Triton - A Report From The Trenches

Published: 2019-03-11 · Archived: 2026-04-05 16:03:27 UTC

Julian Gutmanis was in the plant that was compromised by Triton, and he was involved in the response and recovery. This is his first hand report. Here are some of the highlights:

- the initial outage was related to one down controller on a Saturday in early June, 2017
- six controllers went down in the August, 2017 attack
- DCS reflected normal operation during both outages
- "at this point we had considered the entire organization to be compromised ... we know the ESD systems and the integrity of these systems can no longer be trusted ... we know there is some unknown operating program in the controllers memory, and we could be facing a complete loss of control".
- Schneider Electric did not provide information on Triton; information sharing was in one direction. The asset owner provided the Triton info, but did not get information back. The first they heard about Schneider analysis was at S4x18.
- They were worried about time-delayed attacks after communication to the adversary was terminated.
- "There was a significant eradication event".
- The asset owner was lucky it wasn't worse, but it was expensive.
- Lessons learned.

-
