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

Updated December 2015

Table of Contents

I. Executive Summary 1
II. Problem Statement 1
III. DNS (Domain Name System) 2
SPF (Sender Policy Framework) 2
DKIM (DomainKeys Identified Mail) 2
DMARC (Domain-based Message Authentication, Reporting & Conformance) 2
Null MX 3
SOA (Start of Authority) 4
IV. Examples 4
A. Single Parked Domain 4
B. Single Domain with A or AAAA Record 4
C. Multiple Parked Domains 4
V. Reporting Abuse 5
VI. DNSBL/RPZone (DNS Block Lists/Response Policy Zone) 5
VII. Conclusion 5
VIII. References 5

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 either 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.

Mailbox providers are using techniques to authenticate incoming emails quite effectively, provided such domains have the necessary identifiers. 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 email authentication records signaling that a parked domain does not send or receive email provides opportunities for third parties to abuse domains of this nature. The attack is usually the result of two conditions:

- The domain is similar to a well known domain
- The domain has no assessed reputation

Such attacks, which have been identified in the wild, can be alleviated by the proper use of email authentication techniques. The publication in the DNS of specific types of SPF[1], DKIM[2], DMARC[3] and

MX[4] 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)

Domains that never send email, including parked domains, should publish a 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 of this type is:

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

DKIM (DomainKeys Identified Mail)

A DKIM record is based on a selector linked to a domain key entry to indicate the public key. For instance:

```
selector1._domainkey.example.com TXT "v=DKIM1; p=32AB567E34F…"
```

The proper way to indicate that a key has been revoked is to leave p with no value (see http://tools.ietf.org/html/rfc6376#section-3.6.1 [5]). To ensure any selector can be found, the following wildcard registration can be used:

```
*._domainkey.example.com TXT "v=DKIM1; p="
```

This record indicates that any DKIM key has expired for the domain "example.com." When working with subdomains, the wildcard would have to be used:

```
*.example.com TXT "v=DKIM1; p="
```

This higher level wildcard may overload the SPF record. For a parked domain, with no other usage, the two records as shown here would not be a problem.

While an email with no valid DKIM signature has to be treated as if there was no DKIM signature at all, an email with an expired key is usually treated with more caution.

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

Domains which never send email, including parked domains, should publish a DMARC TXT record in DNS which specifies "p=reject". An example TXT record of this type is:

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

Including the RUA[6] tag is important since it allows the domain owner to receive aggregate reports of potential abuse. The presence of a RUF[7] tag is optional, but recommended to receive failure reports and be able to follow up on the potential abuse when required. The use of a RUF tag may cause domains that are being actively abused to receive extreme quantities of failure reports.

Because the domain involved is publishing as a "naked" -all and is not signing any email with DKIM purporting to come from that domain, such email should be rejected by mailbox providers enforcing DMARC policies. DMARC works, by design, on subdomains of the organizational domain, eliminating the need for another record.

In theory, the DMARC record might be redundant and there is no apparent need to have SPF or DKIM records, but not all receivers implement DMARC.

If the domain itself does not receive email, then the RUA and RUF must point to another domain that does receive emails, such as:

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

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

Changing a DMARC record for each parked domain because the RUA or RUF tags need to be changed is cumbersome. In this instance a CNAME[8] record can be used:

```
_dmarc.example.com CNAME _dmarc.parked.example.net.

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

*._report._dmarc.example.net TXT "v=DMARC1"
```

Null MX

Email receivers sometimes verify that an email can be replied to. For instance, they might receive an email from john@example.com as indicated in one or more of these headers: the envelope MAIL-FROM (5321.From), header From (5322.From) or "Reply-To". In this case, the receiver might attempt to verify that they can email back to this address by looking for the presence of a MX, A, or AAAA record for the domain example.com.

Unfortunately, some domains are used for websites only and will have an A and/or AAAA record without listening on port 25, which is used for SMTP. While doing a DNS check is moderately resource intensive, verifying that port 25 is listening is highly resource intensive.

The recommended way to indicate that a domain is not meant to receive email is by publishing the following null MX record[9] :

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

To work on all subdomains a wildcard should be used:

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

The above method is only implemented by a fraction of email receivers. If receivers only check for the presence of a MX record, they may not see that the record is a null MX record and reach the wrong conclusion. As of late 2015, M[3]AAWG recommends the use of a null MX record only if the domain has an A and/or AAAA record for maximum compatibility with receivers who have not yet implemented the standard.

SOA (Start of Authority)

The SOA[10] can also be used to indicate that a responsible party is reachable, likely at a different domain:

```
example.com SOA ns.example.com hostmaster.example.net 2013020801
900 600 86400 3600
```

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. TXT "v=spf1 -all"
*.example.com. TXT "v=DKIM1; p="
_dmarc.example.com. TXT "v=DMARC1; p=reject;
rua=mailto:rua@example.net; ruf=mailto:ruf@example.net"
example.com._report._dmarc.example.net TXT "v=DMARC1"
```

B. Single Domain with A or AAAA Record

```
example.com. TXT "v=spf1 -all"
*.example.com. TXT "v=spf1 -all"
*.example.com. TXT "v=DKIM1; p="
_dmarc.example.com. TXT "v=DMARC1; p=reject;
rua=mailto:rua@example.net; ruf=mailto:ruf@example.net"
example.com._report._dmarc.example.net TXT "v=DMARC1"
example.com. MX 0 .
example.com. A 192.168.0.1
sub.example.com. A 192.168.0.1
sub.example.com. MX 0 .
```

C. Multiple Parked Domains

```
example.com. TXT "v=spf1 -all"
*.example.com. TXT "v=spf1 -all"
*.example.com. TXT "v=DKIM1; p="
_dmarc.example.com. CNAME _dmarc.parked.example.net.

example.org. TXT "v=spf1 -all"
*.example.org. TXT "v=spf1 -all"
*.example.org. TXT "v=DKIM1; p="
_dmarc.example.org. CNAME _dmarc.parked.example.net.
⋮
_dmarc.parked.example.net TXT "v=DMARC1; p=reject;
rua=mailto:rua@example.net; ruf=mailto:ruf@example.net"
*._report._dmarc.example.net TXT "v=DMARC1"
```

V. Reporting Abuse

If a domain does not receive email, then the address abuse@example.com will not work. To ensure handling of abuse complaints, M[3]AAWG recommends the addition of an abuse point of contact in the domain WHOIS records and the registration of the abuse point of contact at abuse.net.

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

It is common for email receivers to check a DNS block list. While a list of parked domains could be used to block emails, no organization to date is offering such facility.

VII. Conclusion

Mailbox providers are using effective techniques to authenticate incoming emails – when such domains have the necessary identifiers. This M[3]AAWG best practices document describes what identifiers can be used to indicate that a "parked" domain or subdomain is not meant to send or receive emails.

VIII. References

[1]SPF- Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1
http://www.openspf.org/RFC 7208

[2]DKIM DomainKeys Identified Mail, http://www.dkim.org/RFC 5585
and DKIM DomainKeys Identified Mail, draft-ietf-dkim-deployment-11,
http://dkim.org/specs/draft-ietf-dkim-deployment-11.html

[3]DMARC – Domain-based Message Authentication, Reporting & Conformance,
https://tools.ietf.org/html/rfc7489

[4]MX - Mail Exchanger Record, see Domain Names - Implementation and Specification,
https://tools.ietf.org/html/rfc1035

[5]RFC 6376 DomainKeys Identified Mail (DKIM) Signatures, Section 3.6.1 Textual Representation,
http://tools.ietf.org/html/rfc6376#section-3.6.1

[6]RUA - Reporting URI for Aggregate reports, see DMARC.org, "DMARC Overview,"
http://www.dmarc.org/overview.html

[7]RUF - Reporting URI for Forensic reports, see DMARC.org, "DMARC Overview,"
http://www.dmarc.org/overview.html

[8]CNAME - Canonical Name record, see Domain Names - Implementation and Specification,
https://tools.ietf.org/html/rfc1035

[9]A "Null MX" No Service Resource Record for Domains That Accept No Mail,
https://tools.ietf.org/html/rfc7505

[10]SOA – State Of Authority record, see Domain Names - Implementation And Specification,
https://tools.ietf.org/html/rfc1035

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