SOC Incident Report #002

Reason

Connection to Honeypot
Severity: High

Supporting Evidence

Time: 2025-03-14T17:42:13.491396
Source IP: 103.166.137.51
Source Port: 60578
Protocol: TCP
Destination IP: 172.172.168.52
Destination Hostname: 634851ba-c550-11ef-8089-000d3a556b22
Destination Port: 445
Destination Type: dionaea.capture
MD5: 23f751d9ab6fd444e1b6661ae17e78d5
SHA512:
e768777032a5631a335032df03e4fac2971566789db362cd65706eb13bcbed3ca889bb134f69ab01337da062305b92319a55698a0b0403aadb

---

Analysis

Whois Lookup

inetnum: 103.166.136.0 - 103.166.137.255
netname: IDNIC-ADHIKN-ID
descr: PT Adhi Karya Nusa
descr: Corporate / Direct Member IDNIC
descr: Jl Widya Chandra VIII No 23
descr: Senayan, Kebayoran Baru, Jakarta Selatan
descr: DKI Jakarta, 12190
admin-c: HA330-AP
tech-c: HA330-AP
remarks: Send Spam & Abuse Report to: abuse@adhikaryanusa.co.id
country: ID
mnt-by: MNT-APJII-ID
mnt-irt: IRT-ADHIKN-ID
mnt-routes: MAINT-ID-ADHIKN
status: ALLOCATED PORTABLE

IP Reputation Checks

VirusTotal: 0/94
IpVoid: 2/93
IPSpamList: Category MS-DS Attack

MD5 Hash Reputation Checks

VT: 64/71 (wannacry)

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. I conclude 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