README.md

AuditPol (AuditPol.exe)

Table of Contents

Acknowledgement(s)

- 3CORESec - @3CORESec
- Nasreddine Bencherchali - @nas_bench

Description

> **AuditPol is a command-line tool that enables the user to modify the audit policy of the local computer or of any remote computer.**

Versions History

Version	SHA1	VT
Unknown	095915e8067493dabe5031331e78b56374024229	LINK

File Metadata

- TBD

Common CommandLine

```
rem Disable Process, System and Logon tracking
AuditPol /process:none /system:none /logon:none

AuditPol \\[IP] /disable
```

Threat Actor Ops (TAOps)

- TBD

Common Process Trees

- TBD

Default Install Location

- AuditPol is a downloadable portable utility so no installation is required to execute it.
- AuditPol is part of the Microsoft Windows 2000 Resource Kit Tools.

DFIR Artifacts

- TBD

Examples In The Wild

- TBD

Documentation

```
AuditPol 1.1b @1996-97 Written by Christophe ROBERT.


AuditPol [\\computer] [/enable | /disable] [/help | /?] [/Category:Optio

   /Enable   = Enable audit (default).

   /Disable  = Disable audit.

   Category  = System    : System events
               Logon     : Logon/Logoff events
               Object    : Object access
               Privilege : Use of privileges
               Process   : Process tracking
               Policy    : Security policy changes
               Sam       : SAM changes

   Option    = Success   : Audit success events
               Failure   : Audit failure events
               All       : Audit success and failure events
               None      : Do not audit these events
```

```
Samples are as follows:

   AUDITPOL \\MyComputer
   AUDITPOL \\MyComputer /enable /system:all /object:failure
   AUDITPOL \\MyComputer /disable
   AUDITPOL /logon:failure /system:all /sam:success /privilege:none

AUDITPOL /HELP | MORE displays Help one screen at a time.
```

Blogs / Reports References

- TBD

ATT&CK Techniques

- T1562.002 - Impair Defenses: Disable Windows Event Logging

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
- Security Event ID 4719 - System Audit Policy Was Changed

Detection Validation

- TBD

Detection Rules

- TBD

LOLBAS / GTFOBins References

- None