Doing a Regular MX Record Check Can Help Thwart Phishing Attacks

Posted on January 15, 2020

These days, sophistication seems to be the secret behind the most effective cybercriminal schemes. And those behind business email compromise (BEC) scams are just some of the perpetrators raking in millions of cash. Targeting email users remains an effective way for cybercriminals to cripple organizations and lighten their coffers with very clever ruses. In 2018, BEC scammers amassed US $1.3 billion from their victims, according to the Federal Bureau of Investigation (FBI).

BEC attacks involve mimicking the victims' executives or higher-ranking officials and trusted contacts from partner organizations and suppliers in emails to get them to part with corporate funds. In essence, the cybercriminals use effective social engineering tactics and each time make sure that:

- The sender they impersonate is someone the victim knows and trusts.
- The recipients have the authority to release corporate funds or disburse payments.
- The email comes from a seemingly trustworthy domain.

Let us say, for example, that the attackers want to target Google. To do that, they would need to either spoof Google's domain via cybersquatting or look for a dangling mail exchanger (MX) record in the target's network and redirect that to point to their own server. Opting for the second choice, of course, is more effective as they would be sending fake emails from within the target network.

What Are MX Records and How Can Attackers Use Them?

An MX record acts as a resource record present in a network's Domain Name System (DNS) infrastructure. It is responsible for identifying the mail server that would accept email messages for the entire domain. Organizations have at least two mail servers, each with its own MX record, to make sure that if one fails, no email sent to the domain bounces. As such, each MX record has a preference value (i.e., the higher the number, the lower its priority). This number indicates which server is used first, second, and so on.

So, when you send an email over the Internet, the mail transfer agent queries the DNS database to know which mail server should accept it. Should the preferred mail server be unable to receive it, the agent will try the second option and so on. It won't stop trying until the message is successfully delivered.

Cyberattackers have been known to intercept emails via DNS MX record hijacking. In this scenario, they compromise the target's mail server and manipulate its MX record to send emails to a different IP address (i.e., one that they own). That way, every time anyone sends an email to the target, the attackers are the ones who receive it. This tactic allows them to evade detection while spying on the activities of the person they intend to spoof. And because they have access to the target's account, they can also use it to send fake emails to his/her coworkers who have access to the organization's financial accounts. Of course, they make it a point to send emails that won't incriminate them and clue their target into their scheme to the actual recipient.

Once the sender and recipients have been identified, the rest is plain sailing. The attackers just need to wait till their intended sender isn't likely to check his/her inbox, such as when he/she goes on personal time off. They then send a fake invoice to their target recipient and wait for the funds to be transferred to their bank accounts.

How Can an MX Record Check Protect Against BEC Attacks?

Many DNS-based attacks succeed because organizations fail to see the importance of keeping their records up-to-date and properly configured. Often, cyberattacks succeed because their

victims failed to pay their dues. Leaving unused systems connected to the Internet is like leaving your back door open when you go to work. And that's what cyberattackers look for when compromising target networks — gaping holes left unattended.

Making sure your MX records are updated and properly configured is one way to ward off BEC attacks. Organizations can use Reverse MX API to conduct an **MX record check** on their network. This tool reveals all of the domains that use the same mail server. By regularly scrutinizing the list of domains connected to all of your mail servers, you can spot anomalies that can be indicative of ongoing attacks. Severing ties to domains that you do not own, for one, can help protect your company from BEC scammers and other malicious entities.

Maintaining up-to-date and properly configured MX records is vital to ensure that a particular organization receives all of the emails intended for users under its domain. That allows it to keep communications with practically anyone, especially clients, flowing. But that is not all that clean MX records are for. Maintaining their integrity is also critical for protection against costly cyberattacks. For that reason, integrating an **MX record checker** like Reverse MX API into existing solutions and systems can make their defense against sophisticated attacks stronger.