Defensive Measures Taken

This part of a report, typically at the end, will mention the defensive actions that you have taken, or are requesting to be taken in order to protect the organization. From the previous lessons of this domain, you will know that the term defensive measures refer to activities after a phishing attack in order to prevent attacks using the same artifacts observed in the analyzed email. We can perform three main types of actions:

- **Email artifact blocking** (subject line, sending address, sending server IP)
- **Web artifact blocking** (URL, domain, IP)
- **File artifact blocking** (file name, file hash)

Depending on the organization, it is likely there will be one of two paths to complete these actions:

- **Analysts that are able to directly conduct defensive measures themselves.**
- **Analysts that must request defensive measures to be taken by senior analysts or other departments, and need to provide sufficient justification.**

Regardless of which path needs to be followed, your report still needs to clearly state what measures have been taken to provide an audit trail should anything go wrong. Below we will cover two examples, one phishing attack where the analyst has the ability to take defensive measures themselves, and one where the investigating analyst must contact senior analysts and other departments to implement blocks.

EXAMPLE ONE

In this example, the investigating analyst has come across a DHL credential harvester, which has been received by 23 employees. After investigating the email, the analyst retrieves the following artifacts:

- **Sender:** contact@dhl.com
- **Sending Server IP**: 209.85.167.42
- **Reverse DNS**: mail-lf1-f42.google.com
- **Subject**: "Failed Delivery DHL RESPOND NOW – URGENT!!"
- **URL:** hxxps://dhl-faileddelivery.shanepppalkkbc.com *(Example Value)*

Example Report Section:

"**[1]** The sending address was successfully spoofing contact@dhl.com, however, the sending IP revealed it was actually a Gmail address, and therefore not from DHL. **[2]** We are unable to block the sending server IP, as it belongs to Gmail, and would have a negative impact on the business as legitimate emails would be blocked. **[3]** Blocking the sender "contact@dhl.com" is also not appropriate, as legitimate emails coming from that address will be blocked. **[4]** I have blocked the subject line on the email gateway, as it is highly unlikely legitimate DHL emails would use it. **[5]** There would be no negative impact to the business, and this action would prevent any more emails in this attack being delivered to employee mailboxes.

- **[6]** Subject Line Block (Email Gateway) "Failed Delivery DHL RESPOND NOW – URGENT!!" on 22nd December at 12:03 PM by Jane Smith.

[7] The URL used within the credential harvester is a malicious domain "shanepppalkkbc[.]com" that utilizes a subdomain "dhl-faileddelivery" to look more effective when glancing at the link. **[8]** After investigating the domain, it was created purely for malicious purposes, and there is no business justification for employees to visit it, and we can block the entire domain to prevent users from visiting the existing malicious link, or any others that are hosted on the site.

- **[9]** Domain Block (Web Proxy) "shanepppalkkbc[.]com" on 22nd December at 12:07 PM by Jane Smith"

Example One Recap:

The investigating analyst:

1. Summarises that the email sender has been spoofed, and the message actually came from Gmail.
2. Understands and states blocking a Google sending IP would most likely have negative consequences.
3. Explains the spoofed sending address value can't be blocked, as it is used legitimately by DHL.
4. States the action they are taking, and provides justification for this decision.
5. Understands and states there would be no negative impact to the business by blocking the unusual subject line.
6. Lists the type of block taken, the value that was blocked, the time and date of the action, and who took the action (provides accountability).
7. Summarises that the URL is malicious and not owned by DHL. Quickly covers tactics used.
8. States the action they are taking, and provides justification for this decision.
9. List the type of block taken, the value that was blocked, the time and date of the action, and who took the action (provides accountability).

EXAMPLE TWO

In this example, a malicious email was reported to the security team by the payroll department. The email claimed to be from the UK government and tells the recipient to review the attached tax announcement. After analysis of the attachment, it was found to be Emotet malware, which infected two machines before it was contained by the incident response team. The body content also featured a URL that connects to a domain and downloads the exact same file as attached to the email. The investigating analyst retrieved the following IOCs:

- **Sender:** HMRC-0fficial@govpayments.net
- **Sending Server IP**: 129.33.19.188 *(Example value)*
- **Reverse DNS**: mail-govpayments.net *(Example value)*
- **Subject**: 2020 HMRC Tax Announcement IMPORTANT
- **URL:** hxxp://hmrc.announcementsgov.com/1jfa/download.php? *(Example value)*
- **Attachment Name:** HMRC-Tax-Announcement-README.pdf.exe
- **File MD5 Hash:** 0a52730597fb4ffa01fc117d9e71e3a9 *(Example value)*

Example Report Section:

"**[1]** The sending address comes from the sending domain @govpayments.net, which is not a legitimate website used by the UK government and HMRC. **[2]** Although we are able to block the sending domain as it is attempting to pose as a legitimate domain owned by the government, we have only received emails from one sending mailbox, and blocking the domain at this point may be excessive. **[3]** Blocking the sender "HMRC-0fficial@govpayments.net" would stop more malicious emails being delivered by this sender. **[4]** There would be no negative impact to the business by blocking this malicious sending address.

- **[5]** Sending Address Block (Email Gateway) "HMRC-0fficial@govpayments.net" on 1st March at 3:37 PM by Chris C.

[6] The URL used within the email is used to download the same Emotet payload as the attachment. **[7]** After investigating the domain, it was created purely for malicious purposes, and there is no business justification for employees to visit it, and we can block the entire domain to prevent users from visiting the existing malicious link, or any others that are hosted on the site.

- **[8]** Domain Block (Web Proxy) "hmrc.announcementsgov.com" on 1st March at 3:41 PM by Chris C"

Example Two Recap:

The investigating analyst:

1. Summarises that the email sending domain is not a legitimate domain used by government, and is attempting to make itself look somewhat legitimate.
2. Explains that blocking the sending domain, although malicious, is excessive as currently only one sending mailbox has been observed sending malicious emails.
3. Explains that blocking the sending address would prevent more emails from being delivered.
4. Understands and states there would be no negative impact to the business by blocking the sending address.
5. Lists the type of block taken, the value that was blocked, the time and date of the action, and who took the action (provides accountability).
6. Summarises that the URL is malicious and used to download the same file that is included as an email

attachment, and that it is Emotet malware.

7. States the domain is malicious and operating with purely malicious intent, and there is no legitimate reason for employees to visit the domain.
8. List the type of block taken, the value that was blocked, the time and date of the action, and who took the action (provides accountability).

Previous Topic

Mark Complete

Next Topic

Back to Lesson