Threat Category: Remote Access, VNC Detection

Threat Description: The SNORT rule is designed to detect the use of the Virtual Network Computing (VNC) protocol over TCP port 5900. VNC is a graphical desktop-sharing system that allows remote control of another computer.

The rule identifies outbound or inbound TCP connections targeting port 5900, which is the default port for VNC servers.

Indicators of Compromise (IoCs):

Destination Port: 5900

TCP Protocol

Potential presence of VNC server handshake

Detection Mechanism:

Uses alert tcp any any -> any 5900 to capture traffic going to TCP port 5900.

msg:"VNC connection detected" alerts on possible VNC usage.

Possible Attribution & Use Cases:

Used by administrators for remote support and monitoring.

Can be exploited by attackers if VNC is misconfigured or lacks authentication.

Recommended Actions:

Verify if VNC connections are authorized and encrypted.

Block or limit access to port 5900 using firewall rules.

Prefer encrypted remote access solutions like SSH or VPN.

Author & Attribution:

Rule Author: Community

Rule Source:

SID: 1000020

Revision: 1