DNS Amplification Attacks

Preliminary release

Randal Vaughn and Gadi Evron

March 17, 2006

Randy_Vaughn@Baylor.edu
ge@linuxbox.org

Please note that this version of this paper is prior to submission for publication and that the final version may see significant revisions.

DNS Amplification Attacks

Randal Vaughn and Gadi Evron

Abstract

This paper outlines a Distributed Denial of Service (DDoS) attack which abuses open recursive Domain Name System (DNS) name servers using spoofed UDP packets.

Our study is based on packet captures and logs from attacks reported to have a volume of 2.8Gbps. We study this data in order to further understand the basics of the reported recursive name server amplification attacks which are also known as DNS amplification or DNS reflector attacks. One of the networks under attack, Sharktech, indicated some attacks have reached as high as 10Gbps and used as many as 140,000 exploited name servers. In addition to the increase in the response packet size, the large UDP packets create IP protocol fragments. Several other responses also contribute to the overall effectiveness of these attacks.

The risks involved with the recursive name server feature, as well as those of packet spoofing are well known, yet have been treated more as a theoretical issue. The attack under study was anticipated as early as 2002 (gnupg 2002). Earlier attacks using queries to non-authoritative servers were for a reflection attack using MX records (Mirkovic, Dietrich, Dittrich. and Reiher). To our knowledge, this is the first documentation of a new form of a recursive name server reflection attack designed to use the significantly larger data amplification available from the extended capabilities of extended DNS standards . In addition to this attack technique, recursion can be leveraged for other uses such as theft of DNS resources (CERT UNI-Stuttgart 2003).

Introduction

In recent months several attackers massively exploited recursive name servers to amplify DDoS attacks against several networks utilizing IP spoofing. Analysis of three of these attacks makes up the bulk of our study. The addendum to this paper contains a detailed description of three of these attacks.

The DNS uses a tree-like system of delegations. Recursion is the process of following the chain of delegations, starting at the Root zone, and ending up at the domain name requested by a user. A recursive name server may need to contact multiple authoritative name servers to resolve given name on behalf of the requestor. Recursive name servers are similar to SMTP relays and web proxies. They all accept messages (including requests and queries) from clients, which are then forwarded to other servers as necessary.

Ideally, a recursive name server should only accept queries from a local, or authorized clients. Unfortunately, many recursive name servers accept DNS queries from any source. Furthermore, many DNS implementations enable recursion by default, even when the name server is intended to only serve authoritative data. We say that a name server is an "open resolver" if it provides recursion to non-local users.

To establish a perspective, spoofed ICMP attacks are historically well known. On many of today's networks, ICMP Echo replies (message type 0) can be seen at the network perimeter. These replies are generated due to spoofed packets with forged source addresses in the local network space used in remote attacks.

Similarly, recursive name servers can be induced to participate in DDoS attacks in a number of ways. A network of computers distributed on the Internet in a construct such as a Botnet, can send spoofed-address queries to an *Open Resolver* (or resolvers) causing it to send responses to the spoofed-address target. Thereby, the resolver unwittingly participates in an attack on spoofed addresses. For example, high volumes DNS SERVFAIL (RCode 2) responses to a spoofed IP address can equal the damages of spoofed ICMP Echo replies (type 0) without revealing the identity of the attacker. Relatively small DNS requests can be employed to cause significantly larger replies from a name server to the spoofed IP address.

DDoS attacks using recursive name servers can create an amplification effect similar to the now-aged Smurf attack. The Smurf attack works by sending an ICMP Echo request (type 8, a ping) to broadcast

addresses on affected networks. These receiving hosts in turn relay the request and a reply to the spoofed location is initiated. In the Smurf effect, on a multi-access broadcast network, one can expect every single ping to result in attack amplification by triggering replies from all the active computers on the amplification subnet.

The amplification effect in a recursive DNS attack is based on the fact that small queries can generate larger UDP packets in response. In the initial DNS specification, UDP packets were limited to 512 bytes. At most, a 60 byte query could generate a 512 byte response for an amplification factor of 8.5. This amplification effect has been used in DNS based attacks for some time (CIAC 1999) (gnupg 2002).

New RFC specifications,- in support of IPv6, DNSSEC, NAPTR and other extensions to the DNS system, - require name servers to return much larger responses to queries. This increased UDP payload capability is now being used to launch attacks with higher UDP response amplifications. These attacks employ the RFC 2671 (Extension Mechanisms for DNS - EDNS) specification to implement a mechanism whereby the request initiator can advertise a larger UDP buffer size to responders by using an OPT pseudo-RR in the additional data section of the request.

Thus, where the amplification of a standard Smurf attack relies on sending a packet to a broadcast address which then causes multiple systems to respond to a victim, DNS amplification occurs due to the response packet being significantly larger than that of the query. If an *Open Resolver* receives an EDNS (RFC 2671) query containing a large buffer advertisement, its reply to the possibly-spoofed requesting IP address can be quite large. A DNS query consisting of a 60 byte request can be answered with responses of over 4000 bytes amplifying the response packet by a factor of 60.

Both the attacked party and the exploited servers participating in the attack - the recursive name server (or servers) - can **potentially** experience a serious DDoS attack. One report on NANOG (NANOG #1) describes a “deluge” of DNS requests to an exploited server with some addresses making more than 250,000 requests in a short time frame. The server in this report was participating in one of the attacks which we study in this paper. In our case study the DNS entries have a long TTL (minimum-ttl:86400s (24 hours)) to force the exploited servers to cache the real authoritative name server’s resource records. We assume this was an attempt to avoid a DDoS on the real authoritative name server.

By combining different response types, the amplification effect can reach up to a factor higher than 60. If, for example, the response consists of a 122 byte A type response, a 4000 byte TXT response, and a 222 byte SOA response, the total response consists of 4320 bytes. This yields an amplification factor of 73.

Other amplifications are possible depending on the query size and the experienced packet distributions in an actual attack. Due to networking limits, traffic collisions and other factors, the *effective* rate of an attack will be significantly smaller than the amplification’s *theoretical* upper limit.

Recursive DNS name servers prevalence on the Internet

Dan Kaminsky and Mike Schiffman outlined some recursive DNS servers risks in a presentation at the ShmooCon (2006) conference. According to their presentation (yet to be made public) they located about 580 thousand "Open Resolvers" on the Internet.

The Measurement Factory in another recent survey states:
"There are an estimated 7.5 million external DNS servers on the public Internet. Over 75% of domain name servers (of roughly 1.3 million sampled) allow recursive name service to arbitrary queriers. This opens a name server to both cache poisoning and attacks. "Over 40% allow zone transfers from arbitrary queriers. This exposes a name server to attacks and gives attackers information about internal networks."

DNS Amplification Attacks

Randal Vaughn and Gadi Evron

Attack Description

We include a more detailed description of the attack data in the addendum to this paper. Based on reports and our analysis it appears a successful attack requires two preconditions: a valid domain name with a large text record; and; a crafted query using a spoofed IP address.

A valid domain name must exist, preferably without a host address (TYPE A) Resource Record (RR) but with a start of authority (SOA) RR. A long timeout will be established in order to keep it in an exploited name server's cache. Also, a large text resource record (TXT RR) of approximately 4000 bytes must exist, on an EDNS capable name server.

The attacker constructs a query for all records of the domain and specifies a large UDP payload buffer using the RFC 2671 optional resource record (OPT RR) format. Captured ICMP data suggests this UDP payload buffer was as high as 10000 bytes although the actual queries may have used random UDP payload values. Observed packet fragment sizes suggest the effective UDP payload value was 1514 bytes which is consistent with a 1514 octet MTU and with the assumption the UDP payload size specification is geared towards producing fragmentation. The attacker adds the IP address of the target as the request initiator's IP address in this packet, and then repeatedly sends these queries to their established list of name servers, most likely by the use of a Botnet.

It is very likely the attackers harvested a large number of DNS IP addresses. They do not appear to care if the name servers offer EDNS nor if they allow recursive lookups. The same effect could be accomplished with IP addresses chosen at random or with malware selecting their ISP's name servers. There is one NANOG post (NANOG #2 Feb/24/2006) which supports the malware assumption.

The recursive name servers respond to the request for all records with SOA RRs, Standard Query, and fragmented TXT RRs responses. The TXT RR response, in fragments no larger than 1514 bytes, dominates the captured packets. In these captures the SOA RRs were 222 byte records. Standard Query responses were one of:

> root referrals with packet lengths ranging from 501 bytes to 222 bytes;
> Responses with reply code 3 (NXDOMAIN - no such name) with 132 to 141 byte records;
> Address A-type responses with 98 byte packets predominating, or;
> RCODE FORMERR, or SERVFAIL responses of 60, 65 or 82 byte packets.

In one capture, 292 IP addresses responded with ICMP "*Destination Unreachable"* (type 3, codes 0, 1, 3, 10, and 13), "*Time-to-live exceeded"* (type 11), or "*Source Quench"* (type 4) messages. RFC 2671 anticipated attackers may attempt an ICMP Storm Denial of Service using large UDP payloads although it is impossible to tell if this was an intended outcome of this attack.

One capture recorded 8707 incoming packets from 7207 unique IP addresses in 2.44 seconds. This is a packet arrival rate of 3567.packets per second. The total packet size of this capture is 8.5M bytes with an average of 3494088.897 bytes per second or 28Mbps. This corresponds to an average of 979 bytes per packet for an ***effective*** amplification factor between 16 and 19.

Assuming the 7207 unique IP addresses comprise the entire population of exploited name servers, the requisite query rate for the triggering event would require 2953 queries per second. This query rate would be achievable on a connection with an upload rate between 1Mpbs and 2Mbps. This does not preclude the possibility that this attack was launched from a single host nor does this preclude the possibility the attack was conducted from a 3000 member Botnet with each host generating 1 spoofed packet per second to its own ISP's DNS name server. Although it is risky to assume the proportions of exploited hosts increase linearly with the attack volume, an argument could be made that a 1Gbps volume would increase the query rate by a factor of 35 (1G/28M). An example estimating the number of hosts involved can be located in **Appendix 4:** Calculations.

Randal Vaughn and Gadi Evron

Conclusions

DNS denial of service attacks as well as abuse of recursive name servers and abuse of spoofing have been known for some time and on occasion, seen in the past. Some of these attacks may indeed be similar to the one we describe, but they are not the same. The threat behind these attacks is the increased amplification effect over that which was achievable prior to RCF 2671.

We can estimate the maximum amplification possible in this attack mechanism by enumerating the possible packet transmissions and totaling the number of bytes transmitted for each possible response set.

In the real-world network environment many factors may impact the actual number of bytes transmitted from the systems exploited to perform the DDoS attack against the victim. Packets arriving on the victim's end simultaneously collide with the result of only one packet being successfully sent to the victim. Packets arriving during the read cycle of a previously processed packet will be discarded. Collisions and packet discards happen not only on the victim's end but at many other connections and nodes intermediate to the victim and its attackers. These, and other factors, result in the effective packet amplification being different from than that of the *theoretical maximum amplification*.

It is highly likely a Botnet was used to conduct these attacks. Single machine upload limitations and increased query volume needed for a higher volume attack decrease the probability of a single host being used as an attacker. Other amplification factors may account for the experienced higher volume. Mention has been made that certain unexpected NXDOMAIN responses may contribute to the amplification of these attacks. The first NANOG report referenced in this document supports our conclusion of Botnet involvement.

In our opinions these attacks illuminate two main weaknesses in the Internet infrastructure currently being exploited and a third contributing factor:

1. DNS name servers which are recursive and either don't need to be or do not limit the ability to their IP space through appropriate firewall rules or other measures;
2. Networks which allow spoofing; and,
3. Improper management at the domain end-of-life-cycles. RR records for expired domains (see addendum) which remain in existing name server data are problematic and should be periodically cleaned.

The first two are both serious flaws and although they are being utilized together for these attacks, neither is limited to be used with the other. The third problem is a hygiene factor and one which would be extremely difficult to implement on a reasonable scale.

This paper's purpose is to describe the attacks rather than develop solutions. However, there has been considerable discussion among network and DNS operators on what effective steps can be taken, of which three suggestions which seem to be held in wide acceptance:

- DNS name servers facing the world should not be the same ones serving users or clients in your network.
- Limit usage of the DNS name server and the recursive functionality to your network.
- Implement spoofing counter-measures such as those suggested in BCP 38 and SAC004.

It has been pointed out that recursive DNS is a core DNS design artifact and undue constraints or restrictions on this feature may undesirably restrain Internet growth. Limiting UDP buffers to 512 bytes might somewhat limit the attack's effects, but not **dependably**, as reduced UDP payload limits can be countered by increasing the requests rates.

A couple of sites dealing with the subject of recursive DNS attacks and recursive name servers:

1. http://www.us-cert.gov/reading_room/DNS-recursion121605.pdf
2. http://cc.uoregon.edu/cnews/winter2006/recursive.htm

Randal Vaughn and Gadi Evron

Acknowledgments

We would like to thank Sharktech, FDCServers, Cox, and Prolexic for insights into this attack mechanism. Special thanks also go to Paul Vixie, Doron Shikmoni, Florian Weimer, Duane Wessels, Dan Kaminsky, Jaap Akkerhuis, Bill Manning, Barrett G. Lyon, Matt Carothers, Aggelos Pantazopoulos, Edward Aronovich, Dave Dittrich, Bill Cheswick, Steven M. Bellovin, Joe St Sauver, Johannes B. Ullrich, Jon Crowcroft, Roland Dobbins, Brad Knowles, Kurt Erik Lindqvist, and mudge (Peiter Zatko), for their assistance.

The Internet Systems Consortium (ISC) and Paul Vixie have led most of the efforts to understand and develop suggestions on handling this problem. Many of these discussions can be found on the DNS-operations mailing list.

References

(CERT UNI-Stuttgart 2003)
Permitting recursion can allow spammers to steal name server resource
http://cert.uni-stuttgart.de/archive/bugtraq/2003/09/msg00164.html

(CIAC 1999) J-063: Domain Name System (DNS) Denial of Service (DoS) Attacks,
http://www.ciac.org/ciac/bulletins/j-063.shtml

(gnupg 2002) DNS keyserver
http://lists.gnupg.org/pipermail/gnupg-users/2002-July/014057.html

"The Measurement Factory DNS Survey"
http://dns.measurement-factory.com/surveys/sum1.html

(Mirkovic, Dietrich S., Dittrich D. and Reiher P.) 2004, Internet Denial of Service: Attack and Defense Mechanisms, Prentice Hall P, ISBN 0131475738

NANOG #1 : DNS deluge for x.p.ctrc.cc
http://www.merit.edu/mail.archives/nanog/2006-02/msg00579.html

NANOG #2: DNS deluge for x.p.ctrc.cc
http://www.merit.edu/mail.archives/nanog/2006-02/msg00583.html

The DNS-operations mailing list
http://lists.oarci.net/mailman/listinfo/

RFC 1918
http://www.faqs.org/rfcs/rfc1918.html

RFC 2671
http://www.faqs.org/rfcs/rfc2671.html

BCP 38
http://www.faqs.org/rfcs/bcp/bcp38.html

SAC004
http://www.icann.org/committees/security/sac004.txt

SharkTech
Personal Correspondence.

Randal Vaughn and Gadi Evron

Addendum: Case study

In this paper we will describe a case study of three DDoS attacks utilizing this technique to attack different networks

The preceding attack *Technical Description* covers our best guess at how the attack originates and explains the preconditions required for the attack.

Event 1 in our opinion was a test run. It was mostly confined to European IP addresses which were attacking the network in question.

Event 2 in our opinion was also a test run although not as successful in amplification.

Event 3 introduced the 127.0.0.1 A record. At this time we are unsure if that fact somehow assists in amplification. If it does, we cannot at this time see why. This may be an attempt to mimic an older DNS attack which utilized the RFC 1918 address space.

The amplification demonstrated utilizes TXT records and requires recursive name servers which support EDNS. Other packets seen in the attacks are from non-recursive name servers or are from non-EDNS DNS name servers which respond with an appropriate RCODE such as NOTIMPL, FORMERR, or SERVFAIL. These packets are not planned but aide the attackers by contributing to the overall load on the target.

In these test cases, it is possible, although unlikely, that the attackers didn't use a list of recursive name servers but rather chose the brute force approach of blasting out as many IP addresses as possible. Our data contains both FORMERR and SERVFAIL RCODE responses which are consistent with the assumption that the attackers were unaware of the EDNS capabilities of the exploited DNS name servers.

Event 1

October.2005.attack.1

This is our first in a series of events directed towards a specific network. This network experienced multiple attacks in the four month time period included in this analysis.

The logs available for this first event are in the form of netflows. These show an attack pattern similar to subsequent logs but are predominated by DNS IP addresses in the 80.0.0.0/8 network space. The attack packets in the log appear to all be IP protocol fragments with packet lengths of 1500, 1476, 1119, 1380, 572, and 44 bytes. The 1500 and 1119 byte fragments are the predominant fragment sizes in this log.

We ran a set of DNS surveys on 28 of the IP addresses in order to determine if the DNS services were still available. An example of a typical survey is contained in **Appendix1:** Exploited DNS survey. Of the 28 IP addresses surveyed, five of them returned 0.0.0.0 to an A record request for Microsoft.com. We then captured replies from these IP addresses (**Appendix 2:** Packet Captures, **DNS Capture 1**). The captures reveal these five name servers were not supporting recursion to our tests.

We believe two contributing factors to these results are:

1. The amplification attacks are often also devastating to the abused service. The recursive feature may have been disabled.
2. It is also possible that complaints of the attacks have been filed, resulting in the same action.

In all cases, the servers recorded as responding with a 0.0.0.0 IP address have a 0 bit set for the *Recursion available* flag. We did not probe the EDNS capabilities of any of these IP addresses.

Based on these limited and biased measurements, we can not estimate the actual proportion of the

servers tested as allowing recursion. Never-the-less, for the first 28 servers participating in this attack only 14 currently respond as supporting recursion. Again this is consistent with the attacker's not fully gathering intelligence about the exploited servers prior to carrying out this attack.

Event 2

Feburary.2006.attack.2

This is a small packet capture identical to, but chronologically prior, to *Event 3.* The captures for this attack reveal only a single DNS name server attempting to attack several IP addresses on the victim network. Fragmented IP protocol packets were either 1514 or 1092 bytes long.

This is the only capture which shows only a single IP address as the attacking DNS name server. Subsequent *Event 3* logs do show some recycling of exploited DNS attackers but few of these appear more than three times in the captures. This may have been a test run in preparation for *Event 3*.

Event 3

Feburary.2006.attack.3
Feburary.2006.attack.4

In February 2006 another DNS DDoS attack was launched towards a single IP address. Again this attack was precipitated by ANY type queries for a domain using the victim IP address as the spoofed request initiator's.

These captures are of different stages of an attack on the same target and, due to their size, reveal an interesting amount of detail about the attack.

For instance, patterns of this attack include a number of standard query responses. The following packet summaries are representative samples from the second capture in **Event 3 Capture Set 1**. The key information fields in this list are the Info field indicating the type of response and the Source and Destination IP addresses.

Time	Source	SrcPort	Destination	DstPort	Length	Protocol	Info
3.065607	D.D.D.93	53	V.V.V.62	45007	82	DNS	Standard query response, Server failure
3.065920	D.D.D.136	53	V.V.V.62	26572	1498	DNS	Standard query response TXT[Unreassembled Packet]
3.067305	D.D.D.134	53	V.V.V.62	49629	98	DNS	Standard query response A 127.0.0.1
3.067775	D.D.D.13	53	V.V.V.62	41348	139	DNS	Standard query response, No such name
3.068252	D.D.D.161	53	V.V.V.62	19117	141	DNS	Standard query response, No such name
3.068553	D.D.D.8	53	V.V.V.62	10838	501	DNS	Standard query response
3.068963	D.D.D.45	53	V.V.V.62	33738	293	DNS	Standard query response
3.071470	D.D.D.51	53	V.V.V.62	38014	222	DNS	Standard query response SOA ns.SOA A 127.0.0.1 NS ns.SOA NS ns2.SOA
3.071972	D.D.D.190	53	V.V.V.62	60169	554	DNS	Standard query response TXT[Malformed Packet]
3.078041	D.D.D.135	53	V.V.V.62	25632	82	DNS	Standard query response
3.146961	D.D.D.12		V.V.V.62		70	ICMP	Destination unreachable (Host unreachable)
3.211333	D.D.D.113	53	V.V.V.62	28393	60	DNS	Standard query response, Format error
3.393310	D.D.D.222	53	V.V.V.62	856	175	DNS	Standard query response A 127.0.0.1
4.138479	D.D.D.202	53	V.V.V.62	55066	1514	DNS	Standard query response TXT[Malformed Packet]
4.354019	D.D.D.3		V.V.V.62		1092	IP	Fragmented IP protocol (proto=UDP 0x11, off=2960)
4.354104	D.D.D.18		V.V.V.62		1108	IP	Fragmented IP protocol (proto=UDP 0x11, off=2960)
4.784824	D.D.D.136	53	V.V.V.62	23924	87	DNS	Standard query response A 10.61.32.1
4.938324	D.D.D.204	53	V.V.V.62	34611	82	DNS	Standard query response, Refused

Event 3 Capture Set 1

The D.D.D.xxx IP addresses contained in **Event 3 Capture Set 1** are from a wide range, where V.V.V.62 is a single host. Of particular interest are the IP protocol packets which are fragments of a near-4000 byte TXT resource record. Fragmented IP protocol packets come in 38 varieties. The distributions of these fragments are listed in **Appendix 1:** Fragment distributions.

The most devastating packets are those with fragmented packets such as, "Fragmented IP protocol

(proto=UDP 0x11, off=2960)". All of these responses came from DNS name servers with the *Recursion available* flag set.

Packet Captures (listed in **Appendix 2)** contain additional details from selected packets of this attack. For example, the packet labeled "**Standard query response A 127.0.0.1**" is interesting in that it identifies several IP addresses which claim authority for the 2LD.TLD domain used in launching this attack.

In addition to the IP addresses, D.D.D.134 and D.D.D.242, found in **Event 3 Capture Set 1**, six other DNS IP addresses report as authoritative for the 2LD.TLD domain. All of these DNS name servers are on the same /22. All of these servers returned 127.0.0.1 in their A record response. A number of other DNS IP addresses also returned A records. Of these, 11 were on the same broadband network and returned 127.0.0.1, 22 were in the same ASN and returned a RFC 1918 address. A total of 57 DNS name servers returned either 127.0.0.1 or 10.61.31.1. Fifty-six of these 57 servers had the *Recursion available* flag set. Several hundred DNS name servers returned Server Failures. Thirty six servers refused the spoofed request.

Another key to this attack is the 2LD.TLD domain which expired in mid 2005 yet continues to have name server entries for TXT and other records. We believe the use of an expired domain is not critical to the attack. The attacks exploited the expired domain by creating a large TXT record for the domain. The responses for this TXT RR created the fragmentation while various A type and SOA responses exacerbated an already deteriorating situation.

It is unknown if the authoritative name server's assignment of 127.0.0.1 had any impact on the amplification of this request. We suspect this A record may have been entered when the domain record expired; however, older attacks using such 127.0.0.1 A records have been employed in past attacks on the DNS system. We can not determine from the available information if this was an accidental or a malicious A record entry.

Another interesting event in the attack 4 capture log is a response to a query which may have exceeded the UDP buffer limit (**Appendix 2:** Packet Captures, **1280 Byte UDP OPT RR**) of the server. Interestingly, this is the only exploited EDNS-capable recursive DNS name server returning a 1280 byte UDP buffer with a truncated response. It appears this response was to a query for a UDP payload larger than 1280 bytes.

Four EDNS-capable but non-recursive name servers with a 10000 byte UDP buffer responded with FORMERR. 127 EDNS recursive name servers responded with SERVFAIL. These servers all had a 4096 UDP buffer OPT-RR record.

Randal Vaughn and Gadi Evron

Appendix 1: Fragment distributions

Exploited DNS Survey

```
#Using :- microsoft.com
#Start Time:       2006/03/05          15:10:47:987
 DNS IP Address       IP or Cached     #IP     #Alias    LagIn     LagOut    Response
  80.XXX.XXX.92     207.46.250.119      2        0          0        21       328
  80.XXX.XXX.95     207.46.250.119      2        0          0        51       797
  63.XXX.XXX.64     207.46.250.119      2        0          0         3        47
  63.XXX.XXX.66     207.46.130.108      2        0          0         3        47
  63.XXX.XXX.67     207.46.250.119      2        0          0         4        63
 63.XXX.XXX.191     207.46.250.119      2        0          8         3       109
  80.XXX.XXX.22     207.46.250.119      2        0          0        14       219
 80.XXX.XXX.184           0.0.0.0      0        0          0         9       141
  80.XXX.XXX.66           0.0.0.0      0        0          0        11       172
 80.XXX.XXX.218           0.0.0.0      0        0          0        11       171
  80.XXX.XXX.46     207.46.130.108      2        0          0        15       234
 80.XXX.XXX.214     207.46.130.108      2        0          0        14       218
 80.XXX.XXX.201     207.46.250.119      2        0          0        13       203
 80.XXX.XXX.192           0.0.0.0      0        0          0        14       219
 80.XXX.XXX.242           0.0.0.0      0        0          0        13       203
 80.XXX.XXX.205     207.46.130.108      2        0          0        12       188
 80.XXX.XXX.199     207.46.130.108      2        0          0        14       219
 80.XXX.XXX.195     207.46.250.119      2        0          0        17       265
 80.XXX.XXX.230     207.46.250.119      2        0          0        18       281
#         average response   217.0532 ms        stdev 155.556
#         average latency    14.10532 ms        stdev 9.85097
#         average process    622.7862 ms
#         Servers Responding          19
#         Servers in file    28
#         Response Ratio     67.85712 %
#   1.60569 Hosts per second
# End of list
```

Fragment distributions:

Fragment Size	Offset	Frag+offset	#Fragments
60	1472	1532	6
60	1480	1540	1
60	2936	2996	1
60	2952	3012	6
60	4032	4092	1
62	1480	1542	5
66	2928	2994	3
70	1472	1542	3
82	1432	1514	11
82	2880	2962	1
82	2912	2994	13
98	1480	1578	1
98	2896	2994	1
130	1384	1514	1
586	552	1138	1
586	586	1172	1
618	1472	2090	1
1064	2960	4024	6
1080	2944	4024	1
1092	2960	4052	202
1108	2944	4052	3
1108	2960	4068	297
1124	2928	4052	1
1124	2944	4068	5
1140	2928	4068	2
1156	2912	4068	1
1188	2864	4052	3
1204	2864	4068	1
1442	1408	2850	1
1450	1416	2866	1
1458	1424	2882	1
1466	1432	2898	7
1466	1480	2946	1
1498	1464	2962	1
1506	1472	2978	3
1506	1480	2986	1

```
1510          32        1542            1
1514        1480        2994          225
                                Total   821
```

Appendix 2: Packet Captures

DNS Capture 1

```
Frame 3 (284 bytes on wire, 284 bytes captured)
Ethernet II, Src: 00:00:00:ff:ff:ff, Dst: 00:00:00:ff:ff:ff
Internet Protocol, Src Addr: 80.XXX.XXX.242 (80.XXX.XXX.242), Dst Addr: 10.0.1.2
(10.0.1.2)
User Datagram Protocol, Src Port: 53 (53), Dst Port: 1269 (1269)
Domain Name System (response)
    Transaction ID: 0x0001
    Flags: 0x8100 (Standard query response, No error)
        1... .... .... .... = Response: Message is a response
        .000 0... .... .... = Opcode: Standard query (0)
        .... .0.. .... .... = Authoritative: Server is not an authority for domain
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... 0... .... = Recursion available: Server can't do recursive queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not
authenticated by the server
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 13
   Additional RRs: 0
```

Standard query response A 127.0.0.1

```
Number  Time     Source     SrcPort Destination DstPort Length Protocol Info
   1005 3.625707 D.D.D.254  53      V.V.V.62    23783   175    DNS      Standard query
response A 127.0.0.1
Frame 1005 (175 bytes on wire, 175 bytes captured)
    Arrival Time: Feb 14, 2006 21:54:00.383021000
    Time delta from previous packet: 0.000080000 seconds
    Time since reference or first frame: 3.625707000 seconds
    Frame Number: 1005
    Packet Length: 175 bytes
    Capture Length: 175 bytes
Ethernet II, Src: 00:00:00:00:4c:00, Dst: 00:00:00:00:29:26
     Destination: 00:00:5006:00:29:26 (V.V.V.62)
    Source: 00:00:00:00:4c:00 (xxxxxxxxx:4c:00)
     Type: IP (0x0800)
Internet Protocol, Src Addr: D.D.D.254 (D.D.D.254), Dst Addr: V.V.V.62 (V.V.V.62)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
          .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
     Total Length: 161
    Identification: 0x5a3d (23101)
    Flags: 0x00
        0... = Reserved bit: Not set
        .0.. = Don't fragment: Not set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 54
    Protocol: UDP (0x11)
    Header checksum: 0xc8a0 (correct)
     Source: D.D.D.254 (D.D.D.254)
    Destination: V.V.V.62 (V.V.V.62)
User Datagram Protocol, Src Port: domain (53), Dst Port: 23783 (23783)
    Source port: domain (53)
    Destination port: 23783 (23783)
     Length: 141
    Checksum: 0xe318 (correct)
Domain Name System (response)
    Transaction ID: 0x6a32
    Flags: 0x8580 (Standard query response, No error)
        1... .... .... .... = Response: Message is a response
        .000 0... .... .... = Opcode: Standard query (0)
```

```
        .... .1.. .... .... = Authoritative: Server is an authority for domain
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... 1... .... = Recursion available: Server can do recursive queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not
authenticated by the server
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 3
    Queries
        4LD.3LD.2LD.TLD: type ANY, class ANY
            Name: 4LD.3LD.2LD.TLD
            Type: ANY (Request for all records)
            Class: ANY (0x00ff)
    Answers
        4LD.3LD.2LD.TLD: type A, class IN, addr 127.0.0.1
            Name: 4LD.3LD.2LD.TLD
            Type: A (Host address)
            Class: IN (0x0001)
            Time to live: 1 day
            Data length: 4
            Addr: 127.0.0.1
    Authoritative nameservers
        2LD.TLD: type NS, class IN, ns ns1.AUTHNAME_SRV_DOMAIN
            Name: DOMAIN
            Type: NS (Authoritative name server)
            Class: IN (0x0001)
            Time to live: 1 day
            Data length: 15
            Name server: ns1.AUTHNAME_SRV_DOMAIN
        2LD.TLD: type NS, class IN, ns ns2.AUTHNAME_SRV_DOMAIN
            Name: DOMAIN
            Type: NS (Authoritative name server)
            Class: IN (0x0001)
            Time to live: 1 day
            Data length: 6
            Name server: ns2.AUTHNAME_SRV_DOMAIN
    Additional records
        ns1.AUTHNAME_SRV_DOMAIN: type A, class IN, addr E.E.E.4
            Name: ns1.AUTHNAME_SRV_DOMAIN
            Type: A (Host address)
            Class: IN (0x0001)
            Time to live: 1 day
            Data length: 4
            Addr: E.E.E.4
        ns2.AUTHNAME_SRV_DOMAIN: type A, class IN, addr E.E.E.6
            Name: ns2.AUTHNAME_SRV_DOMAIN
            Type: A (Host address)
            Class: IN (0x0001)
            Time to live: 1 day
            Data length: 4
            Addr: E.E.E.6
        <Root>: type OPT
            Name: <Root>
            Type: OPT (EDNS0 option)
            UDP payload size: 4096
            Higher bits in extended RCODE: 0x0
            EDNS0 version: 0
            Z: 0x0
            Data length: 0
```

1280 Byte UDP OPT RR

```
Number  Time        SrcAddr               SrcPort DstAddr               DstPort Proto
Length Info
    957 3.078041    I.I.I.I       53      D.D.D.62         25632   DNS      82
Standard query response

Frame 957 (82 bytes on wire, 82 bytes captured)
    Arrival Time: Feb 14, 2006 22:12:06.520436000
```

```
    Time delta from previous packet: 0.000036000 seconds
    Time since reference or first frame: 3.078041000 seconds
    Frame Number: 957
    Packet Length: 82 bytes
    Capture Length: 82 bytes
Ethernet II, Src: xx:ff:ff:ff:ff:ff, Dst: xx:ff:ff:ff:ff:ff
    Destination: xx:ff:ff:ff:ff:ff (xx:ff:ff:ff:ff:ff)
    Source: xx:ff:ff:ff:ff:ff (xx:ff:ff:ff:ff:ff)
    Type: IP (0x0800)
Internet Protocol, Src Addr: I.I.I.I (I.I.I.I), Dst Addr: D.D.D.62 (D.D.D.62)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
          .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
     Total Length: 68
    Identification: 0x0000 (0)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 53
    Protocol: UDP (0x11)
    Header checksum: 0xac66 (correct)
     Source: I.I.I.I (I.I.I.I)
    Destination: D.D.D.62 (D.D.D.62)
User Datagram Protocol, Src Port: domain (53), Dst Port: 25632 (25632)
    Source port: domain (53)
    Destination port: 25632 (25632)
     Length: 48
    Checksum: 0xe57b (correct)
Domain Name System (response)
    Transaction ID: 0x53a9
    Flags: 0x8380 (Standard query response, No error)
        1... .... .... .... = Response: Message is a response
        .000 0... .... .... = Opcode: Standard query (0)
        .... .0.. .... .... = Authoritative: Server is not an authority for domain
        .... ..1. .... .... = Truncated: Message is truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... 1... .... = Recursion available: Server can do recursive queries
        .... .... .0.. .... = Z: reserved (0)
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not
authenticated by the server
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
    Queries
        4LD.3LD.2LD.TLD: type ANY, class ANY
            Name: 4LD.3LD.2LD.TLD
            Type: ANY (Request for all records)
            Class: ANY (0x00ff)
    Additional records
        <Root>: type OPT
            Name: <Root>
            Type: OPT (EDNS0 option)
            UDP payload size: 1280
            Higher bits in extended RCODE: 0x0
            EDNS0 version: 0
            Z: 0x0
            Data length: 0
```

The response packet for the server returning 127.0.0.1 provides information regarding the domains used to act as the NS for the 2LD.TLD. We obtained Whois for the 2LD.TLD and its NS. This information gives us nothing which identifies the attacker but does show a curious geographic tendency.

Randal Vaughn and Gadi Evron

Example TXT RR used in the attacks

```
1# dig e.xxxxxx.com TXT

; <<>> DiG 8.3 <<>> e.xxxxxx.com TXT
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61376
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0
;; QUERY SECTION:
;;      e.xxxxxx.com, type = TXT, class = IN

;; ANSWER SECTION:
;; ANSWER SECTION:
;; ANSWER SECTION:
e.xxxxxx.com.           1D IN TXT
"xxxxxxxx+xxxxx@efnet.................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
......................................................................................
...................................................................................."
".....................................................................................
............................"
;; AUTHORITY SECTION:
xxxxxx.com.             1D IN NS        ns2.veriserv.com.
xxxxxx.com.             1D IN NS        ns1.veriserv.com.

;; Total query time: 230 msec
```

Appendix 3: Whois Information

WHOIS lookups for domains involved in *Event 3.*

```
==============================================
```

D.D.D.254 PTR record: 207-D-D-D.DDD.DDD.

The Whois information for the 2LD.TLD reveals the domain has been expired since mid 2005. This domain had not A records except as the RFC 1918 addresses already detailed in this document.

```
==========================================
Checking server [whois.....]
Results:
2LD.TLD
Registrant:
        xxxx  xxxxxxxxxxxxxx
        xxx   xxxx
        xxxxxxxxxxxxxxxxxxxx
        San Antonio, TX  78229
        US
        xxxxxxxxxx
Domain Name: 2LD.TLD
Administrative, Technical Contact:
        xxxx  xxxxxxxxxxxxxx
        xxx   xxxx
        xxxxxxxxxxxxxxxxxxxx
        San Antonio, TX  78229
        US
        xxxxxxxxxx
   Record created on xxx 20 2000.
   Record expires on xxx 20 2005.
Domain servers:
        ns1.2LD.TLD_NS_DOM_1
        ns1.2LD.TLD_NS_DOM_2
==============================================


==============================================
AUTHNAME_SRV_DOMAIN CORP NAME
   XXXX XXXXXXX
   Houston, Texas 77478
   US
   Domain Name: AUTHNAME_SRV_DOMAIN
   Administrative Contact:
        XXXXX XXXXXX (XXXX@XXXXXX)
        AUTHNAME_SRV_DOMAIN CORP NAME
        XXXX XXXXXXXXXXX  XXX XXX
        Houston, Texas 77478
        US
        Phone: +X.XXXXX.XXXX
        Fax:
    Technical Contact:
        XXXXX XXXXXX (XXXX@XXXXXX)
          AUTHNAME_SRV_DOMAIN CORP NAME
        XXXX XXXXXXXXXXX  XXX XXX
        Houston, Texas 77478
        US
        Phone: +X.XXXXX.XXXX
        Fax:
   Billing Contact:
        XXXXX XXXXXX (XXXX@XXXXXX)
        AUTHNAME_SRV_DOMAIN CORP NAME
        XXXX XXXXXXXXXXX  XXX XXX
        Houston, Texas 77478
        US
        Phone: +X.XXXXX.XXXX
        Fax:

   Record updated on 2005-06-28 06:30:07
   Record created on 1997-10-23
   Record expires on 2007-10-22
```

Randal Vaughn and Gadi Evron

```
   Database last updated on 2006-03-04 21:24:07 EST
==============================================


==============================================
Registrant:
Registrant Company

   San Antonio, TX xxxx
   US

   Domain Name: 2LD.TLD_NS_DOM_2

   Administrative Contact, Technical Contact:
      xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
      xx     xxxxxxx   xxxxx
      San Antonio, TX xxxx
      US
     xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

   Record expires on 15-Aug-2008.
   Record created on 16-Aug-1995.
   Database last updated on 4-Mar-2006 21:12:43 EST.

   Domain servers in listed order:

   NS1.2LD.TLD_NS_DOM_2                 F.F.F.19
   NS2.2LD.TLD_NS_DOM_2                 G.G.G.19
==============================================
Domain Name:2LD.TLD_NS_DOM_1
Created On:17-Feb-1993 05:00:00 UTC
Last Updated On:07-Feb-2006 21:40:18 UTC
Expiration Date:18-Feb-2009 05:00:00 UTC
Sponsoring Registrar:Network Solutions LLC (R63-LROR)
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:15154812-NSIV
```

Randal Vaughn and Gadi Evron

Appendix 4: Calculations

Example calculations for Query rate estimations.

Description	**Notation**	**Value**
packets	p	8707
IPs	i	7207
Bytes	By	8527296
bits	b	68218368
sec	s	2.440492
packets per IP	p/i	1.2
IPs per packet	i/p	0.8
Bytes per Packet	By/p	979.4
Bytes per IP	By/i	1183.2
packets per second	p/s	3567.7
IPs per second	i/s	2953.1
Bytes per second	By/s	3494088.9
bits per second (volume)	b/s	27952711.2
bits per packet	b/p	7834.9
bits per IP	b/i	9465.6
Assumption: number of Queries equals number of IPs		
Total Queries	TQ	7,207
Queries per second	TQ/s	2,953.1
Response bit Volume per Query	b/s/TQ/s	1,589.25
Response Byte Volume per Query	VpQ	198.66
Assumption: Bytes per Query is 60		
Bytes per Query	BypQ	60.0
bits per query	bpQ	480.0
Observed Amplification	By/P/BypQ	16.3
Measured bit Volume	MsrdVb	27,952,711.1
Reported bit Volume	RepVb	8,000,000,00
Ratio Reported to Measured	Rrm	286
Reported Response Byte Volume per Query	Rrm*VpQ	56855
Estimated Queries per Sec	Rrm*TQ/s	845168

Randal Vaughn and Gadi Evron

Appendix 5: Glossary

Amplification: An attack advantage gained through using additional hosts to reflect an attack or a condition which increases the ratio of attack events to the number of triggering events.

EDNS: Extension Mechanisms for DNS. As outlined in RFC 2671, EDNS provides a method of maintaining compatibility with previous versions of the DNS standards while adding structures and fields in order to allow for future use of the DNS system.

Theoretical amplification: The maximum ratio of attack events to triggering events under ideal conditions.

Effective amplification: The amplification achieved under operational conditions.

MTU: The Maximum transmission unit is the packet maximum size transmission limit for a network.

Netflow: Netflow is a traffic monitoring technology originally developed at CISCO.

*TYPE***:** The DNS system contains several named fields. One of the is the TYPE field which uses two bytes (octets) of data to represent the different types of resources available in the DNS system. The TYPE field has predefined values used to specify the resource such as TYPE=1 being a host address, TYPE=16 being a TXT string. The TYPE field is a subset of a question type, QTYPE field.

CLASS: The Class field, in DNS packets, allows dissimilar networks and applications to use the same name space. For example, the class field allows the concept of address to be used for different host address formats.

QTYPE: The QTYPE is a field contained in a DNS query packet. All TYPE values are also QTYPE values. QTYPE data values are 252 to request a transfer of a specific zone or 255 to request all domain system entries for a domain.