Windows Threat Detection 2

Discovery Commands Powershell

→ Files and Folders: type <file>, Get-Content <file>
dir <folder>, Get-ChildItem <folder>

→ Users and Groups: whoami, net user, net localgroup
query user, Get-LocalUser

→ System and Apps: tasklist /v, systeminfo, Get-Service
wmic product get name, version

→ Network Settings: ipconfig /all, netstat -ano
netsh advfirewall show allprofiles

→ Active Antivirus: Get-WmiObject -Namespace "root\SecurityCenter2" -Query "SELECT * FROM AntivirusProduct"

Discovery Process

Realized that if I run a code in CMD, I can see the logs from Event Viewer (Applications and Services Logs and Microsoft, then Windows, then sysmon Operational) and the logs are going into C:\Windows\System32\net.exe

net user → List all local users
tasklist /v → Show running processes
wmic computersystem get model → Query for Laptop Model

Get-service → list active services
Get-MpPrefence → Check MS Defender settings

C:\Windows\system32\mmc.exe
C:\Windows\system32\compmgmt.msc > Open Computer Management

C:\Windows\system32\control.exe netconnections → List network adapters

C:\Windows\ImmersiveControlPanel\SystemSettings.exe [...]
↳ Access settings panel

C:\Windows\System32\notepad.exe C:\...\secrets.txt → Read a text file

C:\Windows\System32\taskmgr.exe → Run Task Manager

Collection Targets

The datas are collected in user's Appdata's Roaming and local

→ and SSH Credentials and Databases located in Microsoft SQL Server in Program Files

Windows Threat Detection 3

Persistence Method
→ add malware to Startup Folder
→ add malware to "Run" keys

To detect: we can detect it by monitoring file creation events (Sysmon Event ID 11) inside the Startup Folder

To detect Run keys, ~~they never~~ basically as same as the Startup

How threat actors can remain active on the system:

→ Add the host to a botnet and use it for further attacks
→ Spy on the victim as a part of a state-sponsored campaign
→ Use the entry point to the network