                    A Discard Prefix for IPv6
                draft-ietf-v6ops-ipv6-discard-prefix-05

Abstract

   Remote triggered black hole filtering describes a method of
   mitigating the effects of denial-of-service attacks by selectively
   discarding traffic based on source or destination address. Remote
   triggered black hole routing describes a method of selectively re-
   routing traffic into a sinkhole router (for further analysis) based
   on destination address. This document updates the IPv6 Special
   Purpose Address Registry by explaining why a unique IPv6 prefix
   should be formally assigned by IANA for the purpose of facilitating
   IPv6 remote triggered black hole filtering and routing.

Status of this Memo

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

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   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."

   This Internet-Draft will expire on December 11, 2012.

Copyright Notice

carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction

Remote triggered black hole (RTBH) filtering describes a class of
methods of blocking IP traffic either from a specific source
([RFC5635]) or to a specific destination ([RFC3882]) on a network.
RTBH routing describes a class of methods of re-routing IP traffic
destined to the attacked/targeted host to a special path (tunnel)
where a sniffer could capture the traffic for analysis. Both these
methods operate by setting the next-hop address of an IP packet with
a specified source or destination address to be a unicast prefix
which is connected locally or remotely to a router's discard, null or
tunnel interface. Typically, reachability information for this
prefix is propagated throughout an autonomous system using a dynamic
routing protocol such as BGP ([RFC3882]). By deploying RTBH systems
across a network, traffic to or from specific destinations may be
selectively black-holed or re-routed to a sinkhole device in a manner
which is efficient, scalable and straightforward to implement.

On some networks, operators configure RTBH installations using
[RFC1918] address space or the address blocks reserved for
documentation in [RFC5737]. This approach is inadequate because RTBH
configurations are not documentation, but rather operationally
important features of many public-facing production networks.
Furthermore, [RFC3849] specifies that the IPv6 documentation prefix
should be filtered in both local and public contexts. On this basis,
it is suggested that both private network address blocks and the
documentation prefixes described in [RFC5737] are inappropriate for
RTBH configurations, and that a dedicated IPv6 prefix should be
assigned instead.

This document updates the IPv6 Special Purpose Address Registry
[IANA-IPV6REG].

1.1. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in [RFC2119].

2. A Discard Prefix for IPv6

For the purposes of implementing an IPv6 remote triggered black hole
configuration, a unicast address block is required. There are
currently no IPv6 unicast address blocks which are specifically
nominated for the purposes of implementing such RTBH systems.

While it could be argued that there are other addresses and address

prefixes which could be used for this purpose (e.g. documentation
prefixes, private address space), or that an operator could assign an
address block from their own address space for this purposes, there
is currently no operational clarity on what address block would be
appropriate or inappropriate to use for this purpose. By assigning a
globally unique discard prefix for IPv6, the IETF will introduce good
practice for the implementation of IPv6 RTBH configurations and will
facilitate operational clarity by allowing operators to implement
consistent and deterministic inter-domain prefix and traffic
filtering policies for black-holed traffic.

As [RFC3882] and [RFC5635] describe situations where more than one
discard address may be used for implementing multiple remote
triggered black hole scenarios, a single address is not sufficient to
cover all likely RTBH situations. Consequently, an address block is
required.

3. Operational Implications

This assignment MAY be carried in a dynamic routing protocol within
an autonomous system. The assignment SHOULD NOT be announced to or
accepted from third party autonomous systems and IPv6 traffic with a
destination address within this prefix SHOULD NOT be forwarded to or
accepted from third party autonomous systems. If the prefix or a
subnet of the prefix is inadvertently announced to or accepted from a
third party autonomous system, this may cause excessive volumes of
traffic to pass unintentionally between the the two networks, which
would aggravate the effect of a denial-of-service attack.

On networks which implement IPv6 remote triggered black holes, some
or all of this network block MAY be configured with a next-hop
destination of a discard or null interface on any or all IPv6 routers
within the autonomous system.

4. IANA Considerations

This document directs IANA to record the allocation of the IPv6
address prefix xxxx/64 as a discard-only prefix in the IPv6 Address
Space registry and to add the prefix to the IPv6 Special Purpose
Address Registry [IANA-IPV6REG]. No end party is to be assigned this
prefix. The prefix should be allocated from ::/3.

5. Security Considerations

As the prefix specified in this document ought not normally be

transmitted or accepted over inter-domain BGP sessions for the
reasons described in Section 3, it is usually appropriate to include
this prefix in inter-domain BGP prefix filters [RFC3704] or otherwise
ensure the prefix is neither transmitted to or accepted from a third
party autonomous system.

6. References

6.1. Normative References

[IANA-IPV6REG]
          Internet Assigned Numbers Authority, "IPv6 Special Purpose
          Address Registry", 2012, <http://www.iana.org/assignments/
          iana-ipv6-special-registry>.

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

[RFC5635] Kumari, W. and D. McPherson, "Remote Triggered Black Hole
          Filtering with Unicast Reverse Path Forwarding (uRPF)",
          RFC 5635, August 2009.

6.2. Informative References

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., 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.

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

[RFC3849] Huston, G., Lord, A., and P. Smith, "IPv6 Address Prefix
          Reserved for Documentation", RFC 3849, July 2004.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an
          IANA Considerations Section in RFCs", BCP 26, RFC 5226,
          May 2008.

[RFC5737] Arkko, J., Cotton, M., and L. Vegoda, "IPv4 Address Blocks
          Reserved for Documentation", RFC 5737, January 2010.

Authors' Addresses

    Nick Hilliard
    INEX
    4027 Kingswood Road
    Dublin 24
    IE

    Email: nick@inex.ie

    David Freedman
    Claranet
    21 Southampton Row, Holborn
    London WC1B 5HA
    UK

    Email: david.freedman@uk.clara.net