Enumeration of Mounted Shares

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

id:	4d2e7fc1-af0b-4915-89aa-03d25ba7805e
categories:	detect
confidence:	low
os:	windows
created:	11/30/2018
updated:	11/30/2018

MITRE ATT&CK™ Mapping

tactics:	Discovery
techniques:	T1049 System Network Connections Discovery

Query

```
process where subtype.create and
  (process_name == "net.exe" or (process_name == "net1.exe" and parent_process_name != "net
  (command_line == "* use" or command_line == "* use *") and

  // since this command is looking for discovery only, we want to ignore mounting shares
  command_line != "* \\\\*"
| unique parent_process_path, command_line, user_name
```

Detonation

Atomic Red Team: T1049

Contributors

- Endgame

Previous Next

© Copyright 2019, Endgame Revision 30243396.

Built with Sphinx using a theme provided by Read the Docs.

latest