

Atomic Test #2 - System Service Discovery - net.exe

sc query state= all

T1003

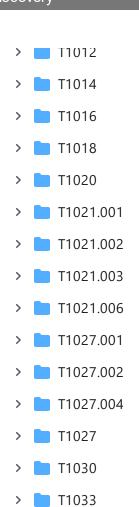
T1006

T1007

> T1010

T1007.md

11007.yaml



T1036.003

T1036.004

T1036.005

T1036.006

T1037.001

T1037.002

T1037.004

T1037.005

T1036

Enumerates started system services using net.exe and writes them to a file. This technique has been used by multiple threat actors.

Upon successful execution, net.exe will run from cmd.exe that queries services. Expected output is to a txt file in c:\Windows\Temp\service-list.txt.s

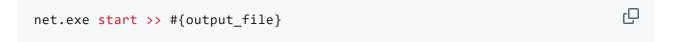
Supported Platforms: Windows

auto_generated_guid: 5f864a3f-8ce9-45c0-812c-bdf7d8aeacc3

Inputs:

Name	Description	Туре	Default Value
output_file	Path of file to hold net.exe output	Path	C:\Windows\Temp\service- list.txt

Attack Commands: Run with command_prompt!



Cleanup Commands:

del /f /q /s #{output_file} >nul 2>&1

Atomic Test #3 - System Service Discovery - systemctl

Enumerates system service using systemctl

Supported Platforms: Linux

auto_generated_guid: f4b26bce-4c2c-46c0-bcc5-fce062d38bef

Attack Commands: Run with bash!

systemctl --type=service