BOTNET AGENTŲ NAUDOJIMO DDOS ATAKOSE STRATEGIJŲ MODELIAVIMAS

Simona Ramanauskaitė, Jonas Juknius
Šiaulių universitetas, Vilniaus Gedimino technikos universitetas

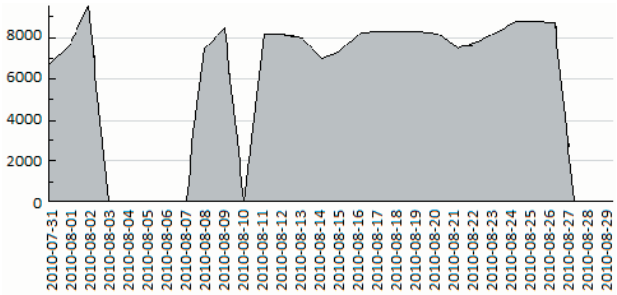
Įvadas

Nuolat didėjantis paslaugų kiekis internete sulaukia ir papildomų grėsmių, kurios gali turėti įtakos ne tik pačiai internetinei paslaugai, bet ir kitoms su ja susijusioms įmonės sritims. Viena iš didžiausių internetinių grėsmių – virusinių programų sukurti *Botnet* tinklai, kurie labiausiai baugina savo dydžiu ir potencialia galia.

Šio darbo ***tikslas*** – ištirti skirtingų *Botnet* agentų kiekio kaitos DDoS atakos metu strategijų įtaką atakos sėkmei. Siekiant užsibrėžto tikslo, keliami šie ***uždaviniai***: susipažinti su *Botnet* ir DDoS atakomis bei egzistuojančiais jų matematiniais / programiniais modeliais; sudaryti DDoS atakų sėkmės vertinimo modelį, kuriame įvertinamos tiek aukos, tiek ir *Botnet* savybės; naudojantis sukurtu modeliu, atlikti skirtingų *Botnet* papildymo naujais agentais strategijų palyginimą DDoS atakos sėkmei.

Botnet

Viena iš didžiausių grėsmių šiuolaikiniame internete yra nuotoliniu būdu valdomi kompiuteriai, sujungti į virusinį *Botnet* tinklą [2]. *Botnet* pagrįstai laikomi didžiausiais šiuolaikinės elektroninės erdvės grėsmės šaltiniais. Vien Lietuvoje kasdien aptinkama iki kelių tūkstančių unikalių kompiuterių, dalyvaujančių *Botnet* veikloje.



1 pav. *Botnet* priklausančių unikalių kompiuterių skaičiaus kaita Lietuvoje [1]

Apkrėstų kompiuterių gausa leidžia padidinti nusikalstamos veiklos mastus ir vykdomų atakų efektyvumą. *Botnet* sudaromi susiejant kiek galima daugiau kompiuterių, apkrėstų piktavališku kodu, leidžiančiu nuotoliniu būdu juos kontroliuoti. Tokiems tinklams sudaryti gali būti naudojami visi kenksmingo kodo platinimo būdai, o pats programinis kodas dažniausiai turi įprastinių kompiuterinių virusų, „kirminų“ ir „Trojos arklių“ požymių [2].

Dauguma Botnet valdomi per vieną ar kelias centrines nusikaltėliams priklausančias (dažniausiai prieš tai užgrobtas) tarnybines stotis [3]. Iki šiol ryšiui tarp pažeistų kompiuterių ir centrinio serverio palaikyti bei valdymo komandoms perduoti dažniausiai naudojamas IRC (ang. *Internet Relay Chat*) protokolas. Siekiant apsunkinti *Botnet* aptikimą, padidinti jų gyvybingumą, naudojamas sudėtingesnis, decentralizuotas *Botnet* valdymo metodas. Šiam tikslui efektyviai naudojami taškas – taškas (angl. *Peer-to-peer*) protokolai. Kiekvienas decentralizuoto *Botnet* dalyvis gali ne tik pats vykdyti gaunamas valdymo komandas, bet kartu atlikti tarpininko vaidmenį, perduoti komandas kitiems tinklo komponentams. Pašalinus vieną iš tokio tinklo segmentų, tai beveik neturi įtakos likusių efektyviam valdymui [4].

Botneto veikloje dalyvauja trys elementai: botneto šeimininkas, užkrėsti kompiuteriai (botai) ir valdymo kanalas (angl. *Command & Control*, toliau – C2), kuriuo šeimininkas valdo botus. Pirmieji Botnet pasirodė 1999 metais, kai paplito ekrano užsklanda apsimetęs kompiuterinis virusas „PrettyPark“ [5]. Šis *botnet* tinklas buvo valdomas naudojant IRC (angl. Internet Relay Chat) ryšio protokolą, tačiau pats botas buvo ribotų galimybių, primityvus. Ilgai netrukus pasirodė ir sudėtingesni botai, pavyzdžiui, „AgoBot“ bei „SDBot“, tačiau valdymo kanalui iki šiol dažnai naudojamas IRC.

Kenksminga programine įranga užkrėstų kompiuterių gausa ne tik sukuria prielaidas privatiems duomenims prarasti, bet jų visuma tampa gerai valdoma zombių armija piktavalių rankose. Dažnas tokios armijos panaudojimas – vykdant paskirstytas paslaugos trikdymo (*angl. DDoS*) atakas. Tai tokios atakos, kurių metu atakuojantysis siekia tam tikrą internetinę paslaugą padaryti neprieinamą jos teisėtiems vartotojams, o tai dažniausiai daroma sistemą vienaip ar kitaip apkraunant itin dideliu parodijuotų, netikrų paslaugos užklausų kiekiu.

Prieš pasirinktus taikinius suvienijus didelius kiekius valdomų kompiuterių, DDoS atakos gali tapti sunkiai įveikiamos ne tik pavienėms tarnybinėms stotims, bet ir ištisoms valstybės struktūroms. Neseniai įvykusios Estijos ir Gruzijos apgultys, pasitelkiant DDoS, pademonstravo galimybes piktavališkas programas paversti ginklais ir politiniais įrankiais.

Botnet ir DDoS modeliai

Norint tinkamai pasirengti potencialioms DDoS atakoms padeda galimų situacijų ir jų skirtingų savybių analizė. Dėl galimos plačios Botnet geografinės aprėpties, didelio atskirų komponentų (agentų) skaičiaus ir kitų su tuo susijusių savybių realūs eksperimentai su *Botnet* ir DDoS atakomis gali būti pernelyg sudėtingi. Tad skirtingoms situacijoms analizuoti neretai pasitelkiami matematiniai / programiniai modeliai:

S. B. Banks ir M. R. Stytz [6] *Botnet* situacijai atskleisti siūlo taikyti bendrąjį ligų plitimo modelį, kuris atitiktų *Botnet* agentų užkrėtimo eigą ir leistų atskleisti „ligos“ populiacijos kaitos tendencijas. Kiti autoriai [4, 8, 9] pateikia išplėstus modelius, kurie atsižvelgia į specifinius kriterijus, turinčius įtakos *Botnet* dydžiui, pavyzdžiui, į valdymo struktūrą, laiko zonų įtaką ir pan. Kadangi agentų valdymo būdai gali labai skirtis tarpusavyje, tad „Modeling Peer-to-Peer Botnets“ ir „Inference and Analysis of Formal Models of Botnet Command and Control Protocols“ darbuose [10, 8] aprašomi konkrečiu protokolu valdomų ir bendraujančių agentų modeliai, skirti taip pat *Botnet* priklausančių agentų skaičiaus dinamikai prognozuoti. Nors didžioji dalis *Botnet* modelių skirta jo dydžio kaitai analizuoti, tačiau atitinkami modeliai gali būti taikomi ir jų nuomojimo bei nuomojimosi pelningumo analizei [12], o V. Segura ir J. Lahuerta [13] aprašytas modelis leidžia vertinti būtent DDoS atakos pelningumą. DDoS modeliais siekiama įvertinti aukos gebėjimą atsilaikyti tam tikro galingumo atakoms [14, 15] bei aukos naudojamų kontrpriemonių efektyvumą [17, 18].

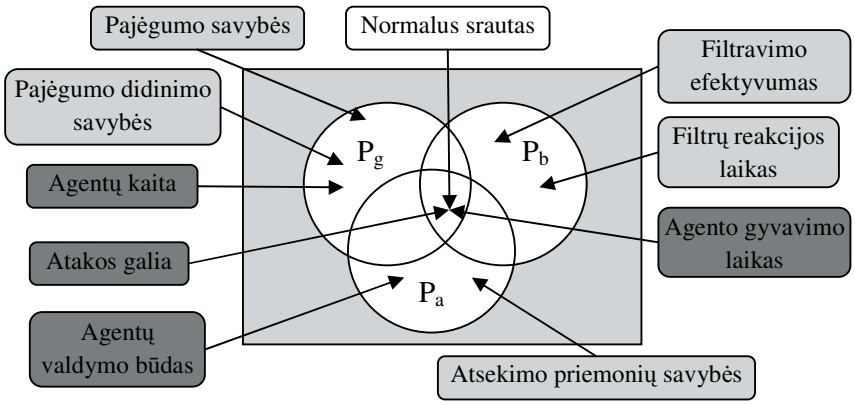
Botnet ir DDoS modeliai dažnai vystomi atskirai vieni nuo kitų, todėl mes siūlome modelį, kuris leistų įvertinti atakos atlaikymo tikimybę, atsižvelgiant į *Botnet* ir aukos savybių rinkinį. Tad šis modelis leistų vertinti, kaip skirtingas atakoje dalyvaujančių kompiuterių (botų) kiekis, jo kitimas gali turėti įtakos visos atakos ar apsaugos nuo jos sėkmei.

Atsparumo srauto išnaudojimo DDoS atakoms modelis

Įvertinant kovos prieš DDoS atakas būdus išskiriamos trys sudedamosios: gebėjimas atlaikyti ataką (prevencija), DDoS efekto mažinimas atakos metu (filtravimas) ir atakos šaltinio atsekimas bei veiksmų prieš jį ėmimasis (postvencija) [16]. Kova prieš DDoS ataką būtų laikoma sėkminga, jei bent vieno iš šių įvykių tikimybė būtų pakankamai didelė. Žinant gebėjimo atlaikyti ataką tikimybę P_g, atakos srauto sėkmingo filtravimo tikimybę P_b ir atakos šaltinio atsekimo tikimybę P_a galima rasti bendrą apsaugos nuo DDoS atakos tikimybę P (žr. 1 formulę).

$$P = 1 - (\overline{P_g} \cdot \overline{P_b} \cdot \overline{P_a}) \quad (1)$$

Toliau pateiksime modelį, leidžiantį nustatyti aukos gebėjimą atsilaikyti srauto išnaudojimo DDoS atakoms. Kokios Botnet ir aukos savybės yra įtraukiamos į šį modelį ir kaip jos susijusios su gebėjimu atlaikyti ataką, sėkmingai ją sumažinti ir atsekti atakos šaltinį, tikimybėmis pavaizduota 1 pav. (šviesiai pilkame fone pavaizduotos savybės gali būti keičiamos pačios aukos, tamsiai pilkame fone – atakuojančiojo, o baltame – tinklo aktyvumo įtaka).



2 pav. DDoS atakos atlaikymo sudedamųjų tikimybių sąveika ir jai įtakos turinčios savybės

Kiekvieną šių savybių būtų galima nusakyti ir apibūdinti taip:

- *Normalus srautas* – teisėtų sistemos vartotojų sudaromas duomenų srautas, kuris išreiškiamas kaip vidutinis teisėtų vartotojų siunčiamas duomenų kiekis per laiko vienetą (T_n, *b / s*).
- *Filtravimo efektyvumas* – kokia dalis iš viso aukai skirto srauto, kuris iki jos ateina taikant įvairias kontrpriemones, tinkle yra teisėtas srautas. Jis nusakomas dviem savybėmis: neteisėtų užklausų nufiltravimo procentas (p_{asb}, *%*) ir teisėto srauto blokavimo procentas (p_{tsb}, *%)*.

- *Filtrų reakcijos laikas* – laikas, kurio reikia sureaguoti į naujai pasirodžiusį srautą ir perderinti filtrų nustatymus, matuojamas sekundėmis (t_r, *s*).
- *Agento gyvavimo laikas* – vidutinis laikas, kiek vienas agentas yra aktyvus ir dalyvauja atakoje. Po šio laiko jis tiesiog pasišalina iš dalyvavimo atakoje. Dydis matuojamas sekundėmis (t_{ag}, *s*).
- *Atsekimo priemonių savybės* – tai savybės, kurios turi įtakos gebėjimui pasiekti teorinį tokio tipo atakų šaltinio atsekimą ir tolesnius veiksmus su juo. Jos išreiškiamos kaip laiko sąnaudos, reikalingos tam darbui atlikti (t_a, *s*).
- *Agentų valdymo būdas* – tai, kokiu būdu yra surenkama ir valdoma agentų armija (Botnet), lemia, kiek sudėtingas bus atakos šaltinio atsekimas. Valdymo būdas išreiškiamas kaip teorinė atakos šaltinio atsekimo galimybė (p_{ta}, *%*).
- *Atakos galia* – turimas Botnet ir jo savybės nulemia, kokia galia bus atakuojama auka. Ji išreiškiama per tris pagrindinius parametrus: atakos pradžioje turimas agentų skaičius (n_{pr}, *vnt*), atakoje dalyvaujančių agentų skaičių (*n, vnt*) ir vieno agento vidutinis išsiunčiamas srautas (λ_a, *b/s*);
  - Laikui bėgant agentų skaičius tinka, o jį galima išreikšti (2) formule

$$n(t) = \begin{cases} n_{pr}, kai\ t = 0 \\ n(t-1) + t_p(t), kai\ t < t_l\ \ ir\ \ t < t_{ag} \\ n(t-1) + t_p(t) - t_p(t - t_{ag}), kai\ t < t_l\ \ ir\ \ t > t_{ag} \\ n(t-1) - t_p(t - t_{ag}), kai\ t \geq t_l\ \ ir\ \ t > t_{ag} \\ n(t-1), kai\ t \geq t_l\ \ ir\ \ t < t_{ag} \end{cases}$$

  - Bendras laiko momentu t atakos srautas paskaičiuojamas pagal (3) formulę.

$$T_a(t) = n(t) \cdot \lambda_a; \quad (3)$$

- *Agentų kaita* – palaikyti ataką pastovią ar vis didinti jos galingumą į ataką gali būti vis įtraukiama naujų agentų. Ji nusakoma dviem savybėmis: atakos papildymo agentais funkcija laiko atžvilgiu (t_p, *(t)*) ir atakos papildymo naujais agentais trukme (t_l, *s*).
- Pajėgumo didinimo savybės – matydama vykstančios atakos dinamiką, auka gali imtis papildomų pajėgumo didinimo priemonių, kurias šiuo atveju išreiškiame kaip galimų naudoti kanalų skaičiaus (*m, vnt*) ir kanalo išnaudojimo ribą, kai turi būti pridedamas vienas papildomas kanalas (p_p, *%*);
  - Kanalo išnaudojimo procentą ρ rasime naudodamiesi (4) formule.

$$\rho(t) = \begin{cases} \frac{T_a(t-1)+T_n}{T_g(t-1)}, kai\ t < t_r \\ \frac{T_a(t-t_r)\cdot(1-p_{asb})+\frac{t_r}{t_p}+T_n\cdot(1-p_{tsb})}{T_g(t-1)}, kai\ t \geq t_r \end{cases} \quad (4)$$

- *Aukos pajėgumo savybės* – numatoma auka turi tam tikras savybes, kurios lemia, kiek pajėgi ji atlaikyti tam tikro dydžio DDoS ataką. Šio tipo atakose pagrindinės aukos pajėgumo savybės yra pradinis kanalo pralaidumas (T_{gpr}, *b / s*) ir dabartinis kanalo pralaidumas (T_g, *b / s*);
  - Tam tikru atakos metu t kanalo pralaidumas gali būti nustatomas pagal (5) formulę.

$$T_g(t) = \begin{cases} T_{gpr}, t = 0 \\ T_g(t-1), \rho(t-1) < p_p\ arba\ \frac{T_g(t-1)}{T_{gpr}} \geq m \\ T_g(t-1) + T_{gpr}, \rho(t-1) \geq p_p\ \ ir\ \ \frac{T_g(t-1)}{T_{gpr}} < m \end{cases} \quad (5)$$

Remiantis aukščiau išskirtomis tokio tipo atakų savybėmis ir pritaikant [17] aprašytą sėkmės tikimybės radimo formulę, srauto išnaudojimo DDoS atakoms tikimybę, galima aprašyti aukos gebėjimo atsilaikyti prieš tam tikro galingumo srauto išnaudojimo DDoS ataką tikimybę P_g:

$$P_g(t) = 1 - \frac{\frac{\rho(t)^i}{i!}}{\sum_{j=0}^{i}\frac{\rho(t)^j}{j!}}; \quad (6)$$

Čia *i* yra šiuo metu naudojamų kanalų skaičius (gali būti randamas kaip $T_g(t)$ ir T_{gpr} santykis). Remiantis [18] galima nusakyti atakos blokavimo tikimybę P_b, kuri turėtų būti lygi iki aukos ateinančio teisėto srauto ir viso, turėjusio pasiekti aukos sistemą, santykiui:

$$P_b(t) = \begin{cases} \frac{T_n}{T_a(t)+T_n}, & t < t_r \\ \frac{T_n\cdot(1-p_{tsb})}{T_a(t-t_r)\cdot(1-p_{asb})+\frac{t_{tr}}{t_p}+T_n}, & t \geq t_r\ \ ir\ t < t_p + t_{tr} \\ \frac{T_n\cdot(1-p_{tsb})}{T_a(t-t_r)\cdot(1-p_{asb})+T_n}, & t \geq t_r\ \ ir\ t \geq t_p + t_{tr} \end{cases} \quad (7)$$

Atakos rengėjo atsekimo tikimybę P_a po kurio laiko reikėtų vertinti kaip teorinės atakos rengėjo atsekimo tikimybės, aukos įvykdyto tam reikiamo laiko dalies ir atsekimui reikiamo analizuoti atakos srauto santykio su visu atakos srautu sandaugą (žr. (8) formulę).

$$P_a(t) = \begin{cases} p_{ta}\cdot\frac{t}{t_a}\cdot\frac{\sum n(t)\cdot\lambda_a}{\sum n(t)\cdot\lambda_a + t\cdot T_n}, kai\ t < t_a \\ p_{ta}\cdot\frac{\sum n(t)\cdot\lambda_a}{\sum n(t)\cdot\lambda_a + t\cdot T_n}, kai\ t \geq t_a \end{cases} \quad (8)$$

Agentų kaitos įtaka atakos atlaikymo tikimybei

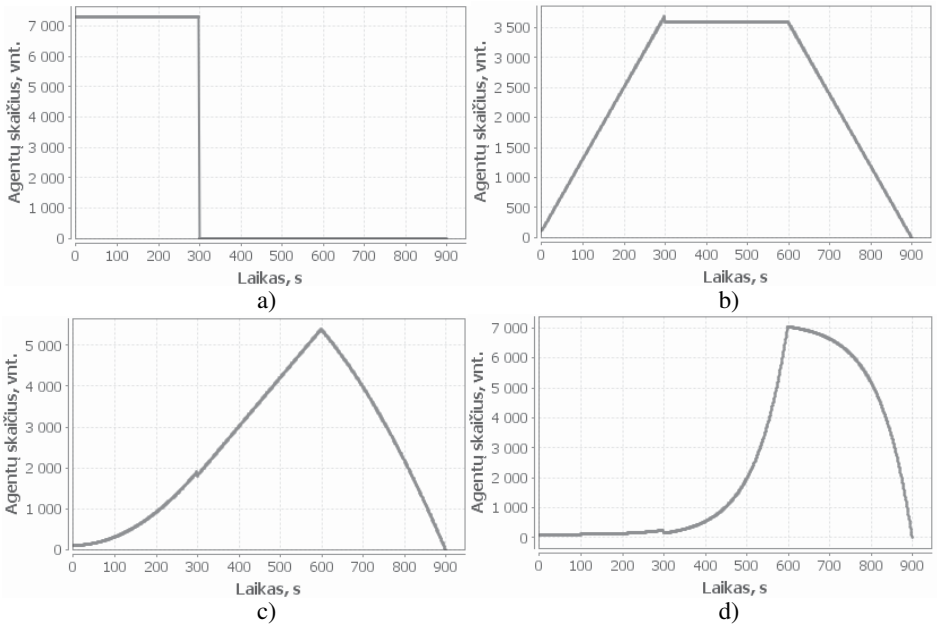
Pasinaudojant aprašytu modeliu buvo atlikti bandymai su skirtingas atakos agentų papildymo funkcijas naudojančiais atakų modeliais. Šių bandymu metu buvo siekiama įvertinti, kiek reikšminga yra atakos galios kaita per tam tikrą laiko tarpą. Bandymams buvo pasirinktas modelis, kuriame auka naudoja 5 MB / s kanalo pralaidumą su galimybe pa-

didinti kanalų skaičių iki 2 kanalo pralaidumui pasiekus 75 proc. išnaudojimą. Auka naudoja tokius filtrų nustatymus, kad vidutiniškai 2 proc. iš 1 MB / s teisėto srauto ir 30 proc. neteisėto srauto yra blokuojama filtravimo sistemos, kurios reakcijos laikas yra 2 s. Pačiai atakai yra naudojamas toks agentų valdymo būdas, kuris leidžia atsekti atakos šaltinį (tikimybė 30 proc.), bet tam aukai reikia vienos valandos.

Kai nenaudojama jokia agentų papildymo strategija, pradinis agentų skaičius parinktas 7288, o visais kitais atvejais jis lygus 100 agentų. Atakos agentai geba siųsti vidutiniškai 25 KB / s srautą numatytajai aukai, o vidutinis agento gyvavimo laikas yra 5 minutės. 10 minučių ataka yra papildoma naujais agentais, naudojant šias agentų kaitos funkcijas, kurios parinktos taip, kad atspindėtų vienodą agentų papildymo kiekį visos atakos metu:

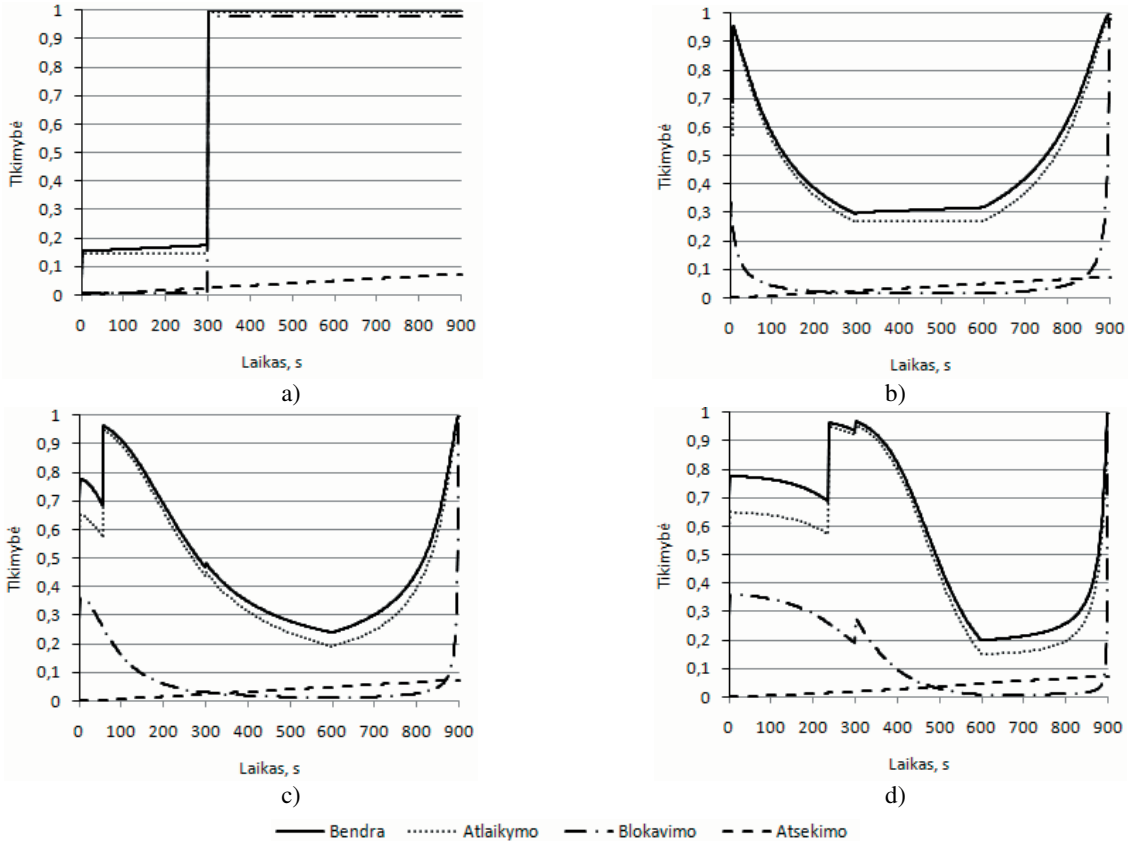
- Pastovus agentų skaičiaus papildymas – $t_p(t) = 12$.
- Tiesiškai didėjantis agentų skaičiaus papildymas – $t_p(t) = 0.04 \cdot t$.
- Eksponentiškai didėjantis agentų skaičiaus papildymas – $t_p(t) = 1.013013^t/25$.

Šios keturios skirtingos atakos galios kaitos strategijos turi įtakos bendro atakos srauto dinamikai: momentinis visų agentų panaudojimas vienu metu leidžia pasiekti itin didelį efektą, tačiau tik tiek, kokia yra agentų gyvavimo trukmė. Tuo pačiu agentų skaičiumi papildoma ataka pasižymi galios pastovumu laikui bėgant, nes, pasiekusi vidutinį agentų gyvavimo laiką, geba likti pastovi iki pat atakos pabaigos. Tiesiškai ir eksponentiškai didinančios agentų papildymo strategijos leidžia atakos pabaigoje pasiekti didžiausią jos galią, o skiriasi tuo, kad, tiesiškai didinant agentų skaičių ir sustojus ataką papildyti naujais agentais, jos galia lygiai taip pat tiesiškai mažėja, o eksponentinio agentų skaičiaus didinimo atveju atakos galia ilgiau išlieka pakilusi.



3 pav. Atakoje dalyvaujančių agentų kaitą per tam tikrą laiką nenaudojant agentų papildymo (a), naudojant pastovų (b), tiesiškai (c) ir eksponentiškai (d) didėjantį agentų skaičiaus papildymą

Jei vertintume šių atakos papildymo agentais strategijų efektyvumą per 15 min. nuo atakos pradžios (iki kol visiškai nebejuntamas DDoS efektas iš atakuojančiojo pusės), galima pastebėti, kad atakuojančiajam šiuo laikotarpiu naudingiausios strategijos gali būti išdėstytos tokia tvarka: pastovus agentų papildymas (vidutinė 54 proc. sėkmė); tolygiai didėjantis papildomų agentų skaičius (vidutinė 50 proc. sėkmė); eksponentiškai didėjantis papildomų agentų skaičius (vidutinė 43 proc. sėkmė); nekintantis agentų skaičius (vidutinė 28 proc. sėkmė).



4 pav. Atakos sėkmės tikimybės kaita per tam tikrą laiką nenaudojant agentų papildymo (a), naudojant pastovų (b), tiesiškai (c) ir eksponentiškai (d) didėjantį agentų skaičiaus papildymą

Apibendrinant tyrimo rezultatus būtų galima teigti, kad vis didėjantis agentų papildymo skaičius yra naudingas norint palaipsniui pasiekti momentinę ir neilgai trunkančią atakos galią. Tuo tarpu staigiai atakai surengti geriausia naudoti iš karto visus galimus valdyti agentus, o tokios strategijos efektyvumas dar labiau išauga didinant vidutinį agentų gyvavimo laiką. Auką labiausiai alina tos atakos, kurios naudoja pastovų agentų papildymo kiekį, nes jos savo vienoda galia gali tęstis itin ilgą laiką.

Išvados

Botnet plitimas ir valdymas nėra ribojami viena technologija ar būdu, tad jų susidarymo prevencija ar pašalinimas tampa vis sudėtingesnis ir reikalauja sudėtingų ir kombinuotų apsaugos priemonių.

Egzistuoja nemažai *Botnet* ir DDoS matematinių ir programinių modelių, tačiau jie orientuoti į tam tikrų savybių vertinimą, o ne bendrą atakos sėkmės tikimybę.

DDoS atakos atlaikymo sėkmės tikimybei didžiausios įtakos turi gebėjimo atlaikyti ir tinkamai filtruoti netinkamą srautą tikimybės, nes atakos atsekimo tikimybė yra gana maža dėl pernelyg didelio ir plataus geografinio *Botnet* paplitimo.

Modeliavimo metu pastebėta, kad atakos sėkmės tikimybei didelę įtaką turi ne tik atakoje dalyvaujančių agentų skaičius, bet ir jų gyvavimo trukmė, todėl norint išvengti itin ilgai užsitęsiančių DDoS atakų, svarbu vystyti atskirų agentų aptikimo ir eliminavimo priemones.

Negalima išskirti vienos geriausios *Botnet* papildymo naujais agentais strategijos DDoS efektui sukelti, nes jos pasirinkimas priklauso nuo pageidaujamos veikimo trukmės ir galios tam tikru atakos metu.

Literatūra

1. *CERT-LT. Botnet tinklų situacija Lietuvoej*. Prieiga internete: http://botnet.esaugumas.lt/.
2. Juknius J., Goranin N., 2010, Botnet Spreading Detection And Prevention Via Websites, *Journal of Young Scientists* No. 1(26).
3. Juknius J., Čenys A. Intelligent botnet attacks in modern Information warfare. *15th International Conference on Information and Software Technologies*.
4. Schoof, R; Koning, R. *Detecting peer-to-peer botnets*. Prieiga internete:http://staff.science.uva.nl/~delaat/sne-2006-2007/p17/report.pdf.
5. TrendMicro white paper. *Taxonomy of botnet threaths*. Priega internete:http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/botnettaxonomywhitepapernovember2006.pdf.

6. Banks S. B., Stytz M. R. *Challanges Of Modeling BotNets For Militaty And Security Simulations*. Prieiga internete: http://www.siaa.asn.au/get/2451313990.pdf.
7. Dagon D., Gu G., Lee C. P., Lee W. *A Taxonomy of Botnet Structures*. Prieiga internete: http://faculty.cs.tamu.edu/guofei/paper/Dagon_acsac07_botax.pdf.
8. Dagon D., Zou C., Lee W. *Modeling Botnet Propagation Using Time Zones*. Prieiga internete: http://www.isoc.org/isoc/conferences/ndss/06/proceedings/papers/modeling_botnet_propagation.pdf.
9. Weaver R. *A Probabilistic Population Study of the Conficker-C Botnet.* Prieiga internete: http://www.cert.org/netsa/publications/weaver-conficker.pdf.
10. Ruitenbeek E., Sanders W. *Modeling Peer-to-Peer Botnets*. Prieiga internete: http://www.perform.csl.illinois.edu/Papers/USAN_papers/08VAN02.pdf.
11. Cho C. Y., Babic D., Shin E. C. R. Song, D. *Inference and Analysis of Formal Models of Botnet Command and Control Protocols*. Prieiga internete: http://bitblaze.cs.berkeley.edu/papers/botinfer_ccs10.pdf.
12. Li Z., Liao Q., Striegel A. *Botnet Economics: Uncertainty* Matters. Prieiga internete: http://weis2008.econinfosec.org/papers/Liao.pdf.
13. Segura V., Lahuerta J. *Modeling the economic incentives of DDoS attacks: femtocell case study*. Prieiga internete: http://weis09.infosecon.net/files/113/paper113.pdf.
14. Boteanu D., Fernandez, J. M., Hugh J. Mc, Mullins J. *Queue Management as a DoS counter-measure?* Prieiga internete: http://www.professeurs.polymtl.ca/jose.fernandez/QueueManagementDoS.pdf.
15. Wang, Y., Lin C., Li Q., Fang Y. *A queueing anglysis for the denial of service (DoS) attacks in computer networks*. Prieiga internete: http://www.fang.ece.ufl.edu/mypaper/comnet07wang.pdf.
16. Mirkovivic J., Dietrich S., Dittrich D., Reiher P., 2004*, Internet Denial of Service: Attack and Defense Mechanisms*.
17. Ramanauskaitė S., Čenys A., 2009, DoS atakų modeliavimas stochastiniais metodais, *Jaunųjų mokslininkų darbai* Nr. 3 (24). Šiauliai.
18. Ramanauskaitė S., Čenys A., 2010, *Stochastinis TCP SYN atakų modelis. Lietuvos XIII-oji jaunųjų mokslininkų konferencija „Mokslas – Lietuvos ateitis“, Informatika, Informacinių technologijų saugumas*. 2010-04-16, Vilnius.

MODELLING OF *BOTNET* AGENT USAGE STRATEGIES IN DDOS ATTACKS

Simona Ramanauskaitė, Jonas Juknius

Summary

The increasing amount of service-oriented web solutions on the internet leads to increase in Botnet usage. It provides the opportunity to carry out powerful attacks even without having a huge amount of own computers. The most popular attack that can be performed using Botnets is the DDoS attack, when Botnet agents try to exhaust all resources of a victim and make its services inaccessible to the legitimate users. This kind of cyber attacks becomes more and more of a threat but real experiments for finding out the influence of different attackers and victims' properties on success of attacks are difficult for a couple of reasons. Therefore mathematical-programmable models are used. In this work we present a mathematical DDoS attack resistance model, which allows us to measure influence of Botnet and victims' properties on overall success of resisting DDoS attacks. Using this model we carried out a research for finding out the differences in Botnet agent usage strategies and its efficiency margins.

Keywords: Botnet agent, DDoS attack, security, cyber attacks.

BOTNET AGENTŲ NAUDOJIMO DDOS ATAKOSE STRATEGIJŲ MODELIAVIMAS

Simona Ramanauskaitė, Jonas Juknius

Santrauka

Vis labiau didėjant į internetines paslaugas orientuotų paslaugų tiekėjų populiarumui, priešingoje barikadų pusėje didėja ir *Botnet* paklausa, kuri leidžia realiai neturint savų atakos resursų pasinaudoti internete užkrėstais kompiuteriais ir taip rengti įspūdingo dydžio internetines atakas. Viena pagrindinių *Botnet* rengiamų atakų yra DDoS ataka, kuri aukos teikiamą paslaugą stengiasi padaryti neprieinamą jos teisėtiems vartotojams. Nors tai gana aktuali problema, o realūs prevenciniai bandymai su skirtingais *Botnet* ir aukos savybių nustatymais yra pernelyg sudėtingi, tyrimų apie *Botnet* dydžio kaitos strategijas ar matematinių / programinių modelių tokiems situacijų modeliavimams dar pasigendama. Tad šiame darbe aprašomas matematinis DDoS atakos atlaikymo modelis, kuris leidžia įvertinti *Botnet* ir aukos savybes, turinčias įtakos numatomos atakos atlaikymo sėkmei. Remiantis šiuo modeliu taip pat atliktas tyrimas, kuris nurodo skirtingų *Botnet* agentų skaičiaus kaitos strategijų efektyvumą ir su tuo susijusias jų taikymo sritis.

Įteikta 2010-09-16