

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

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:

- <https://attack.mitre.org/techniques/T1571/>

Tags:

- Domain: Endpoint
- OS: Linux
- Use Case: Threat Detection
- Tactic: Command and Control
- OS: macOS
- Data Source: Elastic Defend

Version: 6

Rule authors:

- Elastic

Rule license: Elastic License v2

Rule query



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.

```
destination.ip == null or destination.ip == "0.0.0.0" or c
    destination.ip, "10.0.0.0/8", "127.0.0.0/8", "169.254.0.
    "192.0.0.8/32", "192.0.0.9/32", "192.0.0.10/32", "192.0.
    "192.31.196.0/24", "192.52.193.0/24", "192.168.0.0/16",
    "192.175.48.0/24", "198.18.0.0/15", "198.51.100.0/24", "2
    "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/>



The Search AI Company

Follow us

[!\[\]\(0363fbe6789abdbb08e06be2f5f3d58f_img.jpg\)](#)[!\[\]\(a6de2bcec56babf56a42f379afda1e7e_img.jpg\)](#)[!\[\]\(92a1c98eaecbbba5a455f391a60427ca_img.jpg\)](#)[!\[\]\(877c8f38d527f924882aa6efc6e1de56_img.jpg\)](#)[!\[\]\(2d7bbd9fbf9d5be89ee38e02896179e8_img.jpg\)](#)

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.