Fakulta matematiky, fyziky a informatiky
Univerzita Komenského
Bratislava

DDOS útoky

Informatika a spoločnosť

Martin Višňovec

Peter Cieker

Jakub Husár

18. mája 2012, Bratislava

1 Úvod

Dnešná doba, ktorej pevnou súčasťou sa stáva celosvetová sieť internet so sebou okrem množstva benefitov prináša aj riziká, ktoré je nutné pre bezpečné poskytovanie a fungovanie služieb na internete eliminovať. V poslednej dobe sa totiž internet vďaka čiastočnej anonymite ktorú dokáže poskytovať, stal nástrojom vhodným na realizáciu rôznych protestov, zastrašovaní, vydieraní, ale aj spôsobom, ktorým sa dá viesť konkurenčný boj. Ani naše malé Slovensko nie je v tomto smere nijakou výnimkou a možno mnohí z nás sa už stali svedkami tohto fenoménu aj na vlasnej koži. Aj preto sme sa rozhodli uskutočniť prieskum, ako sú na tom s ochranou poskytovaných služieb orgány našej verejnej správy a či aj oni čelia takýmto pokusom o útok.

2 Cieľ

Cieľom nášho projektu bolo zmapovanie situácie a vytvorenie prehľadu miery zabezpečenia webových domén, na ktorých sídlia úrady verejnej správy, vzhľadom na výskyt nežiaducich útokov typu DDoS (Distributed Denial of Service), ktoré majú za následok obmedzenie dostupnosti poskytovaných služieb.

3 Prehľad

Čo je to DDOS?

DDOS (Distributed Denial of Service) je typ útoku, pri ktorom má útočník za svoj cieľ server, komunikačnú infraštruktúru alebo aplikáciu poskytovanú prostredníctvom internetu. Pri tomto útoku dochádza k zahlteniu a obmedzeniu/odmietnutiu dostupnosti poskytovanej služby pre ostatných užívateľov a môže viesť až k pádu systému. Pri útoku sa využíva veľké množstvo nezávislých počítačov, ktoré útočník ovláda a prostredníctvom ktorých zahlcuje ním vybraný cieľ obrovským kvantom odoslaných požiadaviek. Základnú ochranu proti takýmto útokom predstavujú dobre nastavený router a firewall, pokročilejšou metódou je analýza a filtrovanie samotných paketov.

Známe a najčastejšie využívané typy útokov:

- *HTTP flood* – najjednoduchší útok, ale môže byť zároveň najzákernejší a obrana proti nemu môže byť takmer nemožná. Útočník sa pripája na cielené webové sídlo pomocou reálnych IP adries infikovaných počítačov. Server je zahlcovaný obrovským množstvom požiadaviek, ktoré su pre server aj firewall z hľadiska pripojenia úplne korektné, preto ho nie je možné rozoznať od skutočných požiadaviek. Naviac, ak útočník útočí na web, ktorý v určitých miestach pristupuje k veľkej databáze údajov, môže ho svojími požiadavkami na práve toto miesto vyradiť oveľa rýchlejšie.

- *UDP flood* - útok je založený na zasielaní UDP paketov s falošnou adresou odosielateľa. Keďže UDP je protokol bez nadväzovania spojenia, útočník zasiela UDP pakety na náhodné porty cieľového počítača. Ak počítač prijme UDP paket adresovaný na port, ktorý nevyužíva nijaká aplikácia, zašle odosielateľovi ICMP paket s hlásením o chybe. Ak útočník použíje dostatočne veľa UDP paketov, na sieti vznikne veľká (dvojnásobná) prevádzka a počítač zamrzne.

- *SYN flood* - útok využivajúci nedostok pri vytváraní TCP spojenia 2 vzdialených počítačov, keď v jeho druhej sa na cieľovom počítači vyhradí nejaká pamäť pre adresu zdrojového počítača a ďalšie informácie, aby bolo možné identifikovať "ACK"-paket v tretej fáze. Ak útočník inicializuje spojenie "SYN" paketom s falošnou a nedostupnou zdrojovou adresou, cieľový počítač sa snaží odpovedať na túto nedostupnú adresu a pokúša sa o to niekoľko krát, až kým vyprší čas na nadviazanie komunikácie, pričom údaje o tomto (zatiaľ neexistujúcom) spojení si musí udržiavať v pamäti. Ak útočník zašle veľa falošných "SYN" paketov, na cieľovom počítači sa vyčerpá pamäť určená pre TCP spojenia a všetky ďalšie pokusy o spojenia budú preto ignorované.

- *ICMP flood* – útok využívajúci protocol ICMP a najčastejšie sa naňho využívajú pakety ICMP Echo, ktoré pomocou ping-u zisťujú, či je vzdialené zariadenie dostupné. Tým, že útočník môže zvoliť veľkosť odosielaného ICMP paketu až do veľkosti 65 kB a nastaviť frekvenciu odosielania, dosiahne, že dátová linka cielového počitača bude značne preťažená. Navyše, pokiaľ útočník sfalšuje adresu odosielateľa, dátová linka bude zaplavovaná 2-násobne a útok ešte masívnejší.

Ako sa brániť?

Tak ako sa líšia princípy každého z útokov, tak aj možnosti ochrany voči jednotlivým útokom sú rôzne.
Štandardným typom ochrany proti DDos je vhodné nastavenie server, ako aj zaobstaranie kvalitného routeru a firewall. Týmto spôsobom môžme do veľkej miery eliminovať útoky typu UDP, SYN a ICMP flood, pričom takto vedia zneškodniť niekoľko tisíc útočiacich(zombie) počítačov.
Čo sa týka najrozšírenejšieho útoku v dnešnej dobe, HTTP flood, tak požiadavky ktoré zahlcujú server sú preňho aj pre firewall z hladiska pripojenia úplne korektné a preto ich len ťažko rozoznať od skutočných požiadaviek. Aj preto sa proti nemu len ťažko bráni. V malom množstve dokážu pomôcť blacklisty (nazhromaždené zoznamy podozrivých IP adries), avšak najúčinnejším spôsobom ochrany je zvyšovanie kapacity webového sidle, alebo analyzovanie paketov pomocou špecializovaného softvéru.

4 Použitá metodika

Ako metódu na získavanie potrebných údajov sme sa rozhodli zvoliť formu elektronickej pošty, ktorá nám zároveň umožnila oslovovať väčšie množstvá inštitúcii pomerne jednoduchým spôsobom. Jednu z prvých vecí čo sme urobili bolo, že sme spoločne spísali žiadosť, ktorá obsahovala dotazník, kde sme sa pýtali, aké majú v danej inštitúcii skúsenosti s výskytom útokov typu DDoS. Keďže išlo prioritne o inštitúcie verejnej správy, v žiadosti sme sa odvolávali na zákon o slobodnom prístupe k informáciám č. 211/2000 Z.z.

Dotazník bol rozdelený na tri časti – a) Dotazovanie o vyskytnutom útoku, b) Dotazovanie na uskutočnené protiopatrenia, c) Dotazovanie na dodatočné informácie.
Prvá časť mala za úlohu zistiť, či sa v danej inštitúcii už stretli s tým, že bol na nich zahájený niektorý z DDoS útokov a ak áno, ktorý z typov to bol, akú intenzitu mal, ako dlho trval, či išlo len o jednorázovú udalosť alebo sa útok pravidelne opakoval a aj to ako sa tento útok premietol do niektorých prípadne spôsobených škôd a či tieto vedia byť vyčíslené.

Druhá časť dotazníka mala za cieľ zmapovať situáciu, ako sú inštitúcie upovedomené o rizikách DDoS útokov a ako s touto vedomosťou narábajú, v zmysle, či podnikli nejaké z opatrení, ktoré by do budúcna zamedzili výskytu týchto nežiadúcich útokov. Zaujímalo nás zároveň aj to, či tieto opatrenia boli podniknuté preventívne, bez nejakých predošlých komplikácii s útokmi, alebo práve niektorý zaznamenaný útok podnietil k takémuto konaniu. V prípade, keď boli urobené nejaké z opatrení, zaujímalo nás, aký druh ochranných opatrení v tomto prípade prevládal.

Záverečná časť dotazníka sa sústredila na pár doplnkových informácii, ktoré by nám prípadne dopomohli pri určovaní ukazovateľov kde nastáva chyba, ako napríklad súvisí veľkosť kapacity pripojenia servera resp. priemerná prevádzka počas dňa / prevádzka v špičke s tým, aké riziko to prináša.

Pátraním po internete sme zozbierali väčšie množstvo verejne prístupných mailových adries na nami vybrané inštitúcie a na ne sme rozoslali nami sformulovanú žiadosť spolu s dotazníkom.

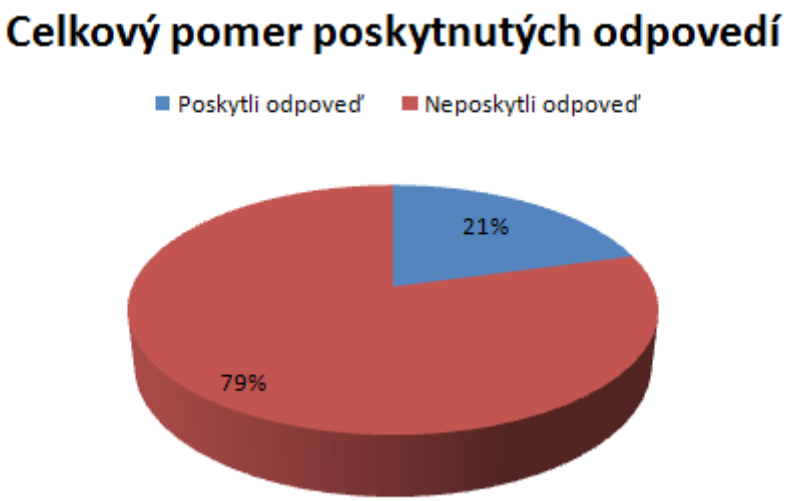
Uvedomovali sme si však, že pracujeme s veľmi citlivou témou, ktorá so sebou prináša riziko zneužitia získaných údajov, čo si môže niekto vysvetliť ako bezpečnostné riziko pre danú inštitúciu a považovať to ako rozpor s nariadením zákona o slobodnom prístupe k informáciam. Na túto skutočnosť sme boli niekoľko násobne dodatočne upozornení a tak sme boli ochotní garantovať výlučne anonymné spracovanie a publikovanie dát výlučne v štatistických ukazovateľoch. Napriek tomu sa niektoré z inštitúcii rozhodli tieto dáta pod týmto dôvodom nezverejniť.

5 Výsledky

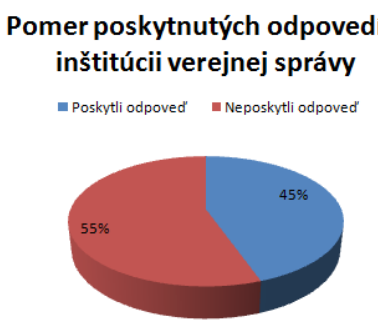
Prichádzajúce odpovede, či už na mailovú adresu, ale občasne aj na poštovú adresu (ktorá bola súčasťou sformulovanej žiadosti) sme zhromaždili, spracovali do tabuliek, tieto potom zosumarizovali a napokon vyhodnotili do štatistických ukazovateľov.

Tak ako čas plynul, potvrdzovalo sa nám, že podiel poskytnutých odpovedí nebude v takej miere, ako by sme pre vyhodnotenie nášho dotazníka uvítali.
Vznikali nám 4 druhy situácii:
a) emailová adresa, ktorá bola pre danú inštitúciu uvedená na internete sa ukázala ako nefunkčná, alebo preplnená a správa sa nám vrátila naspäť
b) správa bola úspešne odoslaná, ale nevrátila sa žiadna odpoveď
c) vrátila sa nám odpoveď bez vyplneného dotazníka s tým, že dané informácie nemôžu byť poskytnuté, keďže by mohla byť narušená bezpečnosť danej inštitúcie
d) bol nám zaslaný (takmer) kompletne vyplnený dotazník

Pôvodná ambícia bola rozposielať naše dotazníky okrem verejnej správy aj súkromným spoločnostiam. Tie však napriek našim ubezpečeniam boli až príliš opatrné a zaslaná odpoveď bola skôr raritou ako pravidlom. To sa odzrkadlilo aj na celkovom pomere poskytnutých odpovedí.



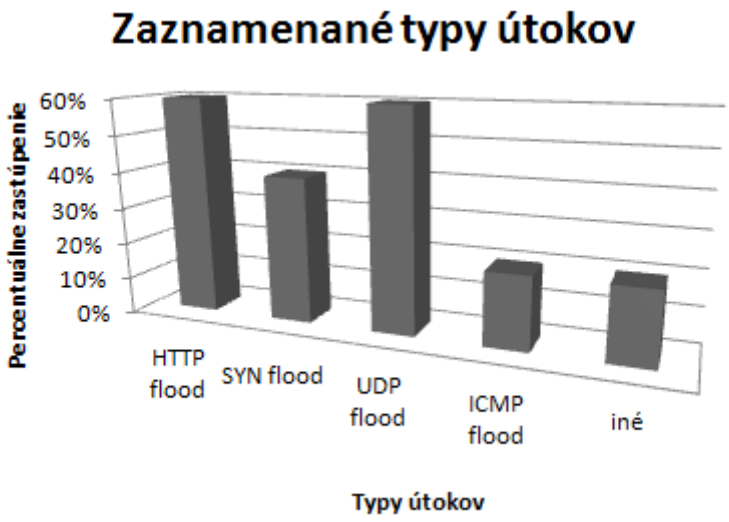
Pomer poskytnutých odpovedí u inštitúcii verejnej správy a u súkromných spoločností.



V ďalšom texte sa budeme venovať už len tej časti respondentov, ktorá nám odoslala nejaké spracovateľné dáta.

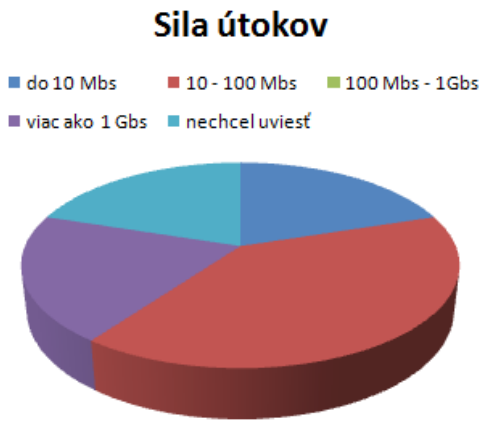
Ako bolo spomenuté, dotazník sa skladal z 3 hlavných častí. Prvou z nich bola časť, v ktorej sme sa zamerali na zisťovanie, aké majú jednotliví respondenti skúsenosti s DDoS útokmi. Prvá otázka mala za zámer zistiť, či už niekedy bol z ich strany zaznamenaný útok typu DDoS.
Očakávania boli také, že nejaké väčšie percento by bolo prekvapením, nakoľko „koho by už len zaujímala naša štátna správa“. A tieto predpoklady sa do veľkej miery naplnili.
Ako vidno z nižšie uvedeného grafu, iba 12% odpovedí sa nám zdôverilo s tým, že takýto typ útoku vo svojej minulosti zažili. Zároveň milo prekvapilo, že iba 2% opýtaných sa k tejto skutočnosti nevedeli vyjadriť(naivne predpokladáme, že tí ktorí uvádzali NIE, mali skutočne overené, že tomu tak nebolo ☺)
Zaujímavejšie štatistické ukazovatele by to určite boli vtedy, keď by sme mali lepšiu odozvu od súkromných spoločností, čo sa však s 2% navrátených odpovedí príliš nedá.

Ďalej v dotazníku sme sa zamerali na tých, ktorí tento útok teda zaevidovali. Zaujímalo nás, aké z útokov už na nich boli skúšané.
Potvrdilo sa, tak ako je aj celosvetový trend, že HTTP flood má najväčšie zasúpenie medzi spomenutými útokmi. Zároveň však bolo prekvapivé veľké zastúpenie aj UDP flood útokov. Medzi inými zaevidovanými útokmi, ktoré nám respondenti vyplnili bol spomenutý ešte útok Slowloris, ktorý sme v možnostiach nemali uvedený.



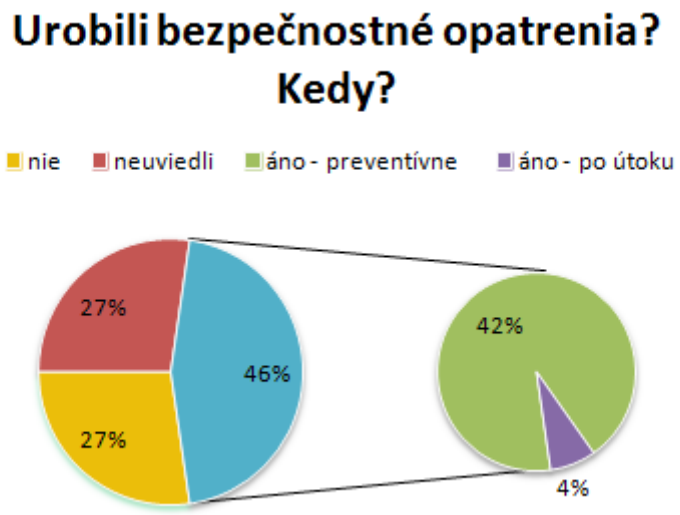
Údaje, ktoré sa nám zdali zaujímavé a na ktoré sme sa ďalej pýtali bola početnosť výskytov útokov(či keď sa útok vyskytol, tak bol uskutočnený len ako jednorázový úder, alebo či sa ten istý útok opakoval aj v ďalšom období). Ďalej sila zaznamenaných útokov a napokon, aké škody tieto útoky daným subjektom spôsobili.
Prvá z otázok týkajúca sa násobnosti bola vyhodnotená tak, že takmer ¾ opýtaných, pokiaľ zažili útok DDoS, tak tento sa vyskytoval iba v jednorázovej nárazovej rorme a najbližšiu dobu mali od tohto útočníka pokoj. Takmer kompletný zvyšok uviedol, že útok sa opakoval práve 2-3x. Viď nižšie.

Sila útokov dosť variovala, čo je spôsobené aj tým, že každá z inštitúcii má vlastnú veľkosť liniek, ktorými komunikuje a tým pádom na inú inštitúciu stačí urobiť iný nápor. Prevládala však odpoveď v rozmedzí 10 – 100 Mbps.



Pri spôsobených škodách sme dali v možnostiach na výber, či útok spôsobil zneprístupnenie nejakej z dôležitých služieb, nejakú menej dôležitú službu, webstránku, alebo iné. Odpovede však nerozlišovali dôležitosť služby a tak sme túto kategóriu zlúčili.
Väčšinu si v tomto prípade podelili odpovede o zneprístupnených stránkach a to, že tieto útoky škody nepriniesli. Iba pomerne malá časť útokov odrovnala aj nejaké spokytované služby.
Z iných škôd boli spomenuté problémy v spojení medzi datacentrami a ešte „lagovanie konektivity“.

Druhá časť dotazníka chcela od respondentov zistiť, či urobili nejaké opatrenia proti výskytom DDoS útokom a ak áno, tak aké.

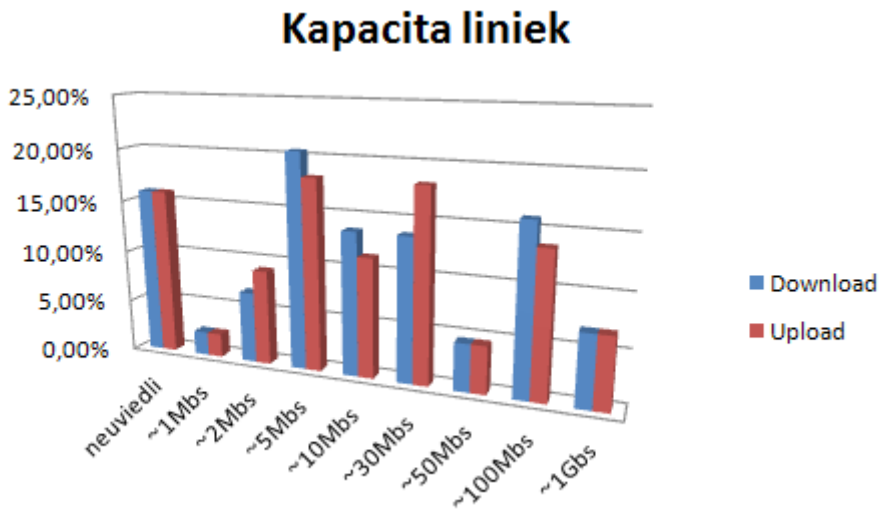


Z vykresleného grafu vidieť pomerne prekvapujúcu odpoveď a to, že dané inštitúcie riziko výskytu tohto útoku neberú na ľahkú váhu a zo 73% percent odpovedí, ktoré sa k danej problematike vyjadrili, 46%, takže väčšina už podnikla nejaké opatrenia.
Z rozšírenej perspektívy tejto odpovede môžeme ďalej vidieť, že tieto opatrenia boli uskutočnené prevažne preventívne a teda nemusel im predchádzať niektorý z útokov DDOS.

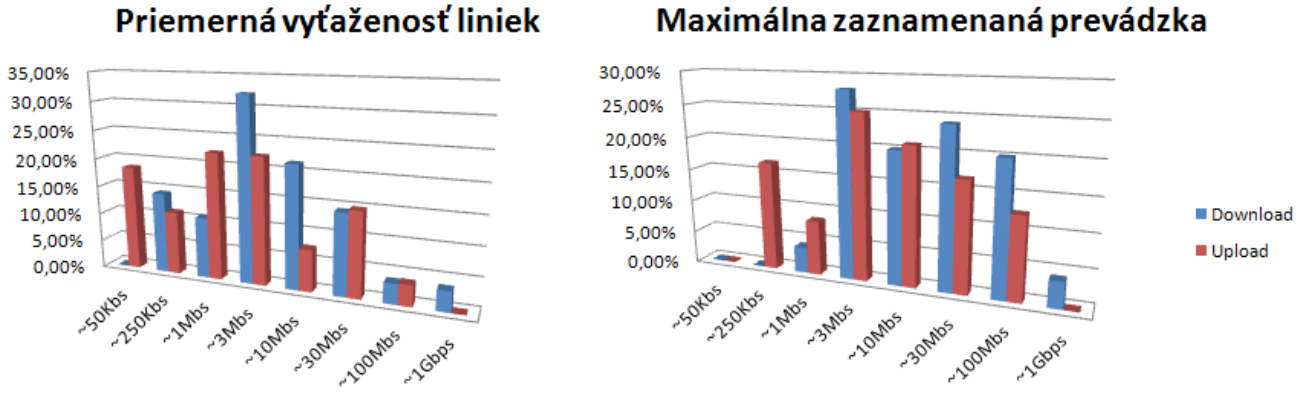
Rovnako tak nás zaujímalo, aké bezpečnostné opatrenia prevládajú u subjektov, ktoré boli nami dotazované.
Z ponúknutých možností u respondentov dominovalo špeciálne nastavenie firewallu.
S odstupom približne 25% bolo zastúpenie nakonfigurovanie routera. Z iných, nami nespomenutých možností sa v odpovediach vyskytlo aj využitie reverznej proxy, ratelimiting, portknocking, konfigurácia servera a zmena bezpečnostných smerníc.

V záverečnej časti sme si „posvietili“ na informácie, ktoré by mohli nejakým spôsobom dopomôcť pri dotváraní obrazu o tom, prečo vznikajú prípadné bezpečnostné riziká u nás dotazovaných subjektoch.

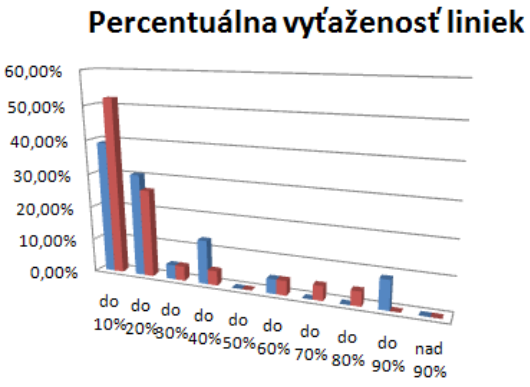
Ako na prvú vec sme sa pýtali na kapacitu a vyťaženosť liniek, ktoré jednotlivé inštitúcie majú. Tieto ukazovatele sme spracovali do nasledujúcich zaujímavých grafov, ktoré nám poskytujú prehľad o daných hodnotách.

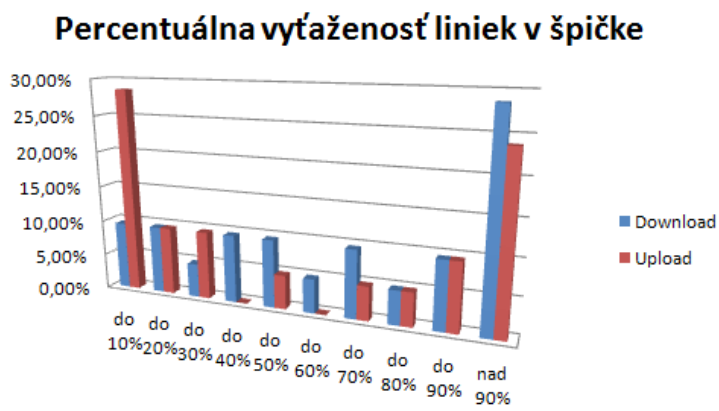


Ako vidno z hore uvedeného grafu, mimo tých čo nechceli uviesť svoje hodnoty, prevažuje v kapacite liniek rozmedzie medzi 5 – 100 Mbps pri downloade a 5 – 30 Mbps pri uploade. Zriedka sa vyskytli aj údaje o kapacite až okolo 1 Gbps.

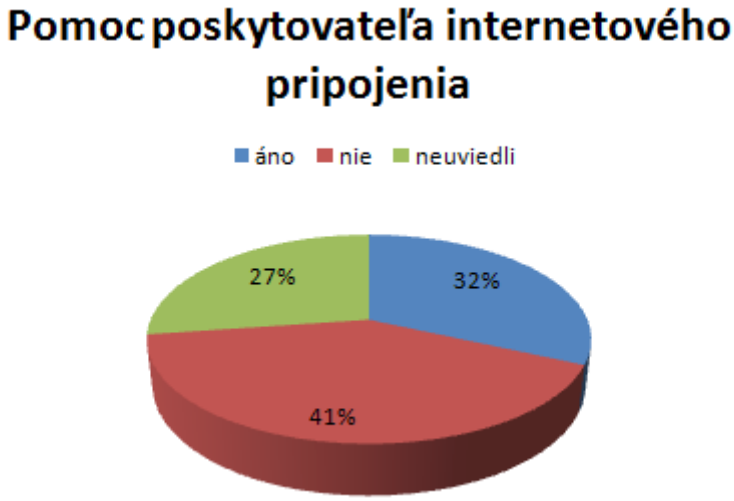


Tieto ďalšie ukazovatele na ktoré sme sa pýtali nám hovoria o priemernom vyťažení liniek a maximálnej zaznamenanej prevádzke ktorú dosahujú v špičke. Dáta sú zaznamenané v objemoch, ktoré prúdia príslušnými linkami a sú zoradené do určitých najčastejších kategórii.
Z daných grafov vidno, že priemerná zaťaženosť download / upload liniek je okolo 3 - 10 / 1 - 3 Mbps. Ako aj, že počas špičky sa tieto čísla pohybujú až okolo hodnôt D/U: 30 - 50 / 5 - 20 Mbps.
Toto pri vyššie spomenutých kapacitách liniek D/U: 5 - 100 / 5 - 30 Mbps sú dosť hraničné čísla.
Preto sme sa v ďalšej štatistike zamerali na to, ako sú percentuálne vyťažené linky počas bežnej prevádzky a vtedy, keď je špička.





Z hore videného nám vyplýva, že veľká väčšina respondentov má ako download linku, tak aj upload linku využitú zhruba na tých 5 – 20%, čo je pomerne dobrý ukazovateľ. Menej príjemne už ale vyzerá fakt, že zhruba 8% subjektov má už aj pri bežnej premávke záťaž liniek okolo 85%. To musí nevyhnutne spôsobovať problém.
To vidíme v grafe napravo, ktorý nám meria vyťaženosť liniek počas špičky, tam sú už údaje dosť „škaredo“ rozložené, keď vidíme, že zhruba ¼ respondentov vykazuje výsledky, že ich linky vtedy fungujú nadoraz. Toto nie je žiaden dobrý signál toho, že pokiaľ by sa niekto rozhodol uskutočniť nejaký útok typu DDoS na veľkú časť dotazovaných respondentov, stačilo by mu k tomu veľmi málo a bol by úspešný.



V záverečnej otázke dotazníka, nakoľko sme si uvedomovali, že respondenti môžu mať častokrát iné starosti ako starať sa o akúsi bezpečnosť . Bolo pre nás zaujímavé vedieť, či prípadne ich poskytovateľ internetových služieb im nejakým spôsobom nedopomáha eliminovať riziká, ktoré vznikajú. Túto skutočnosť uviedla približne 1/3 opýtaných, čo popri tých čo odpovedali negatívne bola menšina a teda väčšina sa spolieha pri riešení bezpečnostnej ochrany hlavne na svoje zdroje.

6 Záver

Po skončení realizovania prieskumu možno skonštatovať, že väčšina inštitúcií, ktoré odpovedali, žiaden útok typu DDOS ešte nezaznamenali, resp. o tom nevedia. Potenciálnym problémom môže byť až 90% vyťaženosť liniek pri maximálnom zaťažení, ktorá nastáva u výrazného množstva inštitúcií.

Ohľadom opatrení možno povedať, že sú takmer výlučne preventívneho charakteru, čo je zapríčinené pravdepodobne práve faktom, že zatiaľ útok nebol evidovaný. Tieto opatrenia sa zameriavajú na celkovú bezpečnosť siete, teda nie špecificky voči DDOS útokom. Najčastejšie sa jedná o konfigurácie routera a firewallu.

Pokiaľ sa pozrieme na zloženie získaných odpovedí, jedná sa takmer výlučne o verejnú správu, ktorá podlieha zákonnej povinnosti na odpoveď, súkromné spoločnosti buď neodpovedali vôbec, alebo – najmä v prípade bánk – poslali najprv oznámenie o preposlaní, na špecializované oddelenie, a neskôr oznámenie o zamietnutí žiadosti z dôvodu neposkytovania takéhoto typu informácií. Z takéhoto dôvodu nám odpovedať odmietlo aj niekoľko verejných inštitúcií, ich počet ale nebol veľmi výrazný, a zväčša sa jednalo o odporúčanie ich IT oddelenia.

Najväčší problém pri spracovaní bol pri vyhodnotení kapacity liniek, a ich záťaže. Viaceré odpovede si pomýlili maximálnu záťaž s priemernou, čoho korigovanie bolo jednoduché. Horšie to už je s možným pomýlením downloadu s uploadom, ktoré je ťažšie odhaliť, ale pri maximálnej kapacite liniek to v pár prípadoch bolo očividné. Podozrivo tiež pôsobili dáta, podľa ktorých je priemerná záťaž vyššia, ako kapacita liniek, ktoré majú k dispozícii. Tieto dáta preto môžu byť mierne skreslené, napriek snahe o korekciu, a vypustenie tých dát, pri ktorých nebolo možné určiť zdroj chyby a teda nebolo ich možné použiť pri štatistickom spracovaní.

A Prílohy

Dotazník

Informácie o vyskytnutom útoku

1. Zaznamenali ste niekedy v minulosti napadnutie Vášho servera útokom typu DDOS? *(áno/nie)*

2. Ak áno, o aký typ útoku išlo? *(pri jednotlivých možnostiach uveďte áno/nie)*

    a, HTTP flood?*(áno/nie)*

    b, UDP flood? *(áno/nie)*

    c, SYN flood? *(áno/nie)*

    d, ICPM flood? *(áno/nie)*

    e, Iný:

3. Ako dlho trval daný útok? *(časová dĺžka od zahájenia až po jeho odznenie)*

4. Aká bola sila útoku? *(traffic zaznamenaný počas útoku) (napr. v Mb/s)*

5. Vyskytoval sa tento útok opakovane, alebo jednorazovo? *(koľko krát)*

6. Spôsobil Vám daný útok nejaké škody? *(áno/nie)*

    a, zneprístupnil vám dôležité služby, ktoré poskytujete

    b, zneprístupnil vám menej podstatné služby, ktoré poskytujete

    c, zneprístupnil web stránku

    d, Iné:

7. V akom rozmedzí sa pohybovala spôsobená škoda?

a, 0 – 1000 eur

b, 1000 – 10000 eur

c, viac

d, škoda bola nefinančného charakteru (strata dobrého mena ....)

Informácie o uskutočnených opatreniach

1. Boli zo strany Vašej organizácie prijaté špeciálne opatrenia na zabránenie takýmto druhom útokov? *(áno/nie)*

2. Boli tieto opatrenia preventívneho charakteru, alebo boli robené až po výskyte útoku? *(preventívne/bezprostredne po útoku/neskôr)*

3. Ktoré z daných opatrení ste urobili? *(uveďte k jednotlivým možnostiam)*

a, Zaobstaranie niektorého zo softwarových produktov? *(áno/nie, akého)*

b, Zakúpenie špecializovaného hardwaru? *(áno/nie, akého)*

c, Zmena konfigurácie routera? *(áno/nie)*

d, Zmena konfigurácie firewallu? *(áno/nie)*

e, Zmena poskytovateľa internetu? *(áno/nie)*

f, Rozšírenie liniek? *(áno/nie)*

g, Iné? *(aké)*

Ďalší prehľad

1. Dopomáha Vám Váš poskytovateľ internetových služieb nejakým konkrétnym spôsobom eliminovať hrozby napadnutia niektorým z útokov DDOS? *(áno/nie, akým)*

2. Aké sú download a upload kapacity pripojenia, ktoré používate? *(napr. v Mb/s)*

3. Aká je bežná priemerná prevázka Vašich komunikačných liniek a aká je ich prevádzka v špičke? *(upload, download napr. v Mb/s)*