Messaging, Malware and Mobile Anti-Abuse Working Group
M³AAWG Protecting Parked Domains Best Common Practices

https://www.m3aawg.org/M3AAWG-Protecting-Parked-Domains-BCP-update-2022-06

Updated June 2022

Table of Contents

I. Executive Summary

Many organizations and individuals register domains without an immediate intent to use these domains or to use them in a limited context. These domains (or subdomains) are not meant to send or receive email traffic. For instance, a domain can be registered to prevent a bad actor from acquiring and abusing the domain, known as a defensive registration. These domains are "parked." In other instances, the domain or subdomain is used exclusively to contain a website with no email service enabled.

This Messaging, Malware and Mobile Anti-Abuse Working Group best practices document describes what identifiers can be used to indicate a domain or subdomain that is not meant to send or receive emails.

II. Problem Statement

Failure to publish DNS records signaling that a parked domain does not send or receive email provides opportunities for third parties to abuse domains of this nature. Domains that are similar to well-known domains are especially vulnerable to such attacks.

The publication in the DNS of specific types of SPF[1], DMARC[2] and MX[3] records can be used to indicate a domain that never sends or receives email. Receivers can rely on these records to reject any email purporting to be from such a domain.

III. DNS (Domain Name System)

SPF (Sender Policy Framework)

Any domain that never sends email, including parked domains, should publish an SPF TXT record in DNS that is referred to as a "naked" -all. An example TXT record of this type is:

```
example.com TXT "v=spf1 -all"
```

This record indicates that no IP is authorized to send email for the domain "example.com."

Subdomain protection is more complicated because a record for each potential subdomain needs to be created unless wildcard records are allowed by the organization's DNS policy. A record using such a wildcard is:

```
*.example.com TXT "v=spf1 -all"
```

DKIM (DomainKeys Identified Mail)

There is no need to publish any DKIM[4] record for a parked domain and in fact none should be published.

If no DKIM records are published for a parked domain, then any mail attempting to forge a DKIM signature using a parked domain will fail to validate due to the nonexistence of the public key in DNS.

DMARC (Domain-based Message Authentication, Reporting & Conformance)

Any domain that never sends email, including any parked domain, should publish a DMARC TXT record in DNS that specifies "p=reject". Because the domain involved publishes a naked -all for SPF and has not published any DKIM public keys using that domain, email attempting to use the domain will fail all DMARC validation checks, as it would be impossible to get an SPF or DKIM pass on an aligned domain. Any mail forging this domain should therefore be rejected by receiving domains enforcing DMARC policies.

An example TXT record of this type is:

```
_dmarc.example.com TXT "v=DMARC1; p=reject; rua=mailto:rua@example.com"
```

Including the "rua" tag,[5] which specifies an address to which DMARC aggregate reports should be sent, is optional.

We deem the "rua" tag optional in this case because aggregate reports are most useful for identifying valid mail streams that might require tweaks to their authentication setup. For parked domains there should be no valid mail streams, and so there should be no tweaks that need to be made to authentication setups. Nonetheless, the aggregate reports might be interesting for some domain owners as a window into the level of attempted abuse that's being mitigated. Some domain owners may even choose to reach out to report generators when the disposition bits of the aggregate report indicate that the generator is not honoring the domain's published DMARC policy; however, mailbox providers who only quarantine mail that has a published reject policy may be resistant to efforts to get them to change their ways.

If the domain itself does not receive email, then the "rua" tag must point to another domain that does receive email, such as:

```
_dmarc.example.com TXT "v=DMARC1; p=reject; rua=mailto:rua@example.net"
```

The DMARC protocol specification[6] requires for such "third-party reporting" that the domain receiving the DMARC reports also publish in DNS a record that effectively confirms that it has consented to receive such reports. The record looks like this example:

```
example.com._report._dmarc.example.net TXT "v=DMARC1;"
```

Null MX

Email receivers sometimes verify that an email message can be replied to before they will accept the message. Such receivers might attempt to verify that the domain parts of the Return-Path and/or visible From email addresses found in an inbound mail message exist by checking for an associated MX, A, or AAAA record for the domain.

There are cases where a domain might be used for websites only and will have an A and/or AAAA record without actually accepting inbound mail connections. While such domains would pass an existence test, it would be impossible to deliver any mail to those domains.

The recommended way to indicate that a domain is not meant to receive email is by publishing the following null MX record[7] for the domain:

```
example.com MX 0 .
```

For the null MX, the hostname on the right side of the DNS record is a bare dot.

To work on all subdomains, a wildcard should be used:

```
*.example.com MX 0 .
```

SOA (Start of Authority)

It is expected (per RFC 2142) that role accounts such as postmaster or abuse will exist and will be the appropriate points of contact for a given domain (e.g., postmaster@example.com, abuse@domain.com). For domains that publish null MX records, this assumption won't hold, because the domain doesn't accept inbound mail. However, since there may still be a need to contact someone responsible for the domain, the domain's SOA record[8] should be used to communicate contact information for the domain.

An SOA record is a special type of DNS record, one that marks the starting point for a part of the DNS namespace for which authority is claimed by a DNS server. An example SOA record for the domain "example.com" might look like this:

```
example.com SOA ns.example.net hostmaster.example.net 2022040200 3600 7200
86400 86400
```

where

- `example.com` is the domain being served.
- `SOA` is the DNS resource record type.
- `ns.example.net` is the hostname of the primary authoritative DNS server for the domain.
- `hostmaster.example.net` specifies the mailbox of the party responsible for the domain. The label before the first dot represents the local mailbox name, so the address here is *hostmaster@example.net*.

- `2022040200` is a number representing the version of the domain, called the *serial number*. This is frequently expressed in the format YYYYMMDDxx, allowing for a rudimentary change tracking system of up to 100 changes per calendar day, so here it would be the first version of the domain published on 2 April 2022.
- `3600` is a number representing the time in seconds before a secondary server should check with the primary for any updates. M[3]AAWG recommends one hour for parked domains, shorter times for active domains.
- `7200` is a number representing the time in seconds before a secondary server should retry a failed refresh. M[3]AAWG recommends two hours for parked domains.
- The first `86400` is the maximum number of seconds since the last refresh before the secondary server should consider its data to be stale. M[3]AAWG recommends one day for parked domains.
- The second `86400` is the minimum Time To Live (TTL) in seconds for any record that doesn't explicitly declare a TTL; this tells a querying server how long to cache an answer before asking for it again, and M[3]AAWG recommends one day for parked domains.

IV. Examples

This section describes which DNS records to add for different scenarios. For an explanation of each record, please see Section III above.

a) Single Parked Domain

```
example.com. TXT "v=spf1 -all"
example.com. MX 0 .
*.example.com. TXT "v=spf1 -all"
*.example.com MX 0 .
_dmarc.example.com. TXT "v=DMARC1; p=reject; rua=mailto:rua@example.net"
example.com._report._dmarc.example.net TXT "v=DMARC1"
```

b) Single Domain with A or AAAA Record

```
example.com. A 192.168.0.1
example.com. TXT "v=spf1 -all"
example.com. MX 0 .
*.example.com. A 192.168.0.1
*.example.com. TXT "v=spf1 -all"
*.example.com. MX 0 .
sub.example.com. A 192.168.0.1
sub.example.com. MX 0 .
sub.example.com. TXT "v=spf1 -all"
_dmarc.example.com. TXT "v=DMARC1; p=reject; rua=mailto:rua@example.net"
example.com._report._dmarc.example.net TXT "v=DMARC1"
```

c) Multiple Parked Domains

```
example.com. TXT "v=spf1 -all"
example.com. MX 0 .
*.example.com. TXT "v=spf1 -all"
*.example.com. MX 0 .
_dmarc.example.com. CNAME _dmarc.parked.example.net.
example.org. TXT "v=spf1 -all"
example.org. MX 0 .
*.example.org. TXT "v=spf1 -all"
*.example.org. MX 0 .
_dmarc.example.org. CNAME _dmarc.parked.example.net.
_dmarc.parked.example.net TXT "v=DMARC1; p=reject; rua=mailto:rua@example.net"
```

```
example.com._report._dmarc.example.net TXT "v=DMARC1"
example.org._report._dmarc.example.net TXT "v=DMARC1"
```

V. DNSBL/RPZone (DNS Block Lists/Response Policy Zone)

It is common for email receivers to check a DNS block list (DNSBL). A domain owner can solicit DNSBL providers who publish domain-based lists (as opposed to IP-based ones) to see if the provider is interested in including the domain owner's parked domain(s) in the DNSBL. Such solicitation should only be done if the domain owner is 100% sure that the domain will never be used to send mail in the future, as it can be hard to undo such a listing. If the domain might be reassigned and the new assignee might use it for email, this is **not recommended.**

VI. Conclusion

This document describes the best practices for maintainers of a parked domain to advertise in DNS the fact that such a domain sends no email. While there is no guarantee that mailbox providers and others will make best use of this information, following these practices will at least ensure that the domain owner did all they could to announce the fact.

VII. References

[1]SPF – Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1 https://www.rfc-editor.org/rfc/rfc7208

[2]DMARC – Domain-based Message Authentication, Reporting and Conformance, https://www.rfc-editor.org/rfc/rfc7489

[3]MX – Mail Exchanger Record, see Domain Names - Implementation and Specification, https://www.rfc-editor.org/rfc/rfc1035

[4]DKIM – DomainKeys Identified Mail (DKIM) Service Overview, https://www.rfc-editor.org/rfc/rfc5585 and DomainKeys Identified Mail (DKIM) Signatures, https://www.rfc-editor.org/rfc/rfc6376

[5]RFC 7489 Domain-based Message Authentication, Reporting, and Conformance (DMARC), Section 6.3, General Record Format, https://www.rfc-editor.org/rfc/rfc7489#section-6.3

[6]CNAME – Canonical Name record, see Domain Names - Implementation and Specification, https://www.rfc-editor.org/rfc/rfc1035

[7]A "Null MX" No Service Resource Record for Domains That Accept No Mail, https://www.rfc-editor.org/rfc/rfc7505

[8]SOA – Start of Authority record, see Domain Names - Implementation and Specification, https://www.rfc-editor.org/rfc/rfc1035

As with all best practices that we publish, please check the M[3]AAWG website (m3aawg.org) for updates to this document.