Reason

Connection to Honeypot
- Severity: High

Supporting Evidence

- Time: 2025-03-14T19:06:39.850031
- Source IP: 115.231.78.11
- Source Port: 49682
- Protocol: TCP
- Destination IP: 172.172.168.52
- Destination Hostname: 634851ba-c550-11ef-8089-000d3a556b22
- Destination Port: 89
- Destination Type: dionaea.connections

Analysis

```
inetnum:        115.231.78.0 - 115.231.78.127
netname:        DUCHUANG-KEJI
descr:          Hangzhou Duchuang Keji Co.,Ltd
descr:
country:        CN
admin-c:        PM543-AP
tech-c:         CJ55-AP
abuse-c:        AC1602-AP
status:         ASSIGNED NON-PORTABLE
mnt-by:         MAINT-CN-CHINANET-ZJ-JX
mnt-irt:        IRT-CHINANET-ZJ
last-modified:  2021-06-24T07:33:45Z
source:         APNIC
```

IP

VT: 14/94
IpVoid: 14/93
AbuseIpDB: Confidence of abuse 100%

Conclusion

Source IP address confirmed abusive by multiple sources. I conclude this is malicious behavior.

Next Steps

Block the IP address at the firewall. This does not need further escalation.