Elastic Security overview

What’s new in 7.17

Upgrade from 7.17 to an 8.x version

Get started with Elastic Security

Elastic Security UI

Explore

Anomaly Detection with Machine Learning

Detections and alerts

Investigate

Manage

Elastic Security APIs

Elastic Security fields and object schemas

Post-upgrade steps (optional)

Troubleshooting

Technical preview

Release notes

Scheduled Task Execution at Scale via GPO

edit

Detects the modification of Group Policy Object attributes to execute a scheduled task in the objects controlled by the GPO.

Rule type: query

Rule indices:

- winlogbeat-*
- logs-system.*

Severity: medium

Risk score: 47

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_changes.md
- https://github.com/atc-project/atc-data/blob/f2bbb51ecf68e2c9f488e3c70dcdd3df51d2a46b/docs/Logging_Policies/LP_0029_windows_audit_detailed_file_s
- https://labs.f-secure.com/tools/sharpgpoabuse
- https://twitter.com/menasec1/status/1106899890377052160
- https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_gpo_scheduledtasks.yml

Tags:

- Elastic
- Host
- Windows
- Threat Detection
- Privilege Escalation
- Active Directory

Version: 2

Rule authors:

- Elastic

Rule license: Elastic License v2

Investigation guide

edit

```
#### Possible investigation steps:
- This attack abuses a legitimate mechanism of the Active Directory, so it is i
is legitimate and the administrator is authorized to perform this operation.
- Retrieve the contents of the `ScheduledTasks.xml` file, ánd check the `<Comma
potentially malicious commands and binaries.
- If the action is suspicious for the user, check for any other activities done

### False Positive Analysis
- Verify if the execution is allowed and done under change management, and if t

### Related Rules
- Group Policy Abuse for Privilege Addition
- Startup/Logon Script added to Group Policy Object

### Response and Remediation
- Immediate response should be taken to validate activity, investigate, and pot
post-compromise behavior.

## Config

The 'Audit Detailed File Share' audit policy is required be configured (Success
Steps to implement the logging policy with with Advanced Audit Configuration:
```
Computer Configuration >
Policies >
Windows Settings >
Security Settings >
Advanced Audit Policies Configuration >
Audit Policies >
Object Access >
Audit Detailed File Share (Success,Failure)
```

The 'Audit Directory Service Changes' audit policy is required be configured (S
Steps to implement the logging policy with 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

```
(event.code: "5136" and winlog.event_data.AttributeLDAPDisplayName:("gPCMachine
   winlog.event_data.AttributeValue:(*CAB54552-DEEA-4691-817E-ED4A4D1AFC72* and
or
(event.code: "5145" and winlog.event_data.ShareName: "\\\\*\\SYSVOL" and winlog
  (message: WriteData or winlog.event_data.AccessList: *%%4417*))
```

Framework: MITRE ATT&CK™

- Tactic:
  - Name: Privilege Escalation
  - ID: TA0004
  - Reference URL: https://attack.mitre.org/tactics/TA0004/

- ID: T1053.005
- Reference URL: https://attack.mitre.org/techniques/T1053/005/

- Technique:
  - Name: Domain 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/

« Group Policy Abuse for Privilege Addition

Potential Privilege Escalation via InstallerFileTakeOver »