Kaj se dogaja na omrežju?

Gorazd Božič

Povzetek — SI-CERT je center za razreševanje varnostnih incidentov na omrežju internet, ki deluje v sklopu Akademske in raziskovalne mreže Slovenije (ARNES). Eden od namenov takega centra je tudi ustvarjanje pregledne slike dogajanja na omrežju, ki ga zaznamujejo različni varnostni incidenti in zlorabe. Ta slika skozi čas pokaže nekaj zaskrbljujočih dejstev.

Ključne besede — SI-CERT, varnostni incidenti, trendi

Abstract — SI-CERT is the incident response team (IRT) that operates within ARNES (Academic and Research Network of Slovenia) and acts as a center for security incident coordination and resolution. One of the goals of an IRT is the formation of a "big picture" with regards to various incidents and abuse on the network. Seen through time, this picture shows some worrying facts.

Keywords — SI-CERT, security incident, trends

I. Uvod

SI-CERT že od svoje ustanovitve leta 1994 sprejema prijave o varnostnih incidentih, ki vključujejo omrežja v Sloveniji. V zadnjih desetih letih smo bili priča neslutenemu razvoju omrežja, kar pa seveda potegne za sabo tudi spremembe na področju varnostnih zlorab in incidentov. Članek podaja pregled teh sprememb, razloge za njih in nekaj najbolj razširjenih tipov varnostnih incidentov oz. zlorab.

II. Ozadja sprememb

A. Širitev omrežja in povzročitelji zlorab

Širitev in dostopnost omrežja je omogočila storitve na omrežju, za katere je redkokdo slutil, da bodo mogoče. Nujna posledica širitve pa je tudi povečanje poskušanih in uspešnih zlorab na omrežju. Število t.im. "hekerjev", ki se s tem ukvarjajo, se je ne le povečalo, ampak se je tudi sama struktura "vdiralcev" razslojila na različne skupine.

Medijska podoba hekerja kot (pravičnega) uporabnika proti velikemu "sistemu" (pa naj gre za korporacije, države ali strukturo vodenja interneta) je sigurno pripomogla k temu, da si dokajšnje število uporabnikov omrežja želi pridobiti ta naziv. Vsaj nekaterim to pomeni željeno potrditev njihovega statusa in je lahko pomemben element samopodobe. Poleg splošne oznake *heker*, lahko govorimo o vsaj še nekaterih: *IRC bojevnikih*, katerih motivacija je pridobivanje nadzora nad kanali pogovornega sistema IRC, *skriptnimi otročaji* (angl. "script kiddies"), ki znajo uporabljati le orodja za vdiranje, ki so jih napisali drugi, ter *razobličevalci* (angl. "defacers"), ki vdirajo v spletne strežnike in spreminjajo njihovo vsebino.

Skupine se seveda deloma prekrivajo, delijo pa si v veliki meri tudi nekaj osnovnih lastnosti: gre za mlajše moške (večinoma najstnike), ki jim je omrežje glavni vir socializacije.

B. Poenotenje platform

Internet je nastal kot omrežje, ki je bilo sposobno na enotnem protokolu združevati naprave različnih proizvajalcev. Temu je še danes tako, vendar pa po zastopanosti izstopa nekaj glavnih igralcev:

- Microsoft z operacijskim sistemom Windows za osebne računalnike in strežnike,
- Linux za strežnike in vedno bolj tudi osebne računalnike,
- Solaris za strežnike,
- Cisco kot glavni proizvajalec usmerjevalnikov prometa.

Čeprav prva dva na seznamu stojita na različnih bregovih (prvi ima izrazito komercialen namen, drugi pa temelji na odprti kodi), razširjenost (tudi zaradi strojne podlage na Intel procesorjih) omogoča zlorabe "po receptu" s pripravljenimi orodji. Eden od najbolj razširjenih primerov so internetni črvi, ki se ravno zaradi tega lahko širijo z veliko hitrostjo po omrežju in dosežejo visoke stopnje okužb[1][2].

Programske napake v operacijskih sistemih in aplikacijah so takorekoč stalnica. Bodisi zaradi pritiskov trga, ki krajša fazo preverjanja programske opreme, ali pa zaradi čisto človeških in razumljivih lastnosti, površnosti in lenobe. Svoje pa prispeva tudi položaj, ki ga je deležna industrija programske opreme in omogoča proizvajalcu izogib kakršnimkoli posledicam zaradi napak, ki so bile odkrite v njegovi programski opremi. Velikokrat naletimo na primerjave z avtomobilsko industrijo, ki se mora podrejati strogim kriterijem pri testiranju svojih proizvodov. Čeprav so, roko na srce, posledice napake na avtomobilu in v programu za osebni računalnik lahko dokaj različne, pa se lahko vseeno vprašamo, ali ne bi potrebovali nekakšnega predpisanega sistema kakovosti tudi za programsko opremo.

C. *Dostopnost vdiralskih orodij*

Pomembna lastnost interneta je široka in hitra dostopnost informacij. Ne glede na njihovo naravo, zato so enostavno dostopna tudi orodja, ki omogočajo vdor v sistem, ali pa kakšno drugačno zlorabo. Današnja orodja dostikrat niso več kosi izvorne kode, ki jih moramo pred uporabo natančno pregledati, da bi ugotovili, kako jih je potrebno zagnati. Orodja se dostikrat ponašajo z uporabniško prijaznimi grafičnimi vmesniki in priloženimi natančnimi navodili, ki sleherniku omogočajo nepooblaščen dostop do sistema, nadzor nad njim, ali pa napade, ki sistem ali del omrežja napravijo začasno nerabne (t.im. "distributed denial-of-service" ali DDoS orodja).

D. *Množični širokopasovni dostop*

Prodor osebnega računalnika je omogočila cenovna dostopnost strojne in programske opreme na eni strani, ter enostavnost uporabe. Podobno velja tudi za prodor interneta, saj se danes ni več potrebno "boriti" z različnimi nastavitvami, preden se uspemo priključiti, ampak operacijski sistem postori takorekoč vse. Hkrati pa je vedno bolj v uporabi *širokopasovni dostop* preko kabelskih omrežij in ADSL tehnologije.

Posledica tega je, da je "domači" uporabnik vedno bolj privlačna tarča napadov. Nudi namreč zadostno komunikacijsko pasovno širino, stalen internetni naslov in odsotnost sistemskega skrbnika, ki je običajno na voljo v omrežjih ustanov. Enostavnost uporabe računalnika in omrežja nas lahko zavede v prepričanje, da je komunikacija na omrežju sama po sebi varna, sam sistem pa zaščiten pred nepooblaščenimi dostopi. Resnica je seveda drugačna in se praviloma pokaže v pravi luči na veliko začudenje uporabnika.

Vdiralci imajo torej na voljo široko izbiro ranljivih sistemov, ki jih lahko uporabijo kot posredniške sisteme za nadaljnje napade, koristni pa znajo biti tudi podatki, ki se na sistemu nahajajo.

E. *Hitri prodor omrežja na "suha" področja*

Proti zlorabam se je možno boriti in se jim izogibati. Za razliko od "neomreženega" dela naših dejavnosti, kjer osnovno in osredno vlogo opravljajo policija in sodišča, je obravnava zlorab na internetu sledila načelu *samoregulacije*, ki je bila poglavitna značilnost omrežja. Po prvem večjem incidentu [3] je postalo očitno, da je potreben center, ki bo omogočal obveščanje skrbnikov omrežij in izvajal strokovno svetovanje. Posledično je bil ustanovljen CERT/CC (Computer Emergency Response Team Coordination Center). V devetdesetih letih pa so se začeli pojavljati podobni centri tudi drugod po svetu, predvsem v zahodni Evropi in Avstraliji. Šele v zadnjih letih lahko opazimo ustanavljanje podobnih centrov v vzhodni Evropi, v Aziji in Južni Ameriki pa so ti centri še danes v povojih.

To dejstvo upočasni reagiranje na varnostne incidente in omogoča napadalcem mirno izrabo tujih sistemov, saj je pri hitri obravnavi varnostnega incidenta izrednega pomena hiter pretok informacij med varnostnimi cetri, ponudniki dostopa in skrbniki lokalnih omrežij. Prav to sodelovanje je povzročilo, da so se izvori napadov iz dobro oskrbovanih omrežij ZDA in velikega dela Evrope skoraj povsem preselili v omrežja, ki se nahajajo recimo na Kitajskem, Tajvanu, Južni Koreji in Braziliji.

F. *Pomanjkanje učinkovite regulacije*

Omenjeni varnostni centri lahko seveda ob incidentih uveljavljajo le omejen nabor ukrepov, saj gre za centre, ki delujejo praviloma v sklopu ponudnikov dostopa do interneta. Država s svojimi organi je tista, ki na podlagi ustrezne zakonodaje lahko učinkovito ukrepa.

Internet je presenetil s svojo hitrostjo tudi tu. Zakonodaja se mu prilagaja počasi, postopki za pridobivanje dokazov in sodno ukrepanje pa se dostikrat izkažejo kot pomanjkljivi in dolgotrajni. Dosti področij je v "sivi coni", ko se ne ve, kako bi nek primer sploh obravnavali.

Poleg novih oblik kaznivih dejanj, ki so lastna telekomunikacijskim omrežjem, so elektronske naprave, računalniki in telekomunikacijska omrežja postala tudi eno od orodij tistih, ki jim je kriminal vsakodnevna dejavnost. Tudi pri nas je policija že naletela na problem šifrirane elektronske pošte pri osumljencu trgovine s prepovedanimi drogami.

Sodelovanje policij iz različnih držvah je zopet poglavje zase. Interpol se izkaže kot počasen in neučinkovit. Veliko je različnih pobud in projektov, a zaenkrat še ni videti luči na koncu tunela...

Velik problem predstavlja tudi pridobivanje ustrezno izobraženega kadra za kriminalistično službo, saj lahko ta kader najde bolje plačano in bolj prijetno delo drugje.

III. NEKAJ IZBRANIH PRIMEROV

A. *IRC vojne in DDoS napadi*

Eden od bolj pogostih razlogov težav na omrežju predstavljajo t.im. DDoS napadi, ki sprožijo koordiniran napad na ciljni sistem ali omrežje. Gre za poplavo podatkov, ki zapolnijo komunikacijske povezave ali pa povzročijo izpad strežnika. Razlog teh napadov je največkrat smešno banalen: prevzem IRC kanala, ali odstranjevanje "neljube" osebe z nekega kanala in dokazovanje moči.

Orodja za DDoS napade so se od pojava prvih množičnih orodij [4] razvile v obliko, ki omogoča napadalcu enostavno uporabo. Ta najprej poišče sisteme, ki so ranljivi (t.im. *skeniranje* omrežja), na njih podtakne DDoS *agente*, ki se po zagonu povežejo na določen kanal izbranega IRC strežnika. Seveda na tem kanalu "kraljuje" napadalec in s sporočili na njem upravlja svoj t.im. "dosnet", skupino svojih agentov. Napadalcu je na voljo nekaj priljubljenih trikov, ki mu omogočijo skrivanje dejanske lokacije, najbolj pogosto uporabljana pa sta: IPv6-in-IPv4 tuneli do eksperimentalnih ponudnikov IPv6 dostopa in upravljanje DNS zapisa za IRC strežnik, na katerega se DDoS agenti povezujejo. S slednjim si zagotovi nemoteno delovanje "dosneta", čeprav se onemogoči IRC strežnik, preko katerega ga nadzira, saj ga namesti na drug sistem in spremeni ustrezne DNS zapise.

B. *Internetni črvi*

Zavedanje o potrebi po varovanju interneta se je dobesedno začelo s črvom (po avtorju imenovan "Morrisov črv"[3]). Črvi so bili že pozabljeni, dokler se niso zopet pojavili deset let kasneje (1999). Poglaviten način širjenja je elektronska pošta. Za širjenje se večinoma uporablja ranljivost poštnega odjemalca, črv pa se samodejno razpošilja na naslove v imeniku okuženega sistema. Pri tem lahko spreminja pošiljateljev naslov in namesti še dodatne komponenta, ki omogočajo nepooblaščen dostop do sistema.

Nekaj zadnjih črvov je uporabljalo ranljivosti v spletnih strežnikih, ki so uporabljali OpenSSL knjižnico, Microsoft SQL strežnikih in Microsoft Internet Information Server.

Med medijsko najbolj izpostavljenimi črvi je tudi "Code Red", ki izvira na Kitajskem, namen prve različice pa je bil DDoS napad na spletno stran www.whitehouse.gov.

IV. ZAKLJUČEK

Lahko bi rekli, da je dogajanje na omrežju prešlo iz obdobja, ko je vsak sumljiv paket na njem povzročil veliko pozornost skrbnikov omrežja, do današnjega stanja, ko med običajnim prometom zaznavamo v ozadju nekakšen "šum", pri katerem gre za promet, ki ima (recimo temu) sporen namen.

Motivacije za zlorabe počasi lahko nehamo označevati kot radovednost in najstniško igranje, ter začenjamo razmišljati o bolj konkretnih in nevarnih oznakah, kot so organizirani kriminal, industrijsko vohunjenje in nevarni vandalizem.

A. *Medijska slika*

Mediji igrajo pomembno vlogo tudi na področju omrežne varnosti. Prav tu pa so dostikrat ujeti v past hitrih novic in senzacionalizma, ki včasih ne prikaže prave slike. Tipičen primer tega je denimo poročanje o MS SQL *Slammer/Sapphire* črvu, ko smo lahko brali in poslušali novice o "internetnem mrku", kar so kasnejše analize ovrgle[5]. Odvisno od dnevnega dogajanja lahko manj pomembni incidenti dobijo veliko večjo medijsko težo, kot pa si jo zaslužijo, in obratno.

B. *Neobveščenost uporabnikov*

Stalnica pri varovanju omrežij je na žalost zelo slaba obveščenost (in ozaveščenost) uporabnikov. Pogoste so zlorabe in vdori, ki izkoriščajo ranljivosti, za katere je proizvajalec že pred leti objavil popravke. Končni uporabnik smatra svoj sistem kot implicitno varen, vodstva (predvsem manjših) podjetij pa nemalokrat smatrajo investicijo (še posebej kadrovsko) v varovanje svojega omrežja kot čisto izgubo denarja.

LITERATURA

[1] SI-CERT 2003-01 / Slammer črv (MS SQL)
http://www.arnes.si/si-cert/obvestila/2003-01.html

[2] Črv Slapper, opis F-Secure
http://www.kabi.si/si21/f-prot/slapper.html

[3] Larry Boetger: The Morris Worm: how it Affected Computer Security and Lessons Learned by it, december 2000
http://www.sans.org/rr/malicious/morris.php

[4] Denial of Service Attack using the TFN2K and Stacheldraht programs, ISS Security Alert, februar 2000
http://www.iss.net/issEn/delivery/xforce/alertdetail.jsp?id=advise43

[5] James Aldridge, Daniel Karrenberg, Henk Uijterwaal and René Wilhelm: Sapphire/Slammer Worm Impact on Internet Performance, RIPE NCC, februar 2003
http://www.ripe.net/ttm/worm/

Gorazd Božič je diplomiral na Fakulteti za računalništvo in informatiko Univerze v Ljubljani leta 1994 in se še istega leta zaposlil na Akademski in raziskovalni mreži Slovenije (ARNES). Ob ustanovitvi varnostnega centra SI-CERT (Slovenian Computer Emergency Response Team) je prevzel njegovo vodenje. Od leta 2000 predseduje takrat ustanovljeni evropski skupini TF-CSIRT, ki združuje evropske centre za obravnavo varnostnih incidentov na omrežju.