Protocol:

- Service Control Manager Remote Protocol (MS-SCMR)

Interface UUID:

- `367ABB81-9844-35F1-AD32-98F038001003`

Server Binary:

- services.exe

Endpoint:

- ncacn_ip_tcp
- ncacn_np: `\PIPE\ntsvcs` alias `\PIPE\svcctl`

ATT&CK Relation:

T1543.003 - Service Creation

Indicator of Activity (IOA):

- Network:
  - Network connection to services.exe over TCP_IP Port
    - Window Security Event 5156
    - Sysmon Event 3
  - Methods seen over network:
    - `ROpenSCManager(A/W)/ROpenSCManager2`
    - `RCreateService(A/W)/RCreateServiceWOW64(A/W)/RCreateWowService`
- Host:
  - Registry Key created / modified within HKLM\SYSTEM\CurrentControlSet\Services subkey
    - Sysmon Event 12/13
  - Window Securty Event 4624:
    - Logon Type 3
    - Account Name isn't a machine account ($)
    - Source IP / Source Port = Network Source Port/IP

    - Window Security Event 4697
    - Windows System Event 7045

Prevention Opportunities:

- Modify permissions for the Services subkey on who can/cannot interact with it.

RPC Filter Example:

```
rpc
filter
add rule layer=um actiontype=permit
add condition field=if_uuid matchtype=equal data=367ABB81-9844-35F1-AD32
add condition field=remote_user_token matchtype=equal data=D:(A;;KA;;;DA
add filter
add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=367ABB81-9844-35F1-AD32
add filter
quit
```

- RPC Filter only allows Domain Administrators to create services remotely. DAs is probably not the group you want in this filter. See Notes.

Notes:

- By default local administrators and above can create services. The RPC filter only allows Domain Admins to have key access. Could create a "services" group and apply that group to the DACL instead. Change DACL to leverage the group SID - like : D:(A;;KA;;;S-1-5-21-3637186843-3378876361-2759896766-2106).
- Have to make sure whatever group you put in the DACL is a local admin on the target host. Still need to pass the access checked based on the Service Control Manager's Security Descriptor.

Useful Resources:

- https://posts.specterops.io/utilizing-rpc-telemetry-7af9ea08a1d5
- https://attack.mitre.org/techniques/T1543/003/