Network Working Group
Internet-Draft
Expires: November 18, 2006

J. Damas
ISC
F. Neves
Registro.br
May 17, 2006

Preventing Use of Nameservers in Reflector Attacks
draft-ietf-dnsop-reflectors-are-evil-00.txt

Status of this Memo

This Internet-Draft will expire on November 18, 2006.

Copyright Notice

Abstract

This document describes the use of default configured recursive name servers as reflectors on DOS attacks. Recommended configuration as measures to mitigate the attack are given.

Table of Contents

1. Introduction 3
2. Problem Description 3
3. Recommended Configuration 4
4. Security Considerations 5
5. References 5
5.1. Normative References 5
5.2. Informative References 5
Authors' Addresses 6
Intellectual Property and Copyright Statements 7

1. Introduction

Recently, DNS [RFC1034] has been named as a major factor in the generation of massive amounts of network traffic used in Denial of Service (DoS) attacks. These attacks, called reflector attacks, while not being due to any particular flaw in the design of the DNS or its implementations, have preferentially used DNS due to common default configurations that allow for easy use of public recursive name servers that make use of such a default configuration.

In addition, due to the small query-large response potential of the DNS system it is easy to yield great amplification of the source traffic as reflected traffic towards the victims.

In this document we describe the characteristics of the attack and recommend DNS server configurations that alleviate the problem, while pointing to the only truly real solution to the problem, the wide-scale deployment of Ingress Filtering to prevent use of spoofed IP addresses [BCP38].

2. Problem Description

Because of the fact that most of the DNS traffic is stateless by design an attacker could make use of the following scenario to start a DOS attack using DNS packets:

1. The attacker starts by configuring a record (LRECORD) on an undistinct zone he has access to (AZONE), normally with large RDATA and TTL.
2. Taking advantage of clients (ZCLIENTS) on non-BCP38 networks, the attacker then crafts a query using the source address of their target victim and sends it to a Public Recursive Name Server (PRNS).
3. The PRNS proceeds with the resolution, caches the LRECORD and finally sends it to the target. After this first packet, access

to the authoritative name servers for AZONE is normally no longer necessary. The LRECORD will remain cached for the duration of the TTL at the PRNS even if the AZONE is corrected.

4. Cleanup of the AZONE might, depending on the implementation used in the PRNS, afford a way to clean the cached LRECORD from the PRNS.

Because the characteristics of the attack normally use a low volume of packets on all the kinds of actors besides the victim (AZONE, ZCLIENTS, PRNS), it's unlikely any one of them would notice their involvement based on traffic pattern changes.

Taking advantage of PRNS that support EDNS0 [RFC2671], the amplification factor (response size / query size) could be around 80. With this amplification factor a relatively small army of ZCLIENTS and PRNS could generate gigabits of traffic towards the targetted victim.

This amplification attack is possible because for historical reasons, out of times when the Internet was a much closer-knit community, some name server implementations have been made available with default configurations that when used for recursive name servers made the server accessible to all hosts on the Internet.

For years this was a convenient and helpful configuration, enabling wider availability of services. As the subject of this document tries to make apparent, it is now much better to be conscious of ones own name server services and focus the delivery of services on the intended audience of those services, may them be a University Campus, an Enterprise or an ISP's customers. The authors also want to draw the attention of small network operators and private server managers who decide to operate name servers with the aim of optimizing their DNS service, as these are more likely to use default configurations as shipped by implementors.

3. Recommended Configuration

From the description of the problem in the previous section it follows that the solution to this sort of attacks is the wide deploying of ingress filtering in routers to prevent use of address

spoofing as a viable course of action to elicit the attacks.

Nonetheless, the fact remains that DNS servers acting as open recursive servers provide an easy means to obtain great rates of amplification for attack traffic, requiring only a small amount of traffic from the attack sources to generate a vast amount of traffic towards the victim.

In this section we describe the Current Best Practice for operating recursive name servers. Following these recommendations would reduce the chances of having a given recursive name server be used for the generation of an amplification attack.

The generic recommendation to name server operators is to use the means provided by the implementation of choice to provide recursive name lookup service only to the intended clients. Client authentication can be usually done in several ways:

- IP based authentication. Use the IP address of the sending host and filter them through and Access Control List (ACL) to service only the intended clients.

- Use TSIG [RFC2845]signed queries to authenticate the clients. This is a less error prone method, which allows server operators to provide service to clients who change IP address frequently (eg. roaming clients). The current drawback of this method is that very few stub resolver implementations support TSIG signing of outgoing queries. The effective use of this method implies in most cases running a local instance of a caching nameserver or forwarder that will be able to TSIG sign the queries and send them on to the recursive name server of choice.

4. Security Considerations

This document does not create any new security issues for the DNS protocol.

It's not excessive to repeat that, although recommended configurations described in this document could alleviate the

problem, the only solution to all kinds of source address spoofing problems is the wide-scale deployment of Ingress Filtering to prevent use of spoofed IP addresses [BCP38].

5. References

5.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC2671] Vixie, P., "Extension Mechanisms for DNS (EDNS0)", RFC 2671, August 1999.

[RFC2845] Vixie, P., Gudmundsson, O., Eastlake, D., and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

5.2. Informative References

[BCP38] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

Authors' Addresses

Joao Damas
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
US

Phone: +1 650 423 1300
Email: Joao_Damas@isc.org
URI: http://www.isc.org/

Frederico A. C. Neves
NIC.br / Registro.br

Av. das Nacoes Unidas, 11541, 7
Sao Paulo, SP 04578-000
BR

Phone: +55 11 5509 3511
Email: fneves@registro.br
URI: http://registro.br/

Intellectual Property Statement

on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.