Clean Zone Procedure Checklist

This procedure should be followed when dealing with a ransomware attack to remove devices from the infected network and transition them safely to the clean network. This procedure also supports disconnecting infected devices from the internet and powering them down, to cease continued command and control by an adversary or malware, or continued encryption from a ransomware that could be running on the device. There is a chance that some devices during a ransomware attack would be compromised and just starting to encrypt their files or mid-way when they are powered down, potentially creating availability of digital evidence for the forensics investigations.

1. Ensure the internet access is disabled to the red zone
2. Ensure the WIFI router is turned off on the red zone
3. Power down all the devices on the red zone
4. Remove one device at a time from the red zone
5. Format each device in isolation with no network connections to either the red zone or green zone
6. Have a second team member verify a device is formatted properly and mark the device as "verified for green zone"
7. Connect the newly formatted device over to the green zone
8. Use the servers and internet access on the green zone to restore the device using a safe backup
9. Walk through the device recovery procedure to ensure the device is configured properly

Some if the steps may seem redundant, however, when dealing with infected devices it only takes one of these devices to be connected to the green zone to ruin the entire attempt which would mean starting over again. The reinfection could take hours, weeks or months, but making a mistake during the cleaning procedure or backup recovery process could become the cause of another cyber incident.