Reactive Measures: Blocking Email-Based Artifacts

Once we have collected and analyzed email artifacts, we are able to take defensive measures in order to block incoming and outgoing emails that feature these artifacts. Just to recap, the email artifacts that are important to us include:

- **Email Sender** (mailbox@domain)
- **Sender Domain** (@domain)
- **Sending Server IP**
- **Subject Line**

EMAIL SENDER

If a large volume of malicious emails are being sent from the same sender, we would definitely want to block it on the email gateway, preventing more emails coming into the domain and landing in employee mailboxes. This is the primary block we will take with phishing attacks.

On the email gateway, we would typically block incoming emails from the specified sender, however, we could make this block bi-directional, and prevent emails from inside being sent to (recipient) the malicious sender – this would stop emails where an employee is trying to reply to the malicious email.

SENDER DOMAIN

The step-up from blocking the sending address (mailbox@domain) is to block the entire sending domain. When receiving emails from @Outlook or @Gmail, it's obviously not feasible to block these entire domains, as there is a large potential for blocking legitimate emails (such as employees contacting Payroll from their personal addresses, HR reaching out to new employees via their personal addresses, etc). This is typically only done when the sending domain is purely malicious or is using a large number of mailboxes to send malicious emails.

REPLY TO ADDRESS

If a phishing email is trying to get recipients to send a response, such as impersonating a fellow employee and trying to receive information or files, and if the reply-to address is different than the sending address, it may be appropriate to block the reply-to address. Doing so means that if any employees reply to the email the message will be blocked by the email gateway and never leave the organization.

SENDING SERVER IP

This is a very serious block, and is not conducted unless it is absolutely necessary. This will drop any emails coming from the specified IP. Whilst similar to a domain block, a domain may use multiple sending servers, so this would be less effective, and is tailored towards rogue IPs that have been compromised or setup to send malicious emails.

SUBJECT LINE

Phishing attacks will typically use one subject line, otherwise, the attackers need to keep modifying it, creating more work (and likely more cost if they're using paid-for email services). Whilst multiple sending addresses can be delivering the same phishing email, if they all share the same subject line we can easily catch them all, instead of blocking multiple senders, by dropping any emails with the subject line in question.

Previous Topic
Mark Complete
Next Topic
Back to Lesson