How Can MX Record Lookups Protect Your Organization Against Compromise?

Posted on December 9, 2019

A mail exchange (MX) record is a Domain Name System (DNS) record that is required to deliver an email to an address. It identifies the mail server in charge of receiving incoming emails for a particular domain and where outgoing mails should be addressed from. In short, it is in charge of email flow. So, if your MX records are not routed to the appropriate location, you will not able to receive or send emails.

One way of ensuring the integrity and reliability of your MX servers is by using Reverse MX API. With it, you can identify all of the domains connected to each of your mail servers. That helps ensure that domain records are updated and servers are correctly configured.

Understanding the MX Record Format

MX records have two components — priority and domain name. An example of a domain name is sample.com. As such, sample.com's MX record format would look something like this:

```
sample.com IN MX 5678 1 sample.com
sample.com IN MX 5678 5 mail1.sample.com
sample.com IN MX 5678 10 mail2.sample.com
```

In this example, "IN" is short for "Internet" and refers to the domain's class, and the numbers 1, 5, and 10 refer to the priority. The lower the number, the higher its priority status. The domain name mail1.sample.com and mail2.sample.com, in this case, are the mail servers' names. The mail servers' names vary depending on the host server. Connections to MX servers follow the priority status. If you have more than one mail server with the same level of priority, the one used for connection is chosen randomly.

What Do MX Records Have to Do with Cybersecurity?

MX records are crucial in maintaining email functionality. Cybersecurity professionals must be adequately acquainted with their fundamentals to protect their organizations from cyber attacks.

Several attacks begin with sending spearphishing emails to employees of a target organization. An example would be business email compromise (BEC) scams, where attackers typically spoof a company executive to ask a subordinate to transfer funds to a particular account. According to the Federal Bureau of Investigation (FBI), victims lost US $1.3 billion to scammers in 2018 alone.

To effectively pull off a BEC scam, attackers would need to either compromise the sender's email account or create a double. Let's say they opted for the second choice. They would need to break into the target organization's mail server, most likely one with the lowest priority, as this is often less secure. They'd hack into it and configure the MX record to point to their own server. Once that's done, they could send an email to the victim's subordinate to initiate the fraud (making sure he/she, of course, has access to and the authority to transfer corporate funds).

The hypothetical scenario above is made possible via DNS cache poisoning and makes it a must for cybersecurity professionals to maintain their domain's integrity, including its MX records. They can use Reverse MX API to keep track of all of their organization's MX records. These must be kept up-to-date and properly configured at all times.

Another potential threat is DNS MX record hijacking, where the attacker poses as or compromises the sender's DNS server to find out where to deliver an email to the intended recipient. Instead of returning the legitimate IP address, the DNS server returns that of a server owned by the attacker. The sender's server believes this IP address belongs to the recipient's server, and thus delivers the email. The attacker reads the email and to evade detection forwards it to the recipient's real server. In this case, users can use Reverse MX API to make sure that the recipient's domain matches the one on record.

Cybersecurity professionals who want to protect their organizations against spear phishers and other attackers can use MX records as an early warning system. Spotting misconfigurations via regular checks on MX records can alert them of ongoing or soon-to-be-launched attacks.

How Can Cybersecurity Professionals Use MX Records to Thwart Attacks?

Apart from using Reverse MX API to monitor your own MX records, you can also use it to check if a mail server address actually belongs to the domain it points to. All suspicious domains can then be flagged for further investigation and, if proven malicious, consequently blocked. A typical MX record lookup query returns the following data for different domains:

- Domain name associated with the mail server
- First seen at (+ the day, date and time)
- Date when the server was last updated

More specifically, Reverse MX API’s output for “smtpin.vvv.facebook.com” (picked randomly JSON for illustration purpose) would look something like this:

```
{
  "current_page": "1",
  "size": 300,
  "result": [
    {
      "name": "0-edge-chat.facebook.com",
      "first_seen": "1552238051",
      "last_visit": "1569750142"
    },
    {
      "name": "1-edge-chat.facebook.com",
      "first_seen": "1552238220",
      "last_visit": "1569750331"
    },
    {
      "name": "126.facebook.com",
      "first_seen": "1567125606",
      "last_visit": "1569751650"
    },
    {
      "name": "163.facebook.com",
      "first_seen": "1567126751",
      "last_visit": "1569752492"
    },
    {
      "name": "2-edge-chat.facebook.com",
      "first_seen": "1553447736",
      "last_visit": "1569754697"
    },
    ...
  ]
}
```

Security professionals can easily integrate Reverse MX API into their existing solutions to automatically determine if a sender’s domain matches his/her MX records. This feature is particularly useful in screening potential spearphishing emails.

Despite the influx of all kinds of communication channels, email remains the top business communication tool. Protecting your mail servers, therefore, aided by tools such as Reverse MX API, is one way to ensure your company's success.