Malicious Driver

The attackers load a malicious driver into the operating system.

DETECTION

Endpoint Security Protection Analysis
Memory Analysis
Endpoint Analysis

TOOLS

Pasam
Wingbird
SeaDuke
ROCKBOOT
Alureon

https://en.wikipedia.org/wiki/Alureon

CDV2_0421

Backdoors™ & Breaches

PERSISTENCE

Created by: BLACK HILLS | Information Security