[illegible] Top close → Excepoiry, remove from [illegible]

Scoping → AffectedMachines (tanium) → or C.S query

Check if any execution → Yara scan to find out → Sig. Based

N/w Based check → C&C → to find out how the attack vector got in.

Find out if C&C happening? → netstat?

Malware Behavior. (Lateral Movement, RDP, Powershell)
(Persistence) → Reboot also → { Start up File
autorun
Schedule ~~[illegible]~~ Scri

Remediation

① Scan
② format
③ re-scan

→ update sig on IDS | AV | IPS | Firewall |