Issued 12/16/18

Operation Sharpshooter Uses Fileless Malware to Attack Global Infrastructure

The McAfee Advanced Threat Research team detected a malware campaign dubbed Operation Sharpshooter which attacked nuclear, defense, energy, and financial targets from all over the world. As detailed by McAfee's research team, the campaign dubbed "Operation Sharpshooter" [link] makes use of an in-memory essential to download and execute a second stage payload named Rising Sun. Moreover, the Rising Sun implant is a fully functional modular backdoor designed to perform surveillance on its compromised victims' network. This second implant also shows multiple similarities with the Trojan Duuzer backdoor employed in attacks designed to compromise targets from the same critical industries during 2015 by the Lazarus Group cyber-espionage threat, known to have been active since at least 2009. The campaign camouflaged itself as a legitimate industry job recruitment operation, and the attack process starts with a document containing malicious macros designed to download the first payload stage into the system memory, stealthily running in the background and collecting intelligence. All the data Rising Sun gathers from infiltrated boxes is sent to the group's control servers, providing its masters with information regarding the system's details and network adapters, local usernames and IP address, as well as allowing them to manage system files and processes.