Enumeration of Remote Shares

Identifies enumeration of remote shares with the built-in Windows tool `net.exe`.

id:	e61f557c-a9d0-4c25-ab5b-bbc46bb24deb
categories:	detect
confidence:	low
os:	windows
created:	11/30/2018
updated:	11/30/2018

MITRE ATT&CK™ Mapping

tactics:	Discovery
techniques:	T1135 Network Share Discovery

Query

```
process where subtype.create and
  (process_name == "net.exe" or (process_name == "net1.ex
  command_line == "* view*" and command_line == "*\\\\*"
```

Detonation

Atomic Red Team: T1135

Contributors

- Endgame

Previous Next