New Service Creation/Modification

The attackers create and load their malware using a new service or existing service modification.

DETECTION

Endpoint Analysis
Endpoint Security Protection Analysis

TOOLS

Sysinternals PSEXEC services.msc
Impacket:
 - psexec.py
Metasploit:
 - psexec
 - getsystem

https://github.com/SecureAuthCorp/impacket

https://www.metasploit.com

Backdoors™ & Breaches

PIVOT and ESCALATE

Created by: BLACK HILLS | Information Security