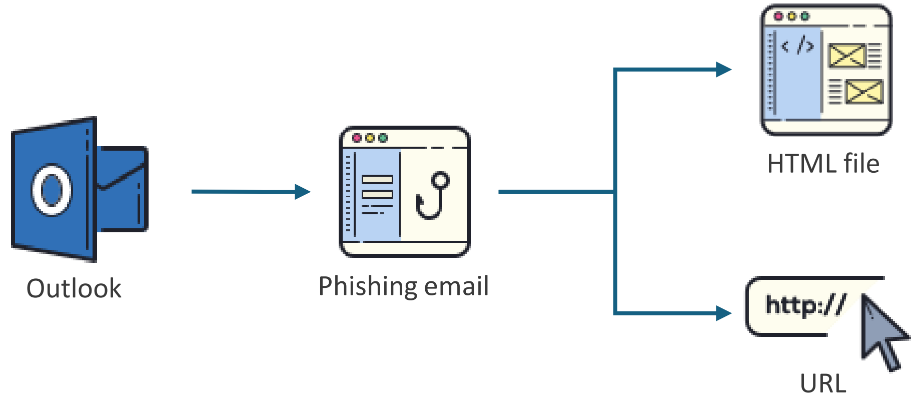
Adversary in the middle (AiTM), MITRE ATT&CK T1557



Case 1 : HTML file redirection

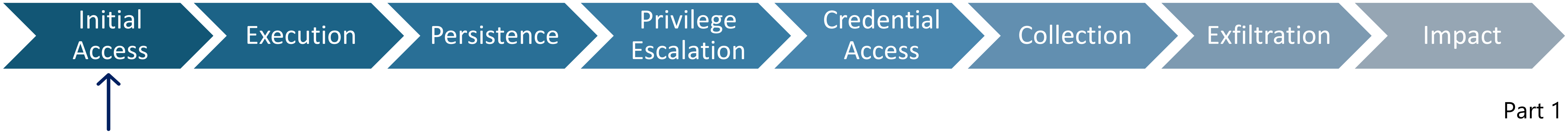
Identify outbound emails with HTML attachments and compile a list of all associated URLs.

Case 2 : Phishing link redirection

Generally, filter suspicious emails and track whether users have clicked on malicious links or not.

```
// case 1 : HTML file redirection
let HTMLfile = (EmailAttachmentInfo
| where FileType =~ "html");
let HTMLurl = (EmailUrlInfo
| where UrlLocation == "Attachment"
| summarize HTMLfile_URL_list =  make_list(Url) by NetworkMessageId);
let Emailurl = (EmailUrlInfo
| where UrlLocation == "Body"
| summarize Email_URL_list = make_list(Url) by NetworkMessageId);
EmailEvents
| where EmailDirection == "Inbound"
| join kind = inner HTMLfile on NetworkMessageId
| join kind = inner HTMLurl on NetworkMessageId
| join kind = leftouter Emailurl on NetworkMessageId
| project Timestamp, ReportId, NetworkMessageId, SenderFromAddress,
RecipientEmailAddress, FileName, FileType, ThreatTypes, ThreatNames,
HTMLfile_URL_list, Email_URL_list
```

```
// case 2 : Phishing link redirection
let UserClickedLink = (UrlClickEvents
| where Workload == "Email"
| where ActionType == "ClickAllowed" or IsClickedThrough != "0");
EmailEvents
| where EmailDirection == "Inbound"
| where ThreatTypes has_any ("Phish", "Malware")
| join kind = inner UserClickedLink on NetworkMessageId
| project Timestamp, ReportId, NetworkMessageId, SenderFromAddress,
RecipientEmailAddress, ActionType, IsClickedThrough, Url
```



Initial Access

Execution

Persistence

Privilege Escalation

Credential Access

Collection

Exfiltration

Impact

Part 1