

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

Elastic Security overview

What's new in 8.15

Upgrade Elastic Security to 8.15.3 >

Post-upgrade steps (optional) >

Get started with Elastic Security >

AI for security >

Detections and alerts ▾

Detections prerequisites and requirements

About detection rules

Create a detection rule >

Install and manage Elastic prebuilt rules

Manage detection rules

Monitor and troubleshoot rule executions

Rule exceptions >

About building block rules

Potential Non-Standard Port SSH connection



Identifies potentially malicious processes communicating via a port paring typically not associated with SSH. For example, SSH over port 2200 or port 2222 as opposed to the traditional port 22. Adversaries may make changes to the standard port a protocol uses to bypass filtering or muddle analysis/parsing of network data.

Rule type: eql

Rule indices:

- logs-endpoint.events.*

Severity: low

Risk score: 21

Runs every: 5m

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

Maximum alerts per execution: 100

References:

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.

- Tactic: Command and Control
- OS: macOS
- Data Source: Elastic Defend

Version: 6

Rule authors:

- Elastic

Rule license: Elastic License v2

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.

```
destination.port != 22 and network.transport == "  
  destination.ip == null or destination.ip == "0.  
    destination.ip, "10.0.0.0/8", "127.0.0.0/8",  
    "192.0.0.8/32", "192.0.0.9/32", "192.0.0.10/3  
    "192.31.196.0/24", "192.52.193.0/24", "192.16  
    "192.175.48.0/24", "198.18.0.0/15", "198.51.10  
    "FF00::/8"  
  )  
)  
]
```

Framework: MITRE ATT&CK™

- Tactic:
 - Name: Command and Control
 - ID: TA0011
 - Reference URL:
<https://attack.mitre.org/tactics/TA0011/>
- Technique:
 - Name: Non-Standard Port
 - ID: T1571
 - Reference URL:
<https://attack.mitre.org/techniques/T1571/>

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](#)

Was this helpful?



The Search AI Company

Follow us



About us

[About Elastic](#)

[Leadership](#)

[DE&I](#)

[Blog](#)

[Newsroom](#)

Join us

Partners

[Find a partner](#)

[Partner login](#)

[Request access](#)

[Become a partner](#)

Trust & Security

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.

Investor relations

- Investor resources
- Governance
- Financials
- Stock

EXCELLENCE AWARDS

- Previous winners
- ElasticON Tour
- Become a sponsor
- All events

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.