Blue Team Level 1 Certification (Standard)

Introduction to BTL1

- ~~Welcome to Blue Team Level 1!~~
  - 4 Topics
- ~~Lab and Forum Access~~

SECURITY FUNDAMENTALS DOMAIN

- ~~Introduction to Security Fundamentals~~
  - 1 Topic
- ~~Soft Skills~~
  - 7 Topics
- ~~Security Controls~~
  - 5 Topics | 1 Quiz
- ~~Networking 101~~
  - 6 Topics | 1 Quiz
- ~~Management Principles~~
  - 4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN

- ~~PA1) Introduction to Emails and Phishing~~
  - 7 Topics | 1 Quiz
- ~~PA2) Types of Phishing Emails~~
  - 10 Topics | 2 Quizzes
  - ~~Section Introduction, Phishing Emails~~
  - ~~Reconnaissance~~
  - ~~Spam~~
  - ~~False Positives~~
  - ~~Credential Harvester~~
  - ~~Social Engineering~~
  - ~~Vishing, Smishing~~
  - ~~Whaling~~
  - ~~Malicious Files~~
  - ~~[Video] Types of Phishing Attacks & Examples~~
  - ~~Lab) Categorizing Phishing Emails~~
  - ~~Activity) End of Section Review, Phishing Emails~~
- ~~PA3) Tactics and Techniques Used~~
  - 12 Topics | 2 Quizzes
- ~~PA4) Investigating a Phishing Email~~
  - 8 Topics | 2 Quizzes
- PA5) Analysing URLs, Attachments, and Artifacts
  - 8 Topics | 1 Quiz
- PA6) Taking Defensive Actions
  - 12 Topics | 1 Quiz
- PA7) Report Writing
  - 7 Topics | 1 Quiz
- PA8) Phishing Response Challenge
  - 3 Topics | 1 Quiz

Reconnaissance

Reconnaissance emails, also referred to as recon emails are used for one reason; getting a response from the recipient. This doesn't mean that the user has to actually reply to the sender, as there are ways that malicious actors can tell if an email has been successfully delivered, or even opened. By the end of this lesson, you will be able to correctly identify recon emails, and if they have used any advanced tactics.

We will be looking at two real-world recon emails using different tactics, but first, let's cover what recon emails are, what they're trying to achieve, and what tactics are sometimes used.

RECON EMAILS EXPLAINED

Recon emails are used to check if the destination mailbox is in use, so that it can be targeted in future phishing attacks. Recon emails can vary in sophistication, there are three types we tend to see in the real world:

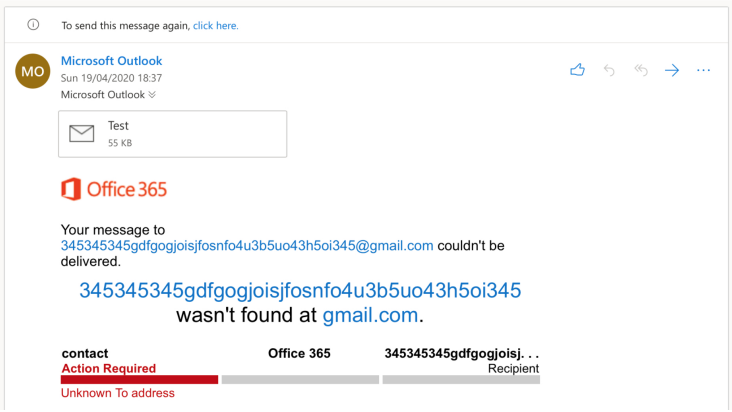
- Recon spam emails that contain nothing except random letters in the body text such as "adjdfkaweasda".
- Emails that use social-engineering techniques to try and get the recipient to respond.
- More complex emails that use tracking pixels to see if the email has been viewed in an email client.

TACTICS USED

Spam Recon Emails

These emails do not use any tactics, and are simply looking to see if an email error code is sent back to the attacker, such as "undeliverable". This allows the attacker to determine whether the mailbox is in use (no error email sent back means the mailbox is in use, and the email was delivered).

Below is an example of an "undeliverable" message that is displayed when sending emails from Outlook. In this case, we have attempted to send a blank message to a Gmail mailbox that isn't in use.



THREAT INTELLIGENCE DOMAIN
TI1) Introduction to Threat Intelligence
7 Topics
TI2) Threat Actors & APTs
6 Topics | 2 Quizzes
TI3) Operational Threat Intelligence
7 Topics | 1 Quiz
TI4) Tactical Threat Intelligence
7 Topics | 2 Quizzes
TI5) Strategic Threat Intelligence
5 Topics | 1 Quiz
TI6) Malware and Global Campaigns
6 Topics | 1 Quiz
DIGITAL FORENSICS DOMAIN
DF1) Introduction to Digital Forensics
5 Topics
DF2) Forensics Fundamentals
10 Topics | 5 Quizzes
DF3) Digital Evidence Collection
8 Topics | 1 Quiz
DF4) Windows Investigations
3 Topics | 3 Quizzes
DF5) Linux Investigations
4 Topics | 2 Quizzes
DF6) Volatility
3 Topics | 1 Quiz
DF7) Autopsy
4 Topics | 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz
SI5) Using Splunk
5 Topics | 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 3 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 5 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz

How to Fix It
The address may be misspelled or may not exist. Try one or more of the following:

Social Engineering Recon Emails

These emails will use social engineering techniques, such as posing as a person that the recipient may know or have regular communications with in order to get a response. Other tactics may include creating a sense of urgency, such as *"I am about to meet with some important stakeholders, have you read the meeting notes yet?"*. This can make people panic and act without thinking properly. Another common tactic includes impersonating someone that is in a higher position within the organization than the target, such as a manager, director, or member of the executive board (this can usually be found fairly easy by searching sites such as LinkedIn). It is thought that being told to do something by someone with more authority is a motivator that sometimes bypasses normal decision making, which can make the phishing email more effective. These emails are also known as impersonation email attacks, or business email compromise attacks (BEC). We will cover these in future lessons.

Tracking Pixel Recon Emails

These emails will typically follow the format of either a spam recon email, or a social engineering email, but are combined with an invisible tracking pixel, which allows the attacker to see if the email has been viewed in an email client. Whilst the other email types can determine if a mailbox is being used, using a tracking pixel can help the attacker understand how **active** the mailbox is. By monitoring the time it takes between sending the email and having it opened, this can help the attacker avoid sending emails to unmonitored mailboxes which would have no impact but increase the risk of detection.

Example of HTML code that can be used to house a tracking pixel, where "src" is the link to a file on the pixel server.

The malicious actor will add the tracking pixel using a code using HTML code in the email body. This code contains an external link to a pixel server. If the email recipient opens the email, the client or webmail provider will load the HTML code, sending a message back to the server.

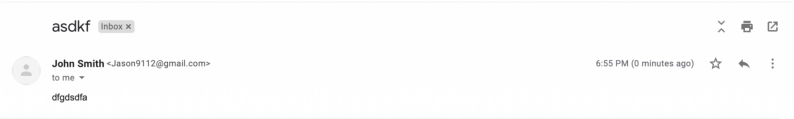
The following data can potentially be acquired and analyzed using a tracking pixel.

- The operating system used (gives information on the use of mobile devices).
- Type of website or email used, for example on mobile or desktop.
- Type of client used, for example, a browser (webmail) or mail program (email client).
- Client's screen resolution.
- Date and time the email was read.
- IP address (gives information on the Internet Service Provider and location).

RECON EMAIL EXAMPLE 1

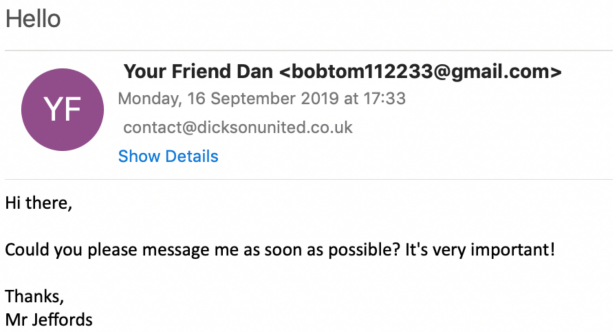
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics | 2 Quizzes
BTL1 EXAM
Exam Preparation
Using RDP and SSH
How to Start Your Exam

In our first example, a Gmail mailbox with the name **John Smith** but the mailbox name **Jason9112@gmail.com** has sent a message with a random subject line **"asdkf"** and body content. This is clearly not a legitimate email, and is using the **spam recon method** to identify if the recipient is a real mailbox or not. The sender is not attempting to retrieve a human response to this email, as there is no question or action to be completed by the recipient. The attacker is simply looking if an "undeliverable" message is generated or not.



RECON EMAIL EXAMPLE 2

In this email, the sender **bobtom112233@gmail.com** is sending a recon email to **contact@dicksonunited.co.uk** with the subject line **"Hello"**. As you can see in the body content, the message is extremely vague and isn't targeted at anyone, using the generic "hi there" opening line. It is also unexpected that a legitimate email from "your friend Dan" would be going to a group mailbox such as "contact@domain".



CONCLUSION

In conclusion, recon emails are often observed daily by large organizations. They will typically always make it through the email gateway as they do not contain any malicious indicators, so they are not inherently malicious. Typical recon emails will only contain body content, more advanced emails could utilize social engineering techniques and tracking pixels to collect more information on their targets. Email addresses that are discovered to be active can be sold to other malicious actors to conduct phishing attacks or can be targeted by the original actor to send further malicious emails.

Privacy & Cookies Policy
Privacy - Terms