CZ.NIC | SPRÁVCE DOMÉNY CZ

Rekapitulace (D)DOS útoků ze dnů 4. 3. – 7. 3.

Tento dokument obsahuje náhled na situaci z období 4. 3. až 7. 3., kdy byla provedena série (D)DOS útoků na www služby provozované v České republice, z pohledu sdružení CZ.NIC a CSIRT.CZ (Národní CSIRT České republiky).

I přes velkou snahu shromáždit co nejvíce informací a dat a snahy průběžně monitorovat situaci, si jsme vědomi, že nemáme k dispozici veškeré informace a náš náhled tudíž nemusí být kompletní.

Popis událostí

V pondělí 4. března 2013 začala série (D)DOS útoků na webové servery provozované v České republice. Útoky probíhaly obvykle ve dvou vlnách – dopoledne mezi 9-11h a odpoledne mezi 14-16h. Každý den byl útok veden vůči jiné skupině cílových serverů:

Pondělí 4. 3. – útoky jsou vedeny proti webovým serverům Novinky.cz, iDNES.cz, IHNED.cz, Lidovky.cz, Denik.cz, Csfd.cz, okolo poledne byly nedostupné weby E15.cz, Živě.cz, Mobilmania.cz.

Úterý 5. 3. – okolo 10h jsou nedostupné služby společnosti Seznam.cz. Seznam.cz o situaci informuje na svém facebookovém profilu. Okolo 11:30 je Seznam.cz opět funkční. Kolem 13:30 se útok opakuje, jsou pozorovány chvilkové nedostupnosti serverů.

Středa 6. 3. – od cca 9:30 do 11:00 jsou nedostupné webové servery bank – České spořitelny, Komerční banky, FIO banky, ČSOB, Raiffeisen banky, České národní banky (www.cnb.cz). V důsledku útoků došlo u České spořitelny i k výpadku e-commerce a k ochromení některých platebních terminálů. Ve 14h došlo ke druhé vlně útoků na weby České spořitelny.

Čtvrtek 7. 3. – od cca 9:30 probíhá útok na servery dvou mobilních operátorů Telefónica O2 a T - mobile. Telefónica útok eliminuje okolo 10:00, T-Mobile okolo 11:00.

Během útoku byly chvílemi nedostupné další služby, jako např. registr vozidel či web dpp.cz. Bylo hlášeno, že v době probíhajících útoků nebylo nějaký čas možné nakupovat SMS jízdenky MHD.

Okolo 20h je zjištěna nedostupnost webů České televize, podle posledních informací však jejich problémy s útokem nesouvisely.

V pátek 8. 3. již nebyl pozorován ani hlášen žádný (D)DOS útok takového typu, že by znepřístupnil některý z často navštěvovaných a viditelných webů. Situace se pomalu uklidňovala jak na straně provozovatelů sítí, tak ve světě médií.

Charakteristiky útoků

V průběhu útoků se obecně hovořilo o útocích typu DDOS (Distributed Denial of Service). V současné chvíli, kdy máme soustředěno velké množství informací a souvisejících dat, není zcela jasné, jestli útok byl opravdu typu DDOS nebo DOS. Většina útoků byla soustředěna na www služby.

Většina toku při útocích přišla přes síť RETN (http://www.retn.net/en/). Ačkoliv napadené strany, ISP i CSIRT.CZ zkoušeli kontaktovat provozovatele této sítě, nepodařilo se nikomu získat relevantní pomoc (data, zablokování útočníků). Je přitom pravděpodobné, že RETN

disponuje daty, která by mohla pomoci blíže specifikovat útočníka (MRTG grafy provozu, poměr odeslaných paketů vs tok atd.)

Při útocích byly použity mechanismy tzv. SYN Flood v kombinaci s podvrženou adresou (IP spoofing). Cílem takového útoku je zahltit stroj, na který je útok veden, nebo jeho síťovou infrastrukturu (např. firewall na předřazeném zařízení) a vyčerpat jejich systémové zdroje.

Další použitá verze útoku spočívala k přidání techniky „odražení“ (bounce traffic). Celý (D)DOS útok pak vypadal tak, že útočící stroje emitovaly velké množství paketů s podvrženou zdrojovou adresou. Jako zdrojová adresa byla použita IP adresa stroje, na který byl veden útok. Pakety byly poslány na jiné stroje, které ale komunikaci vracely na podvrženou zdrojovou adresu. Tato technika založená na emitaci velkého množství paketů s podvrženými zdrojovými adresami a za využití techniky odražení útok ještě více zesílí.

Průběh řešení situace

Od pondělí 4. 3. odpoledne se na tým CSIRT.CZ začali obracet provozovatelé sítí a služeb, na které bylo útočeno, se žádostmi o pomoc, spolupráci a výměnu informací. Myslíme si, že správci v napadených sítích svou roli zvládali dobře, takže nedostupnosti jednotlivých webů byly v řádech jednotek hodin. Jako profesionální se nám jeví přístup ISP, přes které byly napadené weby připojeny. Poskytovali podporu napadeným sítím a byli schopni nasadit efektivní metody obrany. Zdá se pravděpodobné, že nedostupnost webů byla způsobena chybami v konfiguraci a nedostatečně dimenzovanými síťovými prvky a servery samotnými.

Oceňujeme především schopnost a ochotu všech zainteresovaných subjektů komunikovat, sdílet zkušenosti, informace a doporučení.

V průběhu nejsilnějších útoků proti České spořitelně ve středu 6. 3. byla zformována pracovní skupina složená z odborníků z organizací CZ.NIC (CSIRT.CZ), CESNET, GTS a České spořitelny a byla zrealizováno ad-hoc videokonferenční setkání. Na tomto setkání skupina diskutovala aktuálně probíhající útoky, analyzovala provoz a hledala a testovala nejefektivnější způsob obrany. Tato pracovní skupina zůstala v pohotovosti i v průběhu čtvrtka a pátku.

Další pracovní skupina byla zřízena přímo na půdě CZ.NIC a sestávala ze členů týmu CSIRT.CZ, správců sítě CZ.NIC a PR pracovníků. Ta obstarávala komunikaci (v rámci procesu *incident handling*) s provozovateli sítí a služeb, sběr a sdílení informací, dat a zkušeností, komunikaci s pracovní skupinou síťařů, NBÚ (Národním centrem kybernetické bezpečnosti), bezpečnostními složkami, zahraničím a komunikaci s médii.

Ve čtvrtek se na CSIRT.CZ začali obracet pracovníci společností a organizací, které měly obavu, jestli nebudou dalším cílem útoku (např. PRE, ČEPS) a žádali o informace a spolupráci. Jim jsme předali základní informace o útocích a také jsme dohledávali jejich poskytovatele připojení a tranzitní operátory, aby jak oni, tak my byli připravení a věděli, na kterého ISP se případně obrátit.

Technická doporučení

Metod a technologií pro obranu před (D)DOS útoky je celá řada, ale obvykle je potřeba jich zkombinovat několik, nelze se spolehnout pouze na jednu. Na úrovni síťové infrastruktury hovoříme o obraně pomocí RTBH (remotely triggered black hole filtering), použití tzv. Load Balancer zařízení, zařízení typu Scrubber (čističky, kde se oddělí většina špatného provozu od

dobrého), prefix-listy (omezení propagace AS), rate-limity, access listy na síťové vrstvě, firewall, IDS, IPS apod.

Zajištění dostupnosti konkrétní služby může být dále zvýšeno posílením robustnosti celé architektury za použití technologie anycast, DNS round-robin, které zajistí rozklad zátěže mezi více strojů se shodným obsahem a pod. Dalším krokem pak může být umístění serverů poskytujících jednu službu do více sítí.

Jakékoliv rozhodování o architektuře služby a související síťové infrastruktury by ale vždy mělo jít ruku v ruce s rozvahou, do jaké míry se obrana vyplatí. Při tomto rozhodování hraje roli charakter služby a její kritičnost pro uživatele.

V rámci bezpečnostního týmu CZ.NIC bylo v průběhu týdne útoků postaveno řešení, které je schopno vygenerovat tok o síle cca deseti miliónů packetů za vteřinu, tedy několikrát více, než kolik bylo emitováno v proběhlých útocích.

V současné době je toto řešení používáno pro testování vlastní infrastruktury CZ.NIC. Zároveň bylo nabídnuto jako nástroj pro bezplatné otestování infrastruktury dalším zájemcům.

Pozorování a poučení

(D)DOS útoky vedené v období 4. 3. až 7. 3. vůči cílům v ČR měly poměrně slabý charakter, minimálně z pohledu ISP, kteří s útokem měli problém pouze ve vztahu ke koncovým sítím.

Útok svou silou nijak neohrožoval chod páteřních sítí providerů a jejich infrastrukturu.

Podle dostupných informací hovoříme o datových tocích do 1Gbps (maximální zaznamenaný tok 1,5 mil. paketů za sekundu). Útoky způsobily problémy až v koncových sítích.

Podle informací, které máme k dispozici, se ve většině případů útok ani k cílovému serveru nedostal, ale přetížil systém před – obvykle firewall, load balancer nebo podobné zařízení.

Zcela nepopiratelně útoky odhalily řadu slabých míst v síťové architektuře koncových sítí.

Série útoků byla dobře připravena – zajímavě zvolené a dobře „viditelné“ cíle, jejichž nedostupnosti si všimnou jak uživatelé, tak média, byly použity různé techniky útoků a jejich kombinace.

Znalost prostředí potvrzuje i distribuce útoků mezi jednotlivé cíle – zatímco pondělní útok se zaměřil na více cílů, úterní směroval proti jedinému cíli, u něhož se dalo očekávat že robustnost jeho řešení bude větší než u zpravodajských webů. Podobně byl potom ve čtvrtečním útoku „vynechán“ třetí z mobilních operátorů – opět se lze domnívat, že útočník se rozhodl koncentrovat síly na menší počet cílů.

Je tedy pravděpodobné, že za útoky stojí někdo s dobrou znalostí českého internetu.

Závěr

Dění minulého týdne potvrdilo jednu základní věc – správci sítí a služeb jak na úrovni ISP, tak na úrovni koncových sítí jsou schopni a ochotni efektivní spolupráce a výměny zkušeností a některých informací.

Považujeme za vhodné z pozice národního CSIRT týmu ještě více podporovat komunikaci a výměnu informací na technické úrovni, a to pokud možno od prvního okamžiku podobného útoku a zlepšovat prostředky a nástroje pro tuto komunikaci.

V průběhu útoku se dle našeho názoru potvrdilo, že tým CSIRT.CZ se v české prostředí velmi dobře etabloval a má zde svou důležitou roli při událostech podobného typu.

Ukázalo se, že zejména operátoři (ISP) jsou na situaci dobře připraveni jak po stránce technické, tak po stránce organizační.

Jednou z negativních zkušeností, která se potvrdila, je existence nepříjemné bariéry pro sdílení relevantních informací o útocích. Jeden z operátorů se odkazoval na zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů (ZoEk) a na vyhlášky č. 335/2005 Sb. a vyhlášce č. 357/2012 Sb., které upravují podmínky poskytnutí provozních a lokalizačních údajů a uskutečnění odposlechu. Toto přímo brání efektivní spolupráce mezi ISP a bezpečnostními týmy.