Command-Line Creation of a RAR file

Detect compression of data into a RAR file using the `rar.exe` utility.

id:	1ec33c93-3d0b-4a28-8014-dbdaae5c60ae
categories:	detect
confidence:	medium
os:	windows
created:	11/30/2018
updated:	11/30/2018

MITRE ATT&CK™ Mapping

tactics:	Exfiltration
techniques:	T1002 Data Compressed

Query

```
process where subtype.create and process_name == "rar.exe" and
  command_line == "* a *"
```

Detonation

Atomic Red Team: T1002

Contributors

- Endgame

Previous Next