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

ElasticON events are

Learn about

the Elastic Search Al

Platform

from the experts at

our live

events.

Was this helpful?

Learn more

back!

WebServer Access Logs Deleted



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



Setup

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.

ITAIC YACI Y

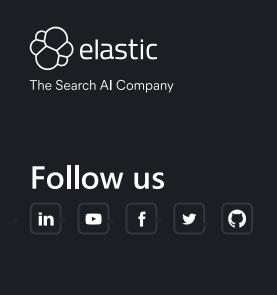
file where event.type == "deletion" and

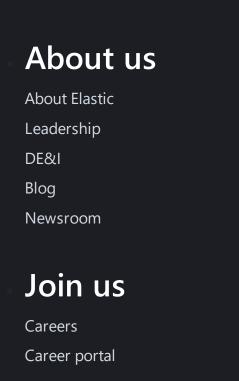
Framework: MITRE ATT&CKTM

- 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 »





Partners Find a partner Partner login Request access Become a partner Trust & Security Trust center EthicsPoint portal

ECCN report

Ethics email

WebServer Access Logs Deleted | Elastic Security Solution [8.15] | Elastic - 02/11/2024 12:55 https://www.elastic.co/guide/en/security/current/webserver-access-logs-deleted.html

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.

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.