Timeline of a Ransomware Attack on a Local Government

A local government employee in the 911 Center starting their shift on a Friday evening logs onto their computer and discovers a message that all files have been encrypted and to contact their IT department for assistance. Then another employee tries to log on and receives the same message. By this time, the entire network has been compromised and the IT help desk has been called to try to rectify the situation. None of the government employees can access their email, any software, or any of their files—it is a chaotic scene!

The IT staff quickly return onsite and realize the issue is a ransomware attack. Swiftly they take down the entire jurisdiction's network and all Internet connections in an effort to prevent any further impact. But when did the attack begin? How did the threat actor enter their government environment? The timeline below outlines how an attack normally occurs and shows the harsh reality that most threat actors are on your network for 90-180 days before the encryption of files alerts you to their malicious presence.