

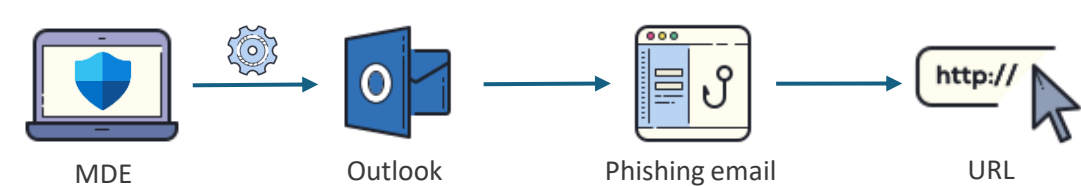
Case 1 : Tracking the clicked URLs with AiTM IoCs



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 2 : Tracking the suspicious link from Email to Endpoint



```
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
```

```
let ClickedURL = EmailEvents
| where EmailDirection == "Inbound"
| where ThreatTypes has_any ("Phish", "Malware")
| join (UrlClickEvents
| where Workload == "Email"
| where ActionType == "ClickAllowed" or IsClickedThrough != "0") on
NetworkMessageId
| project Timestamp, AccountUpn, Url, UrlChain, UrlCount, DeliveryAction;
DeviceEvents
| where ActionType == "BrowserLaunchedToOpenUrl"
| where InitiatingProcessFileName =~ "outlook.exe"
| join kind = inner ClickedURL on $left.RemoteUrl == $right.Url
| project Timestamp, DeviceId, DeviceName, AccountUpn, Url, UrlChain, UrlCount
```

