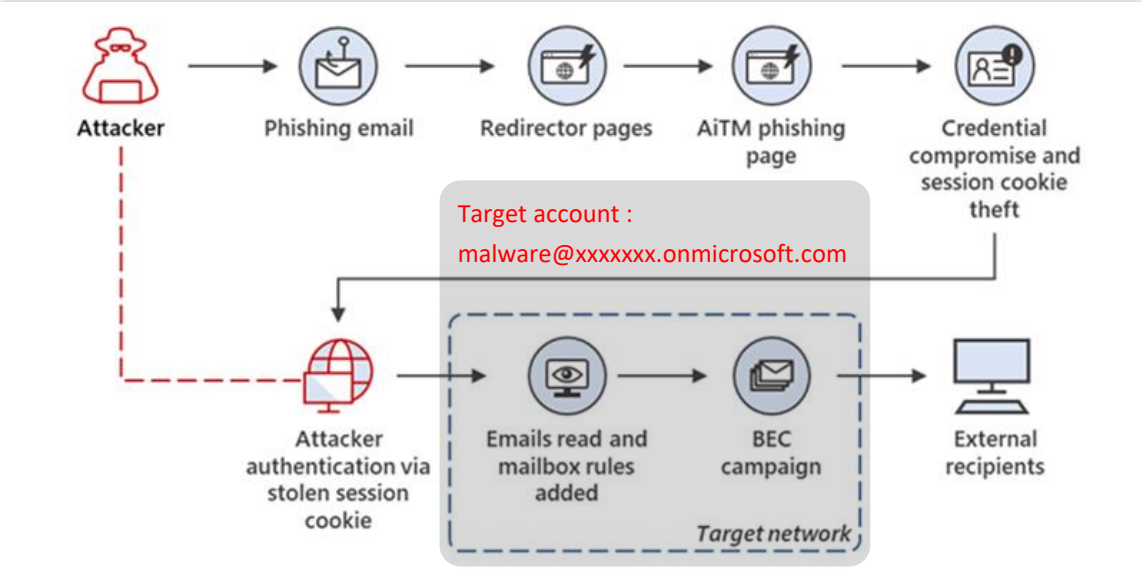
Adversary in the middle (AiTM), BEC MITRE ATT&CK T1557



PowerShell Cmdlets	Note
Add-MailboxPermission	Add permissions to a mailbox
Add-MailboxFolderPermission	Add folder-level permissions for users in mailboxes
New-ManagementRoleAssignment	Assign a management role to a management role group, management role assignment policy, user, or universal security group (USG)
New-InboxRule	Create Inbox rules in mailboxes
Set-InboxRule	Modify existing Inbox rules in mailboxes
New-TransportRule	Create transport rules in your organization
Set-TransportRule	Modify existing transport in your organization
Set-Mailbox	Modify the settings of existing mailboxes

```
// Tracking suspicious Exchange Online (EXO) activities
CloudAppEvents
| where Timestamp > ago(30d)
| extend parsed = parse_json(RawEventData)
| where Application == "Microsoft Exchange Online"
and  ActionType in ("Add-MailboxPermission", "New-ManagementRoleAssignment",
"Add-MailboxFolderPermission", "New-InboxRule", "Set-InboxRule", "Set-
Mailbox", "New-TransportRule", "Set-TransportRule")
and not(parsed.UserId has_any ('NT AUTHORITY¥¥SYSTEM
(Microsoft.Exchange.ServiceHost)', 'NT AUTHORITY¥¥SYSTEM (w3wp)',
'devilfish-applicationaccount'))
| extend parsed = parse_json(RawEventData)
| extend UPN = tostring(parsed.UserId)
| where UPN == "malware@xxxxxxx.onmicrosoft.com"
| extend Parameters = parsed.Parameters
| mv-expand Parameters
| extend Name = tostring(Parameters.Name)
| extend Value = tostring(Parameters.Value)
| extend packed = pack(Name, Value)
| summarize PackedInfo = make_bag(packed), ActionType=any(ActionType) by
ReportId, UPN
| evaluate bag_unpack(PackedInfo)
```

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

Part 4