I'm Being Attacked by PRISONER.IANA.ORG!
draft-jabley-as112-being-attacked-help-help-00.txt

Status of this Memo

   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 December 20, 2006.

Copyright Notice

Abstract

   Many sites connected to the Internet make use of IPv4 addresses which
   are not globally unique. Examples are the addresses designated in
   RFC1918 for private use within individual sites.

   Hosts should never normally send reverse DNS queries for those
   addresses on the public Internet. However, such queries are
   frequently observed. Authority servers are deployed to provide
   authoritative answers to such queries as part of a loosely-
   coordinated effort known as the AS112 project.

Since queries sent to AS112 servers are usually not intentional, the
replies received back from those servers are typically unexpected.
Unexpected inbound traffic can trigger alarms on intrusion detection
systems and firewalls, and operators of such systems often mistakenly
believe that they are being attacked.

This document provides background information and technical advice to
those firewall operators.

Table of Contents

1. **Introduction**

   Readers of this document may well have experienced an alarm from a
   firewall or an intrusion-detection system, triggered by unexpected
   inbound traffic from the Internet. The traffic probably appeared to
   originate from one of the following hosts:

   o PRISONER.IANA.ORG (192.175.48.1)

   o BLACKHOLE-1.IANA.ORG (192.175.48.6)

   o BLACKHOLE-2.IANA.ORG (192.175.48.42)

   The published contacts for those hosts may well have suggested that
   you consult this document.

   If you are following up on such an event, you are encouraged to
   follow your normal security procedures and take whatever action you
   consider to be be appropriate. This document contains information
   which may assist you.

2. **Private-Use Addresses**

   Many sites connected to the Internet make use of address blocks
   designated in [RFC1918] for private use. Examples of such addresses
   are 10.1.30.20, 172.18.24.100 and 192.168.1.1.

   Because these ranges of addresses are used by many sites all over the
   world, each individual address can only ever have local significance.
   For example, the host numbered 192.168.18.234 in one site almost
   certainly has nothing to do with a host with the same address located
   in a different site.

3. **Reverse DNS**

   The Domain Name System (DNS) [RFC1034] can be used to obtain a name
   for a particular network address. The process by which this happens
   is as follows:

   1. The network address is rearranged in order to construct a name
       which can be looked up in the DNS. For example, the IPv4 address
       10.3.70.25 corresponds to the DNS name 25.70.3.10.IN-ADDR.ARPA.

   2. A DNS query is constructed for that name, requesting a DNS record
       of the type "PTR".

   3. The DNS query is sent to a resolver.

   4. If a response is received in response to the query, the answer
       will typically indicate either the hostname corresponding to the
       network address, or the fact that no hostname can be found.

   This procedure is generally carried out automatically by software,
   and is hence largely hidden from users and administrators.
   Applications might have reason to look up an IP address in order to
   gather extra information for a log file, for example.

4. **Reverse DNS for Private-Use Addresses**

   As noted in Section 2, private-use addresses have only local
   significance. This means that sending queries out to the Internet is
   not sensible: there is no way for the public DNS to provide a useful
   answer to a question which has no global meaning.

   Despite the fact that the public DNS cannot provide answers, many
   sites have misconfigurations in the way they connect to the Internet
   which results to such queries relating to internal infrastructure
   being sent outside the site. From the perspective of the public DNS,
   these queries are junk -- they cannot be answered usefully and result
   in unnecessary traffic being received by the nameservers which
   underpin the operation of the public DNS (the so-called root
   servers).

   To isolate this traffic, and reduce the load on the rest of the DNS
   infrastructure, dedicated servers have been deployed in the Internet
   to receive and reply to these junk queries. These servers are
   deployed in many places in a loosely-coordinated effort known as the
   "AS112 Project". More details about the AS112 Project can be found
   at <http://www.as112.net/>.

5. **AS112 Nameservers**

   The nameservers responsible for answering queries relating to
   private-use addresses are as follows:

   o   PRISONER.IANA.ORG (192.175.48.1)

   o   BLACKHOLE-1.IANA.ORG (192.175.48.6)

   o   BLACKHOLE-2.IANA.ORG (192.175.48.42)

   A request sent to one of these servers will result in a response
   being returned to the client. The response will typically be a UDP
   datagram, although it's perfectly valid for requests to be made over
   TCP. In both cases the source port of packets returning to the site
   which originated the DNS request will be 53.

6. **Inbound Traffic from AS112 Servers**

   Where firewalls or intrusion detection systems (IDS) are configured
   to block traffic received from AS112 servers, superficial review of
   the traffic may seem alarming to site administrators.

   o Since requests directed ultimately to AS112 servers are usually
      triggered automatically by applications, review of firewall logs
      may indicate a large number of policy violations occurring over an
      extended period of time.

   o Where responses from AS112 servers are blocked by firewalls, hosts
      will often retry, often with a relatively high frequency. This
      can cause inbound traffic to be misclassified as a denial-of-
      service (DoS) attack. In some case the source ports used by
      individual hosts for successive retries increases in a predictable
      fashion (e.g. monotonically), which can cause the replies from the
      AS112 server to resemble a port scan.

   o A site administrator may attempt to perform active measurement of
      the remote host in response to alarms raised by inbound traffic,
      e.g. initiating a port scan in order to gather information about
      the host which is apparently attacking the site. Such a scan will
      usually result in additional inbound traffic to the site
      performing the measurement, e.g. an apparent flood of ICMP
      messages which may trigger additional firewall alarms and
      obfuscate the process of identifying the original problem traffic.

7. Corrective Measures

   A site which receives responses from one of the nameservers listed in
   Section 5 is probably under no immediate danger, and the traffic
   associated with those responses probably requires no emergency action
   by the site concerned. However, this document cannot aspire to
   dictate the security policy of individual sites, and it is recognised
   that many sites will have perfectly valid policies which dictate that
   corrective measures should be taken to stop the responses from AS112
   servers.

   It should be noted, however, that the operators of AS112 nameservers
   which are generating the responses described in this document are not
   ultimately responsible for the inbound traffic received by the site:
   that traffic is generated in response to queries which are sent out
   from the site, and so the only effective measures to stop the inbound
   traffic is to prevent the original queries from being made.

   Possible measures which might be taken to prevent these queries
   include:

   1. Stop hosts from making these reverse DNS queries in the first
       place. In some cases servers can be configured not to perform
       reverse DNS lookups, for example. As a general site-wide
       approach, however, this measure is frequently difficult to
       implement due to the large number of hosts and applications
       involved.

   2. Block reverse DNS queries to the AS112 servers from leaving the
       site using firewalls between the site and the Internet. Although
       this might appear to be sensible, such a measure might have
       unintended consequences: the inability to receive an answer to
       reverse DNS queries might lead to long DNS lookup timeouts, for
       example, which could cause applications to malfunction.

   3. Configure all DNS resolvers in the site to answer authoritatively
       for the zones corresponding to the private-use address blocks in
       use. This should prevent resolvers from ever needing to send
       these queries to the public DNS. Guidance and recommendations
       for this aspect of resolver configuration can be found in
       [I-D.andrews-full-service-resolvers].

   4. Implement a private AS112 node within the site. Guidance for
       constructing an AS112 node may be found in [I-D.jabley-as112-
       ops].

8. AS112 Contact Information

   Operational contact information for the network addresses of AS112
   servers is registered with Regional Internet Registries (RIRs).
   Readers who continue to have concerns about traffic received from
   AS112 servers after reading this document are encouraged to contact
   the AS112 Network Operations Centre.

   More information about the AS112 project can be found at
   <http://www.as112.net/>.

9. IANA Considerations

   The AS112 nameservers are all named under the domain IANA.ORG (see
   Section 5). The IANA is the organisation responsible for the
   coordination of many technical aspects of the Internet's basic
   infrastructure. The AS112 project nameservers provide a public
   service to the Internet which is sanctioned by and operated in
   coordination with the IANA.

10. Security Considerations

The purpose of this document is to help site administrators properly
identify traffic received from AS112 nodes, and to provide background
information to allow appropriate measures to be taken in response to
it.

Hosts should never normally send queries to AS112 servers: queries
relating to private-use addresses should be answered locally within a
site. Hosts which send queries to AS112 servers may well leak
information relating to private infrastructure to the public network,
which could represent a security risk.

11. References

11.1. Normative References

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

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

11.2. Informative References

   [I-D.andrews-full-service-resolvers]
              Andrews, M., "Configuration Issues Facing Full Service DNS
              Resolvers In The Presence of Private Network Addressing",
              draft-andrews-full-service-resolvers-02 (work in
              progress), February 2006.

   [I-D.jabley-as112-ops]
              Abley, J. and W. Maton, "AS112 Nameserver Operations",
              June 2006.

Appendix A. **Change History**

This section to be removed prior to publication.

It is proposed that this document be published as an informational RFC.

00 Initial draft.

Author's Address

    Joe Abley
    Afilias Canada Corp.
    Suite 204, 4141 Yonge Street
    Toronto, ON M2P 2A8
    Canada

    Phone: +1 416 673 4176
    Email: jabley@ca.afilias.info