INTERNET-DRAFT Expires: January 1, 2010 Yuming Huang AT&T Labs

June 2009

DNS Encoding of Domain Reputation and IP# Classification draft-huang-dnsext-reputation-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of <u>BCP 78</u> and <u>BCP 79</u>.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/lid-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This memo defines an Experimental Protocol for the Internet community. This memo does not specify an Internet standard of any kind. Discussion and suggestions for improvement are requested. Distribution of this memo is unlimited.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to <u>BCP 78</u> and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (<u>http://trustee.ietf.org/license-info</u>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This document defines the format of a new Resource Record (RR) for the Domain Naming System (DNS), (and reserves a corresponding DNS type mnemonic: DRIC and numerical code - to be done) This definition deals with associating a reputation measure to a domain, a host name, or a url before domain name resolution. It also deals with associating a classification of the result ip# after domain name resolution. The data shown in this document is fictitious and does not necessarily reflect the real Internet.

1. Introduction

Online fraud, site spoofing, pharming and phishing are growing by leaps and bounds, and eroding consumer trust in online transaction security. User protection mechanism(Anti-phishing, etc.) is implemented by web browsers or browser plug-ins (toolbar etc).

Compared to the existing mechanisms, a more and maybe the most effective mechanism is to bind the domain reputation and IP# classification measures with the DNS lookup.

When a client (web browser or plug-in) wants a DNS server to resolve a domain name (host name, url) into ip#, the client received the ip# as well as the security info about the ip# and the domain name (host name, url). Therefore, a Resource Record (RR), Domain Reputation and IP# Classification (DRIC), are recommended as an extension to the existing DNS protocol.

2. RDATA Format

													1	1	1	1	1	1
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5			
+++++++++++++																		
	Repu	tat	ion						Cl	ass	ifi	cat	ion					
+++++++++++++																		

where:

Reputation is a byte integer which encodes a reputation measure for a string (domain name, host name, or URL) sent by a DNS client to a DNS server to resolve. The DNS server acquires the reputation measure from various resources: the Resource Record (RR) of its DNS database, a further query to another DNS server to resolve the string whose answer may have the reputation measure, or a communication a clustered server which holds and looks up a blacklist against the string from the DNS client. The value of the byte is agreed upon by client and server. For example, 1 means the string is a hit on the blacklist, while 0 is not a hit. We define 2 as that the host name is a part of a URL which is a hit on the blacklist although the host name is not a hit. This is meaningful because many URLs (web pages) may share a same host name and DNS server only holds reputation and classification as well as an ip# for a host name. If we know all the URLs are "good", we just tell DNS client "No-Hit" for all the URLs sharing the same host name. On the other hand, if some URLs are "bad", the string from DNS client should be matched with the blacklist(which is done on a

```
clustered security server).
```

The reputation measure may come from a third party DNS server if the string from DNS client can not be resolved by this server. However, if an organization or an ISP want to protect its users based on most authentic and updated blacklist and other info, the org should have a clustered (with DNS server) server which handles blacklist and updates RR.

Classification is a byte integer which encodes classification of ip#. For example, zombie ip#; dynamic ip# vs. static ip#; business ip# vs. home ip#. Similar to reputation, a clustered security server handle ip# classification and updates RR. For those ip# not resolved on this DNS server, the clustered security server looks up ip# for its classification and informs DNS server the result. The DNS server sends back the classification byte as well as the reputation byte to its DNS client.

3. The DRIC RR

The Domain Reputation and IP# Classification is defined with the mnemonic DRIC and type code XX (to be determined).

<u>4</u>. Master File Format

Each host requires its own DRIC field (byte integer) in the corresponding DNS RR to explicitly specify its Domain Reputation and IP# Classification. If the DRIC field is omitted, a DNS inquiry will return the value from the clustered security server lookup.

Consider the following example:

```
; Authoritative data for lisle.labs.att.com.
@
      ΤN
            SOA
                  ns1.lisle.labs.att.com.
                (
                        94070503
                                         ; Serial (yymmddnn)
                        10800
                                         ; Refresh (3 hours)
                        3600
                                        ; Retry (1 hour)
                        3600000
                                        ; Expire (1000 hours)
                        86400
                                         ; Minimum (24 hours)
                )
                        NS
                                ns1.lisle.labs.att.com.
                IN
                                10.1.1.1
ns1
                IΝ
                        А
                IΝ
                        DRIC
                                00
machine1
                IΝ
                        Α
                                135.1.1.2
                ΙN
                        DRIC
                                20
```

machine2	IN	A	135.1.1.23
	IN	DRIC	1 1
machine3	IN	А	135.1.1.24
machine4	IN	A	135.7.1.99
	IN	DRIC	0 1

Note:

A generic form of URL is path?parameter#anchor

protocol://userid:password@hostname(ip#):port/

Reference:

http://tools.ietf.org/html/rfc1034 http://tools.ietf.org/html/rfc1035 http://tools.ietf.org/html/rfc1712 http://tools.ietf.org/html/rfc1876 http://tools.ietf.org/html/rfc3596 http://tools.ietf.org/html/rfc4398

Editor's Address

Yuming Huang <u>810</u> Meadowridge Dr. Aurora IL 60504, US +1-630-810-7856 yuming@att.com