









Sign in

 3CORESec / MAL-CL Public

 Notifications

 Fork 43

 Star 308

<> Code

⦿ Issues

🔗 Pull requests

▶ Actions



🛡 Security


📈 Insights

MAL-CL / Descriptors / Sysinternals / PsLogList 





Name	Last commit message	Last commit date
 ..		
 README.md		

README.md 

PsLogList

Table of Contents

- [PsLogList](#)
 - [Table of Contents](#)
 - [Acknowledgement\(s\)](#)
 - [Description](#)
 - [Versions History](#)
 - [File Metadata](#)
 - [Common CommandLine](#)
 - [Threat Actor Ops \(TAOps\)](#)
 - [Common Process Trees](#)

- [Default Install Location](#)
- [DFIR Artifacts](#)
- [Examples In The Wild](#)
- [Documentation](#)
- [Blogs / Reports References](#)
- [ATT&CK Techniques](#)
- [Telemetry](#)
- [Detection Validation](#)
- [Detection Rules](#)
- [LOLBAS / GTFOBins References](#)

Acknowledgement(s)

- 3CORESec - [@3CORESec](#)
- Nasreddine Bencherchali - [@nas_bench](#)

Description

PsLogList lets you dump the contents of an Event Log on the local or a remote computer - [MSDN](#)

Versions History

- TBD

File Metadata

- TBD

Common CommandLine

- Note that most of the time the process is renamed but the flags are the same
- Note that the "/" can be used instead of the "-" when calling the flags.

```
psloglist.exe -accepteula -x security -s -a <current_date>
```



```
psloglist.exe security -d [NumOfDays] /accepteula
```

Threat Actor Ops (TAOps)

- TBD

Common Process Trees

- TBD

Default Install Location

- PsLogList is a downloadable portable utility so no installation is required to execute it.
- The Sysinternals suite is available in the Microsoft Store. If downloaded from there then the `PsLogList` utility will be installed in the following location:

```
C:\Program Files\WindowsApps\Microsoft.SysinternalsSuite_[Version]\Tools\PLogList
```



DFIR Artifacts

- TBD

Examples In The Wild

- [Github Gist - winlogfinder](#)

Documentation

- [Microsoft Docs - PsLogList](#)
- [SS64.com - Windows CMD - PsLogList](#)

Blogs / Reports References

- [nccgroup - Abusing cloud services to fly under the radar](#)
- [Cybereason - DeadRinger: Exposing Chinese Threat Actors Targeting Major Telcos](#)

ATT&CK Techniques

- [T1087 - Account Discovery](#)

Telemetry

- [Security Event ID 4688 - A new process has been created](#)
- [Sysmon Event ID 1 - Process creation](#)
- [PsSetCreateProcessNotifyRoutine/Ex](#)
- [ETW - Microsoft-Windows-Kernel-Process - Event ID 1 - ProcessStart](#)

Detection Validation

- TBD

Detection Rules

- TBD

LOLBAS / GTFOBins References

- None