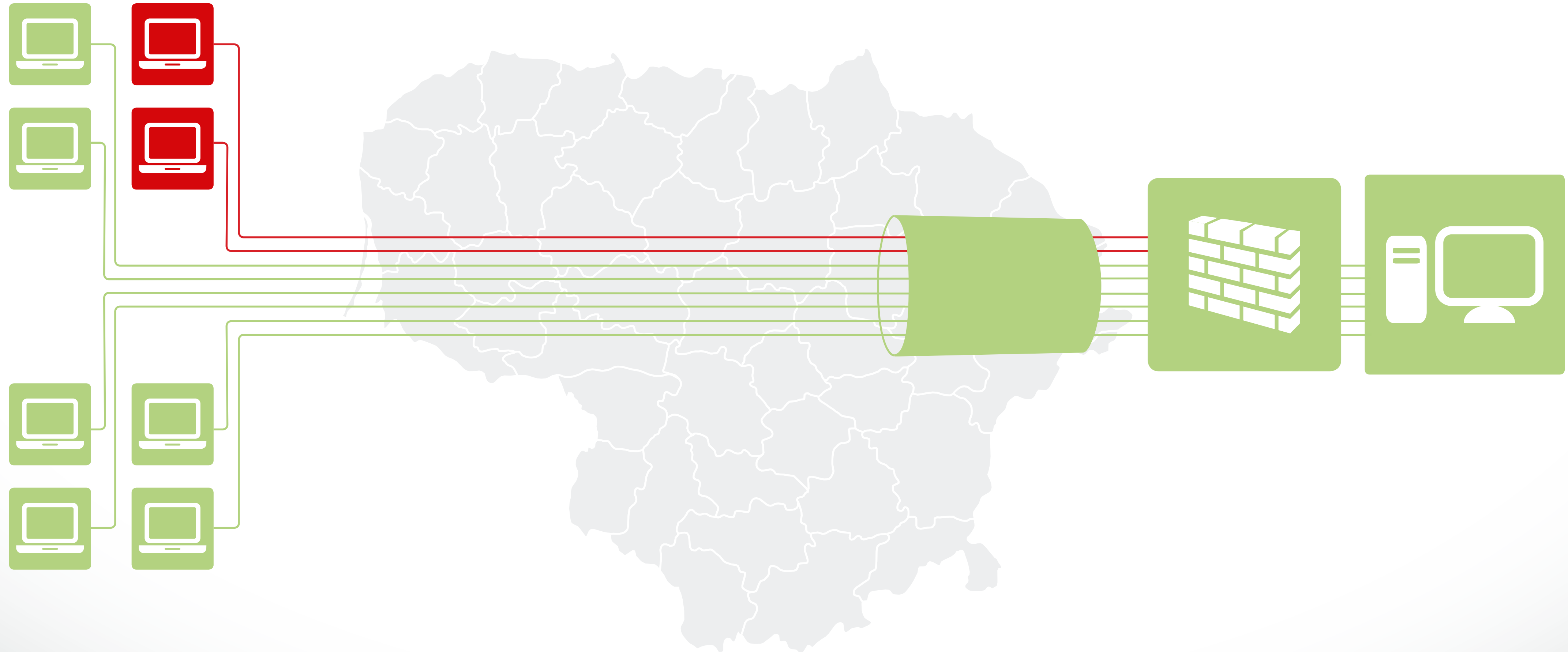
ATAKA, KAI AUKA BE APSAUGOS NUO ATAKOS



ATAKA, KAI AUKA BE APSAUGOS NUO ATAKOS



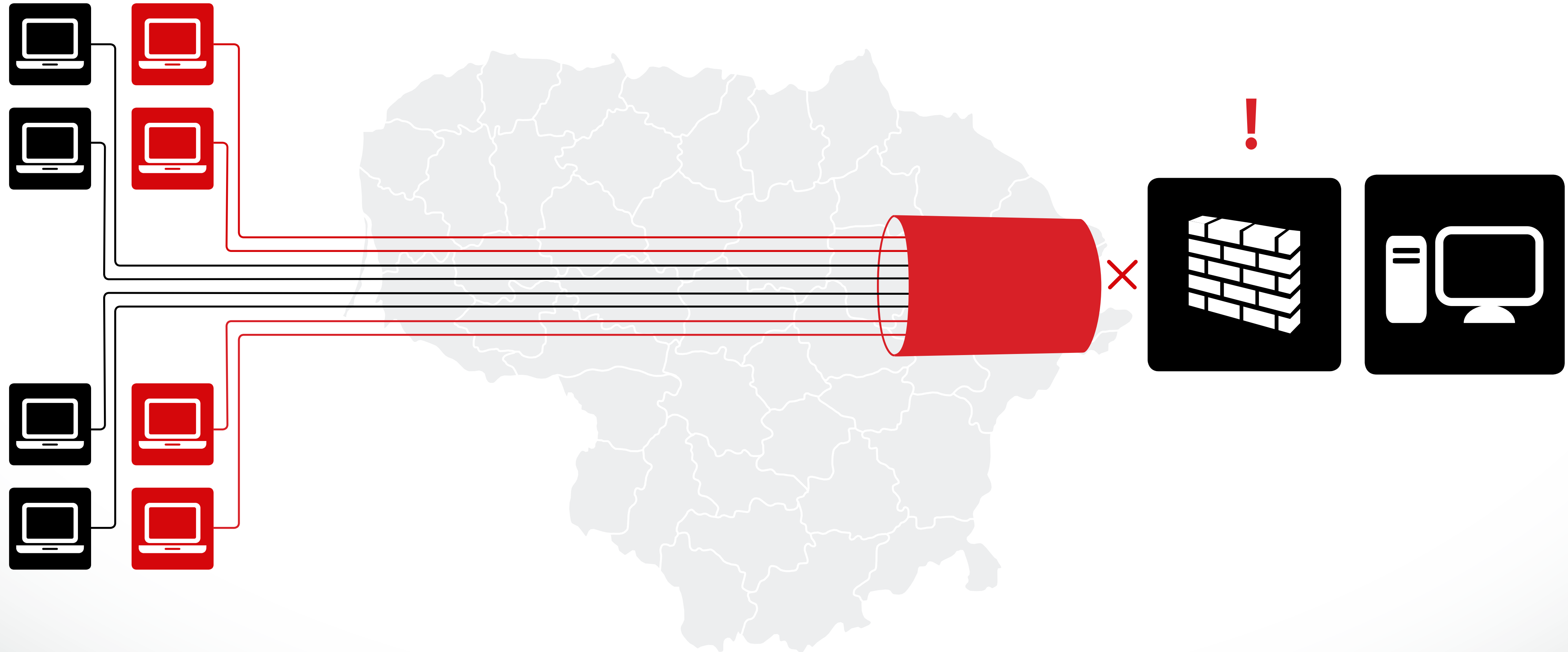
ATAKA, KAI AUKA APSISAUGOJUSI NUO ATAKOS UGNIASIENE



ATAKA, KAI AUKA APSISAUGOJUSI NUO ATAKOS UGNIASIENE



ATAKA, KAI AUKA APSISAUGOJUSI NUO ATAKOS UGNIASIENE



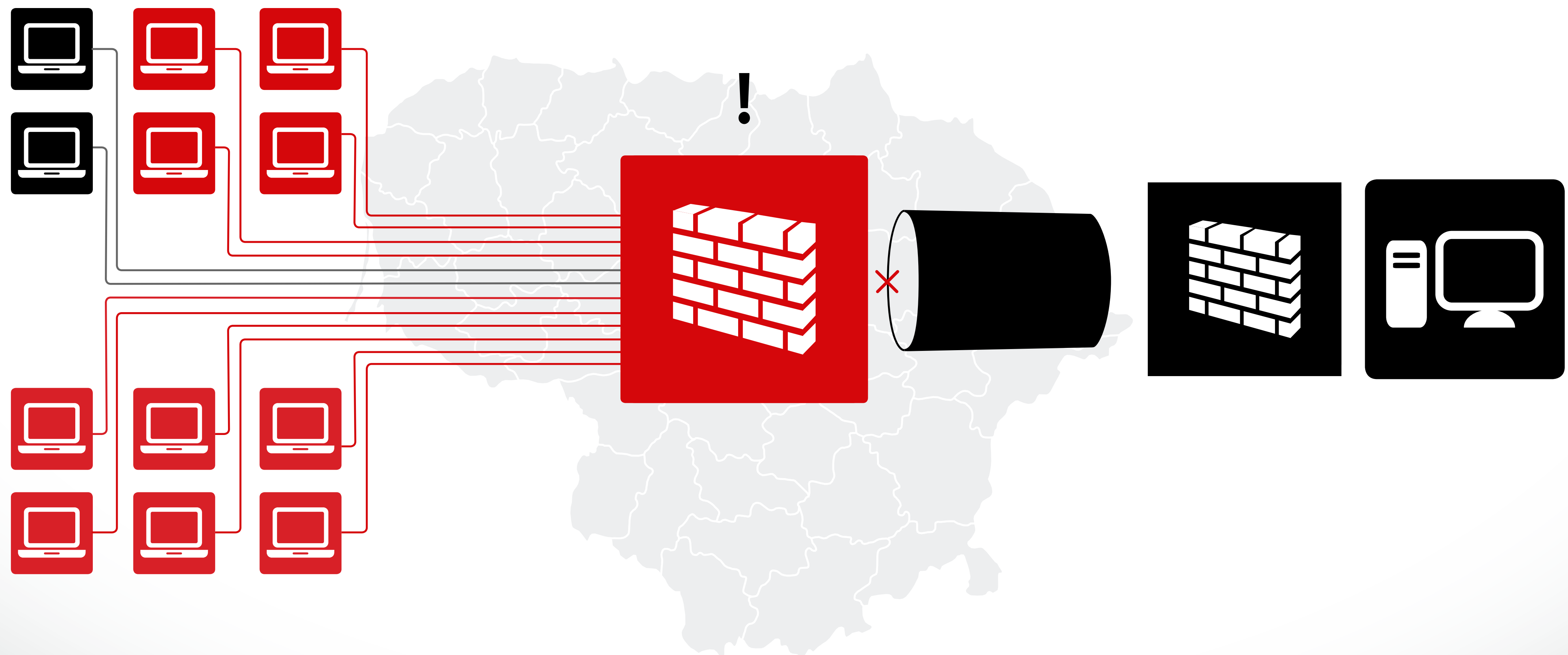
2014-04-30

ATAKA, KAI AUKA APSAUGOTA NUO ATAKOS OPERATORIAUS INFRASTRUKTŪRA



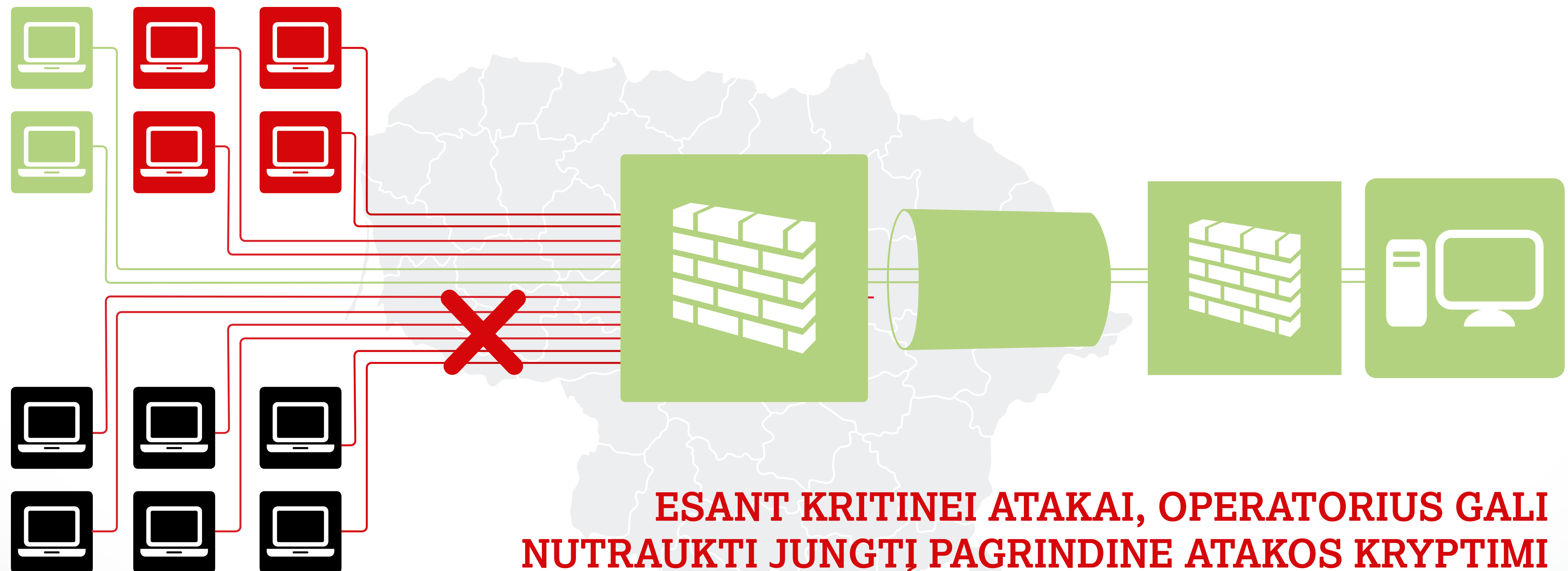
**DIDELIO NAŠUMO UGNIASIENĖ BEI JUNGTYS
OPERATORIAUS TINKLE GALI APSAUGOTI
VARTOTOJĄ NUO DIDELIŲ DDOS ATAKŲ**

LABAI DIDELĖS APIMTIES DDOS ATAKA



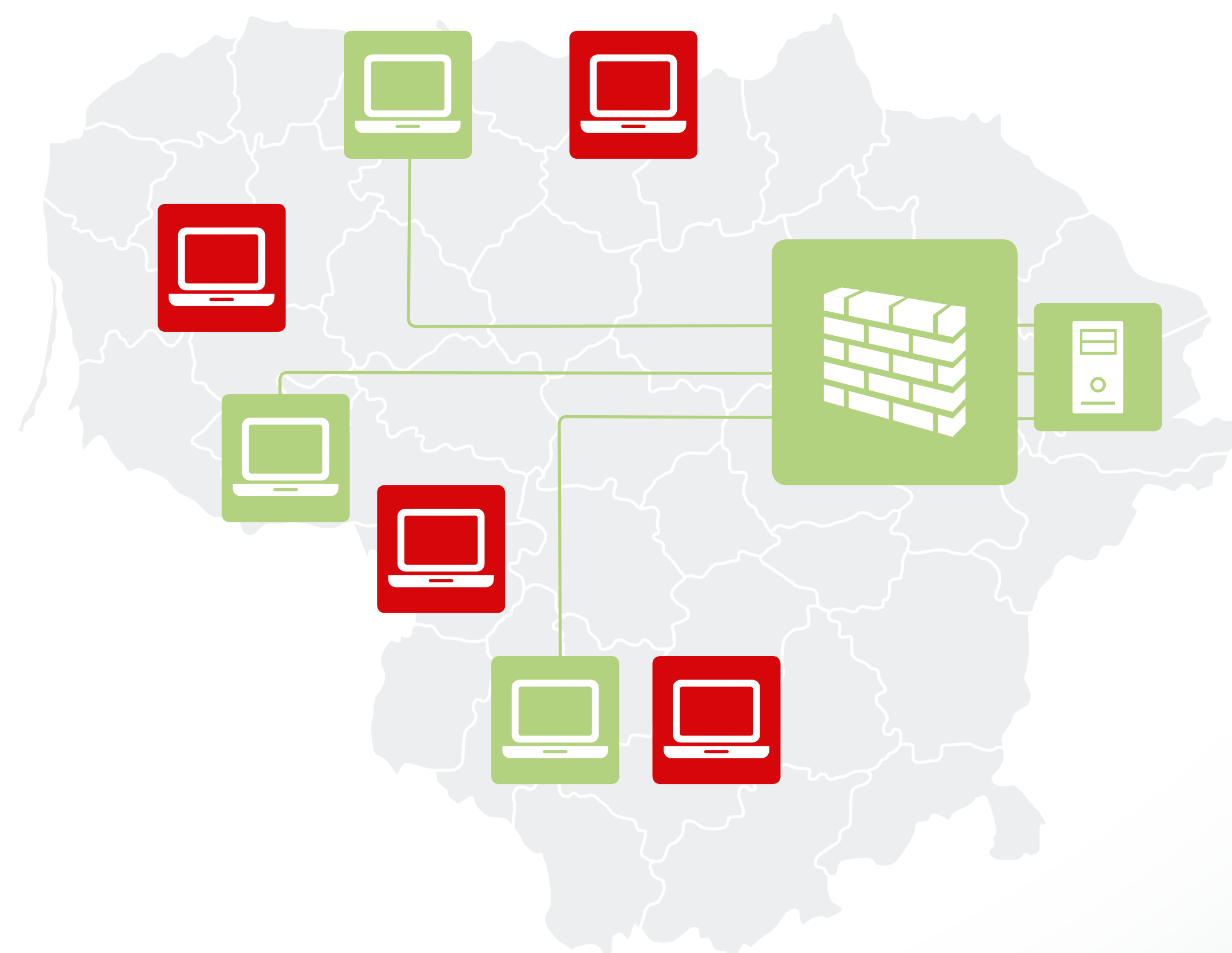
2014-04-30

LABAI DIDELĖS APIMTIES DDOS ATAKA



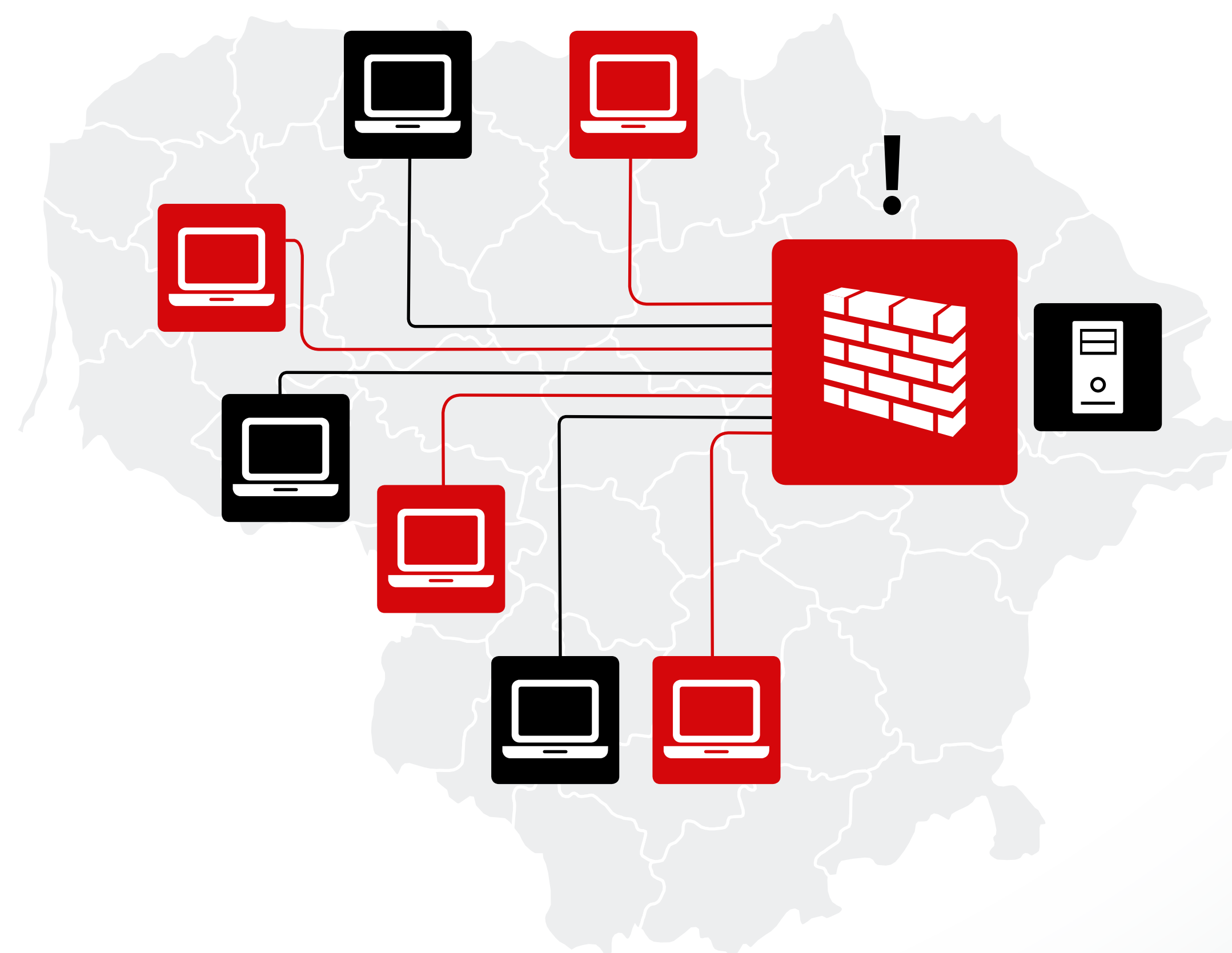
**ESANT KRITINEI ATAKAI, OPERATORIUS GALI
NUTRAUKTI JUNGTĮ PAGRINDINE ATAKOS KRYPTIMI**

DDOS ATAKA IŠ TINKLO VIDAUS

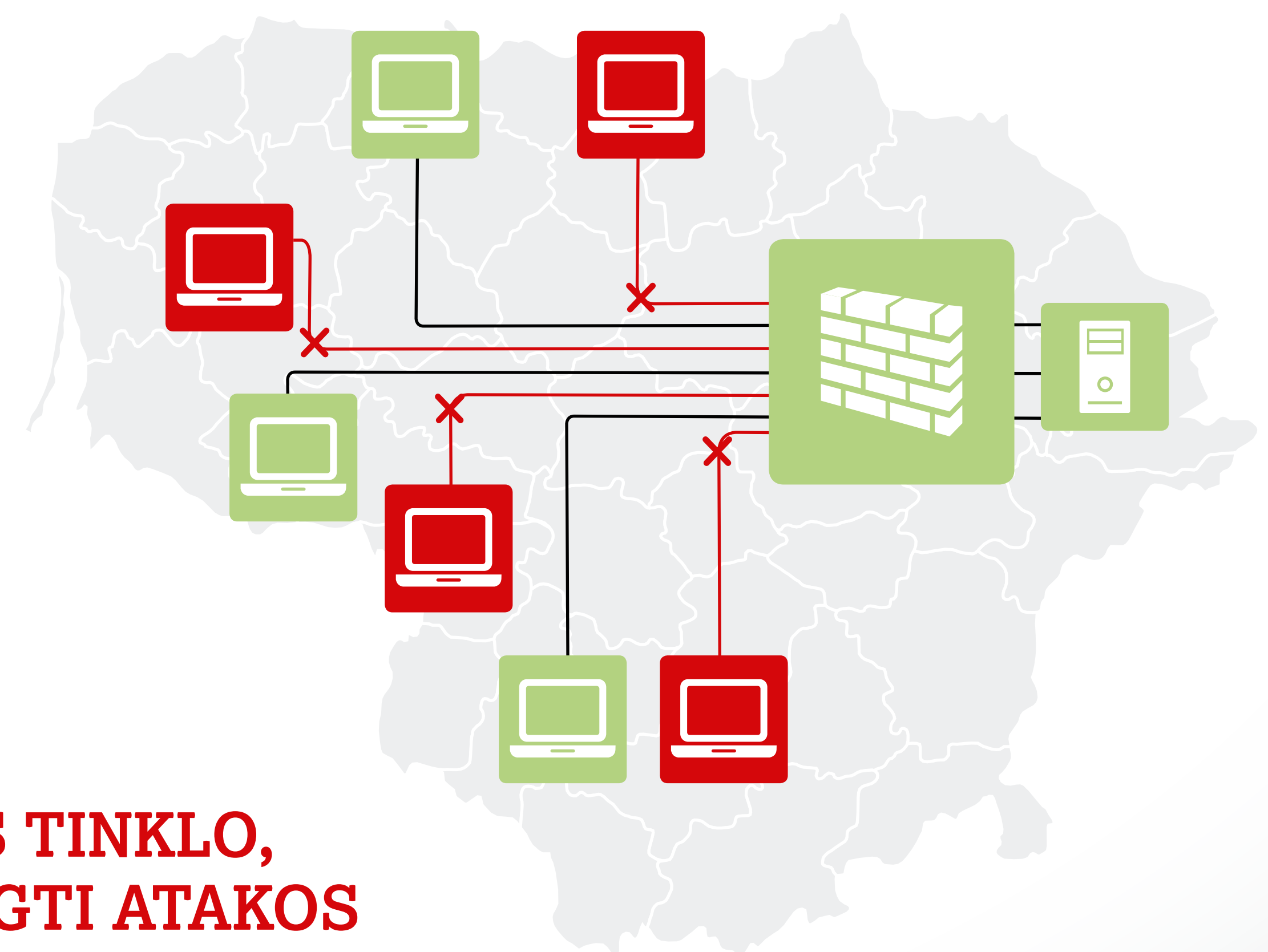


2014-04-30

DDOS ATAKA IŠ TINKLO VIDAUS



DDOS ATAKA IŠ TINKLO VIDAUS



ESANT LABAI DIDELEI DDOS ATAKAI IŠ TINKLO,
OPERATORIUS TURI GALIMYBĘ ATJUNGTI ATAKOS
ŠALTINIUS ATSKIRAI

KAIP SAUGOTIS? ISP – TARPTAUTINĖ INFRASTRUKTŪRA



TARPTAUTINIS INTERNETAS

- 140 Gb/s tarptautinis interneto srautas
- Trys skirtingos kryptys
- Penki nepriklausomi teikėjai
- Diversifikacija – regione skirtingų teikėjų srautai
- Partnerystė su didžiaisiais ES ISP



KAIP SAUGOTIS? ISP – NACIONALINIS LYGIS



TINKLO MAZGŲ STRUKTŪRA

- Geografiškai atskirti pastatai
- Simetriška tinklo struktūra
- Pakankami pajėgumai kiekvienne mazge atskirai

KAIP SAUGOTIS? ISP + VALSTYBĖ - KITOS PRIEMONĖS



- Įsidięti *anti-spoofingą*
- Bendradarbiauti tvarkant atvirus DNS, NTP, SNMP servigus
- Bendradarbiauti mažinant *botnetų* kiekį
- Stebėti ir saugoti tinklą, užkertant kelią didelio masto atakoms ir kitiems pažeidžiamumams



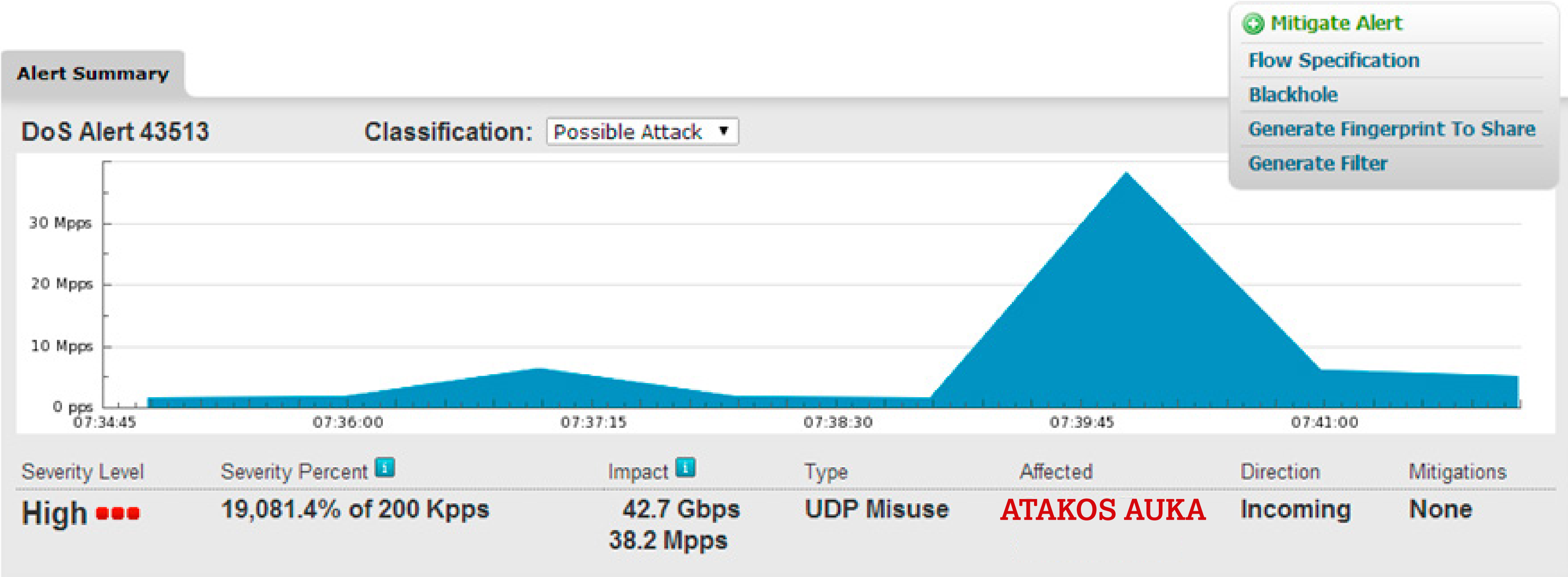
ATAKOS SUVALDYMAS

VIENTELIS REALUS ATAKOS SUVALDYMO BŪDAS, MINIMIZUOJANT ĮTAKĄ VARTOTOJUI, TUOMET, KAI KELIAS ATAKAI UŽKERTAMAS INTERNETO TIEKĖJO TINKLE, T. Y. NEPASIEKIA VARTOTOJO

- Nedidelio masto DDoS atakos suvaldomos aktyvuojant filtrus/ taikant *blackhole route*
- Didelio masto DDoS atakos suvaldomos aktyvuojant *blackhole route* tarptautinio interneto teikėjų tinkle (pvz., „TeliaSonera“)



ATAKOS SUVALDYMAS (2)



KIBERNETINIS SAUGUMAS KLIENTAMS



PRIVATŪS KLIENTAI

Interneto prieigos
apsauga



SMULKUS, VIDUTINIS VERSLAS

Triguba apsauga



STAMBUS VERSLAS

Triguba apsauga



Apsaugos
sprendimai
kliento tinkle



TARPTAUTINIS VERSLAS, DUOMENŲ CENTRAI, SPEC. PROJEKTAI

Individualūs
apsaugos sprendimai



Operatoriaus
lygio centralizuoti
sprendimai



TINKLAS

Operatoriaus
apsaugos specifiniai
sprendimai



2014-04-30

KIBERNETINIS SAUGUMAS IR KRAŠTO APSAUGA



Operatorius gali apsaugoti

- Kuo didesnis ir svarbesnis operatorius, tuo daugiau vidinės šalies komunikacijos ir informacijos sklaidos išsaugoma

KODĖL operatorius?

- Diversifikuota, galinga infrastruktūra
- Apsaugomi ne tik viešųjų paslaugų teikėjai, bet ir vartotojai
- Galimybės:
 - anksčiau pastebėti ataką
 - panaudoti galingas kolektyvinės apsaugos priemones
 - valdyti tarptinklines ir (ar) lygiavertes (angl. peer) jungtis
 - valdyti savo tinklo vartotojus

GALIMI BLOGIAUSI SCENARIJAI (1)



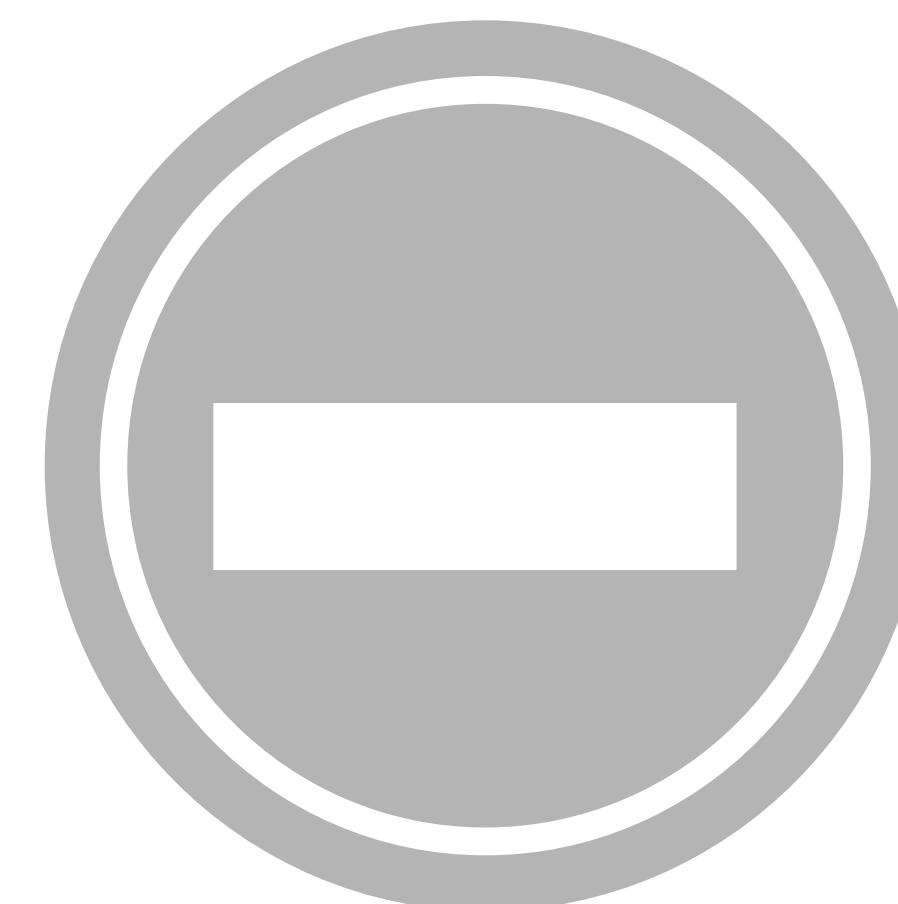
INTERNETO IŠJUNGIMAS

• Neveikia

- Tarptautinė bei tarptinklinė komunikacija, IP telefonija
- „Debesų“ paslaugos, prieiga prie socialinių tinklų
- Visos paslaugos, klientai, kuriems darbui reikalingas internetas bei prieiga prie kitų tinklų
- Dėl to galimi dideli nuostoliai

• Veikia

- Tradicinė telefonija
- Vidinės ISP paslaugos (MPLS VPN, vidinė telefonija, L2 paslaugos)
- Operatoriaus tinkle esančios tarnybos bei internetiniai puslapiai; informacijos sklaida vidiniame tinkle nesustoja
- Vidiniai komunikacijos šaltiniai operatoriaus viduje
- Dalis bankomatų, el. prekyviečių, esančių operatoriaus tinkle



GALIMI BLOGIAUSI SCENARIJAI (2)



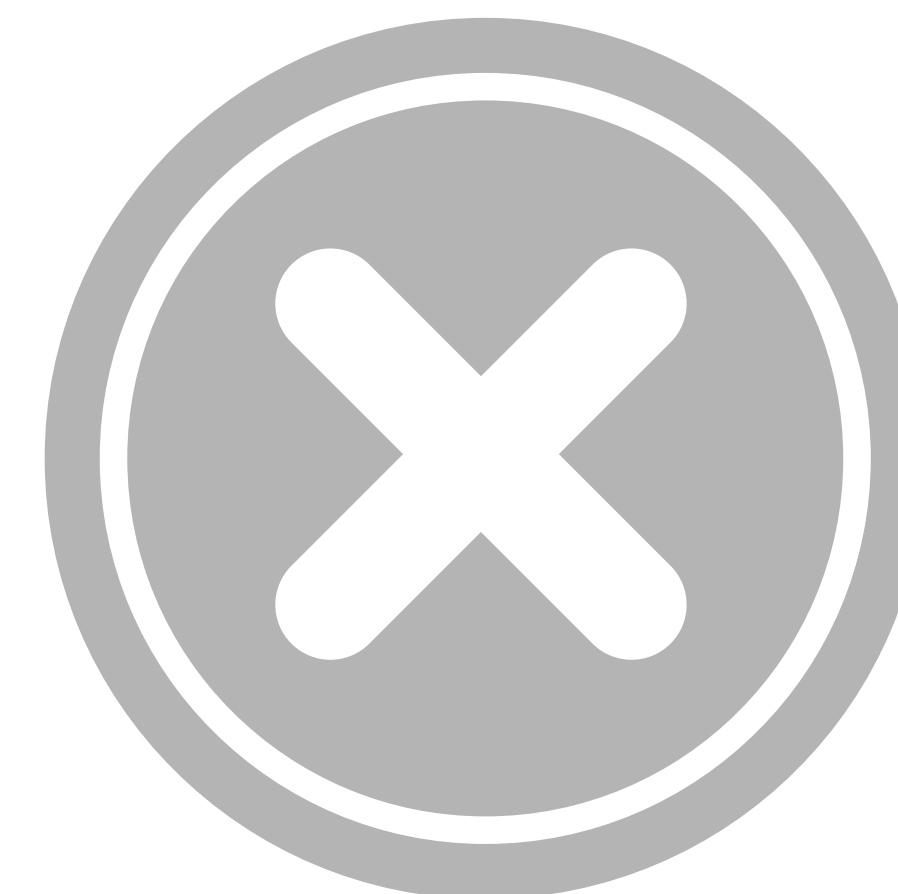
TINKLO IŠJUNGIMAS-UŽGROBIMAS

• Neveikia

- Visa komunikacija (telefonija, internetas, vidinių tinklų sujungimai)
- Visi procesai, tarnybos, informacijos šaltiniai, kurie naudojami operatoriaus paslaugomis
- Operatoriaus tinkle esantys bankai
- Beveik visos operatoriaus paslaugos
- Valstybinės organizacijos operatoriaus tinkle
- Visi mažesni operatoriai, kurie naudojami paslaugomis
- Sustoja informacijos sklaida

• Veikia

- Lokali tradicinė telefonija
- Lokalūs (regioniniai) MPLS tinklai ir paslaugos



KIBERNETINIS SAUGUMAS IR KRAŠTO APSAUGA (2)



Ko trūksta krašto apsaugai?

- Paslaugų ir infrastruktūros apsaugai reikalingos techninės priemonės
 - Neutralizuoti infekuotą srautą - didelio pajėgumo ugniasienės arba UTM



KIBERNETINIS SAUGUMAS IR KRAŠTO APSAUGA (3)



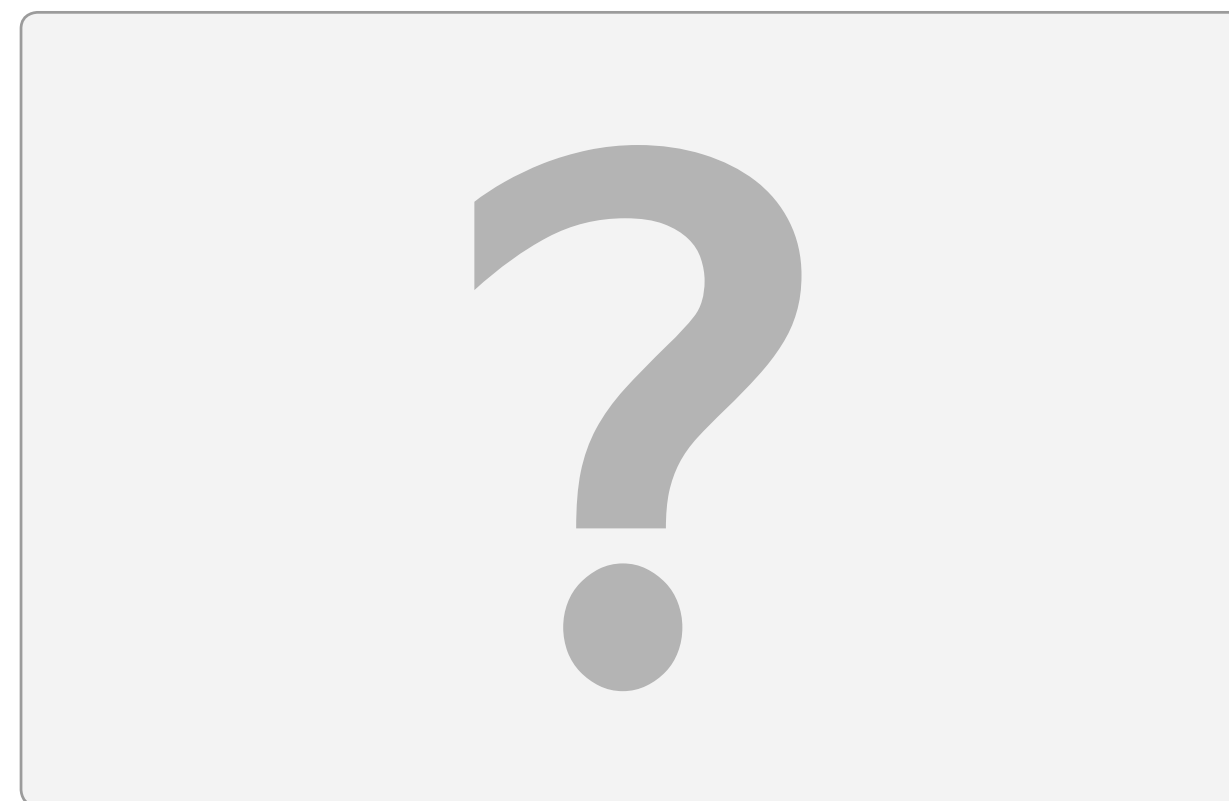
„Kas valdo informaciją – tas valdo pasaulį“
(Napoleono bendražygis)



1917 m.



1991 m.



?

DĒKUI UŽ JŪSŪ DĒMESĪ!



GAL TURITE KLAUSIMŲ?