

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

Startup/Logon Script added to Group Policy Object



Rule query

Detects the modification of Group Policy Objects (GPO) to add a startup/logon script to users or computer objects.

Rule type: eql

Rule indices:

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

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>

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



Triage and analysis

Investigating Startup/Logon Script added to Group Policy Object

Group Policy Objects (GPOs) can be used by attackers to instruct arbitrarily large groups of clients to execute specified commands at startup, logon, shutdown, and logoff. This is done by creating or modifying the `scripts.ini` or `psscripts.ini` files. The scripts are stored in the following paths: - `<GPOPath>\Machine\Scripts\` - `<GPOPath>\User\Scripts\`

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

ElasticON events are back!

Learn about the Elastic Search AI 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.

Verify if the execution is legitimately assigned and executed under a change management process.

Related rules

- Group Policy Abuse for Privilege Addition - b9554892-5e0e-424b-83a0-5aef95aa43bf
- Scheduled Task Execution at Scale via GPO - 15a8ba77-1c13-4274-88fe-6bd14133861e

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.
- Determine the initial vector abused by the attacker and take action to prevent reinfection through the same vector.
- Using the incident response data, update logging and audit policies to improve the mean time to detect (MTTD) and the mean time to respond (MTTR).

Setup



Setup

The *Audit Detailed File Share* 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 >
Object Access >
Audit Detailed File Share (Success,Failure)

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



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.

```
winlog.event_data.AttributeValue : (
  "*40B66650-4972-11D1-A7CA-0000F87571E3*",
  "*40B6664F-4972-11D1-A7CA-0000F87571E3*"
)
) or
(
  winlog.event_data.ShareName : "\\*\\SYSVOL" and
  winlog.event_data.RelativeTargetName : ("*\\scripts.ini", "*\\psscripts.ini") and
  winlog.event_data.AccessList:"*%4417*"
)
)
```

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/>
- **Technique:**
 - Name: Boot or Logon Autostart Execution
 - ID: T1547
 - Reference URL: <https://attack.mitre.org/techniques/T1547/>

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.

Follow us



[Blog](#)

[Newsroom](#)

[Become a partner](#)

[Stock](#)

Join us

[Careers](#)

[Career portal](#)

Trust & Security

[Trust center](#)

[EthicsPoint portal](#)

[ECCN report](#)

[Ethics email](#)

EXCELLENCE AWARDS

[Previous winners](#)

[ElasticON Tour](#)

[Become a sponsor](#)

[All events](#)

[Trademarks](#) [Terms of Use](#) [Privacy](#) [Sitemap](#)

© 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.