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.

Learn more and customize

>

>

>

>

Reject

Accept

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

Machine Learning

Explore

Anomaly Detection with

Detections and alerts

Investigate

Elastic Security fields and

Elastic Security APIs

Manage

object schemas

Post-upgrade steps (optional)

Troubleshooting

Technical preview

Release notes

Elastic Docs > Elastic Security Solution [7.17] > Downloadable rule update v0.16.1

Scheduled Task Execution at Scale via GPO

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

ElasticON events

Elastic Search Al Platform from the experts at our live events.

Learn more

Was this helpful?



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.

```
- This attack abuses a legitimate mechanism of the Active Directory, so it is
is legitimate and the administrator is authorized to perform this operation.
- Retrieve the contents of the `ScheduledTasks.xml` file, and check the `<Comma
potentially malicious commands and binaries.
- If the action is suspicious for the user, check for any other activities done
- Verify if the execution is allowed and done under change management, and if
- Group Policy Abuse for Privilege Addition
- Startup/Logon Script added to Group Policy Object
- Immediate response should be taken to validate activity, investigate, and po
post-compromise behavior.
The 'Audit Detailed File Share' audit policy is required be configured (Succes:
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 (
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



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

Framework: MITRE ATT&CKTM

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

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

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

- 10.11000.000
- 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 »



The Search Al Company

Follow us











About us

About Elastic Leadership Partner login DE&I Blog

Join us

Newsroom

Careers Career portal

Partners

Find a partner Request access Become a partner

Trust & Security

Trust center EthicsPoint portal **ECCN** report Ethics email

Investor relations

Investor resources Governance **Financials** Stock

EXCELLENCE AWARDS

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.