DOI: 10.19279/TVZ.PD.2015-3-3-08

MODEL SUSTAVA ZA SPRJEČAVANJE MREŽNOG MALICIOZNOG PROMETA BLOKIRANJEM IZVORA NAPADA IZVAN ŠTIĆENOG INFORMACIJSKOG SUSTAVA

MODEL OF SYSTEM FOR PREVENTION MALICIOUS NETWORK TRAFFIC WITH BLACK HOLE ROUTING OUTSIDE OF PROTECTED INFORMATION SYSTEM

Miroslav Tarbuk[1]

[1]*Tehničko veleučilište u Zagrebu, Informatičko-računarski odjel*

Sažetak

Tretiranje malicioznog mrežnog prometa, uskraćivanjem komunikacije izvora napada već na točki izvan štićenog informacijskog sustava, predstavlja efektivnu i popularnu metodu borbe protiv malicioznog koda jer štedi procesno vrijeme informacijskog sustava. U prvom redu je cilj rasterećenje procesnog vremena i resursa sigurnosnih komponenata samog sustava. Uvjeti koji se moraju zadovoljiti mogu sadržavati više odlučujućih parametara koji definiraju sam napad, kako bi uskratili komunikaciju malicioznog izvora na temelju njegove izvorišne IP adrese, koja može biti istinita ili lažna (maskirana). Parametri koji okidaju aktivnost, tako da smještaju komunikaciju malicioznog izvora u ništavno odredište, unaprijed su definirane i automatizirane. Sustav definira napad prikupljanjem zapisa sa nekoliko točaka u sustavu kao i analizu zapisa koji je u obliku uzorka produkcijskog prometa uzetog sa mrežnih uređaja.

Ključne riječi: *bgp, maliciozan mrežni promet, blokiranje napada sa Interneta.*

Abstract

Blocking malicious network traffic with black hole routing, based on the IP source address ona a point outside of the protected information on system, represents an effective and popular method for stoping malicious code because it saves process resources of information system network appliances. First of all, the goal is the relieving of the processing time and resources of network security components. Conditions that must be met may containa number of crucial parameters that define the attack. Stoping malicious sources is based on its source IP address which can be true or false (masked). The parameters that trigger activity are placing communication from malicious sources in null destination. The whole process is predefined and automated and defines the malicious traffic from several points in the system.

Keywords: *bgp, malicious network traffic, bgp black hole triggering*

1. Uvod

1. *Introduction*

IP komunikacija svojim razvojem poglavito na segmentu isporučenih brzina uskoro postaje jedinstven protokol za prijenos više tipova podataka kao što su tekstualni, video i govorni tipovi podataka. Unifikacijom komunikacijskog standarda na IP komunikaciju, Internet mreža kao mreža svih mreža je prožeta velikom količinom podataka koje je iz dana u dan nužno analizirati i opisivati. Zašto opisivati?
Količina prenošenih podataka je samo jedan od parametara i to kvantitativan, ali struktura samih podataka koju je nužno opisati kako bi se utvrdilo postoji li neka maliciozna aktivnost, koja je u stanju kompromitirati javno objavljene servise neke organizacije, a kasnije kao posljedicu kompromitirati i interne segmente informacijskog sustava predstavlja dodatan izazov. Prekomjerna količina pristiglih podataka

na ulaz informacijskog sustava ima za cilj uskraćivanje usluga koje sustav nudi na javnom IP adresnom području ili Internetu. Zašto je opasna prekomjerna količina?
Pružatelji Internet usluga danas u standardnoj ponudi imaju brzine pristupa Internetu koje prelaze 1 Gbps i dolaze do 10 Gbps, čak i kada govorimo o njihovim klijentima koji nisu registrirani kao pružatelji Internet usluga. Isporuka brzine najčešće prelazi i procesnu moć usmjernika u domeni samog klijenta ili su sami usmjernici na granici efektivne obrade paketa koja je jednaka nazivnoj brzini veze prema usmjernicima pružatelja usluga. Procesna moć se izražava u obradi paketa u sekundi (pps) na trećem sloju ISO OSI apstraktnog modela. Ukoliko je dolazni promet sa Interneta prema klijentu strukturiran kao DoS (eng. *Denial of Service*) ili DDoS (eng. *Distributed Denial of Service*) onda je cilj imati sustav koji će izvor takvog napada zaustaviti na točki izvan same domene sustava koji štiti i na taj način pomaknuti granicu obrane. Na taj način se štedi procesno vrijeme koje će imati prostora za obradu efektivnog prometa, a ujedno rasterećuje širinu potencijalnog komunikacijskog pojasa za sav budući efektivni promet koji može biti ostvaren preko klijentskih Internet usmjernika.
Važno je napomenuti da se efikasna obrana od DDoS napada ne može temeljiti samo na sustavu koji je ovdje opisan, jer iako je jedna od mjera obrane metodologija opisana u ovom radu, kao dodatak istoj su nužni algoritmi razvijeni za takvu vrstu napada kojih u trenutku pisanja ovog teksta ima otprilike 30, ali je za očekivati da će sa vremenom domišljatost kreatora takvih napada rasti a s time i njihov broj.

2. BGP usmjerivački protokol

2. *BGP routing protocol*

BGP (eng. *Border Gateway Protocol*) usmjernički protokol je protokol zadužen za povezivanje zasebnih usmjerničkih domena koje se identificiraju prema svojem zasebnom autonomnom sistemskom broju ASN (eng. *ASN - Autonomous System Number*). Kao i kod IPv4 i IPv6 adresiranja, definiranje ASN-ova je podijeljeno na privatno i javno numeriranje autonomnih sistema određeno od IANA (eng. *Internet Assigned Numbers Authority*) organizacije koja kasnije dodijeljuje lokalnim Internet organizacijama ili registrima (eng. *RIR – Regional Internet Registries*) određeni niz ASN brojeva [2].
ASN broj je u početku bio 16-bitni cijeli broj, ali porastom opsega Interneta-a je nadograđen na 32-bitni cijeli broj koji je nužan za početak konfiguracije BGP protokola. Tako je raspon brojeva od 1– 64,495 rezerviran za javno korištenje, dok je raspon brojeva od 64,512 – 65,534 rezerviran za privatno korištenje, te se kao i privatne IP adrese ne bi smjelo oglasiti prema Internetu jer će isto biti proglašeno kao ništavan promet. Ostali brojevi iz cijelog niza su rezervirani za unaprjeđenje protokola [2].
BGP usmjernički protokol koristi više mehanizama koji otklanjaju mogućnost pojave usmjerničkih petlji i po svom načinu rada spada u vektorske usmjerničke protokole. Trenutno korištena verzija BGP protokola je verzija 4 [2]. Razmjena BGP usmjerničkih poruka unutar istog ASN-a definira sam protokol kao interni BGP protokol ili iBGP (eng. *Interior Border Gateway Protocol*), dok razmjena poruka između usmjernika koji se nalaze u različitim ASN-ovima definira BGP protokol kao eksterni ili eBGP (eng. *Exterior Border Gateway Protocol*) protokol. Međusobna povezanost zasebnih usmjerničkih domena koje se nalaze iza javno dodijeljenih ASN-ova čini Internet, dok su politike usmjeravanja određenih javnih IP prefiksa dogovorene najboljim praksama prilikom uspostave eBGP susjedstva između ISP-ova (eng. *Internet Service Provider*) [2].
Utjecanje iBGP usmjerničkim porukama od strane pomoćnog usmjernika prema usmjerniku Internet pružatelja usluge u njegovoj ASN domeni je osnovni princip na kojem se temelji kasnije opisani model sustava. ASN domena pružatelja Internet usluge je poveznica prema svim ostalim ASN brojevima koji čine Internet.

3. Načelo okidanja bgp instrukcije

3. *Principle of tiggering bgp black hole routing*

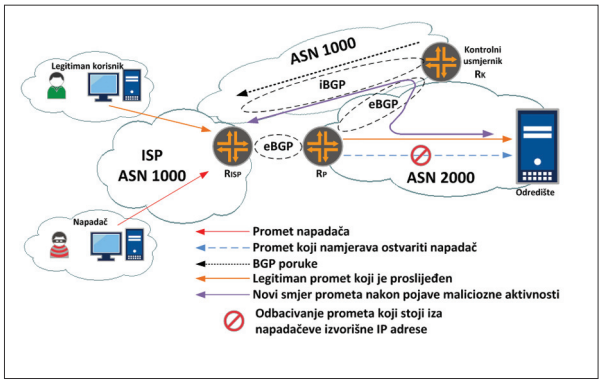
Osnovni koncept je da se izvorna IP adresa ili mreža malicioznog izvora sa Interneta kategorizira

kao ništavan promet okidanjem BGP (eng. *Border Gateway Protocol*) usmjerničke poruke prema usmjerniku pružatelja Internet usluge. Ista će dati instrukciju o preusmjeravanju malicioznog prometa na kontrolni usmjerivač i smještati ga u ništavno sučelje ili Null 0 sučelje [1].
U ostvarenju prethodnog su važna dva elementa u informacijskom sustavu klijenta, a to su produkcijski eBGP usmjernik (RP) i kontrolni eBGP/iBGP usmjernik (RK) od kojih kontrolni usmjernik ostvaruje iBGP vezu sa usmjernikom pružatelja Internet usluge jer se nalazi u istoj ASN domeni i eBGP vezu sa produkcijskim usmjernikom.
Kako bi zadovoljili prethodni scenarij, kontrolni usmjernik koji je u vlasništvu štićenog informacijskog sustava bi trebao biti u usmjerničkoj BGP domeni pružatelja Internet usluge, odnosno unutar njegovog ASN-a što i nije uobičajena praksa [1].
Uvjeti koji će generirati BGP okidač na kontrolnom usmjerniku moraju prije definirati malicioznu aktivnost, a onda izvršiti okidanje. Sama definicija dolazi iz jedne ili više točaka u sustavu ili može biti ručno definirana od strane administratora, odnosno unaprijed definiranim crnim listama sa popisom pojedinačnih IP adresa, mreža i DNS zapisima.
U trenutku t=0 kada se dogodi maliciozna aktivnost, do njezine potvrde od jedne ili više sigurnosnih točaka u sustavu će proći vrijeme t=0+t1 sa dodatkom vremena, dok kontrolni usmjernik ne zada instrukciju kroz BGP poruku, gdje će proći dodatno vrijeme t=0+t1+t2 kako bi sustav efektivno reagirao na prijetnju. Za to vrijeme će produkcijski usmjernik trošiti procesno vrijeme ujedno i zbog malicioznog prometa.
Instrukcija koja će se zadržati na kontrolnom usmjerniku može biti trajna ili sa vremenskim odmakom, što je u konačnici i preporučljivo jer se iza IP adrese sa malicioznom aktivnošću nakon nekog vremena može naći legitiman zahtjev, ukoliko uzmemo u obzir dinamičko dodjeljivanje adresa unutar pružatelja Internet usluge iz čijeg je ASN-a prvotno i došao maliciozan promet.
Eksplicitna zabrana prometa sa određenog izvora ili niza IP izvora sa Interneta je efektivna politika sigurnosti, čak i ako se uzme u obzir da iza jedne IP adrese koja čini maliciozne aktivnosti može stajati organizacija koja sadrži privatne adrese, odnosno računala koje nemaju maliciozni kod na sebi. Druga strana politike sigurnosti, a ujedno i ne toliko efektivna bi bila konstantna duboka inspekcija velikog broja paketa, gdje bi se konstantno vršilo odvajanje malicioznog podskupa prometa od cijelog ostatka legitimnog skupa prometa. Predmetni proces bi iznova trošio procesno vrijeme sigurnosnih točaka u informacijskom sustavu kao što su IPS (eng. *Intrusion Prevention System*) sustava kako bi se zadovoljila forma maksimalne dostupnosti informacijskog sustava.

4. Usmjeriteljski segmet

4. *Routing segment*

Spomenuto je već da se osnovni način rada temelji na slanju iBGP usmjerničke poruke na susjedni BGP usmjernik pružatelja Internet usluge, odnosno ISP.
Smještaj kontrolnog usmjernika u ASN domenu ISP-a je zbog efektivnog utjecaja na usmjerničke BGP informacije koje dolaze iz ASN domene ISP-a u ASN domenu štićenog informacijskog. Dakle, preko kontrolnog usmjernika se prosljeđuje usmjernička informacija u ASN ISP-a sa koje IP adrese ili mreže želimo spriječiti ostvarenje bilo kakvog prometa prema našem ASN-u.
U cijelom procesu nije cilj utjecati na ASN ISP-a tako da ista izvorišna IP adresa ili mreža ne može komunicirati sa nekim mrežnim entitetom unutar ASN-a ISP-a ili nekim mrežnim entitetom koji se nalazi u nekom drugom ASN-u, a nije ASN 2000. Takav scenarij ne bi dozvolio niti jedan ISP [1].



Slika 1 *Okidanje eBGP poruke kontrolnim usmjernikom*
Figure 1 *eBGP message trrigering with control router*

Okidač ili kontrolni usmjernik (RK) na slici 1, nakon inicirane kontrolne poruke koja je generirana po instrukciji sigurnosnih točaka u sustavu generira iBGP poruku, koja daje instrukciju ISP usmjerniku (RISP) da prema ASN 2000 zabrani maliciozan promet. U isto vrijeme kontrolni usmjernik šalje i eBGP poruku RP usmjerniku da je najbolji put do malicioznog izvora preko njega samoga, dok su sve destinacije prema Internetu iz ASN 2000 domene i dalje preko relacije RISP i RP usmjernika [3].

```
interface Loopback0
 ip address 195.25.25.10 255.255.255.255
!
router bgp 1000                                    (1)
 no synchronization
 bgp always-compare-med
 bgp log-neighbor-changes
 neighbor 89.249.99.10 remote-as 2000
 neighbor 89.249.99.10 ebgp-multihop 2
 neighbor 89.249.99.10 update-source Loopback0
 neighbor 89.249.99.10 route-map KLIJENT out       (2)
 neighbor 89.249.100.10 remote-as 1000
 neighbor 89.249.100.10 update-source Loopback0
 neighbor 89.249.100.10 route-reflector-client     (3)
 neighbor 89.249.100.10 next-hop-self
 no auto-summary
!
route-map KLIJENT permit 10                        (4)
 set metric 10                                     (5)
```

Primjer 1 *Konfiguracija RISP usmjernika*

Example 1 *RISP configuration*

Preporučljivo je da kontrolni usmjernik (RK) po svojim performansama bude jednak ili snažniji od RP usmjernika, jer su mogući scenariji da sav promet iz ASN 1000 ide prema ASN 2000 kroz RK usmjernik, odnosno moguće je da RK preuzme u potpunosti ulogu RP usmjernika [3]. Primjer 1 pokazuje konfiguraciju BGP usmjerničkog protokola na RISP usmjerniku s time da je važno napomenuti kako je konfiguracija funkcionalna samo na RISP – RK – RP relaciji u primjeru jer je razumljivo da usmjernik ISP-a u realnosti ima daleko kompleksniju konfiguraciju pošto ostvaruje mnogo eBGP susjedstva istovremeno. (1) naredba nalaže da usmjernik predstavlja ASN 1000, što je ujedno i inicijalizacija BGP usmjerničkog procesa. Naredba (2) i naredba (4) definiraju uvjetnu usmjerničku mapu sa MED (eng. *Multi-Exit Discriminator*) usmjerničkim parametrom prema RP usmjerniku sa vrijednošću 10 (5) [3].

MED vrijednost je izlazna BGP usmjernička metrika koja se tako i primjenjuje prema susjednom usmjerniku, preko koje u ovom slučaju RISP usmjernik određuje usmjerničku metriku svih javnih IP adresa sa Interneta prema RP usmjerniku, osim za javne IP adrese koje se nalaze u samoj ASN 2000 usmjerničkoj domeni. Postoji više BGP parametara koji određuju kako će se promet usmjeravati. Usporedba tih parametara daje konačnu odluku gdje će se paketi usmjeravati [3].

Svi parametri u BGP-u su lokalno važeći, odnosni lokalni usmjernik na temelju konfiguriranih usmjerničkih metrika određuje najbolji put, ali i kako će dolazne IP pakete proslijediti. Jedino je MED vrijednost, parametar kojim utječemo na susjedni usmjernik kako će isti donijeti odluku o usmjeravanju IP paketa. Tako i u ovom slučaju nalažemo RP usmjerniku preko RISP usmjernika da sav Internet promet vidi preko MED metrike 10, dok na isti RP usmjernik preko RK usmjernika utječemo da sav Internet promet "vidi" sa metrikom 20 [3].

Nakon ovoga, RK usmjernik Internet promet vidi sa dva svoja fizička komunikacijska sučelja, gdje sučelje X nalaže "vidljivost" Internet prometa sa metrikom 10 (preko RISP), a sučelje Y nalaže "vidljivost" Internet prometa sa metrikom 20 (preko RK, primjer 3). Ako je odluka definirana samo na MED vrijednostima (nema utjecaja ostalih BGP usmjerničkih parametara) onda će RP usmjernik odabrati sučelje sa nižom metrikom, što znači da će svi zahtjevi za Internet prometom iz ASN 2000 ići preko RIPS usmjernika. Naredba (3) primjera 1 nalaže da RISP usmjernik može utjecati na RISP usmjernik, što će kasnije biti nužno [3].

```
interface Loopback0
 ip address 89.249.99.10 255.255.255.255
!
router bgp 2000                                    (1)
 no synchronization
 bgp always-compare-med
 bgp log-neighbor-changes
 neighbor 89.249.100.10 remote-as 1000
 neighbor 89.249.100.10 ebgp-multihop 2
 neighbor 89.249.100.10 update-source Loopback0
 neighbor 195.25.25.10 remote-as 1000
 neighbor 195.25.25.10 ebgp-multihop 2
 neighbor 195.25.25.10 update-source Loopback0
 no auto-summary
```

Primjer 2 *Konfiguracija RP usmjernika*

Figure 2 *RP configuration*

Primjer 2 pokazuje konfiguraciju BGP usmjerničkog protokola na RP usmjerniku. Naredba (1) nalaže da usmjernik predstavlja ASN 2000. Osnovni cilj je da se na RP usmjerniku ne rade promjene na BGP parametrima ili na bilo kojim drugim usmjerničkim parametrima, već da se isto radi isključivo na RK usmjerniku. Iz toga razloga se i koristi MED usmjernički parametar kojim utječemo na usmjerničku odluku susjednog usmjernika, ili kada je riječ o BGP protokolu utječemo na udaljeni usmjernik jer BGP nije nužno PHB (eng. *Per-Hop Behavior*) usmjernički protokol, odnosno nije nužno da mrežna sučelja egzistiraju u istom mrežnom segmentu [2].
Primjerima 1 i 2 je ostvarena veza između RISP i RP koja u redovnim uvjetima (kada nema malicioznih aktivnosti) uvijek radi na istoj relaciji. RK usmjernik je u "hladnom" pogonu i jedini usmjernik na kojem se rade promjene konfiguracijskih usmjerničkih parametara kada to sigurnosne točke nalažu [3].
Primjer 3 pokazuje konfiguraciju BGP usmjerničkog protokola na RK usmjerniku. Naredba (2) nalaže da usmjernik predstavlja ASN 1000. Ništavno sučelje ili sučelje Null0 je sučelje koje ne predstavlja niti jedno funkcionalno komunikacijsko sučelje preko kojeg se može usmjeriti IP paket, odnosno ukoliko se usmjeri na predmetno sučelje, IP paket će biti odbačen. Null0 sučelje je definirano naredbom (1) [3].
U primjeru 3 je naredbom (4), (12) i (13) konfigurirana metrika prema RP usmjerniku sa vrijednošću 20 sa ciljem da RP uvijek odabire RISP usmjernik kao destinaciju prema cijelom Internet javnom prostoru. Ista relacija uključuje i povratni promet sa Interneta [3].
Naredbama od (5) do (10) je opisan set nepovoljnih BGP usmjerničkih parametara kroz usmjerničku mapu BLOK koja se primjenjuje na maliciozan IP izvor sa Interneta, dok naredba (11) osigurava da se usmjernička mapa BLOK ne bi primijenila za sav drugi promet, odnosno za promet koji nije maliciozan. U primjeru 3 mapa BLOK ne utječe trenutno na niti jednu destinaciju na Internetu [3].

```
interface Loopback0
 ip address 89.249.100.10 255.255.255.255
!
interface Null0                                              (1)
 no ip unreachables
!
router bgp 1000                                              (2)
 no synchronization
 bgp always-compare-med
 bgp log-neighbor-changes
 redistribute static route-map BLOK                          (3)
 neighbor 89.249.99.10 remote-as 2000
 neighbor 89.249.99.10 ebgp-multihop 2
 neighbor 89.249.99.10 update-source Loopback0
 neighbor 89.249.99.10 route-map MED-KONTROLNI out           (4)
 neighbor 195.25.25.10 remote-as 1000
 neighbor 195.25.25.10 ebgp-multihop 2
 neighbor 195.25.25.10 update-source Loopback0
 no auto-summary
!
route-map BLOK permit 10                                     (5)
 match tag 66                                                (6)
 set local-preference 200                                    (7)
 set origin igp                                              (8)
 set community no-export                                     (9)
 set ip next-hop 192.0.2.1                                   (10)
!
route-map BLOK deny 20                                       (11)
!
route-map MED-KONTROLNI permit 10                            (12)
 set metric 20                                               (13)
```

Primjer 3 *Konfiguracija RK usmjernika*

Example 3 *RK configuration*

	Network	Next Hop	Metric	LocPrf	Weight	Path
*	165.40.40.10/32	89.249.100.10	20		0	1000 3000 i
*>		195.25.25.10	10		0	1000 3000 i
*	185.30.30.10/32	89.249.100.10	20		0	1000 i
*>		195.25.25.10	10		0	1000 i

Primjer 4 Usmjernička informacija na RP u normalnom scenariju

Primjer 4 *Usmjernička informacija na RP u normalnom scenariju*

Example 4 *Routing table on RP in normal state*

Primjer 4 pokazuje usmjerničku tablicu RP usmjernika koja ukazuje da je najbolja metrika preko RISP usmjernika, što je ciljano stanje ukoliko nije došlo do okidanja malicioznim prometom [3].
Ukoliko za primjer definiramo da maliciozan promet dolazi sa IP izvorišta 165.40.40.10/32, onda je nužno spriječiti predmetni IP izvor aktiviranjem konfiguracijske skripte opisane u primjeru 5 [3].
Dakle primjer 5 identificira maliciozan izvor koji je definiran sa sigurnosnih točaka u sustavu koje su generirale samu skriptu prema RK usmjerniku [3].

```
ip route 165.40.40.10 255.255.255.255 null 0 tag 66          (1)
!
ip prefix-list MED-PREUS seq 5 permit 165.40.40.10/32        (2)
!
route-map MED-KONTROLNI permit 10                            (3)
match ip address prefix-list MED-PREUS                       (4)
set metric 5                                                 (5)
!
exit
!
exit
!
clear ip bgp 89.249.99.10 soft out                           (6)
```

Primjer 5 *Skripta sa instrukcijom prema RK za onemogućavanje prometa sa malicioznog izvora*

Example 5 *Script for RK for triggering black hole routing*

Naredba (1) statičkom rutom usmjerava IP izvorište u ništavno komunikacijsko sučelje RK usmjernika i označava ga numeracijskom oznakom 66. Oznaka 66 postaje važeća u okviru usmjerničke mape BLOK (5) na primjeru 3 koja je uvijek prisutna na RK usmjerniku i postaje također aktivna ukoliko ima identificiran IP promet, što je u ovom slučaju predmetni maliciozna izvor.

Mapa BLOK kasnije parametrima od (7) do (10) iz primjera 3 daje instrukciju RISP da maliciozan IP izvor usmjeri prema RK usmjerniku koji će kasnije biti proslijeđen na sučelje Null0 i neće uopće biti proslijeđeno RP usmjerniku. Predmetna instrukcija neće utjecati na ostale usmjernike koji komuniciraju prema malicioznom IP izvoru koji ostvaruju BGP susjedstvo sa ASN 1000 usmjerničkom domenom ili su dio iste domene [3]. Iako je mapa BLOK prisutna na RK usmjerniku ona nema nikakvu funkciju dok se na RK ne primijeni statička ruta koja ukazuje na Null0 sučelje i ne označi oznakom 66 kao što je to u primjeru 5 u naredbi (1). Primjer 5 prikazuje skriptu koja se primjenjuje na RK nakon što se identificira maliciozan izvor. Nakon primjene statičke rute naredbom (1) primjera 5, naredba (3) primjera 3 postaje funkcionalna na način da vrši redistribuciju statičke usmjerničke informacije u iBGP susjedstvo u RISP, usmjeravajući maliciozan izvor u Null0 sučelje i pritom pogoršavajući metrike usmjeravanja parametrima (7) i (8) kao na primjeru 3. Kako bi usmjeravanje odlaznog i dolaznog prometa iz ASN 2000 usmjerničke domene išlo samo prema malicioznom izvoru preko RK usmjernika, onda je nužno identificirati promet malicioznog izvora prefiks listom kao na primjeru 5, naredbom (2). U primjeru 5, naredbe (3), (4) i (5) mijenjaju parametre mape MED-KONTROLNI kako bi RK usmjernik samog sebe predstavio kao povoljnije komunikacijsko odredište za usmjeravanje prema malicioznom izvoru. Mapi MED-KONTROLNI se dodaje prefiks lista MED-PREUS koja filtrira, odnosno preusmjerava samo IP destinaciju malicioznog prometa prema RK usmjerniku, a ne i sav Internet promet. Nakon toga naredba (5) smanjuje MED vrijednost na 5 kako bi RK pružao povoljniji put u odnosu na RISP usmjernik [3]. BGP usmjernički protokol je nužno resetirati kako bi usmjernički proces između RK i RP usmjernika primijenio postavke sa skripte. Nakon resetiranja procesa na RK usmjerniku naredbom (6) kao na primjeru 5, RP usmjernik ima usmjerničku tablicu kao na primjeru 6 [3].

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 165.40.40.10/32	89.249.100.10	5	0		1000 3000 i
*	195.25.25.10	10	0		1000 3000 i
*> 185.30.30.10/32	195.25.25.10	10	0		1000 i

Primjer 6 *Usmjernička informacija na RP u slučaju blokiranja malicioznog izvora*

Example 6 *Routing table on RP when malicious traffic occure*

Iz primjera 6 je vidljivo da RP usmjernik za maliciozan izvor 165.40.40.10 odabire RK usmjernik. Neka skripta na primjeru 5 radi lakšeg snalaženja ima ime S1 i ona može biti uklonjena ukoliko se zamijeni skriptom S1(NO) kao na primjeru 7 [3].

```
no ip route 165.40.40.10 255.255.255.255 null 0 tag 66       (1)
!
no ip prefix-list MED-PREUS seq 5 permit 165.40.40.10/32     (2)
!
route-map MED-KONTROLNI permit 10
no match ip address prefix-list MED-PREUS                    (3)
set metric 20                                          ..... (4)
!
exit
!
exit
!
clear ip bgp 89.249.99.10 soft out                           (6)
```

Primjer 7 *Povlačenje skripte sa RK usmjernika*

Example 7 *Script revocation on RK router*

S1 skripta kao varijablu ima prefikse koji su izvori malicioznih napada. Predmetnih prefiksa može biti više od jednog. U skripti S1 varijabla

je i MED vrijednost koja se iz nepovoljnije više mijenja u povoljniju manju [3].

5. Cjeloviti model sustava

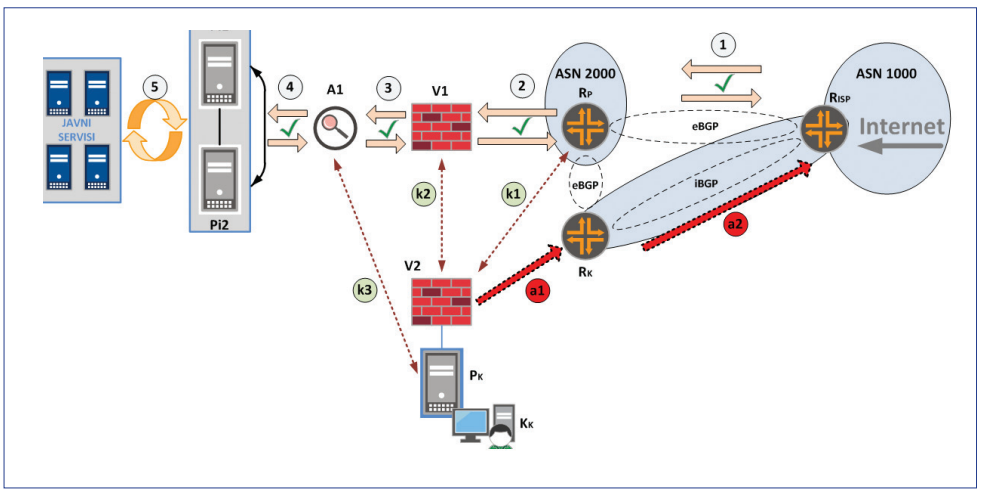
5. *Complete system model*

Prethodnim poglavljem je objašnjena tehnika udaljenog okidanja usmjeravanja bez odredišta (eng. *Remote Triggered Black Hole Routing*) [1]. U poglavlju 4 je tehnika prilagođena potrebama dalje opisanog sustava.
Okidanjem se djeluje na maliciozan napad, no prije djelovanja je nužno definirati nekakav promet kao maliciozan kako bi okidanje imalo svrhu.
Slika 2 prikazuje cjeloviti sustav sa svim svojim elementima i fazama prolaska IP paketa, dok on ne bude proglašen kao maliciozan.

Faze prolaska IP paketa:

1. Izvorište IP paketa je od ISP usmjernika, odnosno iz ASN 1000 usmjerničke domene.
2. Produkcijski usmjernik informacijskog sustava zaprima paket i prosljeđuje ga vatrozidu V1 koji je zadužen za zaštitu javnog IP adresnog prostora unutar ASN 2000.
3. Analizator prometa A1 je zadužen za prosljeđivanje kopije prometa prije nego li nastupi slijedeća faza.
4. IP paket stiže do distribucijskog bloka koji je zadužen za preraspodjelu TCP/UDP zahtjeva prema poslužiteljima javno oglašenih servisa unutar ASN 2000.
5. IP paket je raspodijeljen na odgovarajući poslužitelj temeljem algoritma kojim se služi distribucijski blok unutar informacijskog sustava.
6. Nakon što paket prođe kroz sve svoje faze, odnosno sigurnosne točke u sustavu, isti ostavi i svoj trag u obliku log poruka, sesijskog zapisa ili kao kopija prometa na drugom sloju ISO OSI modela.

Na temelju tragova su generirane kontrolne poruke od strane svih sigurnosnih točaka u sustavu za koje je važno napomenuti da su ujedno i komunikacijske točke sustava koje ostvaruju objavu servisa iz ASN 2000 prema cijelom Internetu.
Sve kontrolne poruke (k oznake) su u obliku TCP/UDP prometa, osim kontrolne poruke k3 koja je na drugom sloju ISO OSI modela kao pcap datoteka.
Kontrolne poruke su odaslane kontrolnom poslužitelju (PK) kroz vatrozid V2 koji ima ulogu zaštite samog poslužitelja, ali nije i komunikacijski element za objavu javnih servisa iz ASN 2000 prema Internetu. Jedino poruka k3 nije odaslana kontrolnom poslužitelju kroz V2 vatrozid,, već direktno na njegovo zasebno fizičko sučelje, pojedine kontrolne poruke su kombinacije neželjenih zapisa u obliku log poruka, pa tako se iste mogu primjerice definirati na slijedeći način:
k1 – zapisi dobiveni identificiranjem pristupnim listama na produkcijskom usmjerniku]RP).
k2 – zapisi dobiveni iz repozitorija odbačenog prometa na vatrozidu V1.
k3 – zapisi dobiveni sa analizatora A1 ili proslijeđeni kao kopija mrežnog prometa sa preklopnika.
Zapisi dobiveni u obliku kontrolne poruke k3 mogu već biti obrađeni od analizatora mrežnog prometa ili mogu biti poslane kao čista kopija prometa. U tom slučaju se analiza prometa radi na



Slika 2
Cjeloviti prikaz modela sustava za sprječavanje mrežnog malicioznog prometa blokiranjem izvora napada izvan štićenog informacijskog sustava

Figure 2
Complete view of system model for prevention malicious network traffic with black hole routing outside of protected information system

```
access-list 120 permit tcp any any fragments log
access-list 120 permit udp any any fragments log
access-list 120 permit icmp any any fragments log
access-list 120 permit ip any any fragments log
access-list 120 permit udp any any eq 1434 log

access-list 121 permit icmp any any ttl-exceeded log
access-list 121 permit icmp any any port-unreachable log
access-list 121 permit icmp any any echo-reply log
access-list 121 permit icmp any any echo log
access-list 121 permit icmp any any packet-too-big log

access-list 122 permit tcp any any eq 639 rst log
access-list 122 permit tcp any any eq bgp rst log
access-list 122 permit ip any any ttl lt 2 log
access-list 122 permit tcp any any syn log
```

Primjer 8 *Identificiranje i logiranje neželjenog prometa na RP*

Example 8 *Identification and logging malicious traffic*

```
iptables -N LOG
iptables -A INPUT -j LOG
iptables -A LOG -m limit --limit 10/sec -j LOG --log- prefix
"ACL-odbaceno: " --log-level 4
iptables -A LOG -j DROP
```

Primjer 9 *Arhiva malicioznog prometa*

Example 9 *Malicious traffic archive*

```
192.168.81.1.23 113.124.90.79.17564 0 0 49312 0 SYN_RCVD

192.168.81.1.23 21.230.247.14.28218 0 0 49312 0 SYN_RCVD

192.168.81.1.23 136.168.88.132.38859 0 0 49312 0 SYN_RCVD

192.168.81.1.23 5.112.17.14.5174 0 0 49312 0 SYN_RCVD

192.168.81.1.23 61.199.84.97.34557 0 0 49312 0 SYN_RCVD

192.168.81.1.23 152.193.254.8.29844 0 0 49312 0 SYN_RCVD

192.168.81.1.23 77.123.221.130.11851 0 0 49312 0 SYN_RCVD
```

Primjer 10 *Zapis proslijeđen kao kopija mrežnog prometa*

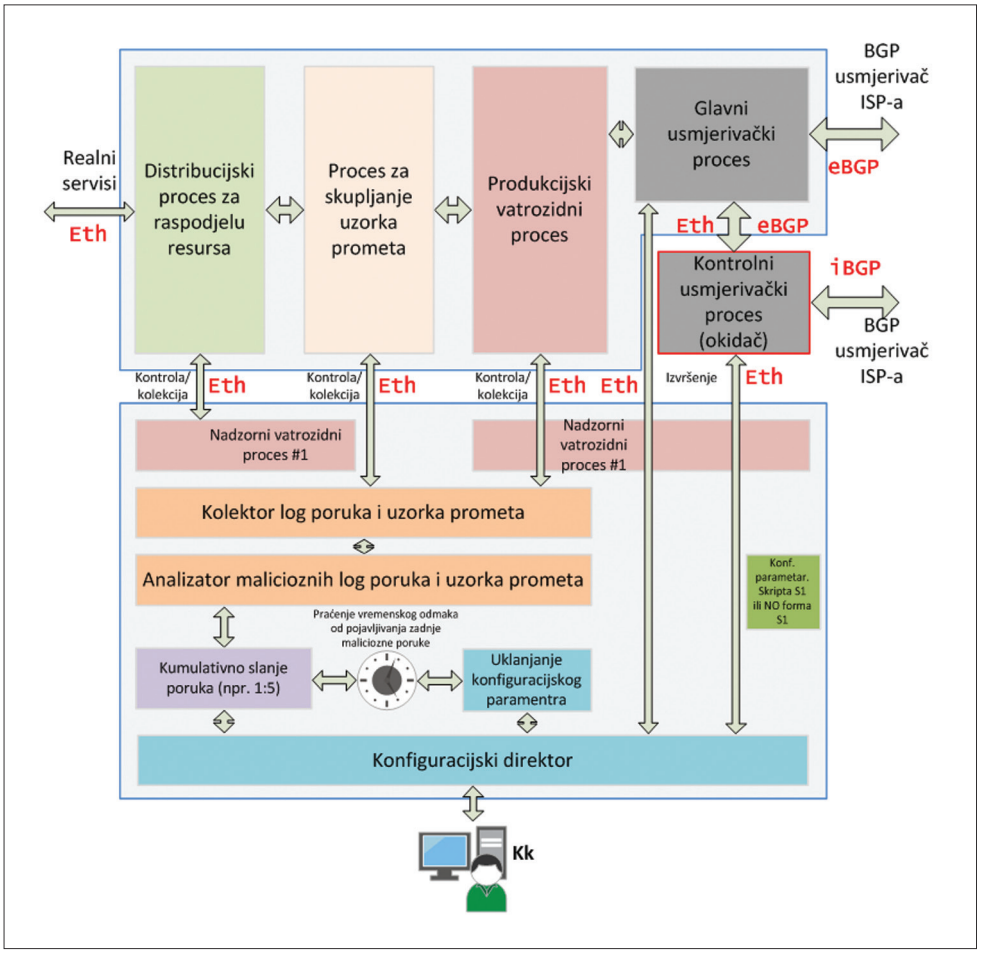
Example 10 *Forwaded log as network traffic copy*

kontrolnom poslužitelju koji će iz kopije prometa sa unaprijed definiranim potpisima definirati radi li se o malicioznom prometu ili ne.
a1 – akcija prema RK temeljena na kombinaciji poruka k1, k2, i k3 u obliku skripte S1.
a2 – akcija na RISP uzrokovana a1.
Osnovna kombinacija kontrolnih poruka je isključivo k1 OR k2 OR k3, odnosno kontrolni poslužitelj aktivira skriptu S1 ako samo i jedna kontrolna poruka opiše mrežni promet kao maliciozan. Hijerarhijski gledano, što dublje unutar informacijskog sustava generiramo kontrolne poruke sa sigurnosnih točaka to se one nalaze na višem nivou ISO OSI apstraktnog modela. Također to znači da je opis njihove malicioznosti teže definirati, ali je isti precizniji jer je prožet iscrpnijem heurističkom pristupu.
Dakle, poruka k1 generirana na RP i identificirana nekom naredbom iz primjera 8 sadrži osnovne informacije iz IP paketa koji su unaprijed definirani. Korisne informacije mogu biti fragmentirani paketi, paketi koji sa Interneta dolaze samo sa SYN zastavicom itd.
Poruka k2 već sadrži stanje sesije na višem sloju ISO OSI modela, pa su tako zastavice unutar TCP/UDP sesije detaljnije analizirane.
Poruka k3 daje slobodu u obliku analize pcap datoteka i samostalno definiranje opasnosti u mrežnom prometu. Također uz pomoć analizatora prometa koji već imaju unaprijed definirane maliciozne potpise, posao postaje jednostavniji ali i dalje analitički zahtjevan za administratora.
Osnovna komponenta svakog zapisa jest izvorišna adresa (SRC IP ADDR) koja se kao promjenjiva varijabla ugrađuje u S1 skriptu ili njezinu NO formu.

6. Procesi sustava

6. *System processes*

Procesi sustava su realizirani kao različite komponente, koje se kao jedinstveni procesi odvijaju na jednom sklopovlju ili više procesa koji se odvijaju na jednom sklopovlju kao što je kontrolni poslužitelj.
Blok shema je prikazana na slici 3, gdje su po principu modela prikazane relacije između procesa. Stabilnost sustava se pospješuje ukoliko je više procesa realizirano na zasebnom sklopolju. Ostvarenje veza između sklopovlja se ostvaruje Ethernet povezivanjem, brzinama 100 Mbps ili 1 Gbps.
Osnovni komunikacijski procesi su usmjerivački i vatrozidni procesi koji su realizirani na za to namijenjenim sklopovskim rješenjima različitih proizvođača.
Obrada poruka i njihovo arhiviranje je realizirano logging servisima. Sama obrada se izvršava sintaksnom analizom gdje se sintakse izdvajaju po ključnim riječima i kumulativnom pojavljivanju u jedinici vremena (najčešće je riječ o sekundama).
Konfiguracijski direktor ima unaprijed definiranu bazu pravila koja se uspoređuje sa izdvojenim ključnim riječima dobivenim sintaksnom



Slika 3
Blok shema relacija između procesa sustava

Figure 3
System porccess relations scheme

analizoma, te se prema tome aktivira skripta S1 sa implementiranom varijablom izvorišne IP adrese koja je također izdvojena kao zasebna sintaksa. Zapisi se analiziraju prihvatom syslog paketa kroz već standardizirani IP paket definiran UDP protokolom i komunikacijskim portom 514, definirano standardom RFC 3164.

7. Reference

7. *References*

[1] Cisco: "Remotely triggered black hole filtering—destination based and source based,", White Paper, San Jose, 2005, 37 stranica

[2] Jeff Doyle: "CCIE Professional Development Routing TCP/IP", Cisco Press,Indianapolis, 2005, 1026 stranica.

[3] Miroslav Tarbuk: "Laboratorijska ispitivanja", Zagreb, 2015

Stručni članak

AUTHOR · *AUTOR*

Miroslav Tarbuk

Na Tehničkom veleučilištu u Zagrebu 2005 godine je diplomirao na studiju elektrotehnike, a kasnije 2010 godine na specijalističkom studiju informatike.Trenutno je zaposlen u Financijskoj agenciji u Sektoru informatike u odjelu komunikacijsko-računalnih mreža. Zadužen je za razvoj mrežne okosnice Financijske agencije i HITRONet mreže, te za razvoj mrežne sigurnosti.
Od 2014 je izabran za nastavno zvanje asistenata na Tehničkom veleučilištu u Zagrebu na kolegiju Operacije i podrška nformacijskim sustavima.

Korespondencija:
mtarbuk@tvz.hr