Network Working Group
Internet Draft
Intended status: Standards Track
Expires: December 30, 2019

J. Bambenek
ThreatSTOP
R. Porter
Palo Alto Networks
June 30, 2019

Domain Contact Information (WHOIS) over DNS
draft-bambenek-porter-dnsop-whois-over-dns-01.txt

Abstract

Domain contact information over DNS provides a vehicle for exchanging contact information in a programmatic and reliable manner. DNS has a ubiquitous presence within the internet infrastructure and will act as a reliable publication method for contact information exchange. This RFC provides an agreed upon structure, voluntarily, to publish points of contact for domains.

This document outlines the methodology for utilizing DNS TXT records for voluntary publication of various forms of contact. The intended purpose is to provide a faster means of reliable contact for professionals, cyber-defense of domains.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

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

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

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

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

This Internet-Draft will expire on December 30, 2019.

Copyright Notice

Table of Contents

1. Introduction

In lieu of recent events and legislation that has impacted the global availability of the current WHOIS protocol and underlying model, a new method for distributing contact information for domains is necessary. This method must rely on the consent of the domain owners and be optional in order to comply with emerging privacy law. As an additional requirement, the existing protocol does not allow for internationalization and that should be corrected with whatever successor system is designed.

The availability of this information has proved an invaluable resource for security and anti-abuse professionals in preventing spam, detecting malicious infrastructure, and preemptive detection of election manipulation operations. Maintaining some system to both distribute this information (should it be voluntarily published) in a manner that allows for automated retrieval and analysis is key.

1.1. Rationale for Using DNS

All resources communicating on the Internet already use DNS to distribute information. In many cases, these domains are already using text records for SPF, DKIM, CAA, and other types to distribute information about their infrastructure and identity to validate communication and prevent abuse.

One of the benefits of the WHOIS system outlined in RFC 3912 [RFC3912] is that records are stored and distributed by a different entity who performs some measure of validation, at least for the e-mail address. This means that if a domain owner were compromised, someone else has contact information to get in touch with the true own to organize remediation. Using WHOIS Over DNS at least separates the distribution of this information from a webserver and makes it less likely a hostile actor could manipulate the contact information as well in the event of a compromise.

It is less ideal that full administrative separation in a different organization, but DNS and webservers are typically separate so compromise of both simultaneously would be rare (albeit not impossible).

Additionally, internationalization is already well-established in DNS using punycode as outlined in RFC 3492 [RFC3492].

DNS TXT records as specified in RFC 1463 [RFC1463] are already in wide use and is where WHOIS over DNS information SHOULD be stored. These TXT records SHALL be tied to "_whois" subdomain TXT record. This roughly follows the convention already used by DMARC records as specified in RFC 7489 [RFC7489] so implementation should be easy and DNS providers should already be able to support the addition of these new records.

1.2. Rationale to Publish or Not Public WHOIS over DNS Information

There are a wide variety of reasons to publish or not publish valid contact information that is available for anyone in the world to use. Those concerned about privacy or who are otherwise at-risk based on their online activities may wish to hide this information. Others may wish to publish it so reputational engines treat their e-mail and other communication as more valid.

Each use case is unique and a "one size fits all" approach cannot work on a global Internet. This document was written so that publishing or not publishing is optional, whether individual or "role-based" information is used is a choice, and that this information is preserved for use by automated systems.

All commercial DNS providers and DNS servers SHALL support these record types.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying significance described in RFC 2119.

In this document, exampledomain.com will be used to describe the DNS TXT records used. It is not intended to point to anything currently or planned to be in use.

3. Administrative Contact Information

Administrative contact information MAY be published as a DNS TXT record that is prefaced with the letter "a". The administrative

contact SHOULD be the person or persons who are representatives of the domain and charged with making business and non-technical decisions. This person or persons may be on other contact records.

3.1. Administrative Contact Name

The administrative contact name MAY be created, but if it is, SHALL be stored using the name "aname". This contact name may refer to an individual or a role name (i.e. "Business Administrator"). Punycode can be used to support internationalization of that name. An example record of this type would be:

```
_whois.exampledomain.com.  14400 IN TXT   "aname=John Bambenek"
```

3.2. Administrative Contact Phone Number

The administrative contact phone number MAY be created, but if it is, SHALL be stored using the name "aphone". This phone number MAY be a direct dial to an individual or to a monitored phone by a group of individuals. It SHOULD however, be a line that would be monitored by a live person. The phone number MUST be stored in accordance with the ITU standard for international numbers [E.164]. An example of the record is would be:

```
_whois.exampledomain.com.  14400 IN TXT   "aphone=+13127254225"
```

3.3. Administrative Contact E-mail Address

The administrative contact e-mail address MAY be created, but if it is, SHALL be stored using the name "aemail". This e-mail may be a role-based e-mail address or an individual e-mail account. In either case, it MUST be monitored for messages. An example of this record would be:

```
_whois.exampledomain.com.  14400 IN TXT
   "aemail=bambenek@illinois.edu"
```

3.4. Administrative Contact Address

The administrative contact address MAY be created, but if it is, SHALL be stored using the name "aaddress". This MUST be stored using the valid convention of mail services for the country where the address resides in and include the country at the end. This address MUST exist and MUST correctly represent an address where the administrative contact can receive mail. An example of this record would be:

```
_whois.exampledomain.com.  14400 IN TXT   "aaddress=201 N. Goodwin
Ave., Urbana, IL 61801, US"
```

4. Technical Contact Information

Technical contact information MAY be published as a DNS TXT record that is prefaced with the letter "t". The technical contact SHOULD be the person or persons who are representatives of the technical aspects of Internet-facing services provided by the domain (i.e. web server administrator, e-mail administrator). This person or persons may be on other contact records.

4.1. Technical Contact Name

The technical contact name MAY be created, but if it is, SHALL be stored using the name "tname". This contact name may refer to an individual or a role name (i.e. "Website Administrator"). Punycode can be used to support internationalization of that name. An example record of this type would be:

```
_whois.exampledomain.com.  14400 IN TXT   "tname=John Bambenek"
```

4.2. Technical Contact Phone Number

The administrative contact phone number MAY be created, but if it is, SHALL be stored using the name "tphone". This phone number MAY be a direct dial to an individual or to a monitored phone by a group of individuals. It SHOULD however, be a line that would be monitored by a live person. The phone number MUST be stored in accordance with the ITU standard for international numbers [E.164]. An example of the record is would be:

```
_whois.exampledomain.com.  14400 IN TXT   "tphone=+13127254225"
```

4.3. Technical Contact E-mail Address

The administrative contact e-mail address MAY be created, but if it is, SHALL be stored using the name "temail". This e-mail may be a role-based e-mail address or an individual e-mail account. In either case, it MUST be monitored for messages. An example of this record would be:

```
_whois.exampledomain.com.  14400 IN TXT
   "temail=bambenek@illinois.edu"
```

4.4. Technical Contact Address

The administrative contact address MAY be created, but if it is, SHALL be stored using the name "taddress". This MUST be stored using the valid convention of mail services for the country where the address resides in and include the country at the end. This address MUST exist and MUST correctly represent an address where the technical contact can receive mail. An example of this record would be:

_whois.exampledomain.com. 14400 IN TXT "taddress=201 N. Goodwin Ave., Urbana, IL 61801, US"

5. Network Contact Information

Network contact information MAY be published as a DNS TXT record that is prefaced with the letter "n". The network contact should be the person or persons who are representatives of the domain and charged with making networking decisions on behalf of the domain. This person or persons may be on other contact records.

5.1. Network Contact Name

The network contact name MAY be created, but if it is, SHALL be stored using the name "nname". This contact name may refer to an individual or a role name (i.e. "Network Administrator"). Punycode can be used to support internationalization of that name. An example record of this type would be:

_whois.exampledomain.com. 14400 IN TXT "nname=John Bambenek"

5.2. Network Contact Phone Number

The administrative contact phone number MAY be created, but if it is, SHALL be stored using the name "nphone". This phone number MAY be a direct dial to an individual or to a monitored phone by a group of individuals responsible for networking. It SHOULD however, be a line that would be monitored by a live person. The phone number MUST be stored in accordance with the ITU standard for international numbers [E.164]. An example of the record is would be:

_whois.exampledomain.com. 14400 IN TXT "nphone=+13127254225"

5.3. Network Contact E-mail Address

The network contact e-mail address MAY be created, but if it is, SHALL be stored using the name "nemail". This e-mail may be a role-

based e-mail address or an individual e-mail account. In either case, it MUST be monitored for messages. An example of this record would be:

```
_whois.exampledomain.com.  14400 IN TXT
   "nemail=bambenek@illinois.edu"
```

5.4. Network Contact Address

The administrative contact address MAY be created, but if it is, SHALL be stored using the name "naddress". This MUST be stored using the valid convention of mail services for the country where the address resides in and include the country at the end. This address MUST exist and MUST correctly represent an address where the network contact can receive mail. An example of this record would be:

```
_whois.exampledomain.com.  14400 IN TXT   "naddress=201 N. Goodwin
Ave., Urbana, IL 61801, US"
```

6. Security / Abuse Contact Information

Security or abuse contact information MAY be published as a DNS TXT record that is prefaced with the letter "s". The security or abuse contact SHOULD be the person or persons who are representatives of the domain and should receive reports on security or abuse concerns from resources under the domain or being targeted to resources served by the domain. This person or persons may be on other contact records.

6.1. Security / Abuse Contact Name

The security or abuse contact name MAY be created, but if it is, SHALL be stored using the name "sname". This contact name may refer to an individual or a role name (i.e. "Business Administrator"). Punycode can be used to support internationalization of that name. An example record of this type would be:

```
_whois.exampledomain.com.  14400 IN TXT   "sname=John Bambenek"
```

6.2. Security / Abuse Contact Phone Number

The security or abuse contact phone number MAY be created, but if it is, SHALL be stored using the name "sphone". This phone number MAY be a direct dial to an individual or to a monitored phone by a group of individuals responsible for security and/or abuse reports for the domain. It SHOULD however, be a line that would be monitored by a live person. The phone number MUST be stored in accordance with the

ITU standard for international numbers [E.164]. An example of the record is would be:

_whois.exampledomain.com. 14400 IN TXT "sphone=+13127254225"

6.3. Security / Abuse Contact E-mail Address

The security or abuse contact e-mail address MAY be created, but if it is, SHALL be stored using the name "semail". This e-mail may be a role-based e-mail address or an individual e-mail account. In either case, it MUST be monitored for messages. An example of this record would be:

_whois.exampledomain.com. 14400 IN TXT
"semail=bambenek@illinois.edu"

6.4. Security / Abuse Contact Address

The security or abuse contact address MAY be created, but if it is, SHALL be stored using the name "saddress". This MUST be stored using the valid convention of mail services for the country where the address resides in and include the country at the end. This address MUST exist and MUST correctly represent an address where the administrative contact can receive mail. An example of this record would be:

_whois.exampledomain.com. 14400 IN TXT "saddress=201 N. Goodwin Ave., Urbana, IL 61801, US"

7. All-in-One Option

In order to create a simple option for those cases where the contact would be the same for all four types of WHOIS contacts, an "all" record MAY be used to take the place of the four individual categories to simplify DNS administration for the domain owner.

7.1. "All" Contact Name

The "all" contact name MAY be created, but if it is, SHALL be stored using the name "allname". This contact name may refer to an individual or a role name (i.e. "Domain Owner"). Punycode can be used to support internationalization of that name. An example record of this type would be:

_whois.exampledomain.com. 14400 IN TXT "allname=John Bambenek"

7.2. "All" Contact Phone Number

The "all" contact phone number MAY be created, but if it is, SHALL be stored using the name "allphone". This phone number MAY be a direct dial to an individual or to a monitored phone by a group of individuals. It SHOULD however, be a line that would be monitored by a live person. The phone number MUST be stored in accordance with the ITU standard for international numbers [E.164]. An example of the record is would be:

```
_whois.exampledomain.com.  14400 IN TXT   "allphone=+13127254225"
```

7.3. "All" Contact E-mail Address

The "all" contact e-mail address MAY be created, but if it is, SHALL be stored using the name "allemail". This e-mail may be a role-based e-mail address or an individual e-mail account. In either case, it MUST be monitored for messages. An example of this record would be:

```
_whois.exampledomain.com.  14400 IN TXT
   "allemail=bambenek@illinois.edu"
```

7.4. "All" Contact Address

The "all" contact address MAY be created, but if it is, SHALL be stored using the name "alladdress". This MUST be stored using the valid convention of mail services for the country where the address resides in and include the country at the end. This address MUST exist and MUST correctly represent an address where the contact can receive mail. An example of this record would be:

```
_whois.exampledomain.com.  14400 IN TXT   "alladdress=201 N. Goodwin
Ave., Urbana, IL 61801, US"
```

8. Security Considerations

As with any publication of potentially personally identifiable information, this could lead to individuals receiving unwanted communication of various sorts. This standard does not require specific individuals to be identified, per se, as all the contact types can be role-based accounts.

The purpose of this document is to establish a standard by which "someone" can be contacted in the case of a need to contact a domain owner and to help establish reputation for those looking to connect with a given domain and have transactions with services on that domain.

The publication of this information is immensely useful to the security and anti-abuse industry for a wide variety of reasons and this information can and should be used for reputational scoring of domains to filter out potentially abusive infrastructure.

The publication of this data in DNS is optional, but third-parties are free to use the lack of this information as a negative indicator when considering interconnectivity (such as the delivery of e-mail).

If the domain registration itself were seized by a hostile third-party, this system would not be able to authoritatively identify the "victim"-owner. Passive DNS, however, will help in an overwhelming majority of these cases.

The limitation of this approach is that there is no true validation of any of the fields that will be published in these records. Under the current system in the general case, an e-mail address is validated before a domain is published. In this case, individuals can use unsuspecting third-parties' contact information. Those incidents, when discovered, are all but certainties that the underlying domain is abusive (except in the case of plausible typos) and provide further negative reputational data that can be used.

A third-party system could be used to provide for such validation but that is outside the scope of this document. Additionally, invalid entries, fake addresses, non-working email addresses or malformed content MAY be used to negatively score a domain for security reputation purposes.

DNSSEC MUST be fully deployed on any domain using these conventions to help ensure reliability of this information.

9. IANA Considerations

There are no IANA considerations as this will use the existing DNS TXT (type 16) RR.

10. References

10.1. Normative References

[RFC1463] Rosenbaum, R., "Using the Domain Name System to Store Arbitary String Attributes", RFC 1463, May 1993.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997.

[RFC3492] Costello, A., "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)", RFC 3492, March 2003.

[RFC3912] Daigle, L., "WHOIS Protocol Specification", RFC 3912, September 2004.

[RFC7489] Kucherawy, M., Zwicky, E., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, March 2015.

10.2. Informative References

[RFC1034] Mockapetris, P., "Domain Names - Concepts and Facilities", RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain Names - Implementation and Specification", RFC 1035, November 1987.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC5322] Resnick, P., "Internet Message Format", RFC 5322, October 2008.

[E.164] International Telecommunications Union, "Recommendatino E.164: The international public telecommuncations number plan", May 1997, http://www.itu.int/.

11. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Appendix A. Copyright Notice

Authors' Addresses

John Bambenek
ThreatSTOP, Inc.
2720 Loker Avenue West, Suite G, Carlsbad, CA 92010, USA

Email: bambenek@illinois.edu

Richard Porter
Palo Alto Networks
3000 Tannery Way, Santa Clara, CA 95054, USA

Email: rporter@paloaltonetworks.com