Stages of a Ransomware Attack

1. Initiation
   - The attacker gains access to the network, typically through a phishing email or by exploiting a vulnerable server.
   - Once inside, the attacker begins to gather information about the network and its defenses.

2. Establish Foothold & Recon.
   - The attacker moves laterally within the network, looking for vulnerabilities and opportunities to escalate privileges.
   - Beaconing connections are established to communicate with the attacker.

3. Lateral Movement
   - The attacker infects more devices and often looks to escalate their privileges – for instance by obtaining admin credentials.
   - This stage is critical as it allows the attacker to move more freely within the network.

4. Data Exfiltration
   - The attacker begins to exfiltrate data, looking for backup servers or easy access points.
   - Exfiltration is often done through removable drives or USBs.

5. Data Encryption
   - The attacker encrypts data on infected devices, demanding a ransom for decryption.
   - Encryption is typically done using ransomware software, which encrypts files and demands a ransom.

6. Ransom
   - The victim organization is asked to pay a ransom to decrypt their data.
   - The ransom demand is usually communicated via the same malware that infected the systems.

7. Clean up & Recovery
   - The victim organization attempts to restore data from backups and clean up the infected systems.
   - Recovery is often slow and expensive, as data might need to be re-encrypted or reconstructed.

8. The Cycle Repeats
   - The attacker returns to the network and repeats the cycle, infecting and exfiltrating data again.
   - The cycle is repeated until the attacker is caught or until the organization pays the ransom.

Autonomous Response capabilities work at later stages as well. Even if familiar tools and methods are used to conduct it, Autonomous Response can enforce the normal pattern of life for devices attempting encryption, without using familiar tools and methods. The success of Autonomous Response is in its ability to respond to anomalies on the network, to prevent the attacker from moving laterally, and to block encryption traffic without disconnecting legitimate users.