.. /Manage-bde.wsf ☆ Star

Execute

Script for managing BitLocker

Paths:
C:\Windows\System32\manage-bde.wsf

Resources:
- https://gist.github.com/bohops/735edb7494fe1bd1010d67823842b712
- https://twitter.com/bohops/status/980659399495741441
- https://twitter.com/JohnLaTwC/status/1223292479270600706

Acknowledgements:
- Jimmy (@bohops)
- Daniel Bohannon (@danielbohannon)
- John Lambert (@JohnLaTwC)

Detections:
- Sigma: proc_creation_win_lolbin_manage_bde.yml
- IOC: Manage-bde.wsf should not be invoked by a standard user under normal situations

Execute

1. Set the comspec variable to another executable prior to calling manage-bde.wsf for execution.

```
set comspec=c:\windows\system32\calc.exe & cscript c:\windows\system32\manage-bde.wsf
```

Use case: Proxy execution from script
Privileges required: User
Operating systems: Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1216: System Script Proxy Execution

2. Run the manage-bde.wsf script with a payload named manage-bde.exe in the same directory to run the payload file.

```
copy c:\users\person\evil.exe c:\users\public\manage-bde.exe & cd c:\users\public\ & cscript.exe
c:\windows\system32\manage-bde.wsf
```

Use case: Proxy execution from script
Privileges required: User
Operating systems: Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1216: System Script Proxy Execution