Group Policy Abuse for Privilege Addition

edit

Detects the first occurrence of a modification to Group Policy Object Attributes to add privileges to user accounts or use them to add users as local admins.

Rule type: eql

Rule indices:

- winlogbeat-*
- logs-system.*
- logs-windows.*

Severity: high

Risk score: 73

Runs every: 5m

Searches indices from: None (Date Math format, see also `Additional look-back time`)

Maximum alerts per execution: 100

References:

- https://github.com/atc-project/atc-data/blob/master/docs/Logging_Policies/LP_0025_windows_audit_directory_service_ch
- https://labs.f-secure.com/tools/sharpgpoabuse

Tags:

- Domain: Endpoint
- OS: Windows
- Use Case: Threat Detection
- Tactic: Privilege Escalation
- Data Source: Active Directory
- Resources: Investigation Guide

- Use Case: Active Directory Monitoring
- Data Source: System

Version: 211

Rule authors:

- Elastic

Rule license: Elastic License v2

Investigation guide

edit

Triage and analysis

Investigating Group Policy Abuse for Privilege Addition

Group Policy Objects (GPOs) can be used to add rights and/or modify Group Membership on GPOs by changing the contents of an INF file named GptTmpl.inf, which is responsible for storing every setting under the Security Settings container in the GPO. This file is unique for each GPO, and only exists if the GPO contains security settings. Example Path: "\\DC.com\SysVol\DC.com\Policies{PolicyGUID}\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf"

Possible investigation steps

- This attack abuses a legitimate mechanism of Active Directory, so it is important to determine whether the activity is legitimate and the administrator is authorized to perform this operation.
- Retrieve the contents of the `GptTmpl.inf` file, and under the `Privilege Rights` section, look for potentially dangerous high privileges, for example: SeTakeOwnershipPrivilege, SeEnableDelegationPrivilege, etc.
- Inspect the user security identifiers (SIDs) associated with these privileges, and if they should have these privileges.

False positive analysis

- Inspect whether the user that has done the modifications should be allowed to. The user name can be found in the `winlog.event_data.SubjectUserName` field.

Related rules

- Scheduled Task Execution at Scale via GPO - 15a8ba77-1c13-4274-88fe-6bd14133861e
- Startup/Logon Script added to Group Policy Object - 16fac1a1-21ee-4ca6-b720-458e3855d046

Response and remediation

- Initiate the incident response process based on the outcome of the triage.
- The investigation and containment must be performed in every computer controlled by the GPO, where necessary.
- Remove the script from the GPO.
- Check if other GPOs have suspicious scripts attached.

Setup

edit

Setup

The *Audit Directory Service Changes* audit policy must be configured (Success Failure). Steps to implement the logging policy with Advanced Audit Configuration:

```
Computer Configuration >
Policies >
Windows Settings >
Security Settings >
Advanced Audit Policies Configuration >
Audit Policies >
DS Access >
Audit Directory Service Changes (Success,Failure)
```

Rule query

edit

```
any where host.os.type == "windows" and event.code: "5136" and
  winlog.event_data.AttributeLDAPDisplayName: "gPCMachineExtensionNam
  winlog.event_data.AttributeValue: "*827D319E-6EAC-11D2-A4EA-00C04F7
  winlog.event_data.AttributeValue: "*803E14A0-B4FB-11D0-A0D0-00A0C90
```

Framework: MITRE ATT&CK™

- Tactic:
  - Name: Privilege Escalation
  - ID: TA0004
  - Reference URL: https://attack.mitre.org/tactics/TA0004/
- Technique:
  - Name: Domain or Tenant Policy Modification
  - ID: T1484
  - Reference URL: https://attack.mitre.org/techniques/T1484/
- Sub-technique:
  - Name: Group Policy Modification

- ID: T1484.001
- Reference URL: https://attack.mitre.org/techniques/T1484/001/

« Google Workspace User Organizational Unit Changed

Group Policy Discovery via Microsoft GPResult Utility »