Phishing Response Brief

This activity incorporates all of the knowledge and skills you have learned throughout the Phishing Analysis domain. You will be analysing a number of emails, and conducting two malicious email investigations and writing a report for each. You will answer a number of questions about the artifacts retrieved, and whilst we are unable to hand-mark reports due to the volume of BTL1 students, we will provide our own reports so you can compare them. This activity is crucial practice for the BTL1 exam, so take your time and put the effort in – it will pay off later!

CHALLENGE BRIEF

You have recently joined the security team at ABC Industries as a Junior SOC analyst within their security operations center (SOC). You are responsible for monitoring the SIEM platform, investigating and responding to security events, and protecting the organization from phishing attacks. You have just begun your shift, and in a new effort to proactively identify phishing emails that have made it past perimeter defenses, you have been given a number of emails that have randomly been copied from employee mailboxes. It is your job to analyze the downloaded emails, identify if any are malicious, and conduct investigations and write reports for any that are deemed to pose a risk to the organization. Reports should include a list of artifacts, analysis activities and results, and suggested defensive measures which will be reviewed by senior analysts.

A fellow analyst has already taken a look at the selection of emails and identified TWO malicious emails out of the sample of 5.

HINTS AND ADVICE

- Set aside time to complete this activity. Having no distractions will allow you to work more effectively.
- Ensure that you are comfortable with all of the content in this domain before starting, specifically; retrieve email, web, and file-based artifacts, performing analysis and suggesting appropriate defensive measures.
- Once you have identified the two malicious emails, follow the *Report Writing* lessons to write two reports that feature all of the sections we've covered.
- If an email is not malicious, you are not required to write a report for it.

RESOURCES

This .zip file contains the 5 emails that have been retrieved for inspection.

Download "ABC Industries Email Sample.zip"

This basic report template is designed to help you write your two reports so you can answer the exercise questions in the next lesson

Download "Investigation Report Document.txt"

EXERCISE QUESTIONS

1. Malicious Email 1: What is the sending address?
2. Malicious Email 1: What is the subject line?
3. Malicious Email 1: Who are the recipients?
4. Malicious Email 1: What is the Reply-to address?
5. Malicious Email 1: What is the date and time the email was sent?
6. Malicious Email 1: What is the sending server IP?
7. Malicious Email 1: What is the reverse DNS hostname of the sending server IP?
8. Malicious Email 1: What is the full URL?
9. Malicious Email 1: What is the root domain?
10. Malicious Email 1: What is the most appropriate defensive measure regarding email artifacts in this scenario? (Multiple Choice)
11. Malicious Email 1: What is the most appropriate defensive measure regarding web artifacts in this scenario? (Multiple Choice)

1. Malicious Email 2: What is the sending address?
2. Malicious Email 2: What is the subject line?
3. Malicious Email 2: Who are the recipients?
4. Malicious Email 2: What is the Reply-to address?
5. Malicious Email 2: What is the date and time the email was sent?
6. Malicious Email 2: What is the sending server IP?
7. Malicious Email 2: What is the reverse DNS hostname of the sending IP?
8. Malicious Email 2: What is the file name, including extension?
9. Malicious Email 2: What is the SHA256 hash value of the file?
10. Malicious Email 2: What is the most appropriate defensive measure regarding email artifacts in this scenario? (Multiple Choice)
11. Malicious Email 2: What is the most appropriate defensive measure regarding file artifacts in this scenario? (Multiple Choice)

Previous Topic
Mark Complete
Back to Lesson