

SPF- Motivations, Risks, and Alternatives

By Douglas Otis, Trend Micro Inc. 10/02/06

The purpose of this paper is primarily to evaluate security risks associated with the use of SPF authorization records. To weigh these risks against the intended benefits of SPF/Sender-ID, a brief analysis of who is publishing these records allows some deductions as to what are the motivating benefits. From the distribution of SPF publishers, the possible purposes appear aimed at white-listing bulk-senders and thwarting phishing attempts.

A pitch often made for implementing SPF/Sender-ID is to ensure delivery at various ISPs. Frequently MSN, Hotmail, and AOL are mentioned. Unfortunately, neither SPF or Sender-ID represents a comprehensive solution that avoids delivery problems, especially when recipients are forwarding their email. For example, Jon Doe might use an account at jon.doe@alumni.some-college.edu forwarding to accounts at a major ISP. Jon does this to avoid checking his accounts separately for arriving email.

A clear warning is included by the IESG within the experimental RFC4406 for Sender-ID:

Participants in the Sender-ID experiment need to be aware that the way Resent-* header fields are used will result in failure to receive legitimate email when interacting with standards-compliant systems (specifically automatic forwarders which comply with the standards by not adding Resent-* headers, and systems which comply with RFC 822 but have not yet implemented RFC 2822 Resent-* semantics). It would be inappropriate to advance Sender-ID on the standards track without resolving this interoperability problem.

This warning relates to these instructions included in RFC4406:

7.2. E-Mail Forwarders

In order to pass the PRA variant of the test, a program that forwards received mail to other addresses MUST add an appropriate header that contains an e-mail address that it is authorized to use. Such programs SHOULD use the Resent-From header for this purpose.

Not all forwarding services violate RFC2822. A method to mitigate SPF/Sender-ID induced delivery problems is to assert a neutral status in SPF records when the SMTP Client is not authorized due to these interoperability issues. In effect, these records ask that messages be treated "as-if" no records were published.

To overcome the purported coercion caused when major ISPs reject messages lacking SMTP Client authorization, these records must then authorize all SMTP Clients! The next concern might be whether authorization is considered by these domains as being sufficient for accruing reputations based upon the referencing domain-name.

One may wonder why large providers publish negative SPF records for email-accounts used by residential users. With respect to Microsoft and Sender-ID, for resolving the resulting forwarding and associated support issues, their solution requires the

acquisition of their proprietary and licensed header selection algorithm. Most open source vendors still consider provisions in this license to be unacceptable. See:

<http://www.apache.org/foundation/docs/sender-id-position.html>

The use of negative SPF records by large providers remains problematic, and might be seen as another means to coerce adoption of Sender-ID and to thwart the distribution of open source software, while simultaneously putting the DNS infrastructure at risk. Often the pretext for the negative authorization records is to protect recipients from being phished. Does Sender-ID actually offer this protection? No. And SPF/Sender-ID increases the risks of far more serious threats that extend well beyond email.

Headers tested by SPF/Sender-ID may remain unseen. For there to be any protection, message annotations must be limited to trusted domains. Various annotation techniques may involve a browser or email client plug-in. It is common for recipients to collect messages from many different sources. To confirm the SPF records for a message being viewed by a recipient, reliance must be placed upon the the Received header (time-stamp). Unfortunately, noting the IP address of the SMTP client is optional in the Received header. While some are suggesting an authentication header may be added by the MDA, without specific knowledge of the MDA domain, there is no way for a generic client to know whether such headers can be used for this purpose.

SPF/Sender-ID results might even be based upon email-addresses not seen by the recipient. As a result, SPF/Sender-ID is not very practical for even annotating known trustworthy domains. In addition, SPF/Sender-ID will not reliably define the authorized SMTP Clients when either referenced from the EHLO, MailFrom, or Purported Responsible Addresses for various reasons. In addition, few SPF records define the intended reference or the email-address selection protocol.

When there is an SPF record published, it is typically just the version 1 record. This version lacks a means to define the intended reference, largely due to the animosity created when Sender-ID utilized SPF version 1 records. Sender-ID only recommends publishing version 2 records, together with version 1, when defining the Purported Responsible Address differently from that of the EHLO and MailFrom.

Will all the overhead involved with SPF records offer reliable benefits? See Appendix C for the example of the paypal.com SPF record which requires 20 DNS transactions to obtain both SPF and Sender-ID mechanisms, and then another 3 transactions to resolve MX addresses. When the goal is to utilize SPF status as a means to prevent spoofing, the PayPal “softfail” is problematic and may cause phished messages to appear more credible when they covertly assert an authorization for all SMTP Clients, as possible when using the SPF “exists” macro, for example.

In addition to not offering a reliable means to annotate messages, SPF/Sender-ID does not resolve look-alike and “cousin” domain risks which remain a serious problem. A list of such domains have been compiled by John Levine:

MYPAYPAL.COM
PAYPALSHOPS.COM

PAYPALSTORES.COM
PAYPALCARDSERVICES.COM
PAYPALMC.COM
PAYPALVISA.COM
PAYPALVERIFY.COM
SECURITY-PAYPAL.COM
PAYPALSTORE.COM
PAYPALSYS.COM
PAYPALMAIL.COM
SECURITIES-PAYPAL.COM
PAYPAL-EBAY.COM
PAYPALESCROW.COM
SECUREDPAYPAL.COM
PAYPALSERVICE.COM
WWW--PAYPAL.COM
PAYPALESHOP.COM
PAYPAL-SIGN-IN.COM
PAYPAL-VERIFYD.COM
PAYPALEMAIL.COM
PAYPAL-DATABASE.COM
PAYPAL-REDIRECT.COM
PAYPAL-BILLING.COM
PAYPALCOM.COM
PAYPALINC.COM
PAYPAL-MEMBERS.COM
PAYPAL-MEMBER.COM
WWWPAYPAL.COM
PAYPAL-VERIFIC.COM
PAYPALMONITOR.COM
SECURITY-MEASURES-PAYPAL.COM
PAYPAL-SECURE-UPDATES.COM
PAYPALPURCHASE.COM
RELOGIN-PAYPAL.COM
WWWPAYPALL.COM
PAYPAL-VERIFICATION-SYSTEM.COM
PAYPALCODE.COM
PAYPAL-SECURED-UPDATE.COM
PAYPAL-SERVICE.COM
PAYPAL-SECURE-INFO.COM
PAYPAL-VERIFICATION-MEMBERS.COM
CUSTOMER-PAYPAL.COM
USERS-PAYPAL.COM
CGI5-PAYPAL-VERIFYUSER.COM
PAYPAL-DBS.COM
ACCOUNTS-PAYPAL.COM
VERIFY-PAYPAL-ACCOUNT.COM
BILLINGUPDATEPAYPAL.COM
SSLSERVER-PAYPAL.COM
PAYPAL-HOME.COM
INFOUPDATE-PAYPAL.COM
PAYPAL-COM.COM

PAYPALSECURITY.COM
UPDATED-PAYPAL.COM
CLIENTS-PAYPAL.COM
REACTIVATE-PAYPAL.COM
SECURIZED-CGI-PAYPAL.COM
PAYPALSUPPORT.COM
EBAYPAYPAL.COM
PAYPALUPD.COM
PAYPAL-UPDATE-VERIFY.COM
WWW-PAYPAL.COM
EXPIRE-PAYPAL.COM
RE-PAYPAL.COM
WWW-PAYPAL-COM-LOGIN-CGI-WEBSER-CMD-LOGIN-RUN.COM
PAYPAL-CGI.COM
SECURE-PAYPAL-LOGIN.COM
UPDATE-YOUR-PAYPAL-ACCOUNT.COM
PAYPAL-INFORMATION-UPDATE.COM
SUSPENDED-PAYPAL.COM
PAYPAL-UPDATE-INFO.COM
UPDATE-PAYPAL-INFORMATION.COM
PAYPAL-UPDATE-INFORMATION.COM
UPDATE-YOUR-PAYPAL-ACCOUNT.COM
UPDATE-YOUR-PAYPAL.COM
PAYPAL-ACCOUNT-UPDATE.COM
PAYPAL-CONTROL.COM
PAYPAL-UPDATE-YOUR-INFO.COM
PAYPALINSURANCE.COM
USERS-UPDATES-PAYPAL.COM
SECURE-PAYPAL.COM
PAYPAL-INFOUP.COM
SAFE-PAYPAL.COM
PAYPALREPORT.COM
VERIFYBILLING-PAYPAL.COM
PAYPALACCOUNTSERVICE.COM
PAYPAL-CREDITCARD.COM
VERIFYBILLING-PAYPAL.COM
PAYPALACCOUNTSERVICE.COM
SUPPORTS-PAYPAL.COM
PAYPALBILLING.COM
PAYPALACCOUNTSERVICES.COM
PAYPALCUSTOMERCARE.COM
US-PAYPAL.COM
PAYPAL-UPGRADE.COM
PAYPAL-SSL.COM
PAYPAL-EUROPE.COM
ALERTS-PAYPAL.COM
PAYPAL-ONLINEINFO.COM
CGI-PAYPAL-UPDATE.COM
SSL-PAYPAL.COM
PAYPAL-CONFIRMINFO.COM
PAYPALNEWUPDATE.COM

PAYPAL-CGI-UPDATE.COM
PAYPAL-CGI-BIN.COM
RESTORE-PAYPAL-ACCOUNTS.COM
CUSTOMER-UPDATE-PAYPAL.COM
PAYPAL1.COM
PAYPAL-CUSTOMER-CENTER.COM
PAYPAL-ACCOUNT-UPDATES.COM
PAYPAL-SM.COM
SERVICE-ACCOUNT-PAYPAL.COM
PAYPAL-ONLINECONFIRM.COM
PAYPAL-INFOCONFIRM.COM
PAYPAL-VALIDATEINFO.COM
PAYPAL-INFO-UPDATE.COM
INFO-PAYPAL-UPDATE.COM
CGI-UPDATE-PAYPAL-ACCOUNT.COM
PAYPAL-SECUREINFOS.COM
PAYPAL-CGI-BIN-SECURE.COM
SECURE-PAYPAL-CGI-URL.COM
PAYPALAUSTRALIA.COM
PAYPAL-INTL-SERVICE.COM
ACCOUNTUPDATE-PAYPAL.COM
PAYPALNEWUPDATES.COM
EMAIL-PAYPAL.COM
PAYPAL-ORGANIZATION.COM
PAYPAL-CUSTOMER-CENTRE.COM
EBAY-AUCTION-PAYPAL.COM
EMAILPENDING-PAYPAL.COM
PAYPALSERVIICE.COM
SSLCONNECTION-PAYPAL.COM
E-PAYPAL.COM
PAYPAL-ACOUNT-CENTER.COM
PAYPAL-UPDATE-CENTER.COM
PAYPALCUSTOMERSERVICES.COM
PAYPALSECUREDPAYMENT.COM
CGI-INFO-PAYPAL.COM
PAYPAL-CLIENT-SUPPORT.COM
CONFIRM-PAYPAL-ACCOUNTS.COM
PAYPAL-INFOVALIDATE.COM
RESTORE-PAYPAL-INFO.COM
CS-PAYPAL.COM
IMG-PAYPAL.COM
PAYPAL-COM-CGI-BIN-CONFIRMATION-PP545454.COM
SIGNIN-ACCOUNT-PAYPAL.COM
PAYPAL-MEMBERS-VALIDATION.COM
PAYPAL-SECURE-UPDATE.COM
PAYPAL-ACCOUNT-SERVICE.COM
UNLOCK-PAYPAL.COM
EMAILS-PAYPAL.COM
PAYPAL-SUBMIT.COM
PAYPAL-SECURITY-SYSTEM.COM
UPDATE-PAYPAL-SYSTEM.COM

CONFIRM-PAYPAL.COM
PAYPAL-SETUP.COM
PAYPAL-SECURITY-UPDATES.COM
ONLINE-PAYPAL-UPDATE.COM
US-PAYPAL-SUPPORT.COM
PAYPAL-SUPPORT-SSL.COM
PAYPAL-PAYMENTS.COM
PAYPAL-SERVERS.COM
PAYPAL3.COM
PAYPAL-LOGIN.COM
VERIFY-PAYPAL-US.COM
VERY-PAYPAL.COM
RESUBMIT-PAYPAL.COM
UPDATEUSER-PAYPAL.COM

One of these domains is valid. Can you spot the real one from the fakes? Since many recipients only view the “display-name”, blocking exact spoofs (which the paypal SPF record does not do) will still provide little protection. Adding annotation that indicates a “pass” SPF result will seriously risk misleading recipients and actually increase their risks. For example, in the case of Sender-ID, the From header field may contain an exact spoof of a phished domain and still obtain a “pass” result.

SPF Adoption

So where does SPF adoption stand, and is there reason to think the risks posed by SPF are increasing? SPF records are published in about 3% of the domain that have an MX record according to a study published by Andrew Newton, one of the chairs of the now closed IETF MARID working group (<http://hxr.us/blojsom/blog/grumpops/>). In comparison, Trend Micro evaluated a small sample of messages from known abusive sources. The results of the referenced SPF records are as follows:

none/invalid/error	130557	#	77%
pass	348	+	0.2%
neutral	24207	?	14%
softfail	9643	~	6%
fail	4417	-	2.6%
TOTAL	169172		

For a better understanding of who is publishing SPF records and perhaps why, a sampling from a group of Fortune 100 and top 20 volume domains were reviewed. While this group has adopted the use of SPF to a greater amount than the typical domain, the distribution of domains tends to suggest some possible motivations.

Percentage distribution of Fortune 100 SPF results:

none/invalid	58%
neutral	9%
softfail	22%
fail	11%.

Of those Fortune 100 domains with above average traffic, the results are:

none/invalid	73%
neutral	6%
softfail	13%
fail	9%,

which is also fairly consistent with the top 20 high volume domains:

none/invalid	70%
neutral	10%
softfail	10%
fail	10%.

There seems to be a disproportionate number of neutral results for known abusive sources compared to the percentages found within the group of Fortune 100 or the top 20 high volume domains. One explanation for a higher number of neutral results of abusive sources could be due to many large providers publishing SPF records that request the neutral handling of undefined sources. In other words, these records request that messages from a source not defined in the SPF record be handled in the same fashion as when no SPF record is published.

Providers, such as AOL, Bell South, Gmail, and Verizon, utilize neutral SPF records. Some providers even request the positive handling of messages when the SMTP client is not authorized, such as Bell Canada. A request for positive handling might indicate that neutral records are not always treated “as-if” no SPF record exists when the source is undefined, or that lacking an SPF record is not always acceptable. Fortunately, providers such as AT&T et al, Cablevision, Comcast, Cox, Earthlink, PeoplePC, Mindspring, and Yahoo!, do not offer any SPF records which should allay some concerns about not publishing.

To summarize, about 10% of the Fortune 100 and top 20 volume domains publish SPF records intended to block messages coming from undefined sources. One of the notable high volume domains is charter.com which uses a strict SPF record that asserts “fail” rather than “softfail” for residential emails. This company uses Hotmail for outbound MTAs and is owned by Paul Gardner Allen, a co-founder of Microsoft.

Charter.com's use of negative SPF records may be seen as a means for inducing the use of Sender-ID in the face of the resulting (and often expensive) support calls. However, Charter Communications (charter.com) may be having difficulties of their own. Either charter.com customers are willing to have their outbound messages blocked when a recipient is using a forwarding account, make irresolvable support calls complaining about the problem, or they find their email-services elsewhere. The other high volume domain asserting a “fail”, unlike charter.com, does not appear to have these SPF records referenced from email-addresses. There is only a single MTA for this high-volume domain which likely ensures this domain is not being used to receive the high volume of email traffic.

Still, when “soft-fail” and “fail” categories are combined, SPF records only differentiate about 20% of domains when a message is from an undefined source. However, combining these categories is not how these results were intended to be

used. The expectation was that a “softfail” only lowered the ratings of a message. Of the known abusive sources, combining these two categories still only blocks about 9% of the messages. When rejection is done properly, i.e. for only those sources that result in a “fail”, less than 3% of the messages are being blocked.

SPF does not appear to be at any tipping point. There also appears to be valid reasons why providers will continue to not publish these records. From our experience, often the CIDRs in these records encompass too many addresses. The lack of granularity makes these records less practical for dealing with abuse related issues. SPF records also create problems when a receiving domain applies more stringent handling than what the SPF record requested. Even requests for neutral handling may still result in strict handling being applied. As a result, message are blocked and support desks are being called.

It might be safe to just let SPF fade away, provided that SPF actually does fall out of favor. Many of the problems which SPF have been unable to resolve are successfully handled by DKIM. DKIM overcomes forwarding issues and does not depend upon any headers added by the MDA for authentication. When the goal is to apply annotations for trustworthy domains, DKIM far better fulfills the role of authenticating the source of the message.

DKIM does not need to stop at just authenticating the source. Names can be associated using a simple MailFrom policy record. For example:

```
<base32(sha-1(signing-domain))>._DKIM-M.<mailfrom domain> TXT “d=signing-domain”
```

See: <http://www.ietf.org/internet-drafts/draft-otis-dkim-dosp-01.txt>

This DKIM Originator's Signing Policy (DOSP) record can indicate which signing-domains validate the MailFrom email-address prior to a bounce being issued, for example. Such a scheme would allow any number of signing-domains to be associated with the MailFrom header and still need only a single DNS transaction. This method would not suffer from the extreme amplification and forwarding concerns created by SPF address path registration schemes. Using this strategy only requires a single DNS transaction prior to safely bouncing a message.

If Microsoft wishes to continue the use of the PRA algorithm, the DOSP draft defines how all the Purported Responsible Address originating domains can be defined by using this scheme. DOSP in conjunction with DKIM can even validate the use of the EHLO. DKIM and DOSP provides a safe means for validating various email message headers while still avoiding much of the risks caused by a need to compile a comprehensive list of IP addresses of all possible SMTP Clients as required by SPF.

The Future of SPF

Should MAAWG promote or demote the use of SPF? This document describes in the text below an email induced Denial of Service threat caused by SPF scripts. These scripts are used to evaluate the association of a source domain-name with the sending-system. SPF scripts attempt to establish a domain-name association through

the construction of an extensive IP address list of all the sending-systems. Expectations of an association have become problematic. Message handling might be negatively affected without an apparent domain-name relationship discovered between the sending-system and either the message envelope or the message itself.

The previous example of the MailFrom policy record illustrated a safe name-based alternative to SPF that associates a source domain-name with the sending-system. This can be done by comparing a domain-name against a verified signing-domain. This alternative name-based association also allows for the verification of the sending-system's EHLO. An EHLO association would insure the message is not being replayed by an unrelated entity. This alternative association method involves a single DNS transaction, instead of potentially the hundreds that might be needed with SPF.

Initially verifying the EHLO by using just an address resource record versus compiling an address list by using SPF is another method for avoiding dangerous multiplicative effects. Amplification is created when a large number of common DNS resources are relied upon by a sequence of Mail Handling Systems (MHS) forwarding a message. A verified EHLO provides a name-based identifier for establishing the requisite DoS protections to mitigate an attack, and will not result in amplification concerns.

SPF's use of indirect references found in the text script, PTR and MX records makes SPF a highly dangerous method to verify an anonymous SMTP Client's authorization because of the amplification risks. Limiting common resources used for evaluating a domain-name to a single conditional DNS transaction, dramatically reduces the scale of the potential amplification. Initiating this process by authenticating the EHLO is invariably safe, as each SMTP Client should incorporate a unique resource record to be accepted.

SPF and the Basic Problem

Two experimental RFCs "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1" (RFC4408) and "Sender ID: Authenticating E-Mail" (RFC4406) relate various email source domains with the IP address of the SMTP client by assembling an extensive list of IP addresses. Both experimental protocols utilize the SPF script syntax to manipulate names and content of Resource Records (RRs) obtained through DNS transactions. The SPF script is stored in one or more TXT RRs that are intended to hold generic character-strings. An additional lookup may be required to ascertain whether SPF specific RR types are being used instead of TXT RRs.

SPF script employs string related macros, Address RRsets containing IP address information, MX RRsets containing the name and preference numbers of Mail Transfer Agents (MTAs), and the PTR RRsets located in the reverse reference IP address domains. Although this SPF script can be utilized in a number of ways, normally the intent is to return IP addresses of all systems directly involved with sending messages for a particular domain. The SPF script may define these addresses with CIDR notation and/or lookups of various RRsets. In doing so, SPF drastically alters the scale of a DNS answer.

The SPF script places limits on the number of DNS transactions permitted at each Mail Handling Service (MHS) in the path of the message when evaluating each source domain-name. SPF script may invoke 10 DNS transactions for various RRsets, where up to 10 follow-on DNS transactions may then occur following each. When the script does not provide a “pass” result, an additional lookup might be made to obtain a macro expanded explanation TXT RR. As an example, evaluating just one domain-name per MHS may involve lookups for 1 TXT RR plus 10 MX RRsets plus 100 A RRsets for a total of 111 DNS transactions. There can be 11 SPF TXT RRs containing script in different domains. However, each of the 10 MX RRsets can contain 10 unique domain-names that can span 100 different victim domains.

Currently, there are two different domain-names in a message that are evaluated using SPF records. There is the RFC2821.MailFrom, and the experimental and proprietary “Purported Responsible Address in E-Mail Messages” (RFC4407), where verifying each domain-name separately invokes the SPF evaluation process that may directly or indirectly reference the same resources. Referencing the same resource by a sequence of MHS creates the basic problem. There have been suggestions that the DKIM signing-domain might also be evaluated using SPF as an added scope, where multiple signatures from different domains may also exist in a single message. This adds to the potential amplification.

SPF script is not predicated upon verifying the domain controlling the MTA. Obfuscation of the controlling domain may even erroneously shift accountability onto the often hapless email-address domain owners who typically rely upon third-party services and may publish open-ended address lists (neutral SPF records).

The address-list approach prevents fair name-based accrual of MTA behaviors as a means to establish effective DoS protections. To be effective and fair, a reputation or DoS protection scheme must indicate specifically what domain is in control. SPF scripts might reference only victim domains unrelated to the control of the MTA, and provide inconclusive results subsequent to the evaluation. Although this may add to the amplification, there would be no indication that there is an amplification problem.

Defense against Denial of Service Attacks

The DoS concern specific to SPF scripts is manifold. SMTP is a store and forward protocol that distributes the SPF script threat to otherwise reputable MHS. This distribution multiplies the impact of the script when many common DNS resources from multiple domains are utilized by subsequent MHS. By encompassing multiple domains, the SPF script may not establish an accountable domain-name subsequent to evaluation when inconclusive results are obtained. Owing to these conditions, there is no reasonable strategy that can be used to mitigate the potential harm created by a distributed SPF script generated DoS attack. To estimate the potential for the SPF script generated threat, the level of network amplification is considered for this SPF DNS scripting scheme.

A typical stance taken when discussing DoS concerns is that there are other network amplification techniques to facilitate DoS exploits. One such exploit utilizes DNS servers. This particular exploit depends upon a lookup to be amplified by the

difference between the query size and that of the answer, in addition to the number of queries made in a recursion process. To roughly estimate the network impact created by DNS UDP traffic, 1.3 queries will be assumed to occur on average from every DNS lookup, with an average query size of 100 bytes and an average answer of 500 bytes. Based upon these coarse assumptions, the resulting DNS amplification is about 13 to 1 when the source IP address of the lookup is also spoofed to be that of the targeted domain. Some techniques have increased the level of this exploit by employing the RFC2671 EDNS0 extension to query large RRsets that exceed the network MTU, and cause packet fragmentation. This technique can achieve an impact with about a 60 times amplification, however, the source of the large RRset can be identified.

About 1 K bytes of outbound TCP traffic may be needed to send a small SMTP message. SPF scripts can target 100 DNS transactions when evaluating a single domain-name. In estimating the targeted amplification, the number of common DNS transactions is multiplied by the number of recipients in different domains, times the different domain-names evaluated within the same message, times the number of each sequential MHS that does not share a common DNS cache. A message sent to only 1 recipient who also utilize SPF evaluation in their MUA could then create about 312 to 1 network amplification directed toward a targeted domain. As a comparison, evaluating domain-names using SPF represents about 24 times the threat caused by an exploit using recursive DNS, and about 5 times the threat caused by the use of EDNS0. Unlike the EDNS0 technique, the source of the problem remains hidden.

The network amplification exploit using SPF may also leverage a provider's SMTP servers that are available from systems an attacker may have compromised. It is common for tens of thousands of compromised systems to act in concert to disseminate spam, while each system may conform to normal use profiles. These spam messages could have a small list of recipients that further amplify the level of the attack. Perhaps these messages contain an average of 10 recipients. These messages may purport to be from email-addresses with random local names and sub-domains, beneath a list of top level domains. All of these different domains can nevertheless reference similarly targeted SPF records. The messages in the attack could be a "stock tip" ending up in a spam folder. No single message may convey the same information, and yet still target the same victim regardless who appears to be the author, or which folder is ultimately selected to receive the message.

$$(1.3 \times (100+500))/1000 = .78 \text{ DNS/SMTP Gain Factor}$$

SPF Script Network Amplification at victim domain:

$$\text{RR} \times \text{MHS} \times \text{Domain-Names} \times \text{Recipients} \times \text{DNS/SMTP} = \text{Gain}$$

$$100 \times 2 \times 2 \times 1 \times .78 = 312$$

$$100 \times 2 \times 1 \times 10 \times .78 = 1560$$

SMTP Name Path Network Amplification at victim domain:

$$\text{RR} \times \text{MHS} \times \text{Domain-Names} \times \text{Recipients} \times \text{DNS/SMTP} = \text{Gain}$$

$$1 \times 2 \times 2 \times 1 \times .78 = 3$$

The SPF script facilitates canvassing by using a covert DNS server that looks for domains that evaluate SPF. This obtained knowledge can help facilitate a sustained DoS attack. Without altering the SPF script, local-part label macros provided by SPF can instantiate different queries for a series of messages from the same set of domains. Attackers using this technique that ensures the DNS information is not locally cached, will inundate the targeted domain with DNS transactions. It will also flood the local DNS cache which may expel previously obtained information prior to its normal expiration.

Using SPF script to evaluate a domain-name poses risk to the integrity of DNS itself. A poisoning exploit often attempts to both flood the DNS answering for the RR being poisoned, and to gain access to the DNS whose cache is to be poisoned. Both of these efforts are facilitated by SPF script. The SPF script also provides the ability to query a covert DNS server that tracks the source IP address, ports, and Transaction IDs of DNS transactions to improve upon the subsequent construction and the timing of poison answers.

In comparison, the name-based path registration approach provides a 100 to 1 reduction in the amount of network amplification with a maximum of only one conditional DNS transaction of a common resource. The name-based approach also always provides an accountable domain-name for effective DoS protections; see "<http://www.ietf.org/internet-drafts/draft-otis-dkim-dosp-01.txt>". The name-based path registration alternative to SPF starts by verifying the EHLO. This establishes a name-based defense that fairly holds the domain controlling each sending system accountable for any abuse. This approach also ensures that prior to acceptance, there is no amplification of DNS transactions made with a victim domain, as each subsequent MTA forwarding a message offers their own EHLO that exists within their own domain or EHLO verification fails. A failure to verify the EHLO allows the recipient to delay subsequent acceptance of messages from both the EHLO and the associated client IP address as an effective DoS defensive tactic. Once EHLO verification is established as a requisite, message refusals could then be handled in a permanent fashion.

The safe name-based alternative to the SPF script method requires just one or two steps. The first step ensures the EHLO of the MTA is directly verified with a single DNS transaction. Once the EHLO is verified, and when the EHLO is within the domain-name in question, no second step is needed. Otherwise, the second step attempts to establish a domain name association by making a single forward reference policy record lookup from the domain in question or as described previously. These associations would simply list the provider's domains used by the owner of the email-address domain. A failure to verify the EHLO or to find an association with the message domain-names can delay acceptance of the message. EHLO verification is comparatively easier to administer than SPF scripts.

The Exploit Example

This section and the accompanying appendix information is in response to requests made by a few large providers. Explaining the threat in general terms proved difficult for many to understand. This example represents one of many possible techniques that are enabled by the various SPF script parsing applications. Other

techniques can further increase the severity of such an attack, but are not reviewed. As with any script, the permutations of possible actions are incredibly vast.

This Exploit Example makes use of script parser capabilities in many SPF libraries, although libspf2 by Wayne Schlitt et al, by default, is at half the recommended limit of RRs processed within an MX RRset. It is not uncommon for an RRset to exceed this lowered limit. For example, more than this number of MX RRs are found within t-online.de or nokia.com. These domains also do not publish SPF TXT records, which means even when a default SPF script containing the MX lookup mechanism is used instead, the lowered RRset cut-off randomly prevents some MX RRs from being examined.

Although several libraries impose the recommended limits, the original SPF script's limiting mechanism was recursion depth. The recursion depth limited DNS transactions to the number of mechanisms that could be defined within 20 records that then was changed to 10 records. Even at a depth of 10, the recursive method allows for an exceedingly high number of DNS transactions. There are several other recent libraries where no limits are imposed upon the number of MX RRsets, other than the number returned within the MX lookup. SPF requires the acquisition of the TXT SPF record, which may then direct queries to 10 or 11 other domains. Most would consider that approach as mandating 10 times the number of DNS transactions, but SPF also adds highly risky indirection enabled through SPF script and macro expansion.

Taking advantage of just one level of indirection made possible by SPF macros, the Exploit Example closely matches the initial amplifications estimates, but where the request size increases and the response is reduced by about the same amount. The Example Exploit therefore represents a fairly symmetrical attack, and requires little knowledge of the victim's DNS information. The traffic required to establish both the TXT and MX resource record sets should be excluded from the gain estimates, as the attack is able to take advantage of a difference between negative cache retention, and the TTL of these RRsets.

Often negative caching lasts for a few minutes, but the RRset could be retained for many hours. After the requesting DNS servers have been seeded, the level of the attack could maintain a steady barrage while requiring far less effort. The Time-To-Live for negative DNS caching may be determined by the recipient, or represent the lesser of the SOA TTL, or the SOA MINIMUM field, depending upon the recipient's implementation, see RFC2308.

The attacker would initially populate TXT and MX RRsets that point toward the victim's domain. Referencing different MX RRsets does not require an additional SPF TXT script. Instead, the macro expansion capability can be used to reference a vast array of MX records, as illustrated by the Example Exploit which uses the local-part as a selector. Optimally, this reference would cycle at a period longer than the resolver's negative cache retention period. A reference to a covert DNS server that replicates the SOA record parameters of the victim could signal the optimal cycle period.

The level of attack described in the presentation made for The DNS Operations,

Analysis, and Research Center (DNS-OARC) called “Recent DNS Reflector Attacks From the Victim and the Reflector POV” by Frank Scalzo of Verisign (see <http://public.oarci.net/files/mlarson-dnsops.pdf>) indicated the 35,000 amplifying reflectors caused on average 144kbps (18KBps) to be exchanged with the victim. A similar level of attack could be achieved by the Example Exploit occurring 0.28 times a second or 17 times per minute. When 2 domains are being examined, as may occur with Sender-ID, this level of attack would require just 8.5 messages per minute.

Processing 8.5 messages per minute would represent a very small percentage of the emails currently being handled by many providers. Already a majority of these emails are considered abusive. A large provider may issue as many as 25,000 messages per minute and receive emails at twice that rate. A strategy that sends messages through network providers, addressed to 10 individuals on average from 35,000 compromised systems at 50 messages per hour, represents a scale of concerted attack commonly seen today. If these messages get processed by spam filtering applications that also uses SPF/Sender-ID, the attack rate could then drop to 25 per hour and still sustain the same barrage.

This type of activity could be considered a good way to leverage efforts. While sending spam, perhaps containing malware, authoritative DNS servers are taken out by knowing which domains incorporate poorly considered, and ultimately fatally flawed, SPF parsers. Once the authoritative DNS servers are disabled, the same SPF script can illicit queries through thousands of provider's DNS servers, and then trigger a barrage of poison answers. These attacks can be done through two levels of indirection where it would be difficult to correlate what domain is inducing the problem, or how it can be stopped. The SPF RRsets causing trouble will not appear in a log. In the Example Exploit, the message is accepted with a neutral status without any evidence it was related to the victim's domain.

SPF/Sender-ID reduces security. Although there was already “A DNS RR Type for Lists of Address Prefixes (APL RR)” (RFC3123) that could serve extremely well for white-listing, SPF was developed as a method that avoids declaring who are the sending system's administrators and offers the feature-rich/security-poor scripting found with HTTP/TCP. Sender-ID was even originally specified using XML contained within 2KB DNS resource records, expecting DNS/TCP would not become a problem. With the highly distributive anonymous nature of email, reducing security while crime is rampant, is foolhardy at best. SPF/Sender-ID continues to place the DNS infrastructure at risk. Adopt DKIM, EHLO verification, Name-Path registration, and the use of APL RRs. This allows SPF to be phased out. Such a change would offer additional security, without actually reducing it instead.

Appendix A

Fortune 100 SPF records

This was not a complete list compiled using public search engines of domains controlled by these companies. Most of the domains considered have published at least two MTA addresses. Those domains marked with an asterisk represent above average traffic. The status of the company's use of SPF is weighted to increase the number of companies reported as using SPF, perhaps even when the majority of the domains are without SPF records.

? Exxon Mobil <exxonmobil.com>=1?* <exxon.com>=# <mobil.com>=# <esso.com>=#
<mobil.com.au>=#

? Wal-Mart Stores <walmart.com>=1?* <seiyu.co.jp>=#* <walmart.ca>=#
<walmartfoundation.org>=# <samsclub.com>=#

General Motors <gm.com>=#* <gmbuypower.com>=# <chevrolet.com>=# <gmacfs.com>=#
<gmfleet.com>=# <gmgoodwrench.com>=# <gmcad.com>=# <pontiac.com>=# <buick.com>=#
<cadillac.com>=# <gmsa.com>=# <oldsmobile.com>=# <saab.com>=# <holden.com.au>=#
<onstar.com>=# <gmacmortgage.com>=# <gmam.com>=#

~ Chevron <chevron.com>=1~* <cpchem.com>=1-* <chevrontexaco.com>=1~ <texaco.com>=#

Ford Motor <ford.com>=#* <mazdausa.com>=#* <hertz.com>=1:!2-* <ford.com.au>=#
<jaguar.com>=# <mclmotorcars.com>=# <landrover.com>=# <lincoln.com>=#
<mercuryvehicles.com>=# <volvocanada.com>=# <astonmartin.com>=# <volvocars.com>=#
<fordvip.com>=#

ConocoPhillips <conocophillips.com>=# <conocophillipsalaska.com>=#
<conoco.com>=# <phillips66.com>=#

General Electric <ge.com>=#* <gepower.com>=#* <gecapital.com>=#* <nbc.com>=#*
<nbcuni.com>=#* <universalstudios.com>=# <gecas.com>=#

~ Citigroup <citigroup.com>=1~* <citibank.com>=1~* <smithbarney.com>=1~*
<citi.com>=1~ <citicorp.com>=1~ <citifinancial.com>=1~ <primerica.com>=#*
<primericaaal.com>=# <primericafna.com>=# <lavatrading.com>=# <yieldbook.com>=#
<citibank.ru>=1~

~ American Intl. Group <aig.com>=1~* <aighawaii.com>=#* <aigag.com>=1~
<aigvalic.com>=1~ <aigenvironmental.com>=#

~ Intl. Business Machines <*.ibm.com>=1~* <lotus.com>=#* <tivoli.com>=#

Hewlett-Packard <hp.com>=#* <compaq.com>=#* <hp.ru>=# <hewlett-packard.de>=#

~ Bank of America Corp <bankofamerica.com>=1~* <mbna.com>=1~*

<bofabusinesscapital.com>=# <bofasecurities.com>=#

- Berkshire Hathaway <berkshirehathaway.com>=# <geico.com>=1-* <genre.com>=#*
<homeservices.com>=#* <businesswire.com>=1~* <pamperedchef.com>=#*
<hhbrown.com>=#* <ctbinc.com>=# <wescofinancial.com>=# <shawfloors.com>=#
<shawadsources.com>=#

? Home Depot <Homedepot.com>=1?* <hughessupply.com>=#* <expo.com>=#
<homedepot.ca>=# <homedepot.com.mx>=# <homedepotfoundation.org>=# <wmsbros.com>=#
<hdsupply.com>=1~ <apexsupply.com>=#

- Valero Energy <valero.com>=1-* <valerolp.com>=1-

McKesson <mckesson.com>=#* <mooremedical.com>=#* <zeemedicalinc.com>=#*
<mckhboc.com>=#* <mckgenmed.com>=# <mckessonaps.com>=#

- J.P. Morgan Chase & Co. <jpmorgan.com>=1-* <chase.com>=1-* <bankone.com>=1-*
<jpmorganfunds.com>=1-

? Verizon Communications <verizon.com>=1~* <verizonwireless.com>=#* <mci.com>=1?*
<vzavenue.net>=#* <uu.net>=#* <superpages.com>=#* <verizonbusiness.com>=1?*
<verizon.net>=1?*

Cardinal Health <cardinalhealth.com>=# <cardinal.com>=#* <alarismed.com>=#*
<medmined.com>=#* <ghx.com>=#* <medicineshoppe.com>=#* <gala.com>=#

Altria Group <altria.com>=#* <kraft.com>=#* <pmusa.com>=#

Kroger <kroger.com>=#* <ralphs.com>=# <kingsoopers.com>=# <citymarket.com>=#
<frysfood.com>=# <food4less1.com>=# <foodsc01.com>=# <fredmeyer.com>=#

State Farm Insurance Cos <statefarm.com>=#*

Marathon Oil <marathon.com>=# <marathonpetroleum.com>=# <speedway.com>=#

Procter & Gamble <pg.com>=#* <gillette.com>=#* <iams.com>=#* <pantene.com>=#*
<duracell.com>=#* <oralb.com>=# <pringles.com>=#

~ Dell <dell.com>=1~* <alienware.com>=1?*

~ Boeing <boeing.com>=1~* <cdgnow.com>=#* <alteontraining.com>=1~*

~ AmerisourceBergen <amerisourcebergen.com>=#* <pharmerica.com>=1~*

Costco Wholesale <costco.com>=#* <costco.ca>=#

? Target <target.com>=1?*

Morgan Stanley <morganstanley.com>=#* <morganstanleyindividual.com>=#
<morganstanley.co.jp>=# <msdwhomeloans.com>=# <morganstanleychina.com>=#
<quilter.co.uk>=#

- Pfizer <pfizer.com>=1-* <pfizer.com.au>=#* <warner-lambert.com>=#
<pfizerindia.com>=#

Johnson & Johnson <jnj.com>=#* <baby.com>=#* <neutrogena.com>=#*
<natrecor.com>=#* <sciosinc.com>=#* <transformpharma.com>=#* <depuyl.de>=#
<spinology.nl>=# <jnjmedical.at>=# <jnjmedical.nl>=# <janssenanimalhealth.be>=#
<canceranemi.nu>=# <jnjaustria.at>=# <jnjcz.cz>=# <mcneilhealth.co.uk>=#
<roc.com>=#

Sears Holdings <searsholdings.com>=# <sears.com>=#* <kmart.com>=#* <osh.com>=#*
<landsend.com>=#* <sears.ca>=#* <dmserv.com>=#* <searsclean.com>=#

Merrill Lynch <ml.com>=#* <freedomfinance.co.uk>=#* <berndale.com.au>=#

MetLife <metlife.com>=#* <texlife.com>=#* <walnutstreet.com>=#* <rgare.com>=#*

Dow Chemical <dow.com>=#* <dowcorning.com>=#* <unioncarbide.com>=#

UnitedHealth Group <unitedhealthgroup.com>=# <uhc.com>=#* <americhoice.com>=#*
<ingenix.com>=#* <unitedbehavioralhealth.com>=# <dbp.com>=# <spectera.com>=#

Wellpoint <wellpoint.com>=#* <healthlink.com>=# <healthcore.com>=#*
<anthem.com>=#* <bluecrossca.com>=#* <bcbsmo.com>=#* <goldenwestdental.com>=#
<meridianresource.com>=# <precisionrx.com>=# <ugsmedicare.com>=# <cmsins.com>=#
<unicare.com>=# <bcbsga.com>=#

AT&T <att.com>=#* <att.net>=#* <cingular.com>=#* <cingular.net>=#* <sbcb.com>=#*
<sbcb.net>=#* <pacbell.net>=#* <swbell.net>=#* <attbusiness.net>=# <attglobal.net>=#
<pacbell.com>=#

? Time Warner <timewarner.com>=# <aol.com>=1:2?* <hbo.com>=#* <newline.com>=#*
<turner.com>=#* <tbs.com>=# <time.com>=# <warnerbros.com>=#*
<timewarnercable.com>=#

~ Goldman Sachs Group <goldmansachs.com>=# <gs.com>=1~*

~ Lowe's <lowes.com>=1~*

United Technologies <utc.com>=#* <carrier.com>=#* <otis.com>=#*
<kiddeaerospace.com>=# <miltonroy.com>=# <sullair.com>=# <sundyne.com>=# <pratt-
whitney.com>=# <sikorsky.com>=# <utcfireandsecurity.com>=# <utcpower.com>=#

United Parcel Service <ups.com>=#* <ups-scs.com>=#* <upsfreight.com>=#*
<upsmailinnovations.com>=#

~ Walgreen <walgreens.com>=1~*

~ Wells Fargo <wellsfargo.com>=1~*

Albertson's <albertsons.com>=#* <savon.com>=#

~ Microsoft <microsoft.com>=1~* <msn.com>=1~* <hotmail.com>=1~*
 # Intel <intel.com>=#* <intc.com>=#
 # Safeway <safeway.com>=#* <safewayfoundation.org>=#
 - Medco Health Solutions <medcohealth.com>=1-* <medco.com>=1-*
 # Lockheed Martin <lockheedmartin.com>=# <lmco.com>=#* <unitedspacealliance.com>=#
 # CVS <cvs.com>=#* <pharmacare.com>=#* <minuteclinic.com>=#
 # Motorola <motorola.com>=#* <meshnetworks.com>=# <winphoria.com>=# <ttpcom.com>=#*
 <4thpass.com>=#
 - Caterpillar <cat.com>=1-*
 ? Archer Daniels Midland <admworld.com>=1?* <admissi.com>=#* <admani.com>=#
 # Wachovia Corp. <wachovia.com>=#* <wachoviasec.com>=#* <wfsfinancial.com>=#*
 <evergreeninvestments.com>=#* <wfb.com>=#
 # Allstate <allstate.com>=#*
 - Sprint Nextel <sprint.com>=1:2-*
 # Caremark Rx <caremark.com>=#* <accordant.net>=#* <neuromedical.com>=#
 <consumerhi.com>=# <iscribe.com>=#
 # PepsiCo <pepsico.com>=#* <pbsg.com>=#* <pepsi.ru>=#* <smiths.com.au>=#*
 <pepsi.com>=# <quakeroats.com>=# <tropicana.com>=# <corpex.com>=#
 <smithssnackvend.com.au>=# <pepsi.be>=# <pepsi.cz>=# <lays.lv>=# <doritos.nl>=#
 <pepsi.no>=# <pepsi.co.uk>=#
 ~ Lehman Brothers <lehman.com>=1~*
 - Walt Disney <disney.go.com>=#* <go.com>=#* <abc.com>=1-* <disney.com>=1-*
 # Prudential Financial <prudential.com>=#* <prudential.co.jp>=#*
 <pramericarei.com>=# <prudential.co.kr>=# <gibraltar.co.kr>=# <pru.co.kr>=#
 # Plains All Amer. Pipeline <paalp.com>=#*
 ~ Sunoco <sunocoinc.com>=1~ <sunoco.com>=#
 - Northrop Grumman <northropgrumman.com>=#* <ngc.com>=1-*
 # Sysco <sysco.com>=#* <syscosac.com>=# <syscodenver.com>=# <syscowcf.com>=#
 <buckheadbeef.com>=# <syscostlouis.com>=# <syscocentralpa.com>=1?
 <syscodallas.com>=# <ambriggs.com>=# <baraboosysco.com>=1? <syscovancouver.com>=1~

~ American Express <americanexpress.com>=1~*

FedEx <fedex.com>=#* <kinkos.com>=#*

Honeywell Intl. <honeywell.com>=#* <fram.com>=#* <grimesaero.com>=#
<holtsauto.com>=# <honeywellauto.com>=#

Ingram Micro <ingrammicro.com>=#* <techpac.co.nz>=#* <avadgp.com>=#
<avadme.com>=#

DuPont <dupont.com>=#* <antecint.co.uk>=# <dupontpowder.be>=#
<dupontelastomers.com>=# <pioneer.com>=#

- New York Life Insurance <newyorklife.com>=1~*

Johnson Controls <jci.com>=#* <york.com>=#*

~ Best Buy <bestbuy.com>=1~*

Delphi <delphi.com>=#*

Hartford Financial Services <thehartford.com>=#*

Alcoa <alcoa.com>=#*

Tyson Foods <tyson.com>=#*

~ TIAA-CREF <tiaa-cref.org>=1~*

~ International Paper <internationalpaper.com>=1~ <hammermill.com>=1~

~ Cisco Systems <cisco.com>=1~*

HCA <hcahealthcare.com>=# <healthonecares.com>=#

~ St. Paul Travelers Cos. <stpaultravelers.com>=1~ <stpaulguarantee.com>=#*

News Corp. <newsCorp.com>=#*

Federated Dept. Stores <fds.com>=#*

Amerada Hess <hess.com>=#*

Coca-Cola <coca-cola.com>=# <cokecce.com>=#* <sacccoke.com>=#

Weyerhaeuser <weyerhaeuser.com>=#*

Aetna <aetna.com>=#*

Mass. Mutual Life Ins. <massmutual.com>=#*

? Abbott Laboratories <abbott.com>=1?*
Comcast <comcast.com>=#* <comcast.net>=#*
Merck <merck.com>=#*
Deere <deere.com>=#*
? Raytheon <raytheon.com>=1?*
Nationwide <nationwide.com>=#*
- Washington Mutual <wamu.com>=1-*
~ General Dynamics <generaldynamics.com>=1~ <gdls.com>=#* <gdeb.com>=#*
<nassco.com>=#

Appendix B

Top 20 high volume domains:

<rima-tde.net>=1- <rr.com>=1~ <verizon.net>=1? <tpnet.pl>=# <comcast.net>=#
<proxad.net>=# <wanadoo.fr>=# <telecomitalia.it>=# <yahoo.com>=# <ttnet.net.tr>=1~
<charter.com>=- <ono.com>=# <hinet.net>=# <telesp.net.br>=# <t-dialin.net>=#
<interbusiness.it>=# <veloxzone.com.br>=# <bezeqint.net>=# <gaoland.net>=#
<brasiltelecom.net.br>=1?

Appendix C

Paypal SPF Example

```
paypal.com. 3600 IN TXT "v=spf1 mx include:s._spf.ebay.com include:m._spf.ebay.com  
include:p._spf.ebay.com include:c._spf.ebay.com include:spf-1.paypal.com ~all"  
paypal.com. 3600 IN TXT "spf2.0/pra mx include:s._sid.ebay.com  
include:m._sid.ebay.com include:p._sid.ebay.com include:c._sid.ebay.com ~all"  
60/415 = 3 addresses (MX repeated in s._spf.ebay.com CIDs)
```

```
s._spf.ebay.com. 3600 IN TXT "v=spf1 ip4:66.135.209.192/27 ip4:66.135.197.0/27  
ip4:64.4.240.64/27 ip4:64.4.244.64/27 ~all"  
65/269 = 128 addresses
```

```
m._spf.ebay.com. 3600 IN TXT "v=spf1 ip4:66.135.215.224/27 ip4:216.33.244.96/27  
ip4:216.33.244.84 ~all"  
65/250 = 65 addresses
```

p._spf.ebay.com. 3600 IN TXT "v=spf1 ip4:67.72.99.26 ip4:206.165.246.83 ip4:206.165.246.84 ip4:206.165.246.85 ip4:206.165.246.86 ip4:64.127.115.252 ip4:194.64.234.129/27 include:p2._spf.ebay.com ~all"
65/347 = 38 addresses

p2._spf.ebay.com. 3600 IN TXT "v=spf1 ip4:65.110.161.77 ip4:204.13.11.49 ip4:204.13.11.51 ~all"
66/242 = 3 addresses

c._spf.ebay.com. 3600 IN TXT "v=spf1 ip4:12.155.144.75 ip4:62.22.61.131 ip4:63.104.149.126 ip4:64.68.79.253 ip4:64.94.204.222 ip4:66.135.215.134 ip4:67.72.12.29 include:c2._spf.ebay.com ~all"
65/338 = 7 addresses

c2._spf.ebay.com. 3600 IN TXT "v=spf1 ip4:80.93.9.10 ip4:195.234.136.12 ip4:203.49.69.114 ip4:209.63.28.11 ip4:210.80.80.136 ip4:212.110.10.2 ip4:212.147.136.123 include:c3._spf.ebay.com ~all"
66/339 = 7 addresses

c3._spf.ebay.com. 3600 IN TXT "v=spf1 ip4:213.219.8.227 ip4:216.113.168.128 ip4:216.113.175.128 ip4:216.177.178.3 ip4:217.149.33.234 ip4:220.248.6.124 ip4:67.72.12.30 include:c4._spf.ebay.com ~all"
66/344 = 7 addresses

c4._spf.ebay.com. 3600 IN TXT "v=spf1 ip4:216.113.188.112 ip4:80.66.137.58 ip4:212.208.64.34 ip4:216.113.188.96 ip4:216.33.244.6 ip4:216.33.244.7 ip4:63.80.14.17 ~all"
66/314 = 7 addresses

spf-1.paypal.com. 3600 IN TXT "v=spf1 ip4:216.113.188.96 ip4:216.113.188.112 ip4:66.211.168.230 ip4:66.211.168.231 ~all"
66/247 = 4 addresses

paypal.com. 3600 IN MX 10 smtp1.nix.paypal.com.
paypal.com. 3600 IN MX 10 smtp1.sc5.paypal.com.
paypal.com. 3600 IN MX 10 smtp2.nix.paypal.com.
60/254

smtp1.nix.paypal.com. 3600 IN A 64.4.240.74
70/162

smtp1.sc5.paypal.com. 3600 IN A 64.4.244.74
70/162

smtp2.nix.paypal.com. 3600 IN A 64.4.240.75
70/162

854/3845 = 4699 == 10 bps/domain for 266 addresses.

s._sid.ebay.com. 3600 IN TXT "spf2.0/prs ip4:66.135.209.192/27 ip4:66.135.197.0/27 ip4:64.4.240.64/27 ip4:64.4.244.64/27 ~all"

m._sid.ebay.com. 3600 IN TXT "spf2.0/prd ip4:66.135.215.224/27 ip4:216.33.244.96/27 ip4:216.33.244.84 ~all"

p._sid.ebay.com. 3600 IN TXT "spf2.0/prd ip4:67.72.99.26 ip4:206.165.246.83 ip4:206.165.246.84 ip4:206.165.246.85 ip4:206.165.246.86 ip4:64.127.115.252 ip4:194.64.234.129/27 include:p2._sid.ebay.com ~all"

p2._sid.ebay.com. 3600 IN TXT "spf2.0/prd ip4:65.110.161.77 ip4:204.13.11.49 ip4:204.13.11.51 ~all"

c._sid.ebay.com. 2231 IN TXT "spf2.0/prd ip4:12.155.144.75 ip4:62.22.61.131 ip4:63.104.149.126 ip4:64.68.79.253 ip4:64.94.204.222 ip4:66.135.215.134 ip4:67.72.12.29 include:c2._sid.ebay.com ~all"

c2._sid.ebay.com. 3600 IN TXT "spf2.0/prd ip4:80.93.9.10 ip4:195.234.136.12 ip4:203.49.69.114 ip4:209.63.28.11 ip4:210.80.80.136 ip4:212.110.10.2 ip4:212.147.136.123 include:c3._sid.ebay.com ~all"

c3._sid.ebay.com. 3600 IN TXT "spf2.0/prd ip4:213.219.8.227 ip4:216.113.168.128 ip4:216.113.175.128 ip4:216.177.178.3 ip4:217.149.33.234 ip4:220.248.6.124 ip4:67.72.12.30 include:c4._sid.ebay.com ~all"

c4._sid.ebay.com. 3600 IN TXT "spf2.0/prd ip4:216.113.188.112 ip4:80.66.137.58 ip4:212.208.64.34 ip4:216.113.188.96 ip4:63.80.14.17 ~all"

Appendix D

Example Attacking Domain Zone File

```
@ IN SOA @ cert-test.mail-abuse.org.(
 2006062022 ;serial yyyymmddnn
 1H ;refresh
 15M ;retry
 1D ;expiry
 1D) ;minimum

 IN NS do-dev0.mail-abuse.org.

$ORIGIN cert-test.mail-abuse.org. ;attacker
EHLO IN A 168.61.5.1

cert-test.mail-abuse.org. IN TXT "v=spf1
mx:0.%[l].%[d] mx:1.%[l].%[d] mx:2.%[l].%[d]
mx:3.%[l].%[d] mx:4.%[l].%[d] mx:5.%[l].%[d]
mx:6.%[l].%[d] mx:7.%[l].%[d] mx:8.%[l].%[d]
mx:9.%[l].%[d] ?all"

$ORIGIN jo.cert-test.
```

123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.
123456789-123456789.
123456789.
example.com. ;victim

0.jo.cert-test.mail-abuse.org.

IN MX 1 0-0
IN MX 1 0-1
IN MX 1 0-2
IN MX 1 0-3
IN MX 1 0-4
IN MX 1 0-5
IN MX 1 0-6
IN MX 1 0-7
IN MX 1 0-8
IN MX 1 0-9

1.jo.cert-test.mail-abuse.org.

IN MX 1 1-0
IN MX 1 1-1
IN MX 1 1-2
IN MX 1 1-3
IN MX 1 1-4
IN MX 1 1-5
IN MX 1 1-6
IN MX 1 1-7
IN MX 1 1-8
IN MX 1 1-9

2.jo.cert-test.mail-abuse.org.

IN MX 1 2-0
IN MX 1 2-1
IN MX 1 2-2
IN MX 1 2-3
IN MX 1 2-4
IN MX 1 2-5
IN MX 1 2-6
IN MX 1 2-7
IN MX 1 2-8
IN MX 1 2-9

3.jo.cert-test.mail-abuse.org.

IN MX 1 3-0
IN MX 1 3-1
IN MX 1 3-2
IN MX 1 3-3
IN MX 1 3-4
IN MX 1 3-5

IN MX 1 3-6
IN MX 1 3-7
IN MX 1 3-8
IN MX 1 3-9

4.jo.cert-test.mail-abuse.org.

IN MX 1 4-0
IN MX 1 4-1
IN MX 1 4-2
IN MX 1 4-3
IN MX 1 4-4
IN MX 1 4-5
IN MX 1 4-6
IN MX 1 4-7
IN MX 1 4-8
IN MX 1 4-9

5.jo.cert-test.mail-abuse.org.

IN MX 1 5-0
IN MX 1 5-1
IN MX 1 5-2
IN MX 1 5-3
IN MX 1 5-4
IN MX 1 5-5
IN MX 1 5-6
IN MX 1 5-7
IN MX 1 5-8
IN MX 1 5-9

6.jo.cert-test.mail-abuse.org.

IN MX 1 6-0
IN MX 1 6-1
IN MX 1 6-2
IN MX 1 6-3
IN MX 1 6-4
IN MX 1 6-5
IN MX 1 6-6
IN MX 1 6-7
IN MX 1 6-8
IN MX 1 6-9

7.jo.cert-test.mail-abuse.org.

IN MX 1 7-0
IN MX 1 7-1
IN MX 1 7-2
IN MX 1 7-3
IN MX 1 7-4
IN MX 1 7-5
IN MX 1 7-6
IN MX 1 7-7
IN MX 1 7-8

IN MX 1 7-9

8.jo.cert-test.mail-abuse.org.

IN MX 1 8-0
IN MX 1 8-1
IN MX 1 8-2
IN MX 1 8-3
IN MX 1 8-4
IN MX 1 8-5
IN MX 1 8-6
IN MX 1 8-7
IN MX 1 8-8
IN MX 1 8-9

9.jo.cert-test.mail-abuse.org.

IN MX 1 9-0
IN MX 1 9-1
IN MX 1 9-2
IN MX 1 9-3
IN MX 1 9-4
IN MX 1 9-5
IN MX 1 9-6
IN MX 1 9-7
IN MX 1 9-8
IN MX 1 9-9

Appendix E

Example Traffic Qualifying jo@cert-test.mail-abuse.org

XMIT ATTACK Time 0.000000 Domain Name System (query)
DNS Standard query TXT cert-test.mail-abuse.org
Frame 1 (74 bytes on wire)
UDP, Src Port: 52407 (52407), Dst Port: domain (53)

RECV ATTACK Time 0.000237 Domain Name System (response)
DNS Standard query response TXT
Frame 2 (286 bytes on wire)
UDP, Src Port: domain (53), Dst Port: 52407 (52407)

XMIT ATTACK Time 0.000387 Domain Name System (query)
DNS Standard query MX 0.jo.cert-test.mail-abuse.org
Frame 3 (79 bytes on wire)
UDP, Src Port: 61719 (61719), Dst Port: domain (53)

RECV ATTACK Time 0.000668 Domain Name System (response)
DNS Standard query response MX 1 0-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.

example.com
MX 1 0-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 4 (535 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 61719 (61719)

XMIT VICTIM Time 0.000800 Domain Name System (query)
Standard query A 0-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 5 (288 bytes on the wire)
UDP, Src Port: 60118 (60118), Dst Port: domain (53)

RECV VICTIM Time 0.000877 Domain Name System (response)
DNS Standard query response, No such name
Frame 6 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 60118 (60118)

XMIT VICTIM Time 0.000938 Domain Name System (query)
DNS Standard query A 0-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 7 (288 bytes on the wire)
UDP, Src Port: 50197 (50197), Dst Port: domain (53)

RECV VICTIM Time 0.001006 Domain Name System (response)
DNS Standard query response, No such name
Frame 8 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 50197 (50197)

XMIT VICTIM Time 0.001064 Domain Name System (query)
DNS Standard query A 0-4.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 9 (288 bytes on the wire)
UDP, Src Port: 64717 (64717), Dst Port: domain (53)

RECV VICTIM Time 0.001143 Domain Name System (response)

DNS Standard query response, No such name
Frame 10 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 64717 (64717)

XMIT VICTIM Time 0.001199 Domain Name System (query)
DNS Standard query A 0-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 11 (288 bytes on the wire)
UDP, Src Port: 63300 (63300), Dst Port: domain (53)

RECV VICTIM Time 0.001266 Domain Name System (response)
DNS Standard query response, No such name
Frame 12 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 63300 (63300)

XMIT VICTIM Time 0.001322 Domain Name System (query)
DNS Standard query A 0-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 13 (288 bytes on the wire)
UDP, Src Port: 63072 (63072), Dst Port: domain (53)

RECV VICTIM Time 0.001388 Domain Name System (response)
DNS Standard query response, No such name
Frame 14 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 63072 (63072)

XMIT VICTIM Time 0.001443 Domain Name System (query)
DNS Standard query A 0-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 15 (288 bytes on the wire)
UDP, Src Port: 63053 (63053), Dst Port: domain (53)

RECV VICTIM Time 0.001509 Domain Name System (response)
DNS Standard query response, No such name
Frame 16 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 63053 (63053)

XMIT VICTIM Time 0.001568 Domain Name System (query)
DNS Standard query A 0-8.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 17 (288 bytes on the wire)
UDP, Src Port: 49717 (49717), Dst Port: domain (53)

RECV VICTIM Time 0.001634 Domain Name System (response)
DNS Standard query response, No such name
Frame 18 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 49717 (49717)

XMIT VICTIM Time 0.001688 Domain Name System (query)
DNS Standard query A 0-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 19 (288 bytes on the wire)
UDP, Src Port: 51282 (51282), Dst Port: domain (53)

RECV VICTIM Time 0.001762 Domain Name System (response)
DNS Standard query response, No such name
Frame 20 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 51282 (51282)

XMIT VICTIM Time 0.001817 Domain Name System (query)
DNS Standard query A 0-0.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 21 (288 bytes on the wire)
UDP, Src Port: 62103 (62103), Dst Port: domain (53)

RECV VICTIM Time 0.001884 Domain Name System (response)
DNS Standard query response, No such name
Frame 22 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 62103 (62103)

XMIT VICTIM Time 0.001949 Domain Name System (query)
DNS Standard query A 0-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 23 (288 bytes on the wire)

UDP, Src Port: 53435 (53435), Dst Port: domain (53)

RECV VICTIM Time 0.002017 Domain Name System (response)
DNS Standard query response, No such name
Frame 24 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 53435 (53435)

XMIT ATTACK Time 0.002077 Domain Name System (query)
DNS Standard query MX 1.jo.cert-test.mail-abuse.org
Frame 25 (79 bytes on the wire)
UDP, Src Port: 59613 (59613), Dst Port: domain (53)

RECV ATTACK Time 0.002310 Domain Name System (response)
DNS Standard query response MX 1 1-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 1-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 1-4.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 1-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 1-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 1-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 1-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 1-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 1-0.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.
123456789.example.com
MX 1 1-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 26 (535 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 59613 (59613)

XMIT VICTIM Time 0.002408 Domain Name System (query)
DNS Standard query A 1-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 27 (288 bytes on the wire)
UDP, Src Port: 59249 (59249), Dst Port: domain (53)

RECV VICTIM Time 0.002478 Domain Name System (response)
DNS Standard query response, No such name
Frame 28 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 59249 (59249)

XMIT VICTIM Time 0.002534 Domain Name System (query)
DNS Standard query A 1-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 29 (288 bytes on the wire)
UDP, Src Port: 61124 (61124), Dst Port: domain (53)

RECV VICTIM Time 0.002612 Domain Name System (response)

DNS Standard query response, No such name
Frame 30 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 61124 (61124)

XMIT VICTIM Time 0.002667 Domain Name System (query)
DNS Standard query A 1-4.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 31 (288 bytes on the wire)
UDP, Src Port: 52851 (52851), Dst Port: domain (53)

RECV VICTIM Time 0.002733 Domain Name System (response)
DNS Standard query response, No such name
Frame 32 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 52851 (52851)

XMIT VICTIM Time 0.002787 Domain Name System (query)
DNS Standard query A 1-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 33 (288 bytes on the wire)
UDP, Src Port: 58726 (58726), Dst Port: domain (53)

RECV VICTIM Time 0.002852 Domain Name System (response)
DNS Standard query response, No such name
Frame 34 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 58726 (58726)

XMIT VICTIM Time 0.002906 Domain Name System (query)
DNS Standard query A 1-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 35 (288 bytes on the wire)
UDP, Src Port: 56126 (56126), Dst Port: domain (53)

RECV VICTIM Time 0.002973 Domain Name System (response)
DNS Standard query response, No such name
Frame 36 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 56126 (56126)

XMIT VICTIM Time 0.003038 Domain Name System (query)
DNS Standard query A 1-7.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 37 (288 bytes on the wire)
UDP, Src Port: 61690 (61690), Dst Port: domain (53)

RECV VICTIM Time 0.003106 Domain Name System (response)
DNS Standard query response, No such name
Frame 38 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 61690 (61690)

XMIT VICTIM Time 0.003161 Domain Name System (query)
DNS Standard query A 1-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 39 (288 bytes on the wire)
UDP, Src Port: 51783 (51783), Dst Port: domain (53)

RECV VICTIM Time 0.003236 Domain Name System (response)
DNS Standard query response, No such name
Frame 40 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 51783 (51783)

XMIT VICTIM Time 0.003292 Domain Name System (query)
DNS Standard query A 1-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 41 (288 bytes on the wire)
UDP, Src Port: 60344 (60344), Dst Port: domain (53)

RECV VICTIM Time 0.003359 Domain Name System (response)
DNS Standard query response, No such name
Frame 42 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 60344 (60344)

XMIT VICTIM Time 0.003413 Domain Name System (query)
DNS Standard query A 1-0.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 43 (288 bytes on the wire)

UDP, Src Port: 63367 (63367), Dst Port: domain (53)

RECV VICTIM Time 0.003479 Domain Name System (response)
DNS Standard query response, No such name
Frame 44 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 63367 (63367)

XMIT VICTIM Time 0.003533 Domain Name System (query)
DNS Standard query A 1-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 45 (288 bytes on the wire)
UDP, Src Port: 51204 (51204), Dst Port: domain (53)

RECV VICTIM Time 0.003603 Domain Name System (response)
DNS Standard query response, No such name
Frame 46 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 51204 (51204)

XMIT ATTACK Time 0.003661 Domain Name System (query)
DNS Standard query MX 2.jo.cert-test.mail-abuse.org
Frame 47 (79 bytes on the wire)
UDP, Src Port: 61534 (61534), Dst Port: domain (53)

RECV ATTACK Time 0.003894 Domain Name System (response)
DNS Standard query response MX 1 2-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 2-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 2-4.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 2-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.

example.com
MX 1 2-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.

example.com
MX 1 2-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.

example.com
MX 1 2-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.

example.com
MX 1 2-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.

example.com
MX 1 2-0.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.

example.com
MX 1 2-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.

example.com
Frame 48 (535 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 61534 (61534)

XMIT VICTIM Time 0.003993 Domain Name System (query)
DNS Standard query A 2-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 49 (288 bytes on the wire)
UDP, Src Port: 50303 (50303), Dst Port: domain (53)

RECV VICTIM Time 0.004071 Domain Name System (response)

DNS Standard query response, No such name
Frame 50 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 50303 (50303)

XMIT VICTIM Time 0.004139 Domain Name System (query)
DNS Standard query A 2-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 51 (288 bytes on the wire)
UDP, Src Port: 52940 (52940), Dst Port: domain (53)

RECV VICTIM Time 0.004206 Domain Name System (response)
DNS Standard query response, No such name
Frame 52 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 52940 (52940)

XMIT VICTIM Time 0.004261 Domain Name System (query)
DNS Standard query A 2-4.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 53 (288 bytes on the wire)
UDP, Src Port: 60474 (60474), Dst Port: domain (53)

RECV VICTIM Time 0.004327 Domain Name System (response)
DNS Standard query response, No such name
Frame 54 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 60474 (60474)

XMIT VICTIM Time 0.004382 Domain Name System (query)
DNS Standard query A 2-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 55 (288 bytes on the wire)
UDP, Src Port: 49663 (49663), Dst Port: domain (53)

RECV VICTIM Time 0.004447 Domain Name System (response)
DNS Standard query response, No such name
Frame 56 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 49663 (49663)

XMIT VICTIM Time 0.004502 Domain Name System (query)
DNS Standard query A 2-6.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 57 (288 bytes on the wire)
UDP, Src Port: 61283 (61283), Dst Port: domain (53)

RECV VICTIM Time 0.004571 Domain Name System (response)
DNS Standard query response, No such name
Frame 58 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 61283 (61283)

XMIT VICTIM Time 0.004625 Domain Name System (query)
DNS Standard query A 2-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 59 (288 bytes on the wire)
UDP, Src Port: 60191 (60191), Dst Port: domain (53)

RECV VICTIM Time 0.004698 Domain Name System (response)
DNS Standard query response, No such name
Frame 60 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 60191 (60191)

XMIT VICTIM Time 0.004753 Domain Name System (query)
DNS Standard query A 2-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 61 (288 bytes on the wire)
UDP, Src Port: 58486 (58486), Dst Port: domain (53)

RECV VICTIM Time 0.004819 Domain Name System (response)
DNS Standard query response, No such name
Frame 62 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 58486 (58486)

XMIT VICTIM Time 0.004874 Domain Name System (query)
DNS Standard query A 2-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 63 (288 bytes on the wire)

UDP, Src Port: 62555 (62555), Dst Port: domain (53)

RECV VICTIM Time 0.004939 Domain Name System (response)

DNS Standard query response, No such name

Frame 64 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 62555 (62555)

XMIT VICTIM Time 0.004993 Domain Name System (query)

DNS Standard query A 2-0.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 65 (288 bytes on the wire)

UDP, Src Port: 49410 (49410), Dst Port: domain (53)

RECV VICTIM Time 0.005060 Domain Name System (response)

DNS Standard query response, No such name

Frame 66 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 49410 (49410)

XMIT VICTIM Time 0.005115 Domain Name System (query)

DNS Standard query A 2-1.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 67 (288 bytes on the wire)

UDP, Src Port: 59650 (59650), Dst Port: domain (53)

RECV VICTIM Time 0.005180 Domain Name System (response)

DNS Standard query response, No such name

Frame 68 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 59650 (59650)

XMIT ATTACK Time 0.005236 Domain Name System (query)

DNS Standard query MX 3.jo.cert-test.mail-abuse.org

Frame 69 (79 bytes on the wire)

UDP, Src Port: 60922 (60922), Dst Port: domain (53)

RECV ATTACK Time 0.005477 Domain Name System (response)

DNS Standard query response MX 1 3-2.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

MX 1 3-3.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

example.com
Frame 70 (535 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 60922 (60922)

XMIT VICTIM Time 0.005592 Domain Name System (query)
DNS Standard query A 3-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 71 (288 bytes on the wire)
UDP, Src Port: 60056 (60056), Dst Port: domain (53)

RECV VICTIM Time 0.005662 Domain Name System (response)
DNS Standard query response, No such name
Frame 72 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 60056 (60056)

XMIT VICTIM Time 0.005717 Domain Name System (query)
DNS Standard query A 3-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 73 (288 bytes on the wire)
UDP, Src Port: 51567 (51567), Dst Port: domain (53)

RECV VICTIM Time 0.005783 Domain Name System (response)
DNS Standard query response, No such name
Frame 74 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 51567 (51567)

XMIT VICTIM Time 0.005839 Domain Name System (query)
DNS Standard query A 3-4.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 75 (288 bytes on the wire)
UDP, Src Port: 55946 (55946), Dst Port: domain (53)

RECV VICTIM Time 0.005904 Domain Name System (response)
DNS Standard query response, No such name
Frame 76 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 55946 (55946)

XMIT VICTIM Time 0.005958 Domain Name System (query)
DNS Standard query A 3-5.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 77 (288 bytes on the wire)
UDP, Src Port: 61606 (61606), Dst Port: domain (53)

RECV VICTIM Time 0.006022 Domain Name System (response)
DNS Standard query response, No such name
Frame 78 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 61606 (61606)

XMIT VICTIM Time 0.006077 Domain Name System (query)
DNS Standard query A 3-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 79 (288 bytes on the wire)
UDP, Src Port: 57948 (57948), Dst Port: domain (53)

RECV VICTIM Time 0.006151 Domain Name System (response)
DNS Standard query response, No such name
Frame 80 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 57948 (57948)

XMIT VICTIM Time 0.006205 Domain Name System (query)
DNS Standard query A 3-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 81 (288 bytes on the wire)
UDP, Src Port: 62371 (62371), Dst Port: domain (53)

RECV VICTIM Time 0.006270 Domain Name System (response)
DNS Standard query response, No such name
Frame 82 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 62371 (62371)

XMIT VICTIM Time 0.006325 Domain Name System (query)
DNS Standard query A 3-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 83 (288 bytes on the wire)

UDP, Src Port: 51455 (51455), Dst Port: domain (53)

RECV VICTIM Time 0.006390 Domain Name System (response)
DNS Standard query response, No such name
Frame 84 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 51455 (51455)

XMIT VICTIM Time 0.006444 Domain Name System (query)
DNS Standard query A 3-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 85 (288 bytes on the wire)
UDP, Src Port: 50959 (50959), Dst Port: domain (53)

RECV VICTIM Time 0.006510 Domain Name System (response)
DNS Standard query response, No such name
Frame 86 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 50959 (50959)

XMIT VICTIM Time 0.006569 Domain Name System (query)
DNS Standard query A 3-0.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 87 (288 bytes on the wire)
UDP, Src Port: 50458 (50458), Dst Port: domain (53)

RECV VICTIM Time 0.006635 Domain Name System (response)
DNS Standard query response, No such name
Frame 88 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 50458 (50458)

XMIT VICTIM Time 0.006688 Domain Name System (query)
DNS Standard query A 3-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 89 (288 bytes on the wire)
UDP, Src Port: 55297 (55297), Dst Port: domain (53)

RECV VICTIM Time 0.006762 Domain Name System (response)
DNS Standard query response, No such name
Frame 90 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 55297 (55297)

XMIT ATTACK Time 0.006829 Domain Name System (query)
DNS Standard query MX 4.jo.cert-test.mail-abuse.org
Frame 91 (79 bytes on the wire)
UDP, Src Port: 55642 (55642), Dst Port: domain (53)

RECV ATTACK Time 0.007064 Domain Name System (response)
DNS Standard query response MX 1 4-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 4-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 4-4.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 4-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 4-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 4-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789
.example.com
MX 1 4-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 4-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 4-0.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 4-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 92 (535 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 55642 (55642)

XMIT VICTIM Time 0.007173 Domain Name System (query)
DNS Standard query A 4-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 93 (288 bytes on the wire)
UDP, Src Port: 60109 (60109), Dst Port: domain (53)

RECV VICTIM Time 0.007243 Domain Name System (response)
DNS Standard query response, No such name
Frame 94 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 60109 (60109)

XMIT VICTIM Time 0.007299 Domain Name System (query)
DNS Standard query A 4-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 95 (288 bytes on the wire)
UDP, Src Port: 59804 (59804), Dst Port: domain (53)

RECV VICTIM Time 0.007365 Domain Name System (response)
DNS Standard query response, No such name
Frame 96 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 59804 (59804)

XMIT VICTIM Time 0.007419 Domain Name System (query)
DNS Standard query A 4-4.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 97 (288 bytes on the wire)
UDP, Src Port: 59201 (59201), Dst Port: domain (53)

RECV VICTIM Time 0.007486 Domain Name System (response)
DNS Standard query response, No such name
Frame 98 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 59201 (59201)

XMIT VICTIM Time 0.007540 Domain Name System (query)
DNS Standard query A 4-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 99 (288 bytes on the wire)
UDP, Src Port: 54029 (54029), Dst Port: domain (53)

RECV VICTIM Time 0.008675 Domain Name System (response)
DNS Standard query response, No such name
Frame 100 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 54029 (54029)

XMIT VICTIM Time 0.008773 Domain Name System (query)
DNS Standard query A 4-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 101 (288 bytes on the wire)
UDP, Src Port: 60108 (60108), Dst Port: domain (53)

RECV VICTIM Time 0.013443 Domain Name System (response)
DNS Standard query response, No such name
Frame 102 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 60108 (60108)

XMIT VICTIM Time 0.013561 Domain Name System (query)
DNS Standard query A 4-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 103 (288 bytes on the wire)

UDP, Src Port: 52259 (52259), Dst Port: domain (53)

RECV VICTIM Time 0.014616 Domain Name System (response)
DNS Standard query response, No such name
Frame 104 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 52259 (52259)

XMIT VICTIM Time 0.014701 Domain Name System (query)
DNS Standard query A 4-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 105 (288 bytes on the wire)
UDP, Src Port: 59589 (59589), Dst Port: domain (53)

RECV VICTIM Time 0.014866 Domain Name System (response)
DNS Standard query response, No such name
Frame 106 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 59589 (59589)

XMIT VICTIM Time 0.014928
DNS Standard query A 4-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 107 (288 bytes on the wire)
UDP, Src Port: 49838 (49838), Dst Port: domain (53)
Domain Name System (query)

RECV VICTIM Time 0.015609 Domain Name System (response)
DNS Standard query response, No such name
Frame 108 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 49838 (49838)

XMIT VICTIM Time 0.015681 Domain Name System (query)
DNS Standard query A 4-0.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 109 (288 bytes on the wire)
UDP, Src Port: 61868 (61868), Dst Port: domain (53)

RECV VICTIM Time 0.015753 Domain Name System (response)
DNS Standard query response, No such name
Frame 110 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 61868 (61868)

XMIT VICTIM Time 0.015826 Domain Name System (query)

DNS Standard query A 4-1.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 111 (288 bytes on the wire)

UDP, Src Port: 54485 (54485), Dst Port: domain (53)

RECV VICTIM Time 0.015897 Domain Name System (response)

DNS Standard query response, No such name

Frame 112 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 54485 (54485)

XMIT ATTACK Time 0.015963 Domain Name System (query)

DNS Standard query MX 5.jo.cert-test.mail-abuse.org

Frame 113 (79 bytes on the wire)

UDP, Src Port: 62648 (62648), Dst Port: domain (53)

RECV ATTACK Time 0.016223 Domain Name System (response)

DNS Standard query response MX 1 5-2.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

MX 1 5-3.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

MX 1 5-4.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

MX 1 5-5.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.

123456789.example.com

MX 1 5-6.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.
123456789.example.com
MX 1 5-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 5-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 5-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 5-0.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 5-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 114 (535 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 62648 (62648)

XMIT VICTIM Time 0.016326 Domain Name System (query)
DNS Standard query A 5-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 115 (288 bytes on the wire)
UDP, Src Port: 64862 (64862), Dst Port: domain (53)

RECV VICTIM Time 0.016397 Domain Name System (response)
DNS Standard query response, No such name
Frame 116 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 64862 (64862)

XMIT VICTIM Time 0.016453 Domain Name System (query)

DNS Standard query A 5-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 117 (288 bytes on the wire)

UDP, Src Port: 55595 (55595), Dst Port: domain (53)

RECV VICTIM Time 0.016530 Domain Name System (response)

DNS Standard query response, No such name

Frame 118 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 55595 (55595)

XMIT VICTIM Time 0.016590 Domain Name System (query)

DNS Standard query A 5-4.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 119 (288 bytes on the wire)

UDP, Src Port: 59040 (59040), Dst Port: domain (53)

RECV VICTIM Time 0.016658 Domain Name System (response)

DNS Standard query response, No such name

Frame 120 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 59040 (59040)

XMIT VICTIM Time 0.016712 Domain Name System (query)

DNS Standard query A 5-5.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 121 (288 bytes on the wire)

UDP, Src Port: 64566 (64566), Dst Port: domain (53)

RECV VICTIM Time 0.016778 Domain Name System (response)

DNS Standard query response, No such name

Frame 122 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 64566 (64566)

XMIT VICTIM Time 0.016833 Domain Name System (query)

DNS Standard query A 5-6.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 123 (288 bytes on the wire)
UDP, Src Port: 57893 (57893), Dst Port: domain (53)

RECV VICTIM Time 0.016899 Domain Name System (response)
DNS Standard query response, No such name
Frame 124 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 57893 (57893)

XMIT VICTIM Time 0.016966 Domain Name System (query)
DNS Standard query A 5-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 125 (288 bytes on the wire)
UDP, Src Port: 50080 (50080), Dst Port: domain (53)

RECV VICTIM Time 0.017033 Domain Name System (response)
DNS Standard query response, No such name
Frame 126 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 50080 (50080)

XMIT VICTIM Time 0.017089 Domain Name System (query)
DNS Standard query A 5-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 127 (288 bytes on the wire)
UDP, Src Port: 59589 (59589), Dst Port: domain (53)

RECV VICTIM Time 0.017163 Domain Name System (response)
DNS Standard query response, No such name
Frame 128 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 59589 (59589)

XMIT VICTIM Time 0.017218 Domain Name System (query)
DNS Standard query A 5-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 129 (288 bytes on the wire)
UDP, Src Port: 51145 (51145), Dst Port: domain (53)

RECV VICTIM Time 0.017284 Domain Name System (response)
DNS Standard query response, No such name
Frame 130 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 51145 (51145)

XMIT VICTIM Time 0.017339 Domain Name System (query)

DNS Standard query A 5-0.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 131 (288 bytes on the wire)

UDP, Src Port: 55246 (55246), Dst Port: domain (53)

RECV VICTIM Time 0.017405 Domain Name System (response)

DNS Standard query response, No such name

Frame 132 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 55246 (55246)

XMIT VICTIM Time 0.017459 Domain Name System (query)

DNS Standard query A 5-1.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 133 (288 bytes on the wire)

UDP, Src Port: 65477 (65477), Dst Port: domain (53)

RECV VICTIM Time 0.017525 Domain Name System (response)

DNS Standard query response, No such name

Frame 134 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 65477 (65477)

XMIT ATTACK Time 0.017656 Domain Name System (query)

DNS Standard query MX 6.jo.cert-test.mail-abuse.org

Frame 135 (79 bytes on the wire)

UDP, Src Port: 50935 (50935), Dst Port: domain (53)

RECV ATTACK Time 0.017899 Domain Name System (response)

DNS Standard query response MX 1 6-2.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

MX 1 6-3.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

MX 1 6-4.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

MX 1 6-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

MX 1 6-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

MX 1 6-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

MX 1 6-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

MX 1 6-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

MX 1 6-0.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

MX 1 6-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 136 (535 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 50935 (50935)

XMIT VICTIM Time 0.018001 Domain Name System (query)

DNS Standard query A 6-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 137 (288 bytes on the wire)
UDP, Src Port: 65317 (65317), Dst Port: domain (53)

RECV VICTIM Time 0.018072 Domain Name System (response)
DNS Standard query response, No such name
Frame 138 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 65317 (65317)

XMIT VICTIM Time 0.018141 Domain Name System (query)
DNS Standard query A 6-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 139 (288 bytes on the wire)
UDP, Src Port: 65391 (65391), Dst Port: domain (53)

RECV VICTIM Time 0.018209 Domain Name System (response)
DNS Standard query response, No such name
Frame 140 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 65391 (65391)

XMIT VICTIM Time 0.018264 Domain Name System (query)
DNS Standard query A 6-4.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 141 (288 bytes on the wire)
UDP, Src Port: 61277 (61277), Dst Port: domain (53)

RECV VICTIM Time 0.018330 Domain Name System (response)
DNS Standard query response, No such name
Frame 142 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 61277 (61277)

XMIT VICTIM Time 0.018384 Domain Name System (query)
DNS Standard query A 6-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 143 (288 bytes on the wire)
UDP, Src Port: 62266 (62266), Dst Port: domain (53)

RECV VICTIM Time 0.018459 Domain Name System (response)
DNS Standard query response, No such name
Frame 144 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 62266 (62266)

XMIT VICTIM Time 0.018515 Domain Name System (query)
DNS Standard query A 6-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 145 (288 bytes on the wire)
UDP, Src Port: 56381 (56381), Dst Port: domain (53)

RECV VICTIM Time 0.018585 Domain Name System (response)
DNS Standard query response, No such name
Frame 146 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 56381 (56381)

XMIT VICTIM Time 0.018640 Domain Name System (query)
DNS Standard query A 6-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 147 (288 bytes on the wire)
UDP, Src Port: 50878 (50878), Dst Port: domain (53)

RECV VICTIM Time 0.018707 Domain Name System (response)
DNS Standard query response, No such name
Frame 148 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 50878 (50878)

XMIT VICTIM Time 0.018761 Domain Name System (query)
DNS Standard query A 6-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 149 (288 bytes on the wire)
UDP, Src Port: 51814 (51814), Dst Port: domain (53)

RECV VICTIM Time 0.018826 Domain Name System (response)
DNS Standard query response, No such name
Frame 150 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 51814 (51814)

XMIT VICTIM Time 0.018881 Domain Name System (query)

DNS Standard query A 6-9.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 151 (288 bytes on the wire)

UDP, Src Port: 57344 (57344), Dst Port: domain (53)

RECV VICTIM Time 0.018946 Domain Name System (response)

DNS Standard query response, No such name

Frame 152 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 57344 (57344)

XMIT VICTIM Time 0.019000 Domain Name System (query)

DNS Standard query A 6-0.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 153 (288 bytes on the wire)

UDP, Src Port: 54706 (54706), Dst Port: domain (53)

RECV VICTIM Time 0.019076 Domain Name System (response)

DNS Standard query response, No such name

Frame 154 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 54706 (54706)

XMIT VICTIM Time 0.019131 Domain Name System (query)

DNS Standard query A 6-1.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 155 (288 bytes on the wire)

UDP, Src Port: 61147 (61147), Dst Port: domain (53)

RECV VICTIM Time 0.019197 Domain Name System (response)

DNS Standard query response, No such name

Frame 156 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 61147 (61147)

XMIT ATTACK Time 0.019254 Domain Name System (query)

DNS Standard query MX 7.jo.cert-test.mail-abuse.org

Frame 157 (79 bytes on the wire)

UDP, Src Port: 59174 (59174), Dst Port: domain (53)

RECV ATTACK Time 0.019487 Domain Name System (response)
DNS Standard query response MX 1 7-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 7-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 7-4.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 7-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 7-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 7-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 7-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 7-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 7-0.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 7-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 158 (535 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 59174 (59174)

XMIT VICTIM Time 0.019601 Domain Name System (query)

DNS Standard query A 7-2.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 159 (288 bytes on the wire)

UDP, Src Port: 49466 (49466), Dst Port: domain (53)

RECV VICTIM Time 0.019673 Domain Name System (response)

DNS Standard query response, No such name

Frame 160 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 49466 (49466)

XMIT VICTIM Time 0.019729 Domain Name System (query)

DNS Standard query A 7-3.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 161 (288 bytes on the wire)

UDP, Src Port: 56355 (56355), Dst Port: domain (53)

RECV VICTIM Time 0.019795 Domain Name System (response)

DNS Standard query response, No such name

Frame 162 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 56355 (56355)

XMIT VICTIM Time 0.019849 Domain Name System (query)

DNS Standard query A 7-4.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 163 (288 bytes on the wire)
UDP, Src Port: 64811 (64811), Dst Port: domain (53)

RECV VICTIM Time 0.019924 Domain Name System (response)
DNS Standard query response, No such name
Frame 164 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 64811 (64811)

XMIT VICTIM Time 0.019979 Domain Name System (query)
DNS Standard query A 7-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 165 (288 bytes on the wire)
UDP, Src Port: 65350 (65350), Dst Port: domain (53)

RECV VICTIM Time 0.020046 Domain Name System (response)
DNS Standard query response, No such name
Frame 166 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 65350 (65350)

XMIT VICTIM Time 0.020101 Domain Name System (query)
DNS Standard query A 7-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 167 (288 bytes on the wire)
UDP, Src Port: 54501 (54501), Dst Port: domain (53)

RECV VICTIM Time 0.020165 Domain Name System (response)
DNS Standard query response, No such name
Frame 168 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 54501 (54501)

XMIT VICTIM Time 0.020220 Domain Name System (query)
DNS Standard query A 7-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 169 (288 bytes on the wire)
UDP, Src Port: 55871 (55871), Dst Port: domain (53)

RECV VICTIM Time 0.020285 Domain Name System (response)
DNS Standard query response, No such name
Frame 170 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 55871 (55871)

XMIT VICTIM Time 0.020340 Domain Name System (query)

DNS Standard query A 7-8.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 171 (288 bytes on the wire)

UDP, Src Port: 60209 (60209), Dst Port: domain (53)

RECV VICTIM Time 0.020406 Domain Name System (response)

DNS Standard query response, No such name

Frame 172 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 60209 (60209)

XMIT VICTIM Time 0.020461 Domain Name System (query)

DNS Standard query A 7-9.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 173 (288 bytes on the wire)

UDP, Src Port: 50737 (50737), Dst Port: domain (53)

RECV VICTIM Time 0.020534 Domain Name System (response)

DNS Standard query response, No such name

Frame 174 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 50737 (50737)

XMIT VICTIM Time 0.020598 Domain Name System (query)

DNS Standard query A 7-0.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 175 (288 bytes on the wire)

UDP, Src Port: 54327 (54327), Dst Port: domain (53)

RECV VICTIM Time 0.020706 Domain Name System (response)

DNS Standard query response, No such name

Frame 176 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 54327 (54327)

XMIT VICTIM Time 0.020761 Domain Name System (query)

DNS Standard query A 7-1.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 177 (288 bytes on the wire)
UDP, Src Port: 58995 (58995), Dst Port: domain (53)

RECV VICTIM Time 0.020827 Domain Name System (response)
DNS Standard query response, No such name
Frame 178 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 58995 (58995)

XMIT ATTACK Time 0.020885 Domain Name System (query)
DNS Standard query MX 8.jo.cert-test.mail-abuse.org
Frame 179 (79 bytes on the wire)
UDP, Src Port: 55097 (55097), Dst Port: domain (53)

RECV ATTACK Time 0.021120 Domain Name System (response)
DNS Standard query response MX 1 8-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 8-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 8-4.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 8-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 8-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 8-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 8-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 8-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 8-0.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 8-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 180 (535 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 55097 (55097)

XMIT VICTIM Time 0.021243 Domain Name System (query)
DNS Standard query A 8-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 181 (288 bytes on the wire)
UDP, Src Port: 60196 (60196), Dst Port: domain (53)

No. 182 Time 0.021313 Domain Name System (response)
DNS Standard query response, No such name
Frame 182 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 60196 (60196)

XMIT VICTIM Time 0.021369 Domain Name System (query)
DNS Standard query A 8-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 183 (288 bytes on the wire)
UDP, Src Port: 54875 (54875), Dst Port: domain (53)

RECV VICTIM Time 0.021445 Domain Name System (response)
DNS Standard query response, No such name
Frame 184 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 54875 (54875)

XMIT VICTIM Time 0.021501 Domain Name System (query)
DNS Standard query A 8-4.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 185 (288 bytes on the wire)
UDP, Src Port: 54995 (54995), Dst Port: domain (53)

RECV VICTIM Time 0.021571 Domain Name System (response)
DNS Standard query response, No such name
Frame 186 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 54995 (54995)

XMIT VICTIM Time 0.021625 Domain Name System (query)
DNS Standard query A 8-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 187 (288 bytes on the wire)
UDP, Src Port: 51443 (51443), Dst Port: domain (53)

RECV VICTIM Time 0.021691 Domain Name System (response)
DNS Standard query response, No such name
Frame 188 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 51443 (51443)

XMIT VICTIM Time 0.021744 Domain Name System (query)
DNS Standard query A 8-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 189 (288 bytes on the wire)
UDP, Src Port: 49195 (49195), Dst Port: domain (53)

RECV VICTIM Time 0.021810 Domain Name System (response)
DNS Standard query response, No such name
Frame 190 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 49195 (49195)

XMIT VICTIM Time 0.021863 Domain Name System (query)

DNS Standard query A 8-7.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 191 (288 bytes on the wire)

UDP, Src Port: 57078 (57078), Dst Port: domain (53)

RECV VICTIM Time 0.021928 Domain Name System (response)

DNS Standard query response, No such name

Frame 192 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 57078 (57078)

XMIT VICTIM Time 0.021982 Domain Name System (query)

DNS Standard query A 8-8.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 193 (288 bytes on the wire)

UDP, Src Port: 57749 (57749), Dst Port: domain (53)

RECV VICTIM Time 0.022056 Domain Name System (response)

DNS Standard query response, No such name

Frame 194 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 57749 (57749)

XMIT VICTIM Time 0.022110 Domain Name System (query)

DNS Standard query A 8-9.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 195 (288 bytes on the wire)

UDP, Src Port: 52752 (52752), Dst Port: domain (53)

RECV VICTIM Time 0.022176 Domain Name System (response)

DNS Standard query response, No such name

Frame 196 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 52752 (52752)

XMIT VICTIM Time 0.022730 Domain Name System (query)

DNS Standard query A 8-0.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 197 (288 bytes on the wire)
UDP, Src Port: 51832 (51832), Dst Port: domain (53)

RECV VICTIM Time 0.022809 Domain Name System (response)
DNS Standard query response, No such name
Frame 198 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 51832 (51832)

XMIT VICTIM Time 0.022886 Domain Name System (query)
DNS Standard query A 8-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 199 (288 bytes on the wire)
UDP, Src Port: 50808 (50808), Dst Port: domain (53)

RECV VICTIM Time 0.022953 Domain Name System (response)
DNS Standard query response, No such name
Frame 200 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 50808 (50808)

XMIT ATTACK Time 0.023015 Domain Name System (query)
DNS Standard query MX 9.jo.cert-test.mail-abuse.org
Frame 201 (79 bytes on the wire)
UDP, Src Port: 59035 (59035), Dst Port: domain (53)

RECV ATTACK Time 0.023258 Domain Name System (response)
DNS Standard query response MX 1 9-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 9-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 9-4.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
MX 1 9-5.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

MX 1 9-6.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

MX 1 9-7.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

MX 1 9-8.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

MX 1 9-9.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

MX 1 9-0.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

MX 1 9-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 202 (535 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 59035 (59035)

XMIT VICTIM Time 0.023359 Domain Name System (query)
DNS Standard query A 9-2.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 203 (288 bytes on the wire)
UDP, Src Port: 50611 (50611), Dst Port: domain (53)

RECV VICTIM Time 0.023440 Domain Name System (response)
DNS Standard query response, No such name
Frame 204 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 50611 (50611)

XMIT VICTIM Time 0.023496 Domain Name System (query)
DNS Standard query A 9-3.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 205 (288 bytes on the wire)
UDP, Src Port: 61681 (61681), Dst Port: domain (53)

RECV VICTIM Time 0.023567 Domain Name System (response)
DNS Standard query response, No such name
Frame 206 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 61681 (61681)

XMIT VICTIM Time 0.023622 Domain Name System (query)
DNS Standard query A 9-4.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 207 (288 bytes on the wire)
UDP, Src Port: 58347 (58347), Dst Port: domain (53)

RECV VICTIM Time 0.023688 Domain Name System (response)
DNS Standard query response, No such name
Frame 208 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 58347 (58347)

XMIT VICTIM Time 0.023742 Domain Name System (query)
DNS Standard query A 9-5.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com

Frame 209 (288 bytes on the wire)
UDP, Src Port: 54368 (54368), Dst Port: domain (53)

RECV VICTIM Time 0.023808 Domain Name System (response)
DNS Standard query response, No such name
Frame 210 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 54368 (54368)

XMIT VICTIM Time 0.023861 Domain Name System (query)

DNS Standard query A 9-6.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 211 (288 bytes on the wire)

UDP, Src Port: 60614 (60614), Dst Port: domain (53)

RECV VICTIM Time 0.023925 Domain Name System (response)

DNS Standard query response, No such name

Frame 212 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 60614 (60614)

XMIT VICTIM Time 0.023991 Domain Name System (query)

DNS Standard query A 9-7.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 213 (288 bytes on the wire)

UDP, Src Port: 55345 (55345), Dst Port: domain (53)

RECV VICTIM Time 0.024068 Domain Name System (response)

DNS Standard query response, No such name

Frame 214 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 55345 (55345)

XMIT VICTIM Time 0.024123 Domain Name System (query)

DNS Standard query A 9-8.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.

123456789-123456789-123456789.123456789-123456789.123456789.

example.com

Frame 215 (288 bytes on the wire)

UDP, Src Port: 51591 (51591), Dst Port: domain (53)

RECV VICTIM Time 0.024188 Domain Name System (response)

DNS Standard query response, No such name

Frame 216 (348 bytes on the wire)

UDP, Src Port: domain (53), Dst Port: 51591 (51591)

XMIT VICTIM Time 0.024243 Domain Name System (query)

DNS Standard query A 9-9.jo.cert-test.

123456789-123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789-123456789.

123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 217 (288 bytes on the wire)
UDP, Src Port: 63273 (63273), Dst Port: domain (53)

RECV VICTIM Time 0.024307 Domain Name System (response)
DNS Standard query response, No such name
Frame 218 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 63273 (63273)

XMIT VICTIM Time 0.024362 Domain Name System (query)
DNS Standard query A 9-0.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 219 (288 bytes on the wire)
UDP, Src Port: 55263 (55263), Dst Port: domain (53)

RECV VICTIM Time 0.024427 Domain Name System (response)
DNS Standard query response, No such name
Frame 220 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 55263 (55263)

XMIT VICTIM Time 0.024483 Domain Name System (query)
DNS Standard query A 9-1.jo.cert-test.
123456789-123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789-123456789.
123456789-123456789-123456789-123456789.
123456789-123456789-123456789.123456789-123456789.123456789.
example.com
Frame 221 (288 bytes on the wire)
UDP, Src Port: 49820 (49820), Dst Port: domain (53)

RECV VICTIM Time 0.024551 Domain Name System (response)
DNS Standard query response, No such name
Frame 222 (348 bytes on the wire)
UDP, Src Port: domain (53), Dst Port: 49820 (49820)