

# Investigating Windows

WMI Backdoor



- \*Executes after a set time and logon
- \*Prevents process execution
- \*Retrieve further payloads from C2

Scheduled Task



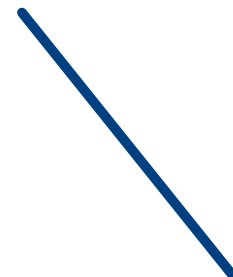
- \*Dump Passwords every 5 Minutes from SAM
- \*Executes Powershell

Listener



Listens on port 1348

Trojan



APT

Exe payload