**Reason**

Connection to Honeypot
- Severity: High

**Supporting Evidence**

- Time: 2025-03-04T23:59:59.103067
- Source IP: 147.185.133.121
- Source Port: 50067
- Protocol: TCP
- Destination IP: 172.172.168.52
- Destination Hostname: 634851ba-c550-11ef-8089-000d3a556b22
- Destination Port: 54500
- Destination Type: dionaea.connections

**Analysis**

```
NetRange:       147.185.132.0 - 147.185.139.255
CIDR:           147.185.132.0/22, 147.185.136.0/22
NetName:        PAN-22
NetHandle:      NET-147-185-132-0-1
Parent:         NET147 (NET-147-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Palo Alto Networks, Inc (PAN-22)
RegDate:        2023-09-07
Updated:        2023-09-07
Ref:            https://rdap.arin.net/registry/ip/147.185.132.0

OrgName:        Palo Alto Networks, Inc
OrgId:          PAN-22
Address:        Palo Alto Networks
Address:        3000 Tannery Way
Address:        Santa Clara, CA 95054
City:           Santa Clara
StateProv:      CA
PostalCode:     95054
Country:        US
RegDate:        2017-11-22
Updated:        2024-11-25
```

**IP**

VT: 6/94
IpVoid: 6/93
IPSpamList: Category Unclassified
HoneyDb: Google LLC hosting

**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.