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

Case 1 : Tracking the clicked URLs with AiTM IoCs

Step 1

Collect insights on IoCs from sources such as the MSTIC blog, NIST, cybersecurity vendors and so on.

Step 2

Import the IoCs into a csv file and upload it to an external storage such as GitHub.

Step 3

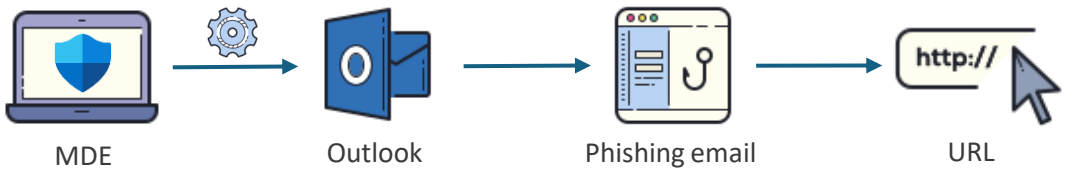
Use the 'externaldata' operator to hunt suspicious activities in M365 Defender or Microsoft Sentinel.

Security blog insights

- ✓ Zscaler : AiTM Phishing Attack Targeting Enterprise Users of Gmail
- ✓ Zscaler : Large-Scale AiTM Attack targeting enterprise users of Microsoft email services
- ✓ Microsoft : From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud

```
// case 1 : Tracking the clicked URLs with AiTM IoCs
let Zscaler_IoC = externaldata(Type:string, Value:string)
[@'https://raw.githubusercontent.com/LearningKijo/KQL/main/KQL-XDR-
Hunting/ThreatHunting/IOCs-Folder/AiTM-Zscaler-IoC.csv'] with (format='csv',
ignorefirstrecord = true);
let Microsoft_IoC = externaldata(Type:string, Value:string)
[@'https://raw.githubusercontent.com/LearningKijo/KQL/main/KQL-XDR-
Hunting/ThreatHunting/IOCs-Folder/AiTM-Microsoft-IoC.csv'] with
(format='csv', ignorefirstrecord = true);
let Zscaler = (Zscaler_IoC | project Value);
let Microsoft = (Microsoft_IoC | project Value);
UrlClickEvents
| where Workload == "Email"
| where ActionType == "ClickAllowed" or IsClickedThrough != "0"
| where Url has_any (Zscaler) or Url has_any (Microsoft)
| extend IoC = case(Url has_any (Zscaler), "Zscaler",
                    Url has_any (Microsoft), "Microsoft", "N/A")
| project Timestamp, NetworkMessageId, ReportId, AccountUpn, Url,
ThreatTypes, DetectionMethods, IoC
```

Case 2 : Tracking the suspicous link from Email to Endpoint




```
// case 2 : Track the suspicous link from Email to Endpoint
let UserClicked = (UrlClickEvents
| where Workload == "Email"
| where ActionType == "ClickAllowed" or IsClickedThrough != "0");
DeviceEvents
| where ActionType == "BrowserLaunchedToOpenUrl"
| where InitiatingProcessFileName =~ "outlook.exe"
| join kind = inner UserClicked on $left.RemoteUrl == $right.Url
| project Timestamp, DeviceId, DeviceName, AccountUpn, Workload, Url
```

Initial Access | Execution | Persistence | Privilege Escalation | Credential Access | Collection | Exfiltration | Impact

Part 2