Ransomware Response Checklist

Step 1. Determine and immediately isolate systems impacted

[ ] If feasible, disconnect individual systems

[ ] If several systems are impacted, temporarily take the network offline at the switch level, if possible

[ ] If taking the network temporarily offline isn’t immediately possible, unplug affected devices from the network or remove them from Wi-Fi

[ ] Isolate systems in a coordinated way using out-of-band communication methods like phone calls or other means to avoid letting actors know that we’ve discovered the problem and are taking actions to mitigate it

Step 2. (*To be taken only if it’s impossible to temporarily shut down the network or disconnect affected hosts from the network*). Power down devices to avoid further spread of the ransomware infection

Step 3. Triage impacted systems

[ ] Identify and prioritize critical systems for restoration and data recovery based on a predefined critical asset list

[ ] Keep track of systems and devices not impacted so they can be deprioritized for restoration and recovery

Step 4. Take stock

[ ] Confer with response team to determine and document an initial understanding of what happened

Step 5. Communicate & coordinate

[ ] Communicate and share your determination and the information you have at your disposal to secure appropriate assistance, potentially including from law enforcement

[ ] Provide regular updates to management, senior leaders, the IT department, and other stakeholders as the situation develops

[ ] Communicate and coordinate with communications and public information personnel to ensure accurate and effective information sharing, both internally within the organization and with the public

Step 6. Eradicate & contain

If initial mitigation actions seem impossible:

[ ] Take a system image and memory capture of a sample of workstations, servers, and other affected devices

[ ] Gather up relevant logs and samples of any “precursor” malware binaries and associated observables or indications of compromise

[ ] Protect system memory, firewall log buffers data and other evidence that’s highly volatile in nature (or limited in retention) from tampering or loss

[ ] Ask federal law enforcement whether there are any decryptors available (in case researchers have broken the encryption algorithm for the ransomware involved