Modification of Boot Configuration

Identifies use of the bcdedit command to delete boot configuration data. This tactic is sometimes used as by malware or an attacker as a destructive technique.

id:	c4732632-9c1d-4980-9fa8-1d98c93f918e
categories:	detect
confidence:	low
os:	windows
created:	11/30/2018
updated:	05/17/2019

MITRE ATT&CK™ Mapping

tactics:	Impact
techniques:	T1490 Inhibit System Recovery

Query

```
process where subtype.create and
  process_name == "bcdedit.exe" and command_line == "*set *" and
  (command_line == "* bootstatuspolicy *ignoreallfailures*" or command_line == "* recoverye
```

Detonation

Atomic Red Team: T1490

Contributors

- Endgame

Previous Next