.. /Mftrace.exe

☆ Star 7,060

Execute

Trace log generation tool for Media Foundation Tools.

Paths:
C:\Program Files (x86)\Windows Kits\10\bin\10.0.16299.0\x86\mftrace.exe
C:\Program Files (x86)\Windows Kits\10\bin\10.0.16299.0\x64\mftrace.exe
C:\Program Files (x86)\Windows Kits\10\bin\x86\mftrace.exe
C:\Program Files (x86)\Windows Kits\10\bin\x64\mftrace.exe

Resources:

- https://twitter.com/0rbz_/status/988911181422186496

Acknowledgements:

- fabrizio (@0rbz_)

Detections:

- Sigma: proc_creation_win_lolbin_mftrace.yml

Execute

1. Launch cmd.exe as a subprocess of Mftrace.exe.

```
Mftrace.exe cmd.exe
```

Use case: Local execution of cmd.exe as a subprocess of Mftrace.exe.
Privileges required: User
Operating systems: Windows
ATT&CK® technique: **T1127**: Trusted Developer Utilities Proxy Execution

2. Launch cmd.exe as a subprocess of Mftrace.exe.

```
Mftrace.exe powershell.exe
```

Use case: Local execution of powershell.exe as a subprocess of Mftrace.exe.
Privileges required: User
Operating systems: Windows
ATT&CK® technique: **T1127**: Trusted Developer Utilities Proxy Execution