Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the <u>cookie policy</u>.

Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

Learn more and customize

Reject Accept

Rule query

ElasticON events are

Learn about the Elastic

Search Al Platform

from the

events.

Was this

helpful?

experts at our live

Learn more

16 91

back!

Group Policy Abuse for Privilege Addition

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 lookback time)

Maximum alerts per execution: 100

References:

- https://github.com/atc-project/atcdata/blob/master/docs/Logging_Policies/LP_0025_windows_audit_directory_service_changes.md
- 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

ec

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the cookie policy.

Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

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



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)
```

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the <u>cookie policy</u>.

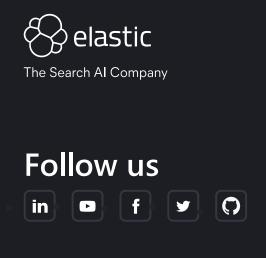
Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

Framework: MITRE ATT&CKTM

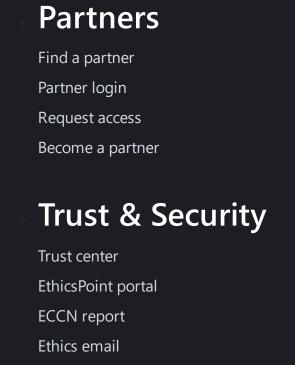
- Tactic:
 - Name: Privilege Escalation
 - ID: TA0004
 - Reference URL: https://attack.mitre.org/tactics/TA0004/
- Technique:
 - Name: Domain or Tenant Policy Modification
 - ID: T1484
 - Reference URL: https://attack.mitre.org/techniques/T1484/
- Sub-technique:
 - Name: Group Policy Modification
 -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



About us About Elastic Leadership DE&I Blog Newsroom Join us Careers



Investor relations

Career portal

Group Policy Abuse for Privilege Addition | Elastic Security Solution [8.15] | Elastic - 02/11/2024 11:25 https://www.elastic.co/guide/en/security/current/group-policy-abuse-for-privilege-addition.html#_setup_275

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the cookie policy.

Use the "Accept" button to consent. Use the "Reject" button to continue without accepting.

Previous winners

ElasticON Tour

Become a sponsor

All events

<u>Trademarks</u> <u>Terms of Use</u> <u>Privacy</u> <u>Sitemap</u> © 2024. Elasticsearch B.V. All Rights Reserved Elastic, Elasticsearch and other related marks are trademarks, logos or registered trademarks of Elasticsearch B.V. in the United States and other countries.

Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.