https://www.cisa.gov/sites/default/files/2023-11/aa23-320a_scattered_spider_0.pdf

##

Emulation request

“In 300 words or less pick 1 or 2 TTPs that Scattered Spider uses and explain how you would structure and perform an adversary emulation as Scattered Spider. “

Assumptions

-The commands are only one example of multiple non-disclosed options to achieve TTP objectives.

-No other references are available for further TTPs.

-Other techniques are completed and threat actor has access:
Reconnaissance (TA0043)
Resource Development (TA0042)
Initial Access (TA0001)
Credential Access (TA0006)

TTP Selection

1- Credential Access (TA0006) - MFA Token Manipulation (T1556.006)
2- Privilege Escalation (TA0004) - SSO Federation Hijacking (T1484.002)

Emulation Preparation

Set up the lab/test env with the applicable orgs for the selections TTPs, SSO and MFA configuration:

```
az ad sp create --display-name "notsus"
az ad user update --id user@mal.com --force-change-password-next-login --mfa-required true
```

TTP Execution

Emulate compromised user accounts by registering a new MFA token to bypass traditional authentication.

```
curl -X POST
https://graph.microsoft.com/v1.0/users/{userId}/authentication/methods
\
-H "Authorization: Bearer {access_token}" \
-H "Content-Type: application/json" \
-d '{"methodType": "FIDO2", "state": "enabled"}'

az ad sp create-for-rbac --name rogue-federated-idp
```

TTP Persistence
Maintain persistence by reusing the federated identity provider, which controls login access even if passwords are changed.

```
az ad sso add --federation-settings --attribute-match-rule
"attribute=value"
```

TTP Privilege Escalation
Exploit the EDR tools' remote-shell capabilities to execute privileged commands.

```
cscli remote-exec --command "powershell.exe Invoke-Command
-ScriptBlock"
```

##
Hunt Assignment
"In addition please provide 2-3 pseudocode sample queries you could use to hunt for this threat actor in a system. Specific IOCs can be found in CISA document and additional links with more IOCs can be found in the references on page 14. "

Pseudocode Hunt Queries
IOC's are for noobs, TTP's yo:

Assumptions
Key value pairs or fields are normalized for queries and 30 days for log retention.

SQL, Lucene, KQL, and SumoLogic:

Execution

```
-- SQL Query
SELECT * FROM audit_logs
WHERE event_type = 'IdentityProviderAdded'
AND account_linking = 'enabled' AND timestamp > NOW() - INTERVAL '24
HOURS';

-- Lucene Query
message.event_type: /.*IdentityProviderAdded.*/
AND message.account_linking: "enabled"
AND message.timestamp: [now-30d TO now]

-- KQL Query
message.event_type: "*IdentityProviderAdded*"
AND message.account_linking: "enabled"
AND message.timestamp >= now-30d

-- SumoLogic Query
_sourceCategory = your/source/category
| parse regex "IdentityProviderAdded"
| where account_linking = "enabled"
| where _messageTime > now() - 30d
```

Persistence

```
-- SQL Query
SELECT * FROM audit_logs
WHERE action = 'register_token'
AND timestamp > NOW() - INTERVAL '30 DAYS'
AND device NOT IN ('approved_devices')
AND user NOT IN ('approved_users'');

-- Lucene Query
message.action: /.*register_token.*/
AND message.timestamp: [now-30d TO now]
AND NOT message.device: ("approved_devices")
AND NOT message.user: ("approved_users");
```

```
-- KQL Query
message.action: "*register_token*"
AND message.timestamp >= now-30d
AND NOT message.device: ("approved_devices")
AND NOT message.user: ("approved_users")

-- SumoLogic Query
_sourceCategory = your/source/category
| parse regex "register_token"
| where _messageTime > now() - 30d
| where !(device in ("approved_devices"))
| where !(user in ("approved_users"))
| count by user, device
```

Privilege Escalation

```
-- SQL Query
SELECT *
FROM authentication_logs
WHERE (
  action IN ('MFA_TOKEN_REGISTERED', 'MFA_METHOD_ADDED',
'AUTHENTICATION_METHOD_CHANGED')
  OR event_type LIKE '%MFA%'
  OR event_description LIKE '%multi-factor%'
)
AND timestamp > NOW() - INTERVAL '30 DAYS'
AND (
  user_id NOT IN (SELECT user_id FROM approved_users)
  OR device_id NOT IN (SELECT device_id FROM approved_devices)
)
ORDER BY timestamp DESC;

-- Lucene Query
(action:("MFA_TOKEN_REGISTERED" OR "MFA_METHOD_ADDED" OR
"AUTHENTICATION_METHOD_CHANGED")
OR event_type:*MFA*
OR event_description:*multi-factor*)
AND timestamp:[now-30d TO now]
```

```
AND (-user_id:("approved_user_list")
OR -device_id:("approved_device_list"))

-- KQL Query
AuthenticationLogs
| where TimeGenerated > ago(30d)
| where Action in ("MFA_TOKEN_REGISTERED", "MFA_METHOD_ADDED",
"AUTHENTICATION_METHOD_CHANGED")
    or EventType contains "MFA"
    or EventDescription contains "multi-factor"
| where UserId !in (approved_users)
    or DeviceId !in (approved_devices)
| order by TimeGenerated desc

-- SumoLogic Query
_sourceCategory = authentication_logs
| parse "action=\"*\"" as action
| parse "event_type=\"*\"" as event_type
| parse "event_description=\"*\"" as event_description
| parse "user_id=\"*\"" as user_id
| parse "device_id=\"*\"" as device_id
| where (
    action in ("MFA_TOKEN_REGISTERED", "MFA_METHOD_ADDED",
"AUTHENTICATION_METHOD_CHANGED")
    or event_type matches "*MFA*"
    or event_description matches "*multi-factor*"
  )
  and _messageTime > now() - 30d
  and (
    !(user_id in (approved_users))
    or !(device_id in (approved_devices))
  )
| sort by _messageTime desc
```