SOC Incident Report #001

Reason

Connection to Honeypot
Severity: High

Supporting Evidence

Time: 2024-10-07T14:16:17.687258
Source IP: [39.37.138.107]
Source Port: [52584]
Protocol: TCP
Destination IP: [20.217.82.118]
Destination Hostname: [ec7c2d8e-8429-11ef-916b-000d3a556b22]
Destination Port: [445]
Destination Type: [dionaea.capture]
MD5: [996c2b2ca30180129c69352a3a3515e4]
SHA512:
[da2acf9fd0553b473802b6dd8cf35a0ac4e734f0a790f9c260db06f46f84ff452bd888297f662540bf60a895a3f196368d3e24d13dd9e0d4ca9e83d3cc1076de]

Analysis

Whois Lookup

```
inetnum:        39.32.0.0 - 39.63.255.255
netname:        PTCLBB-PK
descr:          Pakistan Telecommuication company limited
descr:          CDDT Building, H-9/1, Room No. 15, Training Block
descr:          Islamabad, Pakistan
country:        PK
org:            ORG-PTCL1-AP
admin-c:        MA527-AP
tech-c:         MA527-AP
abuse-c:        AP1078-AP
status:         ALLOCATED PORTABLE
```

IP Reputation Checks

VT: 0/94
IpVoid: 1/93
Barracuda: listed as poor

MD5 Hash Reputation Checks

VT: 69/73 (wannacry)
Hybrid Analysis: Malicious

Conclusion

Source IP address confirmed malicious for sending port 445 traffic. Hash of file found is known to be malicious and of a wannacry variant from multiple sources. This is malicious behavior.

Next Steps

Block the IP address at the firewall and blacklist the hash on all endpoints. Escalated to Incident Response for further action.

Prepared by: Taji Abdullah