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

WebServer Access Logs Deleted

edit

Identifies the deletion of WebServer access logs. This may indicate an attempt to evade detection or destroy forensic evidence on a system.

Rule type: eql

Rule indices:

- auditbeat-*
- winlogbeat-*
- logs-endpoint.events.*
- logs-windows.sysmon_operational-*

Severity: medium

Risk score: 47

Runs every: 5m

Searches indices from: now-9m (Date Math format, see also `Additional look-back time`)

Maximum alerts per execution: 100

References: None

Tags:

- Domain: Endpoint
- OS: Linux
- OS: Windows
- OS: macOS
- Use Case: Threat Detection
- Tactic: Defense Evasion
- Data Source: Elastic Defend
- Data Source: Sysmon

Version: 207

Rule authors:

- Elastic

Rule license: Elastic License v2

Setup

edit

Setup

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.

Rule query

edit

```
file where event.type == "deletion" and
  file.path : ("C:\\inetpub\\logs\\LogFiles\\*.log",
               "/var/log/apache*/access.log",
               "/etc/httpd/logs/access_log",
               "/var/log/httpd/access_log",
               "/var/www/*/logs/access.log")
```

Framework: MITRE ATT&CK^{TM}

- Tactic:
  - Name: Defense Evasion
  - ID: TA0005
  - Reference URL: https://attack.mitre.org/tactics/TA0005/
- Technique:
  - Name: Indicator Removal
  - ID: T1070
  - Reference URL: https://attack.mitre.org/techniques/T1070/

« WebProxy Settings Modification Werfault ReflectDebugger Persistence »

elastic
The Search AI Company

Follow us

About us
About Elastic
Leadership
DE&I
Blog
Newsroom

Join us
Careers
Career portal

Partners
Find a partner
Partner login
Request access
Become a partner

Trust & Security
Trust center
EthicsPoint portal
ECCN report
Ethics email

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.

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.