Potential Email Compromise via Dangling DNS MX

Joshua Avery Reed J. C. Reed
DNS Institute

July 25, 2020

Abstract

Routing of email generally relies on DNS MX (Mail Exchange) resource records. In addition, the MX definition may be used in Sender Policy Framework (SPF) rules. In this paper, we explore Dangling MX record targets which are available for third-party purchase and control. Depending on corresponding, potentially valid MX records and SPF rules, the vulnerabilities range from little impact to complete two-way email communication compromise, without snooping or man-in-the-middle techniques. Even if the organization does not use the domain for email, a third-party could still use it in a phishing attack where the phisher can actually use a valid and legitimate domain for increased credibility. We discovered 393 domain names with a Dangling MX record. This paper shares real-world examples of Dangling MX records and techniques for finding them. While the Dangling MX concept is already known, this paper also describes a novel vulnerability and research approach where the Dangling MX or other DNS target is an existing registered domain, but available for purchase or unknown third-party use.

1 Introduction

As an educational exercise in 2019, we were analyzing some domains for an IPv6 report related to Fortune 500 companies' domain names and DNS services and noticed a security vulnerability with a MX mail exchange target pointing to another domain name no longer in association with the company and was available for purchase through a domain reseller service. A third-party could purchase that domain name and maliciously or unknowingly setup a mail server which could accept mail for the company domain containing the MX record. Since then, we found many additional domains with the same issue of unregistered or available domain name targets also known as stale DNS records, dangling DNS records, or Dare.

The 2016 paper "All Your DNS Records Point to Us" by Liu, Hao, and Wang defines Dangling DNS records (aka "Dare") as resources pointed to by an existing DNS record that are discontinued or invalid as a "largely overlooked, and ... serious and widespread security threat." The paper discusses probable causes and potential effects and presents attack vectors. As part of a larger Dare research, their study briefly introduced email fraud possibilities and dangling MX records: "If a Dare-MX could be exploited, an adversary may be able to send and receive emails in this vulnerable domain."[1]

Dangling MX records are generally caused by domain owners neglecting or forgetting about their related DNS records. In our research we also found the problem caused by parent companies that bought other companies and forgot about existing DNS MX settings, backup mail services that were abandoned, ignorant assumptions, and simple typos in the DNS zone file configurations.

2 DNS MX Record Explained

The DNS MX "mail exchange" resource record was initially documented in RFC 974 "Mail Routing and the Domain System" in January 1986 to define the host (or server) that will handle incoming email for a domain. A domain may have multiple MX resource records and an MX record also defines a preference (or priority) value.[2]

As also further explained in newer RFC 5321 "Simple Mail Transfer Protocol" from October 2008, the sending mailer (or SMTP client) looks up the MX resource record in DNS for the domain and then should try the lowest preference numbered target mail server first. It looks up the A or AAAA address record for that new target domain name and attempts to connect and send the email via the SMTP service there. It can then try in order of higher numbers (or lower priority) MX hosts. Multiple MX records with the same preference number are allowed and the sending system may choose one randomly to use first. Multiple MX records are not required and multiple preference numbers are not needed.[3]

Note that SMTP and MX does not define the final destination host, but also may be used for relaying emails between mail servers. Lower priority (higher preference number) MX targets have historically been used for just accepting and queueing emails to be then relayed on to the final SMTP server destination.

If a MX record is not found, then the sending mailer will fall back to look up the A (or AAAA) address record instead.

If no SMTP service is connected to, the sending mailer may queue the message and retry sending it periodically later following the same MX lookup sequence before it ultimately fails (typically at least four days).[3]

Note that the target host name may be completely

different from the domain name for the MX record. For example, many organizations use an outsourced service, such as aspmx.l.google.com, to handle their email[4] or use a different domain name for organizational purposes, such as the microsoft.com MX target is a name under outlook.com.

The following is an example of an MX record in DNS zone file format which contains a round-robin of equal-preference email servers that are under a different domain name:

```
yahoo.com.  1800 IN MX  1 mta5.am0.yahoodns.net.
yahoo.com.  1800 IN MX  1 mta6.am0.yahoodns.net.
yahoo.com.  1800 IN MX  1 mta7.am0.yahoodns.net.
```

In our own research in May 2020 of 100 random domains from a list of over 3600 Fortune 500 domains, only two domains had an SMTP service listening via the IPv4 address from the domain's A record (which is also used for the website). This was for both SMTP TCP port 25 and Message Submission port 587, and one also had a Submission over TLS port 465 service listening. One of these domains had an MX record with different SMTP servers and the other did not have any MX record. (We didn't validate if the SMTP services accepted email for the domains for any of our research.) In most cases, email services use the MX record and do not fall back to use the A record.

3 Vulnerability Scenarios

The inbound mail problems found vary:

- All MX targets or all highest priority MX targets vulnerable (where incoming email take over is trivial).
- Some same highest priority MX targets vulnerable (and may randomly get some of the emails).
- Low priority MX targets vulnerable (and also may randomly get some of the emails).

An inbound email compromise does not require a man-in-the-middle technique to intercept the communication nor does it require snooping to observe the communications.

Received emails could be used to learn trade secrets, customer details, and for private conversations which may be used to compromise transactions, for example.

In some cases, email for an existing domain is not used at all and is known to not work because all the existing MX targets (at all priorities) do not work. Nevertheless, their existing or potential customers or partners could be convinced to use the legitimate email domain which is related to the organization.

These same issues may be applicable for SRV records, but our research didn't find any Dangling SRV records specifically for the SMTP services.

We didn't verify working SMTP nor mail receipt for the MX targets in our study.

(Another related issue is Dangling "email addresses" where published or previously used email addresses use domains no longer registered or now squatted. We didn't research this issue, but an example is the contact email address for the hybrid-pop service in the IANA Service Name and Transport Protocol Port Number Registry.)[5]

3.1 Highest Priority MX Targets

If all the MX targets or all the highest priority MX targets have dangling MX records (which may be just one MX), full inbound email can be taken over.

In this case, either the email didn't work at all before (and the domain owner may have not cared) or it worked with the lower priority MX records (so mail was getting through).

For example, here are steps for compromising inbound email for a domain name that has a single MX target under a domain name which is not registered:

- Register, purchase, or lease the target's domain name.
- Setup an SMTP server (such as Postfix) to handle emails for the main domain (not the target's domain name). It could be setup to capture all mail for that domain (and child or wildcard domains).
- Setup the A (and/or AAAA) address for the MX target — the full hostname — to point to that new mail server's IP address. (The email domain name's DNS does not need to be modified – that is the point, it already has the mistake of pointing to the now newly-setup MX target.)
- Wait for the incoming emails. A marketing effort or phishing campaign can be utilized to encourage emails to be sent.

Note when the primary MX target is established at some attacking site, mail would stop working (for the lower priority MX records) and likely the organization would soon notice that incoming email stop or decreased — so they can examine the mail routing problem.

Attackers may choose to observe and pass on the emails to the previous working MX targets to attempt to hide their compromise.

3.2 Some MX Targets

If not all of the highest priority MX records have dangling records, but are at the same preference number, the sending mailers may randomly choose one to send to. The new mail server may be able to get some random fraction of the incoming email traffic. Even one mistake out of five MX targets at the same priority, for example, might be bad.

In addition, depending on the other mail servers, possibly a denial of service attack (DDoS) could be triggered

targetting the valid higher-priority (lower number) target mail servers so they will become less available so mail senders will send to the compromised MX targets instead.

3.3 Lower Priority MX Targets

Lower priority (larger preference number) MX targets may periodically still get email traffic due to network issues or temporary outages for the valid higher-priority mail servers.

(And again DDoS attacks could be used to limit the other valid target mail servers to encourage mail senders to relay the mail to the compromised MX target instead.)

An attack against the lower priority MX records could remain unnoticed and operational for a long time as occasional or intermittent mail loss is less likely to be investigated.

4 Attack Comparison

An alternative attack methodology could be done by registering a similar name which may provide a more diverse attack vector. In addition to just email, they can control web servers with the ability to use certificates — without being defeated by simply correcting MX records.

Our research data showed many similar names, but we didn't study this specifically.

5 SPF, DKIM, DMARC

The Dangling MX problem can be abused for spoofing the senders email address too.

The Sender Policy Framework (SPF) rules (which are also stored in DNS) is used to help prevent forgery or email spoofing by senders using other's domain names. The rules define what hosts are allowed (or authorized) to send emails from a domain name. SPF is not used to prevent sending to a domain name. Implementing SPF will not stop inbound mail to a compromised MX target.

The SPF rules have an "mx" mechanism which may be used to authorize senders use of a domain name based on the IP address lookups for each of the MX record targets. Outbound email fraud can be done by spoofing the sender's from email address using the domain name by sending from the mail server with the IP for the address for the target of the now-compromised Dangling MX target. SPF rules using this "mx" feature may allow that.

Note that not all mail server software even checks for SPF nor honors it. Commonly SPF is configured in the "SOFT" FAIL mode which means to accept the mail regardless of the SPF settings (while possibly logging and tagging about the problem instead).

DKIM or DomainKeys Identified Mail (as described in RFC 6376) provides another way for receiving mail servers to verify the sender is allowed to use that domain name (as a sender). The receiving mail servers use a DKIM key found via the sender's DNS TXT record to verify a header signature.[6] An impersonator can bypass this by not providing the DKIM signature in the spoofed emails.

DMARC, or the Domain-based Message Authentication, Reporting, and Conformance mechanism (as documented in RFC 7489), extends both SPF and DKIM technologies by allowing the sending and receiving email software to indicate what to do when the sent email doesn't authenticate, including rejection. This may be utilized to help reduce spoofing.[7]

As also noted in the "All Your DNS Records Point to Us" paper, by exploiting dangling targets, anti-spam technologies like DKIM and SPF can be bypassed.[1]

We evaluated many authentication records and identified many problems, but it was not the focus of this research.

6 Two-way Sending and Receiving Complete Email Compromise

Complete email compromise for both sending and receiving emails for an organizations domain name may be possible if the MX record is the highest priority (or the higher priority mail servers are disabled or diminished) and SPF, DKIM, and/or DMARC or similar technologies are not used or misconfigured.

7 Phishing Attacks

Phishing is a method of tempting people to share (often personal) information by pretending to be a legitimate organization related to the disclosed information. Email spoofing by pretending to be a legitimate sender is a common example of phishing, but phishing can be done without sending emails or fake websites, etc. External communications, such as phone calls, billboards, and fraudulent advertisements can be used to trick people to contact the malicious party by sending to a legitimate email address domain (as compromised via this Dangling MX vulnerability).

A phishing attack could be done by using the compromised domain email for incoming correspondence to help legitimize the phishing story. Or in the two-way communication compromise, a phishing attack could be sent from using that domain name. It looks legitimate as the "From" email address is official.

In our research, we didn't learn of any phishing attacks that relied on Dangling MX records. (There are much simpler, more effective, and less preventative phishing techniques.)

8 Dangling MX Results

We found 393 domain names that had at least one Dangling MX record from our research of our domain lists

of Fortune 500 companies and S&P Global largest 100 banks and from checking domains in the Tranco one million top websites list. This represented 1,003,477 domains checked with 1,640,528 MX records and 431,496 unique MX target hostnames. (The list contained around 25,993 domains that didn't appear to be registered and 10,948 domains that didn't return answers due to timeouts or SERVFAILs.)

The MX target domains in this study are either: unregistered/expired (NXDOMAIN); available via a domain squatter or reseller; or used via an unrelated advertising link farm (which could be sold like a reseller too). We combined the unrelated link farm and resellers in our squatters counts.

We found 30 domains that had MX squatted target hostnames. There were 35 MX squatted target hostnames from 29 squatted domain names. We also found an additional five MX target domains which are unknown if are squatted or not.

We found 363 domains that had MX target hostnames that were under unregistered base domain names. that resulted in NXDOMAIN. There were 316 MX target hostnames from 305 unregistered domain names. (These were identified using ICANN's and IANA's domain lists.[8])

We found an additional 35 domains that had unregistered MX target hostnames that were under the following subdomain hosting providers: amazonaws.com, bytemark.co.uk, cloudapp.net, ddns.net, dnsalias.com, dyndns.org, iobb.net, kasserver.com, linode.com, and selfip.com. (These were identified using the Public Suffix List.[9])

While we don't name the most frequent available domain names in this report, we did see 34 examples due to misspellings or typos involving Google's mail server hostnames.

Some of these mistakes are for domains that have active websites and some are for domains for old corporate domains which redirect to other websites. They have been forgotten about or mismanaged.

Around half of the findings were caused by typing or data entry mistakes including missing trailing letters (e.g., "co" instead of "com"), missing other letters (e.g., "c" in "com"), added letters, translitered characters (e.g., "squaer" instead of "square"), missing period between DNS labels (e.g., "mxbmail" instead of "mxb.mail" or "aspmx4googlemail") or other misspellings (like "shanhai" instead of "shanghai").

Some of the examples were a purposeful but misunderstood misuse of public DNS by using assumed private names which could be registered later (like under new TLDs).

Also some mail or DNS administrators purposefully used invented — assumed to be garbage — domains, possibly with the goal to disable mail with assumption it wouldn't work later. (For example: "youspammersucksreally1234.com".)

The rest of the examples are likely to be lack of tracking due to email service providers disappearing and domains becoming unregistered and some ultimately squatted.

(Future research and reports may share counts for non-existing TLDs such as "*invalid*", counts based on MX priorities, SPF records using dangling names, abuse via subdomain hosting providers, further IPv6/AAAA data, MX targets that are are registered and unknowingly controlled by others, use of passive dns historical databases to find existing problems, and research other dangling targets (we have already found), such as SRV, NS, and CNAME. If you'd like to collaborate on any research, please contact DNS Institute.)

9 Finding Dangling MX Targets

Dangling MX targets are trivial to find. First perform a DNS MX query for a domain; and then do address queries (A and AAAA) for the MX target mail server hostname. If it doesn't exist, proceed to check if its base domain exists in DNS by looking for its SOA and/or NS records. You may also consult the corresponding WHOIS database to see about its DNS registration status. In addition to top-level domains (TLDs),[8] we also used the ICANN domains sections from the Public Suffix List[9] to help identify domain suffixes that domain names can be registered under, such as *co.uk* and *k12.mi.us*.

The basic steps follow:

1. Do DNS queries for MX record type for the list of domains (and store the results).

2. For the received MX record answers, get the domain name part of the MX target hostnames.

3. For names not looked up yet, do DNS queries for IPv4 address (A) records for the MX hostnames and the corresponding domain names (and store the results).

4. From the recorded addresses answers, identify the domain names (only) that returned a NXDOMAIN status.

5. And find their referring domain name and corresponding MX record target hostname (from the first query results) and report those that have a valid TLD.

(We only attempted one DNS query with standard timeout of five seconds at a time. On a later day, we attempted second DNS queries for previous failed attempts. Our research also lowercased all names. We also excluded domain names where the final label was not an ICANN TLD.)

Note that some target base domains may result in a NXDOMAIN DNS status when queried even if they do exist, because their authoritative nameservers are configured to provide answers for child domains or labels under their base domain but not the base domain itself

(except for maybe NS records). These are called empty non-terminals.[10]

To research, use a parent domain's nameserver to verify if it exists or not. (If it exists, it should return an authority section with the child's authoritative NS records.) Also some nameservers return a NXDOMAIN status even though it appears to have other record types at the same label (and normally would have returned a NOERROR status).

We audited our results by looking at all the SOA records returned with the NXDOMAINs to make sure the DNS owner returned was for the parent domain. (Only one name was a mistake.)

10 Finding Domain Squatters or Resellers

We didn't exclude the target MX hostname from further research even if its does exist (or even responds to SMTP service). We looked up the resolved A record addresses of the hostname and its base domain name in a database of IPv4 and IPv6 addresses of known domain resellers or squatters. We built a database of over one hundred IPv4 and IPv6 addresses that were known to host reseller websites for domains available for purchase or lease or were otherwise squatted on for non-content advertising purposes.

This IP address database was partially built by doing simple HTTP GET downloads of common words in several different languages with corresponding ccTLDs. Generally, domains for resell have a corresponding webpage. The content was analyzed for key terms (in various languages) to recognize if it was a squatted domain. For example, morte.com.br website served a sponsored links service and tag.de was hosted by a domains reseller. In addition known domain resellers were researched to find additional IP addresses.

Cross-referencing against this list of IPs resulted in many domains that were available for sale. We also excluded entries where the dangling MX targets were under the same domain as its MX record label.

The basic steps follow. Some step are identical the previous (NXDOMAIN) checks so re-use the same initial data, but this also adds looking up IPv6 AAAA addresses.

1. Do DNS queries for MX record type for the list of domains (and store the results).

2. For the received MX record answers, get the domain name part of the MX target hostnames.

3. For names not looked up yet, do DNS queries for IPv4 address (A) and IPv6 address (AAAA) records for the MX hostnames and the corresponding domain names (and store the results).

4. Compare the recorded address answers against our domain squatters IP addresses database (containing both IPv4 and IPv6 addresses).

5. For the names with addresses that match a known squatters IP address, report the original referring domain name (with a valid TLD) that has the corresponding MX target domain name (from the first query results).

Our data had various false positives mostly due to some known squatter IP addresses also host legitimate domains. Our initial research and later analysis was done by attempting HTTP GET downloads (on port 80) for the MX target hostnames and reviewing any resulting webpage content.

Note other domains are likely to use the same Dangling MX targets (and we found examples of this in our research). A resellers address database can be supplemented and other domains using the same MX targets can be trivially found using Passive DNS research and historical DNS databases. (This may be a followup study.)

11 Unregistered (NXDOMAIN) Examples

The following few examples (out of 363 discovered) had an unregistered domain name (and returned an NXDOMAIN status) for the target MX hostname.

The website https://www.chevrolet.com.br/ is an apparently maintained website. The domain name chevrolet.com.br had the following MX record on 2019-11-12:

```
chevrolet.com.br. 600 IN MX (
            10 mail.popstats.com.br. )
```

The domain name had a single MX target under a domain name (popstats.com.br) which is not registered.

The compromise process would be simple: register domain name; setup a VM with a mail server to handle emails for chevrolet.com.br; and setup the DNS address for the MX target (mail.popstats.com.br) to point to that mail server. It could be setup to capture all mail for that domain (and child domains). A phishing attack could be sent from using that domain name. It looks legitimate as the email address is official.

As another unregistered MX target domain example, the only MX records for seb.ua (Skandinaviska Enskilda Banken) on 2020-03-06 were:

```
seb.ua.    10800  IN  MX  20 mx2.seb-life.com.
seb.ua.    10800  IN  MX  10 mx1.seb-life.com.
```

A third example is lorealparisusa.com (L'Oreal) which had the following MX records as of 2020-03-31:

```
lorealparisusa.com.   600  IN  MX  (
 5 mail.nurunnewyork.com. )
lorealparisusa.com.   600  IN  MX  (
 0 lorealparisusa-com.mail.protection.outlook.com. )
```

Its lower priority MX target domain was not registered. (L'Oreal had three domains with problems.)

For additional unregistered examples, visit https://dnsinstitute.com/research/dangling-mx/.

12 Squatted Examples

The following four domains (out of 30 found) had MX targets hostnames that had squatted base domains. As seen on the following page, web browser screenshots were captured showing the domains for sale and/or being used for advertising.

The domain shoppersfood.com (United Natural Foods) was seen on 2019-11-01 to have the following MX records:

```
shoppersfood.com. 900 IN MX (
    10 mail.farmfreshmarkets.com. )
shoppersfood.com. 900 IN MX (
    5 supervaluinc.mail.protection.outlook.com. )
shoppersfood.com. 900 IN MX (
    20 mail2.farmfreshmarkets.com. )
```

The MX target base domain name farmfreshmarkets.com was available for lease or sale as seen in Figure 1.

The domain name berlinerbank.de (Deutsche Bank) had the following MX records as of 2020-03-14:

```
berlinerbank.de. 1800 IN MX (
                    10 airmail.bb-data.de. )
berlinerbank.de. 1800 IN MX (
                    10 airmail2.bb-data.de. )
berlinerbank.de. 1800 IN MX (
                    30 mx2.mail.psinet.de. )
```

The higher priority MX targets domain name bb-data.de was available for sale as seen in Figure 2.

The domain names fox29.com, fox5ny.com, and myfoxphilly.com (Fox Communications) were seen on 2020-03-30 to have a lower priority MX record target of placeholder.securehostedemail.com. Its based domain was registered but for sale and used for advertising links as seen in Figure 3.

The domain coca-cola.co.uk (Coca-Cola) had the following MX records as of 2020-04-04:

```
coca-cola.co.uk. 3000 IN MX (
                    10 mx.postredirect.com. )
coca-cola.co.uk. 3000 IN MX (
                    10 ns3-old.ko.com. )
```

Its equal priority target MX mx.postredirect.com record's base domain is registered and is available via a domain reseller and used in an advertising link farm as seen in Figure 4.

For additional squatted examples, visit https://dnsinstitute.com/research/dangling-mx/.

13 Unknown Mail Service Setup

It is possible that the dangling target domain may be purchased and a mail server setup there without knowledge that the other domain names are using it for their MX setup. In common usage, a receiving SMTP mail server is configured to accept mail for specific domain names, but possibly but highly unlikely a mail server may be configured to accept mail for all domain names. Mail logs or other network snooping may identify the incoming mail domains. Unmatching mailbox (or user) names will cause the mail to bounce or lost. Matching mailbox names may unknowingly collect mail for the unknown domain names.

Also the domain purchaser may learn about the MX mistake via port scan checkers or other network analysis that shows the IP being targetted for SMTP port(s) and then they could listen or watch that to learn more about the use.

14 Vulnerability Disclosure Discussion

As part of our study, we didn't purchase nor register any of the target domains. We did not attempt to contact the resellers or squatters about these problems.

We attempted to contact many of the organizations that we knew about owning the domain names with the initial problems starting in November 2019. We tried contacting the companies via DNS SOA RNAME email addresses, website contact forms, bug report forms, email addresses found via company websites, Twitter contacts, LinkedIn contacts, and more. We also utilized the HackerOne and BugCrowd services to assist with security disclosures. In some cases they had existing relationships with the companies.

We were able to help some of the companies understand and then fix the problems. A few of the companies acknowledged the details but declined to fix problems. Some of the companies did not understand the technology nor the vulnerability. After months of frequent failed attempts to contact most organizations, we admit defeat and have decided to just share the domain names and/or organization names publicly.

15 Fixes and Mitigations

The immediate fix is to remove the errant MX record from the domain's DNS zone configuration. Note that a time-to-live (TTL) may temporarily keep the old record in others' caches (up to a common maximum time override of one week). A replacement MX record is not needed to remove the problem record.

A second fix is to change the MX record target to be the correct, desired mail server hostname. This may be a simple typo fix or replacement.

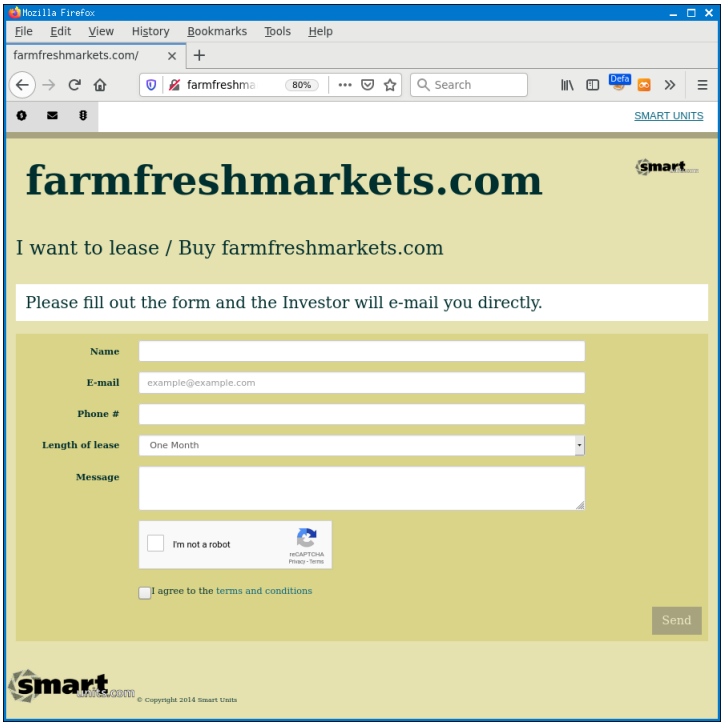

Figure 1: farmfreshmarkets.com 2020-04-04

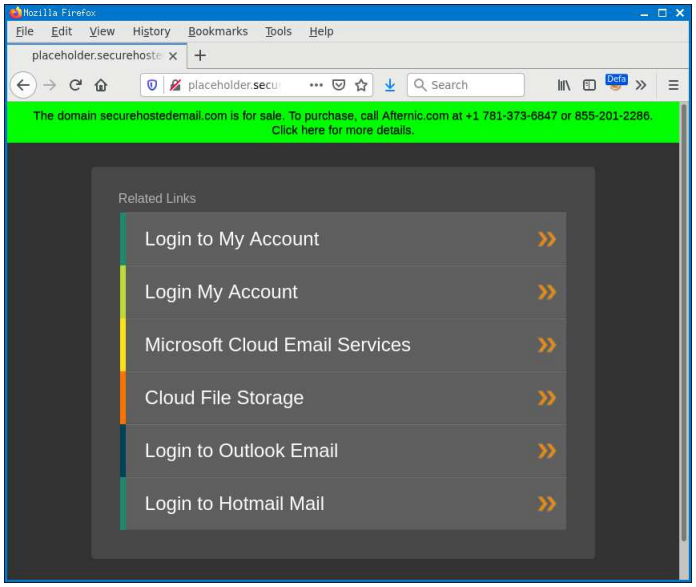

Figure 3: placeholder.securehostedemail.com 2020-04-01

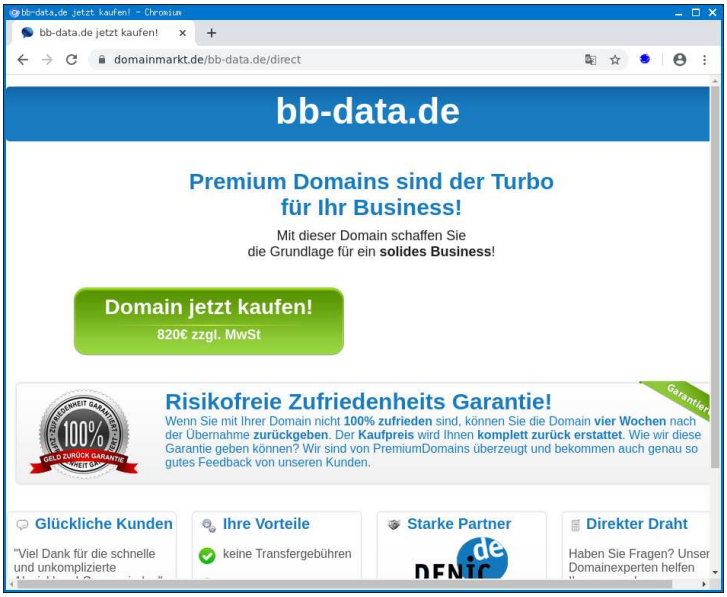

Figure 2: bb-data.de 2020-07-08

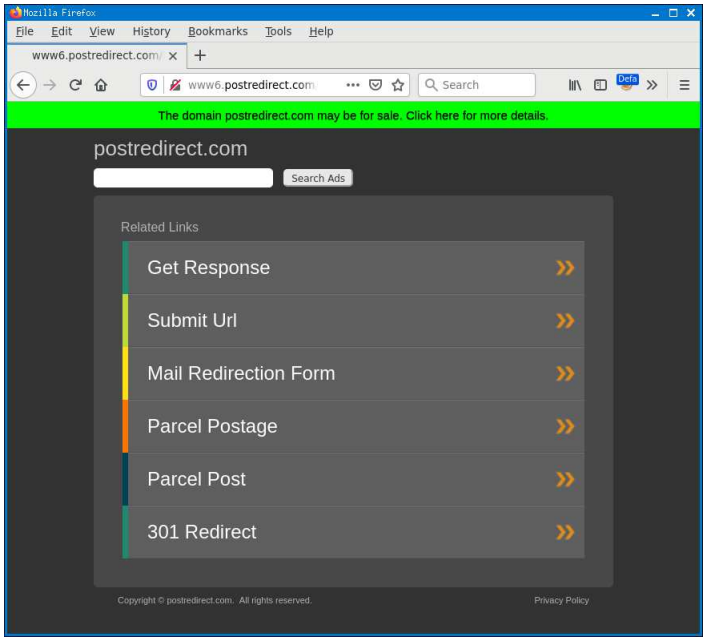

Figure 4: postredirect.com 2020-04-04

While defining MX records, correct the ordering of priorities as needed and verify with any third-party or outsourced mail services the correct mail server hostnames (and MX priorities) to use.

For changes, consider having a quality assurance and audit step to review the changes before publishing them live. Then use a DNS monitoring system that will periodically check the MX targets for correctness.

(These same steps may be applicable to other DNS records too.)

As for mitigating abuse of wrong mail servers being used, individual email messages may be encrypted using GPG, for example, to prevent content disclosure.

If using SPF policies, evaluate any hostname references — including in *include* references – for valid hostnames and consider to not use the *mx* feature as part of SPF rules.

In addition, if the DNS MX target was a domain previously in the organization's control, they can consider repurchasing it and maintaining it. Organizations should keep track of upcoming domain expirations. An unused domain should not be abandoned (to allow it to expire) without removing any references to it.

As a correct practice do not add bogus or fake MX entries. If no mail service is desired, still setup a single MX record, such as defined in RFC 7505 "A 'Null MX' No Service Resource Record for Domains That Accept No Mail" with a preference of 0 and host target of "." (period). This should cause the mail delivery to immediately fail without falling back to address lookups.[11] (In our research of 104,639 domains for MX records, we only found 136 RFC 7505 style MX records.)

16 Conclusion

In this paper, we presented about Dangling MX records. where the MX targets are available for purchase and control by a third-party. We shared techniques for finding dangling DNS records which are registered but still available for control. Without requiring DNS or email software vulnerabilities and independent of the DNS or email softwate used, Dangling MX records may allow an adversary to compromise email communications to impersonate an organization or to collect private conversations. We showed that the problems effect different organizations regardless of their size or DNS experience. We stress that organizations should review and monitor their DNS configurations for dangling targets.

For further research and additional examples, visit https://dnsinstitute.com/research/dangling-mx/.

Acknowledgements

We want to thank HackerOne and BugCrowd who helped us contact a few of the companies for responsible disclosures. We thank the world's largest company, an American multinational retail corporation, for the bounty they paid for our reported research. Furthermore, we would like to thank R. Elz and C. Zoulas for valuable feedback on a draft of this paper.

References

[1] Daiping Liu, Shuai Hao, and Haining Wang. All Your DNS Records Point to Us: Understanding the Security Threats of Dangling DNS Records. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS*, pages 1414–1425, Oct. 2016.

[2] Mail routing and the domain system. RFC 974, January 1986.

[3] Dr. John C. Klensin. Simple Mail Transfer Protocol. RFC 5321, October 2008.

[4] Google G Suite Support. *G Suite Admin Help: Configure MX Records (Other domain hosts*, (Accessed April 3, 2020). https://support.google.com/a/answer/33915?hl=en.

[5] Internet Assigned Numbers Authority (IANA). *Service Name and Transport Protocol Port Number Registry*, Last Updated 2020-05-06. (Accessed May 9, 2020). https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

[6] Murray Kucherawy, Dave Crocker, and Tony Hansen. DomainKeys Identified Mail (DKIM) Signatures. RFC 6376, September 2011.

[7] Murray Kucherawy and Elizabeth Zwicky. Domain-based Message Authentication, Reporting, and Conformance (DMARC). RFC 7489, March 2015.

[8] Internet Assigned Numbers Authority (IANA). *List of Top-Level Domains*, Last Updated 2020-07-13. https://data.iana.org/TLD/.

[9] *Public Suffix List*, 2020. https://publicsuffix.org/.

[10] Paul A. Vixie, Dr. Susan Thomson, Yakov Rekhter, and Jim Bound. Dynamic Updates in the Domain Name System (DNS UPDATE). RFC 2136, April 1997.

[11] John R. Levine and Mark Delany. A "Null MX" No Service Resource Record for Domains That Accept No Mail. RFC 7505, June 2015.

