Data collection date: 6th December 2019

Time zone: GMT +8 , 24 hours format

Prepared by: Shrivastava Siddhant, Francisco Furtado, Desmond Wan

|  |  |
| --- | --- |
| **Time** | **Event** |
| 1005 | Capture pre-attack pcap for 15 mins |
| 1020 | Capture pcap for actual attack in 15 mins intervals |
| 1020 | Infiltrate SCADA WS via USB thumb drive with first malware |
| 1030 | First attack: Exfiltrate Historian Data (5 mins attack + 10 mins sleep) x 4 cycles |
| 1030 | Exfiltrate Historian Data |
| 1035 | Sleep |
| 1045 | Exfiltrate Historian Data |
| 1050 | Sleep |
| 1100 | Exfiltrate Historian Data |
| 1105 | Sleep |
| 1115 | Exfiltrate Historian Data |
| 1120 | Sleep |
| 1130 | Rest 60 mins |
| 1230 | Infiltrate SCADA WS with second malware, via downloading from C2 server |
| 1230 | Second attack: Disrupt sensor readings and process (3 mins + 10 mins sleep) x 5 cycles |
| 1230 | Disrupt Sensor and Actuator |
| 1233 | Sleep |
| 1243 | Disrupt Sensor and Actuator |
| 1246 | Sleep |
| 1256 | Disrupt Sensor and Actuator |
| 1259 | Sleep |
| 1309 | Disrupt Sensor and Actuator |
| 1312 | Sleep |
| 1322 | Disrupt Sensor and Actuator |
| 1325 | Sleep (5 mins) |
| 1330 | Stop actual attack pcap capture |
| 1330 | Capture post-attack pcap for 15 mins |
| 1345 | Stop post attack pcap capture |
| 1345 | RAM memory dump using FTKImager, extract when done |
| 1345 | Extract Historian .csv files |
| 1345 | Extract malware .exe file for both attacks |
| 1345 | Extract VM image (.vmdk) of both SCADA WS and C2 server |
| 1345 | Extract capture pcap files from external monitoring VM |