.. /Sqldumper.exe

Dump

Debugging utility included with Microsoft SQL.

Paths:
C:\Program Files\Microsoft SQL Server\90\Shared\SQLDumper.exe
C:\Program Files (x86)\Microsoft Office\root\vfs\ProgramFilesX86\Microsoft Analysis\AS OLEDB\140\SQLDumper.exe

Resources:
- https://twitter.com/countuponsec/status/910969424215232518
- https://twitter.com/countuponsec/status/910977826853068800
- https://support.microsoft.com/en-us/help/917825/how-to-use-the-sqldumper-exe-utility-to-generate-a-dump-file-in-sql-se

Acknowledgements:
- Luis Rocha (@countuponsec)

Detections:
- Sigma: https://github.com/SigmaHQ/sigma/blob/683b63f8184b93c9564c4310d10c571cbe367e1e/rules/windows/process_creation/proc_creation_win_lolbin_susp_sqldumper_activity.yml
- Elastic: https://github.com/elastic/detection-rules/blob/f6421d8c534f295518a2c945f530e8afc4c8ad1b/rules/windows/credential_access_lsass_memdump_file_created.toml
- Elastic: https://github.com/elastic/detection-rules/blob/5bdf70e72c6cd4547624c521108189af994af449/rules/windows/credential_access_cmdline_dump_tool.toml

Dump

. Dump process by PID and create a dump file (Appears to create a dump file called SQLDmprXXXX.mdmp).

```
sqldumper.exe 464 0 0x0110
```

Use case: Dump process using PID.
Privileges required: Administrator
Operating systems: Windows
ATT&CK® technique: T1003

. 0x01100:40 flag will create a Mimikatz compatible dump file.

```
sqldumper.exe 540 0 0x01100:40
```

Use case: Dump LSASS.exe to Mimikatz compatible dump using PID.
Privileges required: Administrator
Operating systems: Windows
ATT&CK® technique: T1003.001