In pratica

Applicazioni per la protezione delle reti con sinkhole IP fissi e ad eventi

Victor Oppleman

Grado di difficoltà

Una tecnica alquanto trascurata per la protezione delle reti si è dimostrata una delle difese più efficienti contro gli attacchi di tipo denial-of-service.

Questa tecnica è usata dagli Internet Service Provider di tutto il mondo per proteggere i loro clienti in ricezione. Come spiegheremo più avanti, questa tecnica conosciuta con il nome di sinkholing, può essere anche usata come modo intelligente per affrontare gli attacchi che minacciano una rete. Con l'implementazione dei sinkhole avrete un ulteriore modo per difendere la vostra rete e raccogliere informazioni valide sui pericoli e gli errori di configurazione della rete stessa.

Rivolto ad utenti esperti, questo articolo fornirà:

- informazioni e funzionalità dei sinkhole – una breve spiegazione dei sinkhole IP e di come molte organizzazioni sono riuscite ad implementarli con successo,
- uso di Decoy Network – la tecnica dei sinkhole con le darknet e le honeynet, le reti-esca che possono catturare e analizzare lo scanning da parte dei malware, i tentativi di infiltrazione ed altri eventi legati al monitoraggio della vostra rete, come la rilevazione delle intrusioni,
- protezione dai Denial-of-Service – il modo in cui le aziende e i loro Internet Service Provider in trasmissione sono riusciti a sviluppare un metodo di difesa contro gli attacchi denial-of-service attraverso l'ampio utilizzo di sinkhole guidati da eventi,
- backscatter e Traceback – una breve spiegazione dei backscatter e di come i traceback possono essere usati per identificare un punto di ingresso di un attacco di tipo denial-of-service in una grande rete.

Informazioni e funzionalità

In questo testo il termine sinkhole verrà usato per definire un modo per reindirizzare il traffico di rete IP per motivi di sicurezza, tra cui l'esecuzione di analisi dei dati e forense,

Dall'articolo imparerai...

- l'uso delle tecniche di sinkholing e come proteggersi dagli attacchi di tipo Denial of Service.

Cosa dovresti sapere...

- conoscenza base degli attacchi di tipo Denial of Service,
- argomenti legati al traffico di rete su lato ISP.

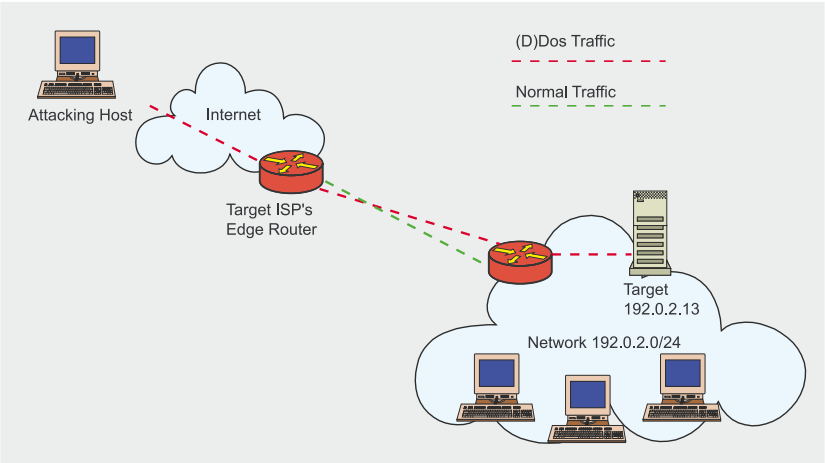

Fig. 1: *Un attacco all'indirizzo IP 192.0.2.13 (prima del sinkholing)*

la diversione di attacchi e la rilevazione di attività anomale. Gli ISP Tier-1 furono i primi a implementare i sinkhole, usati di solito per proteggere la clientela in ricezione. Da allora, questa tecnica è stata adottata per raccogliere informazioni riguardanti possibili attacchi alla rete e per la sicurezza della rete stessa. Per avere un'idea della forma più semplice di sinkhole, considerate il seguente esempio: traffico sospetto e disturbato originato da diverse reti è destinato alla rete 192.0.2.13, come mostrato nella Fig. 1. L'azienda colpita da questo traffico utilizza l'indirizzo di rete 192.0.2.0/24 che è instradato dal suo ISP. L'attacco diventa debilitante, interrompendo le operazioni dell'azienda ed aumentando potenzialmente i costi a causa del maggiore utilizzo di banda, quindi necessita di un'azione da parte dell'ISP poiché la grande quantità di traffico generato dall'attacco disturba anche i client adiacenti, come una sorta di effetto collaterale.

L'ISP reagisce e, sul momento, inizializza un sinkhole di tipo blackhole iniettando un route più specifico (192.0.2.13/32) all'interno del backbone dell'azienda colpita, il cui salto successivo (next-hop) è l'interfaccia scartata sul loro edge router (noto anche come null0 o *bit bucket*), come rappresentato dalla Fig. 2.

Questa tattica reindirizza il traffico verso il sinkhole dell'ISP invece di portarlo al destinatario originale. Il vantaggio è che, dal momento in cui il sinkhole entra in funzione, i client ISP adiacenti (se l'ISP ha implementato correttamente la protezione del sinkhole) sono probabilmente immuni da effetti collaterali e la vittima dell'attacco ha riacquistato l'uso della connessione Internet e l'accesso locale ai dispositivi. Sfortunatamente, l'indirizzo IP specifico (il dispositivo) sotto attacco non può comunicare con sistemi remoti attraverso Internet se prima il sinkhole non viene rimosso (presumibilmente dopo che l'attacco si è risolto). Ovviamente, i servizi originariamente forniti dal dispositivo di destinazione possono essere migrati verso un dispositivo alternativo ad un indirizzo IP diverso, ma sono necessarie altre considerazioni in termini di scadenza DNS TTL e cose del genere.

Quanto appena descritto è solo un esempio di sinkhole, di norma chiamato ISP-induced blackhole route, ma doverebbe aiutarvi a capire il concetto base ed introdurvi ai diversi usi dei sinkhole.

Uso dei sinkhole per le decoy network

Un altro modo per utilizzare i sinkhole è quello di impiegarli nelle reti usate per la cattura, l'esposizione e la raccolta dei dati, le cosiddette *decoy network*.

Decoy \De*coy"\, (esca, richiamo) n. Qualsiasi cosa con cui si attira in una trappola; richiamo per ingannare e portare verso un pericolo o un nemico; esca.

In questo articolo parleremo in dettaglio di due tipi di decoy network, cioè le darknet e le honeynet. Entrambe possono essere usate per raccogliere informazioni sulla sicurezza della rete, ma una di esse è particolarmente utile per lo sviluppo di reti sicure.

L'uso delle darknet

In genere, una darknet è una parte di uno spazio IP instradato ed assegnato in cui non ci sono servizi sensibili. Queste reti sono classificate come *dark*, cioè oscure, perché sembra che non ci sia niente di *acceso* al loro interno. Invece, una darknet contiene almeno un server, concepito per agire come *attira pacchetti*. Questo server raccoglie ed organizza i pacchetti che accedono alla darknet

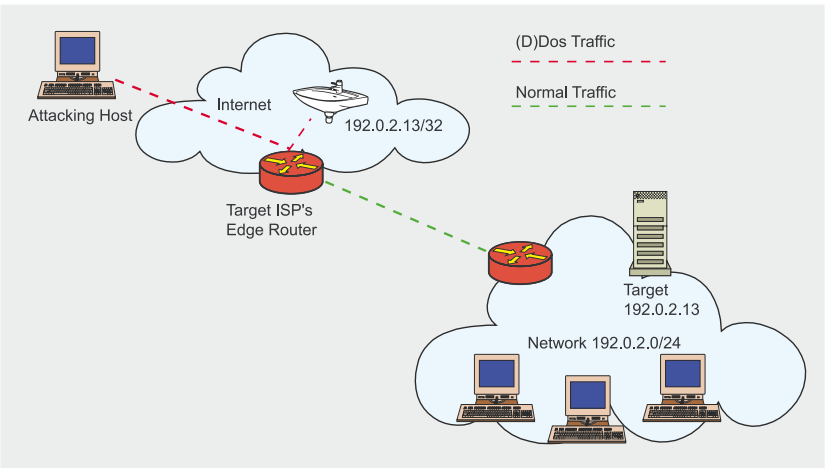

Fig. 2: *Un attacco all'indirizzo IP 192.0.2.13 (durante il sinkholing)*

Listing 1. *Esempio di una configurazione BGB*

```
router bgp XXX
redistribute static route-map static-to-bgp
# Route-map è un meccanismo per
# permettere la modifica di attributi di prefisso, o speciali
# politiche di filtraggio
route-map static-to-bgp permit 10
match tag 199
set ip next-hop 192.0.2.1
set local-preference 50
set community no-export
set origin igp
```

Listing 2. *La configurazione base del lato ISP*

```
router bgp XXX
# Route-map è semplicemente un meccanismo
# per inviare informazioni di routing come
# l'impostazione del salto successivo
neighbor < customer-ip > route-map customer-in in
# prefix-list è una lista statica di prefissi di clienti e nasconde le
                    lunghezze che
# sono accettate.  Il cliente dovrebbe essere in grado di
# annunciare un host singolo
# nel/i prefisso/i come 172.16.0.1/32
neighbor < customer-ip > prefix-list 10 in
# ebgp-multihop è necessario per evitare
# annunci di prefissi continui e
# ritiro di
neighbor < customer-ip > ebgp-multihop 2
# Adesso definiamo la route-map per la politica di corrispondenza
# e l'impostazione del blackhole
# salto successivo
route-map in-customer permit 5
# il cliente imposta questa community sul proprio lato,
# e l'ISP trova il corrispondente
# sul proprio lato.  XXXX  è probabilmente l'ASN del cliente,
# e NNNN è un numero arbitrario prestabilito
# da ISP e cliente
match ip community XXXX:NNNN
set ip next-hop < blackhole-ip>
set community additive no-export
```

e che sono usati per l'analisi in tempo reale, o forense post-eventi, della rete.

I pacchetti che entrano in una darknet sono inaspettati. Poiché una darknet non dovrebbe contenere pacchetti legittimi, la loro presenza indica una configurazione sbagliata della rete oppure, più comunemente, sono inviati da un malware. Questo malware, durante la ricerca di dispositivi vulnerabili, invia pacchetti alla darknet, esponendosi all'analisi di sicurezza. Con un pizzico di genio è possibile usare questa tecnica per cercare dei worm o altri malware propaganti. Senza falsi positivi e senza signature o analisi statiche complicate, un amministratore che usa correttamente una darknet è in grado di scoprire lo scanning (i tentativi fatti dal malware per scoprire host adiacenti su cui propagarsi) in una rete di qualsiasi dimensione. Questo è quello che si chiama uno strumento di sicurezza veramente efficace. Inoltre, i pacchetti che arrivano alla darknet mettono in evidenza eventuali errori di configurazione di reti innocue, che gli amministratori saranno lieti di correggere. Naturalmente, le darknet possono essere usate in diversi modi nell'ambito della sicurezza. Possono anche essere usate per ospitare flow collector, rilevatori di backscatter, packet sniffer e sistemi di rilevazione delle intrusioni. Il vantaggio delle darknet è che riducono notevolmente i falsi positivi per qualsiasi dispositivo o tecnologia attraverso una semplice riduzione del traffico.

L'implementazione di una darknet è abbastanza semplice. Di seguito vi forniamo cinque facili passi:

Selezionate una o più regioni non usate dello spazio di indirizzo IP della vostra rete, che invierete alla darknet. Potrebbe essere un prefisso /16 o superiore oppure un unico indirizzo (/32). Più alto è il numero degli indirizzi è più la vostra rete risulterà colpita da attività non sollecitata. Si raccomanda di selezionare diversi segmenti di indirizzi, come un /29 da ognuna delle diverse reti interne e un /25 dalla vostra rete pubblica (esterna). Potete anche inserire nella darknet una porzione dello spazio del vostro indirizzo privato (per esempio, spazio RFC 1918, 10.0.0.0/8). Infatti, selezionando le regioni della vostra rete interna verso la darkent, sarete in grado di vedere lo scanning interno che potreste non vedere se eseguite nelle darknet solo i segmenti di rete esterna (pubblica). Un'altra strategia che potrebbe rivelarsi utile per le aziende che utilizzano specifici routing per le loro reti interne è di affidarsi alla regola secondo cui *il route più specifico vince* (di solito distribuito attraverso un qualche tipo di protocollo gateway interno). In altre parole se si usano le reti 10.1.1.0/24 e 10.2.1.0/24 internamente, basta semplicemente instradare l'intera rete 10.0.0.0/8 nella darknet. Se la mia rete è configurata correttamente, la darknet riceverà tutto il traffico 10.0.0.0/8 ad eccezione delle reti in essa contenute che sto usando/instradando (queste hanno di solito voci di routing statiche nella mia infrastruttura di rete).

Successivamente, dovrete configurare la vostra topologia fisica. Avrete bisogno di un router o di uno switch (livello-3) che inoltrerà

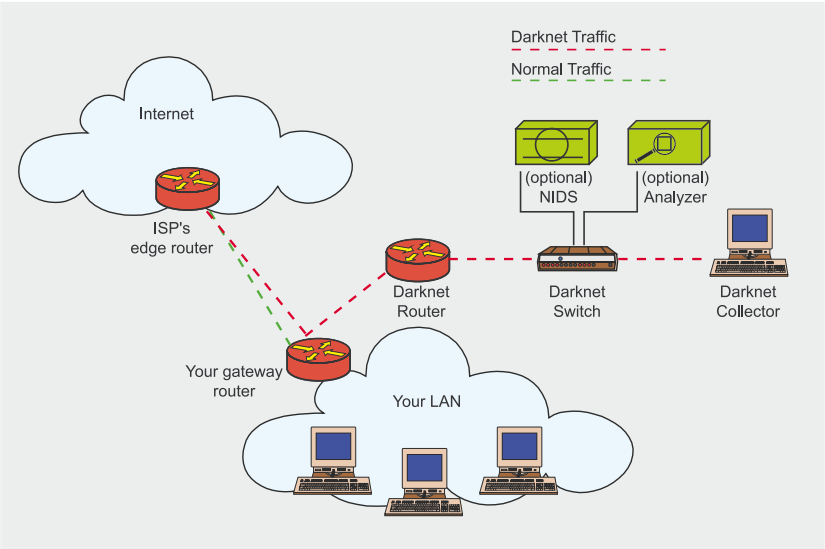

Fig. 3: *Un modello di topologia fisica per una darknet*

il traffico nella darknet, un server con un ampio archivio per raccogliere i dati e uno switch Ethernet che userete per collegare questi componenti, e quelli opzionali in seguito, tra cui un sensore IDS o un analizzatore di protocollo. Per il router potete decidere di usare un dispositivo gateway interno o esterno (o entrambi, anche se non lo consigliamo) — la maggior parte delle darknet *aziendali* (al contrario di quelle dei carrier delle telecom) sono posizionate all'interno di una delle DMZ di una organizzazione e separata dal resto della rete. Pertanto, potete pensare di usare un firewall al posto di uno dei vostri router. Tuttavia, raccomandiamo di usare il vostro router gateway esterno per darknet esterne e uno switch interno livello-3 per le darknet interne. In ogni caso, l'importante è configurare questo dispositivo router in modo da inoltrare il traffico per la darknet ricevuto al di fuori all'interfaccia ethernet della darknet (attraverso lo switch) verso il server di raccolta, che configurerete per accettare questi pacchetti. Per l'amministrazione, il server di raccolta richiederà almeno una interfaccia Ethernet aggiuntiva (da posizionare su una LAN separata). Assicuratevi di seguire tutte le migliori procedure per la sicurezza in modo da essere certi che i potenziali pericoli passeranno per questi segmenti di rete. Combattete la tentazione di usare uno switch DMZ per collegare queste componenti a meno che non abbiate dimestichezza nella configurazione di VLAN, in modo che nessun pacchetto broadcast possa accedere alla darknet — ricordate che la darknet è solo per traffico illegittimo quindi non vogliamo che dei braodcast legittimi provenienti da altre LAN invadano il territorio della darknet. La Fig. 3 mostra un esempio di questa configurazione. Nei nostri esempi, usiamo un router o uno switch che esegue un IOS Cisco con licenza software livello-3, un server FreeBSD e uno switch commodity unmanaged livello-2 per collegare i dispositivi.

Affinché il server di raccolta eviti di eseguire un ARP (address resolution protocol) per ciascun indirizzo nello spazio della darknet, configureremo il router per inoltrare il traffico destinato alla darknet ad un unico indirizzo finale IP sulla interfaccia Ethernet del server della darknet. Per eseguire questa operazione consigliamo di dedicare una rete /30 per la connessione punto a punto tra il router e l'interfaccia della darknet, come per esempio 192.0.2.0/30. Questo farà in modo che l'interfaccia Ethernet del vostro router sarà 192.0.2.1/30 e il server di raccolta potrà essere raggiunto attraverso 192.0.2.2/30. La configurazione dell'interfaccia dipende dalle piattaforme che avete selezionato, quindi diamo per scontato che siete in grado impostarla da soli. Nei nostri esempi, usiamo un IOS Cisco con un software con licenza livello-3. Fatto questo, dovrete semplicemente inserire i comandi di routing giusti allo switch per inoltrare tutto il traffico a 192.0.2.2 sul server di raccolta, e sarete salvi:

```
router#conf t
router(config)# ip route 10.0.0.0 ←
255.0.0.0 192.0.2.2
router(config)# ^Z
router# wr
```

A questo punto dovreste essere in grado di ricevere il traffico sulla darknet. Un esempio di topologia logica è raffigurato nella Fig. 4.

Cosa fare del traffico una volta raggiunta la darknet è un altro paio di maniche. Il server dovrebbe essere configurato per non rispondere ai dati che riceve sulla sua interfaccia darknet. Naturalmente, eseguirà un ARP per l'indirizzo configurato (solo 192.0.2.2/30) per stabilire le comunicazioni con il router, tuttavia tutti gli altri pacchetti dovrebbero essere rifiutati da un firewall basato sull'host. Come detto in precedenza, l'interfaccia della darknet non necessita di alcun tipo di gestione –per la gestione e l'amministrazione è necessario configurare un'altra interfaccia Ethernet. Il route di default per il sistema dovrebbe essere il gateway dell'interfaccia di amministrazione. Per il firewall, la scelta del server da parte della piattaforma influenzerà la scelta del firewall stesso, ma raccomandiamo di usare un sistema BSD e un firewall pf o ipfw2. Se abilitare o meno il logging del firewall dipende soprattutto da quello che ci farete. Usare strumenti per l'analisi del logfile richiede di abilitare il logging (in modo che i log possano essere analizzati e gli alert generati); tuttavia, a seconda degli hardware e/o software scelti e della dimensione della vostra darknet, questo

logging potrebbe nuocere gravemente alle prestazioni della darknet stessa. Come difesa aggiuntiva (i firewall possano bloccarsi o essere accidentalmente disabilitati), è buona norma effettuare un null-route del traffico della darknet, se questa non dovesse essere filtrata. Un esempio di null-route con FreeBSD potrebbe essere:

```
route add -net 10.0.0.0/8 ←
127.0.0.1 -blackhole
```

Adesso che la vostra darknet funziona e avete protetto il vostro server di raccolta, dovete memorizzare i dati in un formato che possa essere letto dai software di analisi dei dati e forense. La scelta più ovvia è di usare dei file binari formattati pcap essendo quasi onnipresenti poiché la maggior parte delle applicazioni di analisi funzionano con questi file. Il modo più semplice per eseguire questa operazione in modo continuativo è di usare la funzionalità di rotazione del programma tcpdump. Il programma tcpdump è fornito dal Network Research Group del Lawrence Berkeley National Laboratory. Una riga di comando del tcpdump per ottenere la rotazione del log è:

```
tcpdump -i en0 -n -w darknet_dump -C125
```

In questo esempio, il tcpdump deve ascoltare sull'interfaccia en0, la risoluzione DNS è disabilitata e un file chiamato `darknet_dumpN` viene scritto per ogni 125 milioni di byte usati, dove N aumenta per rendere il filename unico. Inoltre, questo genererà un file binario formattato pcap contenente il traffico di rete. Potete quindi usare questo file come input per il vostro software di analisi della rete. L'idea in questo caso è di tenere una copia dei dati per poter poi usare una marea di software diversi per rianalizzare i file in un secondo momento alla ricerca di caratteristiche interessanti nel traffico. In una situazione normale, userete un programma come tcpdump e una espressione BPF (Berkeley packet filter) per la vostra ricerca. Questa operazione può essere eseguita run-time (capture-time), mantenendo i dati di tutto il traffico potere poi usare software diversi, in un secondo momento, senza il rischio di perdere dati importanti.

Un altro software utile che facilita la visualizzazione dei flussi di traffico è argus, la rete Audit Record Generation e l'Utilization System sviluppato dalla QoSient. Anche se la sua configurazione è troppo lunga per essere descritta in dettaglio in questo articolo, utilizzeremo argus per osservare i flussi interessanti nelle nostre darknet. Argus fornisce un'interfaccia di riepilogo molto interessante, basata sul traffico, che dovrebbe aiutarvi a capire esattamente cosa succede in termini di traffico sospetto.

Per visualizzare il volume del traffico in entrata nella vostra darknet, i software basati su interfacce di monitoraggio come MRTG (vedere *http://www.mrtg.org/*) di Tobias Oetiker dovrebbero fare al vostro caso. MRTG può aiutarvi a produrre bellissime tabelle sul traffico nella darknet. Esistono anche una dozzina di strumenti per analizzare i log dei firewall che possono essere una alternativa rapida e facile agli strumenti di analisi più complessi basati su pcap o argus. Ma non dimenticate i problemi di prestazione con il logging basato sul testo, del filtraggio dei pacchetti e della successiva analisi di questi file.

Esistono letteralmente una dozzina di software che possono essere usati in una darknet. Per iniziare, ecco cosa troverete in alcuni dei nostri strumenti:

- un sensore IDS (Bro, Snort, et al.),
- uno sniffer dei pacchetti (tcpdump come descritto in precedenza),
- un analizzatore di flusso (argus, netflow export da router, SiLK, flow-tool),
- un parser per l'analisi del log del firewall che popola i database RRD per le tabelle,
- MRTG per rappresentare il traffico,
- p0f (di Michal Zalewski) per catalogare le piattaforme dei dispositivi infetti/in esecuzione.

L'uso delle honeynet

Come le darknet, le honeynet sono di solito una porzione di uno spazio IP assegnato ed instradato. Tuttavia, invece di fornire una destinazione a cui indirizzare i pacchetti, esse imitano un servizio reale (o più servizi), instaurando la connessione (handshake) e stabilendo una comunicazione a due-vie. Un *honeypot* è un sistema che imita il servizio ed è una valida risorsa che serve a spingere gli aggressori ad usarla e/o penetrarla. Benché esistono diversi tipi di honeypot, il loro scopo è sempre lo stesso: imparare le tecniche di attacco e raccogliere più informazioni possibili sull'aggressore.

Listing 3. *La configurazione base del lato cliente*

```
router bgp XXXX (ASN del cliente)
# il cliente installa un route statico,
# che viene ridistribuito nel BGP
# la route-map statica alla route static-to-bgp è ridistribuita
# proprio come l'ISP, usate una route-map per impostare
# e trovare il prefisso specifico equivalente e
# attribuito
route-map static-to-bgp permit 5
# condivisione del tag arbitrario,
# scelto dal cliente insieme all'ISP
match tag NNNN
set community additive XXX:NNNN
# NNNN è il tag, scelto dal cliente insieme all'ISP
ip route 192.168.0.1 255.255.255.255 Null0 tag NNNN
```

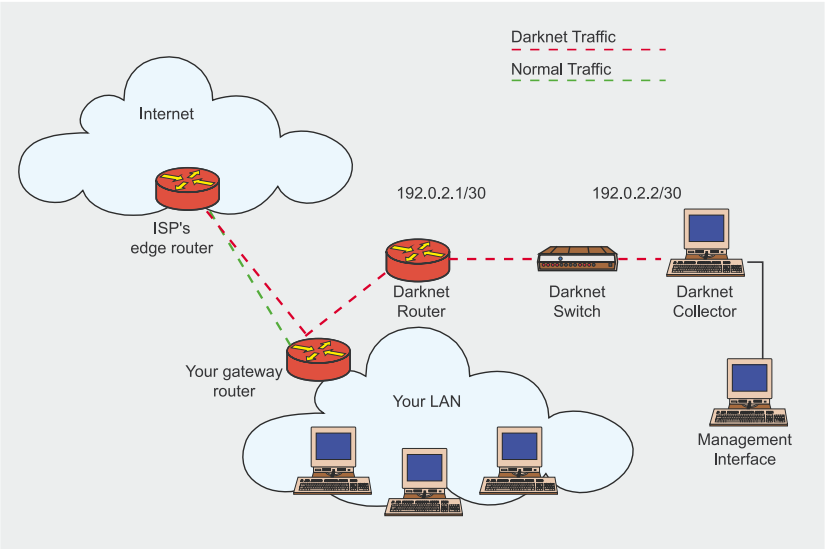

Fig. 4: *Un modello di una topologia logica per una darknet*

Gli honeypot fisici

Gli honeypot fisici sono macchine all'interno di una honeynet con un proprio indirizzo IP, sistema operativo e software che servono a imitare diversi servizi.

Gli honeypot virtuali

Gli honeypot virtuali sono sistemi *software-simulated* all'interno di una honeynet che imitano un ambiente di rete inclusi il sistema operativo, la pila della rete e i servizi forniti come esche. Un server fisico può contenere una rete di migliaia di honeypot virtuali.

Gli honeypot a bassa interazione

Gli honeypot a bassa interazione (il tipo più usato) sono concepiti per spingere un aggressore a credere in una o più vulnerabilità, stabilire una comunicazione e catturare i primi pacchetti della comunicazione con l'aggressore. Ovviamente, prima o poi l'aggressore o il malware che comunicano con l'honeypot capiranno il trucco, ma prima di allora, riveleranno alcune informazioni valide, come la tattica di attacco o la signature del malware. Gli honeypot a bassa interazione sono usati oggi per emulare le tattiche degli spammer (tentando di ottenere dati come la tempistica delle transazioni SMTP, per esempio).

In genere esistono pochi honeypot a pagamento, e lo strumento più popolare è un progetto open source chiamato honeyd di Niels Provos. Per maggiori informazioni su come acquistare e installare honeyd andate su *http://www.honeyd.org*.

Consiglio: honeyd è concepito per essere un honeypot/honeynet virtuale in grado di emulare una serie di sistemi operativi e componenti software per attirare gli aggressori.

Un'altra interessante forma di honeypot a bassa interazione è un nuovo tool creato da Tom Liston chiamato LaBrea. LaBrea (dal nome del tar pit) è un demone (servizio) in grado di generare risposte autonome alle richieste di connessione attraverso blocchi di indirizzi IP potenzialmente enormi. In breve, esso crea un ambiente che attira malware per lo scanning/propagazione di virus, ma con un trucco interessante. Appena il malware cerca di collegarsi alla vittima, LaBrea rallenta la pila della rete del mittente, a volte in modo notevole. In senso lato, la pila di rete del sistema infetto dal malware rimane bloccato in un tar pit. Pertanto, non c'è interazione a livello di applicazione, ma c'è un'interazione notevole a livello 4, quando si hanno i tentativi di connessione handshake (TCP). LaBrea è anche in grado di eseguire un ARP su tutti gli indirizzi IP virtuali nella sua configurazione senza assegnarli alle interface del sistema host rendendo la sua implementazione estremamente facile. Per maggior informazioni su LaBrea visitate il sito *http://labrea.sourceforge.net/labrea-info.html*.

Nota bene: Molti enti di ricerca hanno calcolato che gli honeypot a bassa interazione sono una valida tattica contro i worm propagatori, rallentandoli e proteggendo l'infrastruttura di rete. Riteniamo che la configurazione richiesta per ottenere questo vantaggio sia molto semplice. LaBrea e honeyd possono essere entrambi configurati per creare un ambiente adatto a combattere la propagazione di worm.

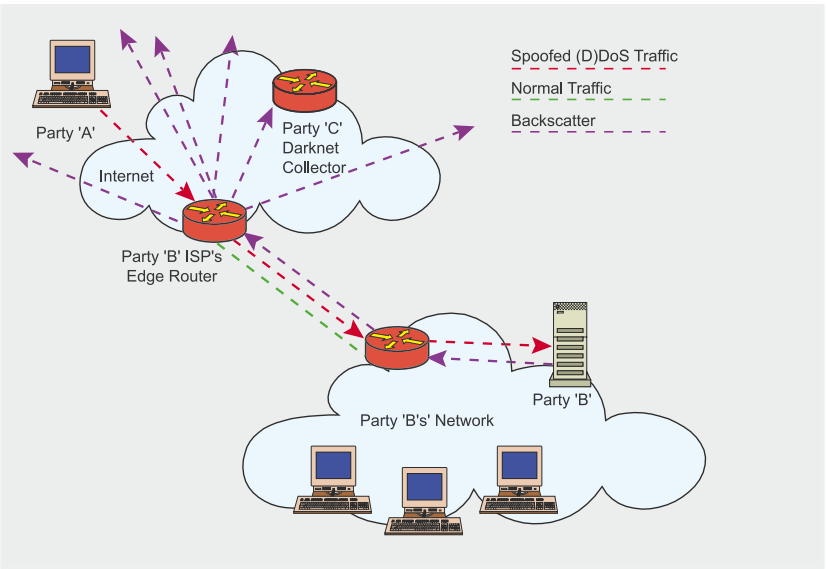

Fig. 5: *Un esempio di backscatter durante un attacco DDoS*

Gli honeypot ad alta interazione

Gli honeypot ad alta interazione sono meno usati, ma eccezionalmente preziosi. Invece di catturare semplicemente le prime transazioni di un dialogo tra l'aggressore e un honeypot, un honeypot ad alta interazione lascia che l'attacco penetri completamente il sistema su cui risiede. In questo caso, le informazioni utili catturate non includeranno solo la tecnica di penetrazione e l'attacco usato, ma permetterà all'amministratore di osservare l'aggressore una volta conquistato l'accesso al sistema, esponendone involontariamente intenzioni e strumenti.

Esiste una organizzazione no-profit nota come The Honeynet Project (vedere *http://www.honeynet.org/*) che sviluppa molte idee ed alcuni strumenti facili da usare per permettere agli utenti di usare honeypot ad alta interazione. Inoltre, i suoi membri forniscono strumenti eccellenti per l'analisi forense con cui studiare i dati raccolti durante le penetrazioni negli honeypot.

Consiglio: The Honeynet Project (*http://www.honeynet.org/*) pubblica una serie di tool fantastici per le honeynet. Raccomandiamo in particolar modo Honeywall, Termlog e Sebek. Inoltre, il team del progetto ha anche redatto un ottimo libro sulla psicologia, le tecniche e gli strumenti per attirare gli aggressori nelle honeynet. Il libro, *Conosci il tuo nemico,* attualmente alla seconda edizione, è disponibile sul sito *honeynet.org* e i ricavi delle vendite sono devoluti alla ricerca sulle honeynet.

Raccomandazione sull'uso delle honeynet

Per gli istituti di ricerca o per coloro che hanno molto tempo e denaro a disposizione (ne conoscete?), gli honeypot possono essere uno strumento inestimabile, ma non raccomandiamo l'utilizzo di honeypot all'interno di un'azienda per le attività quotidiane. Tuttavia, anche se inadatto per l'uso quotidiano, quando un software potenzialmente dannoso si fa sentire e nessuno sniffer o software di analisi forense riesce a identificare il problema come farebbe il vostro amministratore, potete implementare una honeynet specifica tesa a stabilire una connessione avendocome vittima il software dannoso, ottenendo quindi abbastanza informazioni per identificare adeguatamente l'aggressore. Un altro uso a richiesta, è l'impiego come mezzo per verificare una infiltrazione sospetta, risultando una ulteriore freccia all'arco dell'amministratore del sistema.

Una implementazione che vale la pena menzionare è quella usata da uno dei produttori di chip più importanti del mondo. La loro rete è munita di un server Linux che esegue VMWare su cui girano quattro macchine virtuali, una per ogni versione di OS Windows usata – NT, 2000, 2003, e XP. Ogni server è aggiornato con diverse patch dell'azienda. Gli OS Linux controllano il traffico e le modifiche, come mezzo per rilevare i worm (o altre minacce) che possono circolare all'interno dell'azienda. In sostanza usano l'ambiente come una combinazione di honeynet e IDS per i worm. Per maggior dettagli su questa implementazione visitate il sito *http://phoenixinfragard.net/meetings/past/200407hawrylkiw.pdf*

Implementazione di sinkhole per difendersi dagli attacchi DDoS (Blackhole Routing)

I sinkhole possono anche essere usati per difendersi dagli attacchi di tipo denial-of-service distribuiti (DDoS). Nella sezione *Informazioni e funzionalità* di questo articolo, il primo esempio presentato era la forma più semplice della tecnica di blackhole routing. Una volta identificata la vittima dell'attacco, l'indirizzo IP da colpire veniva deviato verso un'interfaccia scartata ai margini della rete, prima di attraversare l'ultimo collegamento della vittima. Questa operazione libera la rete da una totale rottura dovuta alla saturazione del collegamento, ma influenza le prestazioni di tutta la rete, soprattutto per client adiacenti che condividono parte della topologia del carrier. Oggi, i carrier delle grandi telecom hanno strutturato la loro architettura includendo versioni sofisticate di questo tipo di protezione come parte integrante della loro rete. In molti casi, i carrier adesso sono in grado di usare una tecnica traceback per posizionare i punti di ingresso dell'attacco e inviarli nel blackhole (nei punti di ingresso stessi) invece di permettere all'attacco di ostruire il backbone del carrier in tutta la rete. Tale tecnica di traceback è del tutto inutile, perché i route blackhole dei carrier sono di solito annunciati a livello di rete tra gli edge router, attraverso la community BGP, è quindi implementare un blackhole ad ogni punto di ingresso dove inviare il traffico infetto, neutralizzando gli attacchi al loro ingresso e (in molti casi) evitando i backbone e la congestione degli edge. Alcuni hanno esteso il controllo e l'automazione di questa abilità al cliente finale, attraverso quello che è conosciuto con il nome di customer-triggered real-time blackhole.

Triggered blackhole routing

Come detto in precedenza, molti grandi ISP hanno implementato un sistema distribuito e automatico per *lanciare* l'instradamento dei blackhole sugli indirizzi IP di interesse. Il trigger potrebbe essere lanciato dall'ISP o dai clienti, sia manualmente che in modo automatico. La tecnica del triggered blackhole routing utilizza il sinkhole descritto nella sezione *Informazioni e funzionalità*. Il sinkhole potrebbe essere configurato su tutti i router di ingresso (edge) nella rete ISP dove gli ISP scambiano il traffico con altri provider o clienti. Quando viene identificato un attacco contro la sua rete, l'ISP o il cliente può annunciare il prefisso *attaccato* (o un prefisso più specifico) nella tabella di routing BGP. Il prefisso attaccato viene etichettato con un

Tabella 1. *Pacchetti ICMP*

Pacchetti ICMP	Descrizione
3.0	Rete irraggiungibile
3.1	Host irraggiungibile
3.3	Porta irraggiungibile
3.4	Richiesta frammentazione
3.5	Route a sorgente non esatta
3.6	Rete di destinazione sconosciuta
3.7	Host di destinazione sconosciuta
3.10	Accesso all'host negato
3.11	Servizio di rete irraggiungibile
3.12	Servizio di host irraggiungibile
3.13	Comunicazione negata
11.0	TTL scaduto durante transito
11.1	Riassemblaggio del frammento scaduto

Pacchetti TCP	Descrizione
bit set RST	Resettaggio TCP

next-hop che è instradato statisticamente all'interfaccia rifiutata su tutti gli edge router e propagato nella rete dell'ISP attraverso un BGP interno (iBGP). Poi, quando i pacchetti destinati al prefisso attaccato entrano nella rete ISP (attraverso il punto di ingresso), essi sono immediatamente inviati all'interfaccia rifiutata sul router più vicino annunciando il prefisso attaccato.

Affinché l'ISP possa implementare il meccanismo di blackhole distribuito sono necessari i seguenti passi:

- selezionare un prefisso non instradato a livello globale, come Test-Net (RFC 3330) 192.0.2.0/24, per usarlo come salto successo di qualsiasi prefisso attaccato da inviare al blackhole. Con un prefisso di lunghezza 24 è possibile usare diversi tipi di indirizzi IP per tipi specifici di blackhole routing. È possibile distinguere tra blackhole route interni, esterni o dei clienti,
- configurare un route statico di ogni router di ingresso/condiviso per 192.0.2.0/24, puntando alla interfaccia rifiutata. Per esempio: `ip route 192.0.2.0 255.255.255.0 Null0`,
- configurare la politica BGP e route-map per annunciare un prefisso da inviare al blackhole come raffigurato nel Listing 1.

Nella configurazione di esempio, distribuiremo i route statici in BGP che combaciano con la *tag 199* (vedere di seguito), impostando il salto successivo ad un indirizzo IP che è instradato all'interfaccia rifiutata, impostando la preferenza locale a 50 (meno preferito), e assicurandosi di non mostrare questi route a nessuno dei nostri peer esterni (no-export).

Una volta terminata questa configurazione base, il trigger può essere lanciato dall'ISP che entra in un route statico per il prefisso attaccato (o host) da inviare al blackhole, per esempio:

```
ip route 172.16.0.1 255.255.255.255
192.0.2.1 Null0 tag 199
```

Il route statico di prima è il *trigger* che dà il via al processo di blackhole routing. Il router su cui è configurato il route annuncerà il route attraverso iBGP a tuti i router interni, inclusi gli edge router. Qualsiasi router con un route statico alla interfaccia rifiutata per 172.16.0.1/32 eseguirà a livello locale un blackhole sul traffico.

L'ISP potrebbe anche impostare un trigger automatico attraverso BGP, quindi un cliente BGP potrebbe lanciare un blackhole route senza l'intervento dell'ISP. Questo è l'aspetto più potente della tecnica di triggered blackhole routing. La configurazione del lato ISP è leggermente diversa nel senso che le community e le ebgp-multihop sono abituati a ricevere e etichettare in modo corretto i route ricevuti dai clienti. La configurazione base del lato ISP è raffigurata nel Listing 2.

L'ISP ha già un < *blackhole-ip* > instradato staticamente per rifiutare le interfacce attraverso la rete quindi, appena il cliente annuncia il prefisso al blackhole, l'ISP lo ridistribuisce internamente e il traffico verso questo prefisso viene inviato al blackhole ai *margini* della rete ISP.

La configurazione di base è raffigurata nel Listing 3.

Una volta sistemata la configurazione BGP, il cliente deve solo installare un route statico per il prefisso attaccato. Con una semplicissima configurazione in BGP e l'aiuto dell'ISP, adesso avete un metodo molto veloce per rispondere agli attacchi denial-of-service contro un unico host, o un intero prefisso.

Nota bene: Assicuratevi di verificare con il vostro contatto tecnico ISP prima di implementare la soluzione blackhole-triggering poiché le interpretazioni dei vari ISP di questo concetto variano da operatore a operatore.

Backscatter e traceback

In questa sezione, esploreremo gli usi più comuni delle reti decoy per scoprire i vari tipi di attacchi e tecniche di spoofing, nonché il modo per stanare i malintenzionati.

I backscatter

Dopo aver parlato ampiamente di decoy network e di attacchi DDoS, è opportuno introdurre il concetto di backscatter. Durante un intero semestre del primo anno di università, ho scritto lettere (ebbene sì, lettere su carta) ai miei amici che avevano l'abitudine di cambiare spesso domicilio. Da persona distratta quale sono, continuavo a sbagliare l'indirizzo del mittente sulla busta. Dimenticavo sempre di mettere il numero di camera oppure era totalmente illeggibile (avevo da poco scoperto la birra). Poi, quando un amico si trasferiva, la lettera che gli avevo inviato ritornava indietro con una nota dell'ufficio postale *rispedire al mittente*. L'unico problema era il mio indirizzo sbagliato, quindi non ricevevo la lettera direttamente ma arrivava prima alla portineria, che mi cercava (dal nome sulla lettera) e mi informava che la lettera che avevo spedito era ritornata indietro e che avevo sbagliato lindirizzo. Il meccanismo *rispedire al mittente* è una forma di backscatter. Ovviamente, il backscatter in portineria indicava che avevo inviato una lettera (e a chi).

In Internet, quando A intende eseguire un attacco di tipo denial-of-service contro B, ma senza rivelare la propria identità, di solito scrive sui pacchetti un indirizzo di origine sbagliato (le intestazioni IP sono alterate per sembrare provenire, per esempio, da A-Z solo che A-Z in Ipv4 ha 2^{32} permutazioni). Durante questi attacchi, i router e gli altri dispositivi di rete lungo il cammino inevitabilmente inviano una varietà di messaggi di errore che notificano su interruzioni di rete, richieste di quench oppure notifiche di irraggiungibilità. Poiché questi messaggi sono di tipo *rispedire al mittente* e poiché il mittente è alterato, A-Z li riceveranno tutti e scopriranno che B sta subendo un attacco, così come la portineria aveva scoperto che avevo inviato una lettera. Questo processo è raffigurato nel Listing 5.

Oggi, nel filtraggio dei pacchetti, la maggior parte di questi messaggi backscatter sono silenziosamente rifiutati dai firewall perché vengono visti come risposte a messaggi non inviati. Ma con l'implementazione di una darknet esterna, possiamo cercare questi pacchetti backscatter e determinare quando il nostro

Tabella 2. *Scheda riepilogativa*

Passo	Descrizione
Capire in che modo il vostro ISP può aiutarvi durante un attacco di tipo DDoS.	Preparate un piano d'azione su come gestire gli attacchi DDoS che comprenda strategie per verificare le abilità del vostro ISP nell'ambito di real-time blackholing. Stabilite un contatto tra la vostra azienda e il vostro ISP su come creare un customer-triggered real-time blackhole per proteggervi senza sprecare tempo prezioso e denaro.
Considerare l'implementazione di una darknet interna.	Ricordate che una darknet interna vi offre la possibilità di catturare worm prima di un anti-virus. Inoltre mette in evidenza eventuali errori di configurazione della rete, che sarete felici di correggere.
Considerare l'implementazione di una darknet esterna.	Le darknet esterne possono offrivi una panoramica di quello che colpisce la vostra rete dall'esterno e gli strumenti usati possono essere più facili da vedere rispetto ad un firewall normale. Il backscatter raccolto da una darknet esterna può offrivi informazioni sul momento in cui la vostra rete viene attaccata da un malintenzionato.
Esplorare la rete con degli honeypot se disponete di tempo e risorse necessarie.	Anche se molte aziende non vedranno i vantaggi nell'implementazione di una honeynet (a parte quello della consapevolezza dell'attività della rete), esse sono preziosissime per la ricerca di informazioni sulla sicurezza della rete. Considerate le implicazioni legate all'uso di una honeynet nella vostra azienda. Non dimenticate di tenere in considerazione la legislazione in materia per aiutarvi nella vostra decisione.

In Rete

- *http://www.amazon.com/gp/product/0072259558/* – Extreme Exploits: Advanced Defenses against Hardcore Hacks, pubblicato da McGraw-Hill/Osborne Copyright 2005,
- Internet RFC 3330 (Indirizzi Ipv4 speciali) e 3882 (Configurazione di BGP per bloccare attacchi Denial of Service),
- *http://www.cymru.com/Darknet/* – il team del Cymru Darknet Project,
- *http://www.tcpdump.org/* – il sito di tcpdump e libpcap,
- *http://www.qosient.com/argus/flow.htm* – il sito di ARGUS,
- *http://www.honeyd.org* – il sito di Honeyd,
- *http://www.honeynet.org* – il sito di HoneyNet Project,
- *http://lcamtuf.coredump.cx/p0f.shtml* – il sito di p0f,
- *http://www.secsup.org/Tracking/* – l'articolo di Chris Morrow e Brian Gemberling sull'analisi di ISP blackholing e backscatter,
- *http://phoenixinfragard.net/meetings/past/200407hawrylkiw.pdf* – la presentazione di Dan Hawrylkiw sulle honeynet,
- *http://www.openbsd.org/faq/pf/* – le FAQ sul filtro del pacchetto OpenBSD.

Cenni sull'autore

Oppleman è un noto autore, conferenziere e professore di sicurezza informatica e consulente in molte delle aziende più rinomate del mondo. Il software open source di Oppleman è stato distribuito in centinaia di migliaia di computer in tutto il mondo e possiede brevetti per quanto riguarda applicazioni per il routing adattivo distribuito e consumer wireless. Parte del contenuto di questo articolo è stato estratto dal libro pubblicato da Oppleman intitolato *Extreme Exploits: Advanced Defenses Against Hardcore Hacks* edito dalla McGraw-Hill/Osborne (Copyright 2005) e disponibile nelle migliori librerie.

spazio di indirizzo è attaccato da un malintenzionato. I seguenti tipi di pacchetto in una darknet possono essere classificati come backscatter e indicano che il vostro spazio di indirizzo (darknet) sta subendo un attacco:

Traceback

Adesso che siamo riusciti a gestire un backscatter, come possiamo usarlo? In una rete con molti Internet gateway, potrebbero rivelarsi utili per localizzare il punto di ingresso dei *pacchetti cattivi* contenenti l'attacco. Questa tecnica, conosciuta con il nome di *traceback*, è utile perché una volta identificato il punto di ingresso della nostra rete (o del nostro ISP), possiamo abbandonare il traffico e ridurre il carico sui nostri collegamenti, facendo passare anche traffico *buono* (attraverso gateway alternativi), al contrario della tattica più semplice della protezione da DDoS blackhole discusso prima. Il traceback ci consente di utilizzare il backscatter raccolto nella darknet per trovare i punti in cui l'attacco entra nella rete. Sfortunatamente, questa tecnica è valida solo per ISP o per reti di dati di grande portata e con molti gateway Internet. Alcuni software annessi includono l'uso di meccanismi di difesa di blackhole su *ogni* gateway Internet. Poiché questa procedura è usata dai principali ISP e da molte reti aziendali, è necessario spiegare almeno come funziona.

Supponiamo di avere impostato la rete come prima, a questo punto possiamo eseguire un traceback nel mezzo di un attacco di tipo denial-of-service in tre facili passi:

- identificare il target e verificare che il traffico che sta subendo l'attacco sia alterato (in caso contrario, il traceback sarà inutile),
- eseguire un blackhole del route per gli host specifici (possibilmente /32) che subiscono l'attacco su ogni gateway. Siate cauti e seguite le procedure più sicure per quanto riguarda l'invio di interfacce, rifiutate invece di usare i filtri di pacchetti per evitare i pacchetti con l'attacco. Questa operazione di blackhole porterà il gateway router a generare messaggi di tipo ICMP non raggiungibile che vengono rispediti (o almeno cercano di essere rispediti) alla fonte alterata dei pacchetti con l'attacco,
- all'interno delle darknet, usate i tool per cercare il traffico backscatter (probabilmente nella forma di ICMP irraggiungibile) con l'indirizzo IP del vostro router del gateway. Gli indirizzi IP dei vostri gateway sono la fonte di questi pacchetti backscatter e confermano il fatto che questi gateway sono effettivamente i punti in cui l'attacco entra nella vostra rete. E voilá, avete identificato l'attacco. E tutto questo senza aver abilitato i tool darknet, e la seguente lista di accesso applicata alla interfaccia del router della darknet può fare al caso vostro:

```
access-list 105 permit icmp any
any unreachables log; access-
list 105 permit ip any any
```

Successivamente, se entrate in modalità monitoraggio da terminale su questa lista di accesso (o semplicemente osservando il log), riceverete un report backscatter dove cercare gli indirizzi IP dei vostri gateway.

La tecnica di traceback e la difesa blackhole dagli attacchi DDoS sono situazioni utili in cui il flusso di traffico infettato ha alterato (spoffing) le intestazioni. Fino a qualche tempo fa, questo era il modo più comune per eseguire questi tipi di attacco. Ma con la proliferazione di macchine zombie e di botnet, molti aggressori hanno smesso di alterare i pacchetti DDoS — non vi è motivo di alterare le intestazioni se gli attacchi sono dovunque. Allo stesso modo, gli attacchi DDoS alterati sono diminuiti considerevolmente a causa di un uso più ampio di uRPF e filtraggio di ingresso. ●