



Start free trial

Contact Sales

[Platform](#) [Solutions](#) [Customers](#) [Resources](#) [Pricing](#) [Docs](#)

[Elastic Docs](#) › [Elastic Security Solution \[8.15\]](#) › [Detections and alerts](#)  
› [Prebuilt rule reference](#)

# Remote File Copy to a Hidden Share



Identifies a remote file copy attempt to a hidden network share. This may indicate lateral movement or data staging activity.

**Rule type:** eql

**Rule indices:**

- logs-endpoint.events.process-\*
- winlogbeat-\*
- logs-windows.forwarded\*
- logs-windows.sysmon\_operational-\*
- endgame-\*
- logs-system.security\*
- logs-m365\_defender.event-\*
- logs-sentinel\_one\_cloud\_funnel.\*

**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:**

- <https://www.elastic.co/security-labs/hunting-for-lateral-movement-using-event-query-language>

**Tags:**

- Domain: Endpoint
- OS: Windows
- Use Case: Threat Detection
- Tactic: Lateral Movement
- Data Source: Elastic Endgame
- Data Source: Elastic Defend
- Data Source: System
- Data Source: Microsoft Defender for Endpoint
- Data Source: Sysmon
- Data Source: SentinelOne

**Version:** 311

**Rule authors:**

- Elastic

**Rule license:** Elastic License v2

## Rule query



```
process where host.os.type == "windows" and event.type  
(  
  process.name : ("cmd.exe", "powershell.exe", "xc  
  process.args : ("copy*", "move*", "cp", "mv") or  
  process.name : "robocopy.exe"  
) and process.args : "*\\*\\*\\*\\*$*"
```

### Framework: MITRE ATT&CK™

- Tactic:
  - Name: Lateral Movement
  - ID: TA0008
  - Reference URL:  
<https://attack.mitre.org/tactics/TA0008/>
- Technique:
  - Name: Remote Services
  - ID: T1021
  - Reference URL:  
<https://attack.mitre.org/techniques/T1021/>
- Sub-technique:
  - Name: SMB/Windows Admin Shares
  - ID: T1021.002
  - Reference URL:  
<https://attack.mitre.org/techniques/T1021/002/>

---

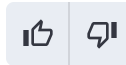
« Remote Execution via File Shares      Remote File Copy via TeamViewer »

**ElasticON events are back!**

Learn about the Elastic Search AI Platform from the experts at our live events.

[Learn more](#)

Was this helpful?



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

## Investor relations

Investor resources  
Governance  
Financials  
Stock

## 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.