Executive Overview:

On the morning of March 18, 2024, our network monitoring systems flagged an unusual activity indicative of a potential security breach within our internal network. An immediate investigation was launched by our Incident Response Team (IRT) to ascertain the nature and scope of the incident. The investigation revealed that an adversary had gained unauthorized access to our network and employed a sophisticated technique to maintain persistence and evade detection.

Incident Details:

The adversary managed to exploit a previously unidentified vulnerability within our perimeter defenses, gaining initial access to a low-level user account. Following the initial compromise, the adversary utilized a PowerShell script to change the Remote Desktop Protocol (RDP) service port on compromised machines from the standard port (TCP 3389) to a non-standard port. This technique allowed the adversary to blend in with legitimate traffic and reduced the likelihood of detection by traditional network monitoring tools that may not scrutinize non-standard ports with the same rigor.