Sign in

redcanaryco / atomic-red-team Public

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 4 Actions Wiki Security Insights

atomic-red-team / atomics / T1484.001 / T1484.001.md

101 lines (57 loc) · 6.32 KB

Preview Code Blame Raw

T1484.001 - Group Policy Modification

Description from ATT&CK

> Adversaries may modify Group Policy Objects (GPOs) to subvert the intended discretionary access controls for a domain, usually with the intention of escalating privileges on the domain. Group policy allows for centralized management of user and computer settings in Active Directory (AD). GPOs are containers for group policy settings made up of files stored within a predicable network path `\\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\`.(Citation: TechNet Group Policy Basics)(Citation: ADSecurity GPO Persistence 2016)
> Like other objects in AD, GPOs have access controls associated with them. By default all user accounts in the domain have permission to read GPOs. It is possible to delegate GPO access control permissions, e.g. write access, to specific users or groups in the domain.
>
> Malicious GPO modifications can be used to implement many other malicious behaviors such as Scheduled Task/Job, Disable or Modify Tools, Ingress Tool Transfer, Create Account, Service Execution, and more.(Citation: ADSecurity GPO Persistence 2016)(Citation: Wald0 Guide to GPOs)(Citation: Harmj0y Abusing GPO Permissions)(Citation: Mandiant M Trends 2016)(Citation: Microsoft Hacking Team Breach) Since GPOs can control so many user and machine settings in the

> AD environment, there are a great number of potential attacks that can stem from this GPO abuse. (Citation: Wald0 Guide to GPOs)
>
> For example, publicly available scripts such as `New-GPOImmediateTask` can be leveraged to automate the creation of a malicious Scheduled Task/Job by modifying GPO settings, in this case modifying `<GPO_PATH>\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml` .(Citation: Wald0 Guide to GPOs)(Citation: Harmj0y Abusing GPO Permissions) In some cases an adversary might modify specific user rights like SeEnableDelegationPrivilege, set in `<GPO_PATH>\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf` , to achieve a subtle AD backdoor with complete control of the domain because the user account under the adversary's control would then be able to modify GPOs.(Citation: Harmj0y SeEnableDelegationPrivilege Right)

Atomic Tests

- Atomic Test #1 - LockBit Black - Modify Group policy settings -cmd
- Atomic Test #2 - LockBit Black - Modify Group policy settings -Powershell

Atomic Test #1 - LockBit Black - Modify Group policy settings - cmd

An adversary can modify the group policy settings.

Supported Platforms: Windows

auto_generated_guid: 9ab80952-74ee-43da-a98c-1e740a985f28

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

```
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" /v GroupPolicyRefreshTim
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" /v GroupPolicyRefreshTim
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" /v GroupPolicyRefreshTim
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" /v GroupPolicyRefreshTim
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" /v EnableSmartScreen /t
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" /v ShellSmartScreenLevel
```

Cleanup Commands:

```
reg delete "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" /v GroupPolicyRefresh
reg delete "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" /v GroupPolicyRefresh
reg delete "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" /v GroupPolicyRefresh
reg delete "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" /v GroupPolicyRefresh
reg delete "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" /v EnableSmartScreen
reg delete "HKLM\SOFTWARE\Policies\Microsoft\Windows\System" /v ShellSmartScreenLe
```

Atomic Test #2 - LockBit Black - Modify Group policy settings - Powershell

An adversary modifies group policy settings

Supported Platforms: Windows

auto_generated_guid: b51eae65-5441-4789-b8e8-64783c26c1d1

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

```
New-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" -Name GroupPol
New-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" -Name GroupPol
New-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" -Name GroupPol
New-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" -Name GroupPol
New-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" -Name EnableSm
New-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" -Name ShellSma
```

Cleanup Commands:

```
Remove-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" -Name Group
Remove-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" -Name Group
Remove-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" -Name Group
Remove-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" -Name Group
Remove-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" -Name Enabl
Remove-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows\System" -Name Shell
```