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

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

Framework: MITRE ATT&CK^{TM}

- 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 »

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

Join us

Careers

Career portal

Investor relations

Investor resources

Governance

Financials

Stock

EXCELLENCE AWARDS

Previous winners

ElasticON Tour

Become a sponsor

All events

Become a partner

Trust & Security

Trust center

EthicsPoint portal

ECCN report

Ethics email

Trademarks Terms of Use Privacy Sitemap