Opsec Working Group
Internet Draft
<draft-ietf-opsec-blackhole-urpf-00>
Category: Informational
Expires: July 19, 2009

W. Kumari
Google
D. McPherson
Arbor Networks

January 19, 2009

Remote Triggered Black Hole filtering with uRPF
<draft-ietf-opsec-blackhole-urpf-00.txt>

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on July 13, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

Remote Triggered Black Hole (RTBH) filtering is a popular and effective technique for the mitigation of denial-of-service attacks. This document expands upon destination-based RTBH filtering by outlining a method to enable filtering by source address as well. It also defines a standard BGP community for black hole prefixes to simplify associated semantics.

Table of Contents

1. Introduction

This document expands upon the technique outlined in "Configuring BGP to Block Denial-of-Service Attacks" [RFC3882] to present a method that allows filtering by source address(es). It also defines a standard BGP community to signal that Remote Triggered Black Hole (RTBH) filtering should occur for a network.

1.2 Terminology

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

2. Background

Network operators have developed a variety of techniques for mitigating these types of attacks. While the different techniques have varying strengths and weaknesses from an implementation perspective, the selection of which method to use for each type of attack involves evaluating tradeoffs.

A common DoS attack directed against a customer of a service provider involves generating more attack traffic destined for the target than will fit down the links from the service provider to the victim (customer). This traffic "starves out" legitimate traffic and often results in collateral damage or negative effects to other customers or the network infrastructure as well. Rather than having all of their network affected the attack, the customer may ask their service provider to filter traffic destined to the target destination IP address(es), or the service provider may determine that this is necessary themselves, in order to preserve network availability.

One method that the service provider can use to implement this filtering is to deploy access control lists on the edge of their network. While this technique provides a large amount of flexibility in the filtering, it runs into scalability issues, both in terms of the number of entries in the filter and the packet rate.

Most routers are able to forward traffic at a much higher rate than they are able to filter, and are able to hold many more forwarding table entries and routes than filter entries. RTBH leverages the forwarding performance of modern routers to filter both more entries and at a higher rate than access control lists would allow.

However, with destination-based RTBH filtering, the impact is that the attack is complete. That is, with destination-based RTBH filtering you inject a discard route into the forwarding table for the prefix in question. All packets towards that destination, attack traffic AND legitimate traffic, are then dropped by the participating routers, thereby taking the target completely offline. The benefit is that collateral damage to other systems or network availability at the customer location or in the ISP network is limited, but the negative impact to the target itself is arguably increased.

By coupling unicast reverse path forwarding (RPF) [RFC3704] techniques with RTBH, BGP can be used to distribute discard routes that are based not on destination or target addresses, but based on source addresses.

3. Destination address RTBH filtering

3.1. Overview

A "discard" route is installed on each edge router in the network with the destination set to be the discard (or null) interface. In order to use RTBH filtering for an IP address (or network) a BGP route for the address to be filtered is announced, with the next-hop set as the "discard" route. This causes traffic to the announced network to be forwarded to the discard interface and so it does not transit the network and waste resources or trigger collateral damage or negative impact to other resources along the path towards the target.

While this does "complete" the attack in that the attacked address(es) are made unreachable, it minimizes collateral damage. It may also be possible to move the host / service on the attacked IP address(es) to another address and keep the service up, for example by updating associated DNS resource records.

3.2. Detail

Steps to configure destination based RTBH filtering:

1: An address is chosen to become the "discard address". This is often chosen from 192.0.2.0/24 (TEST-NET [RFC3330]), or from RFC 1918 [RFC1918] space.

2: A route for the "discard address" is installed on the routers that form the edge/perimeter of the network, in all routers in the network, or some subset (e.g., peering, but not customer, etc.), with the destination of the route being the "discard" or "null" interface. This route is called the "discard route".

3: A BGP policy is configured on all routers that have the discard route so that routes announced with the community [TBD1] will have their next hop set to the discard address. The BGP policy should be made restrictive so that only BGP routes covering a defined number of hosts addresses will be accepted. That is, typically, only specific /32s are necessary, unless shorter prefix blocks are required. When filtering based on shorter prefixes, extreme caution should be used as to avoid

collateral damage to other hosts that reside within those address blocks.

4: When RTBH filtering is desired for a specific address, that address is announced from a central router (or route server), tagged with the community [TBD1]. The receiving routers check the BGP policy, setting the next-hop to be the discard route, which resolves to the discard interface.

5: Traffic entering the network will now be forwarded to the discard interface on all edge routers and so will be dropped at the edge of the network, saving resources.

This technique can be expanded by having multiple discard addresses, routes and communities to allow for monitoring of the discarded traffic volume on devices that support multiple discard interfaces.

The technique can also be expanded by relaxing the AS path rule to allow customers of a service provider to enable RTBH filtering without interacting with the service provider. If this is configured, an operator MUST only accept announcements for prefixes from the customer that the customer is authorized to advertise, to prevent the customer accidentally (or intentionally) black-holing space that is not theirs.

A common policy for this type of setup would be to accept from a

customer their authorized aggregate block and then permit any more specific of the authorized prefix only if the blackhole communities are equal or similar to attached, append NO_EXPORT, NO_ADVERTISE.

Extreme caution should be used in order to avoid leaking any more specifics beyond the local routing domain, unless policy explicitly aims at doing just that.

4. Source address RTBH filtering.

In many instances the denial-of-service attacks are being sourced from botnets and are being configured to "follow DNS" (the attacking machines are instructed to attack www.example.com, and re-resolve this periodically. Historically the attacks were aimed simply at an IP address and so renumbering www.example.com to a new address was an

effective mitigation). This makes a technique that allows black-holing based upon source address desirable.

By combining traditional RTBH filtering with unicast Reverse Path Forwarding (uRPF) a network operator can filter based upon the source address. uRPF performs a route lookup of the source address of the packet and checks to see if the ingress interface of the packet is a valid egress interface for the packet source address (strict mode) or if any route to the source address of the packet exists (loose mode). If the check fails, the packet is typically dropped. In loose mode some vendors also verify that the destination route does not point to a discard interface - this allows source based RTBH filtering to be deployed in networks that cannot implement strict (or feasible path) mode uRPF.

By enabling the uRPF feature on interfaces at pre-determined points of their network and announcing the source address(es) of attack traffic, a network operator can effectively drop the attack traffic at specified devices (ideally ingress edge) of their network based on source addresses.

While administrators may choose to drop any prefixes they wish, it is recommended when employing source-based RTBH inter-domain that explicit policy be defined that enables peers to only announce source-based RTBH routes for prefixes which they originate.

4.1 Steps to deploy RTBH with uRPF for source filtering.

The same steps that are required to implement destination address RTBH filtering are taken with the additional step of enabling unicast reverse path forwarding on predetermined interfaces. When a source address (or network) needs to be blocked, that address (or network)

is announced using BGP tagged with a community. This will cause the route to be installed with a next hop of the discard interface, causing the uRPF check to fail. The destination based RTBH filtering community ([TBD1]) should not be used for source based RTBH filtering, and the routes tagged with the selected community should be carefully filtered.

The BGP policy will need to be relaxed to accept announcements tagged

with this community to be accepted even though they contain addresses not controlled by the network announcing them. These announcements must NOT be propagated outside the local AS and should carry the NO_EXPORT community.

As a matter of policy, operators SHOULD NOT accept source-based RTBH announcements from their peers or customers, they should only be installed by local or attack management systems within their administrative domain.

5. Security Considerations

The techniques presented here provide enough power to cause significant traffic forwarding loss if incorrectly deployed. It is imperative that the announcements that trigger the black-holing are carefully checked and that the BGP policy that accepts these announcements is implemented in such a manner that the announcements:

- Are not propagated outside the AS (NO_EXPORT).
- Are not accepted from outside the AS (except from customers).
- Except where source based filtering is deployed, that the network contained in the announcement falls within the address ranges controlled by the announcing AS (i.e.: for customers that the address falls within their space).

6. IANA Considerations

This document requests registration of a regular Type, non-transitive BGP Extended Communities Attribute [RFC4360] from the First Come, First Served range to be named "Remote Triggered Black Hole Filter".

This community will provide a standard method to signal a provider that RTBH filtering should occur for a destination and will eliminate the need for customers to track different communities for each provider.

7. Acknowledgments

I would like to thank Joe Abley, Rodnet Dunn, Alfred Hoenes, Donald Smith, Joel Jaeggli and Steve Williams for their assistance, feedback and not laughing *too* much at the quality of the initial drafts.

I would also like to thank all of the regular contributors to the OpSec Working Group and Google for 20% time :-)

The authors would also like to thank Barry Greene for his efforts in getting this implemented and Chris Morrow for publicizing the technique in multiple talks.

8. References

8.1. Normative References

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3330] IANA, "Special-Use IPv4 Addresses", RFC 3330, September 2002.

[RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, February 2006.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC3882] Turk, D., "Configuring BGP to Block Denial-of-Service Attacks", RFC 3882, September 2004.

8.2. Informative References

[2223BIS] Reynolds, J. and R. Braden, "Instructions to Request for Comments (RFC) Authors", draft-rfc-editor-rfc2223bis-08.txt, August 2004.

Appendix A: Cisco Router Configuration Sample

This section provides a partial configuration for configuring RTBH on a Cisco router. This is not a complete configuration and should be customized before being used.

Announcing router:

```
! The discard route
ip route 192.0.2.1 255.255.255.255 Null0
!
! Matches and empty AS-PATH only.
ip as-path access-list 10 permit ^$
!
! This route-map matches routes with tag 666 and sets the next-hop
! to be the discard route.
route-map remote-trigger-black-hole permit 10
 match tag 666
 set ip next-hop 192.0.2.1
 set local-preference 200
 set community no-export
 ! The community used internally to tag RTBH announcements.
 set community 65505:666
 set origin igp
!
route-map remote-trigger-black-hole permit 20
!
router bgp 65505
 no synchronization
 bgp log-neighbor-changes
 redistribute static route-map remote-trigger-black-hole
 no auto-summary
!
! An example IP that we are applying RTBH filtering to.
! All traffic destined to 10.0.0.1 will now be dropped!
ip route 10.0.0.1 255.255.255.255 null0 tag 666
!
```

Filtering router:

```
!
! The discard route
ip route 192.0.2.1 255.255.255.255 Null0
!
! Matches and empty AS-PATH only.
ip as-path access-list 10 permit ^$
!
route-map black-hole-filter permit 10
```

```
 match ip address prefix-list only-host-routes
 match as-path 10
```



```
 match community 65505:666 no-export
!
! Don't accept any other announcements with the RTBH community.
route-map black-hole-filter deny 20
 match community 65505:666
!
route-map black-hole-filter permit 30
!
! An interface for source-based RTBH with uRPF loose mode.
interface FastEthernet 0/0
ip verify unicast source reachable-via any
```

Appendix B: Juniper Configuration Sample

This section provides a partial configuration for configuring RTBH on a Juniper router. This is not a complete configuration and should be customized for before being used.

Announcing router:

```
routing-options {
   static {
       /* EXAMPLE ATTACK SOURCE */
       route 10.11.12.66/32 {
           next-hop 192.0.2.1;
           resolve;
           tag 666;
       }
       /* EXAMPLE ATTACK DESTINATION */
       route 10.128.0.2/32 {
           next-hop 192.0.2.1;
           resolve;
           tag 666;
       }
   }
   autonomous-system 100;
}

protocols {
   bgp {
       group ibgp {
           type internal;
           export rtbh;
           neighbor 172.16.0.2;
```

```
        }
    }
}

policy-options {
    policy-statement rtbh {
        term black-hole-filter {
            from {
                tag 666;
                route-filter 0.0.0.0/0 prefix-length-range /32-/32;
            }
            then {
                local-preference 200;
                origin igp;
                community set black-hole;
                community add no-export;
```



```
                next-hop 192.0.2.1;
                accept;
            }
        }
    }
    community black-hole members 100:666;
    community no-export members no-export;
}
```

Filtering router:

```
policy-statement black-hole-filter {
    from {
        protocol bgp;
        as-path LocalOnly;
        community black-hole;
        route-filter 0.0.0.0/0 prefix-length-range /32-/32;
    }
    then {
        community set no-export;
        next-hop 192.0.2.1;
    }
}
community black-hole members 100:666;
```

```
   community no-export members no-export;


   routing-options {
      forwarding-table {
          unicast-reverse-path feasible-paths;
      }
      static {
          route 192.0.2.1/32 discard;
      }
   }

   interfaces {
      xe-1/0/0 {
          vlan-tagging;
          mtu 9192;
          unit 201 {
              vlan-id 201;
              family inet {
                  rpf-check;
                  address 10.11.12.1/24;
              }
          }
```



```
      }
   }
```

Authors' Addresses

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
Email: warren@kumari.net

Danny McPherson
Arbor Networks, Inc.
Email: danny@arbor.net