//adamnet.works

CASE STUDY

IR for Manufacturing Enterprise:
Ransomware Defeated by adam:ONE® ZTc

Incident Response:

- adam:ONE® was used as the central tool for IR.
- Existing Firewalls were replaced immediately with adam:ONE® and all sites were moved into a Zero Trust connectivity (ZTc) posture.
- Full radio-silence to all C2 servers was achieved within hours, shutting out all potential activity of the threat actors.
- Microsegmentation and ZTc facilitated a hardened posture for all devices, including IT | IoT | OT & ICS.
- adam:ONE® ZTc severed all connections for all devices via DTTS® defeating all circumvention attempts by default. Adaptive AI™ was used to facilitate dynamic allowlists to get critical and ancillary services back up. Only a single weekend shift was lost globally.
- The full Layer2 visibility of adam:ONE® facilitated automatic device inventory. An automatic device quarantine default was used by the IR team to take control of all connections and orchestrate recovery for each endpoint. Any connection attempts by lingering malware or new attempts from the threat actors were defeated by the deny-by-default posture of ZTc. To this day, the live log provides clear visibility into all connection attempts across IT | OT for remediation without allowing the threat actors to execute an attack.

Breach Summary:

Anycorp (Name Redacted for confidentiality)

- Automotive Manufacturing Enterprise.
- Over 10 000 Employees.
- 5 Major facilities across 4 Countries: N-America, Europe & Asia.
- Protected by Enterprise Grade managed security systems.
- Initial access gained via phishing campaigns.
- Over 6 months dwell time resulted in all but one of the backups being encrypted.
- 400/3000 devices infected with *TrickBot*.
- Severe technology debt in IT | OT & ICS.

Attackers COMPLETELY EVADED DETECTION OVER 6 MONTHS and ran circles around enterprise grade security.

Outcomes:

- The ransom was never paid.
- Only a single weekend shift was lost globally.
- adam:ONE® still protects Anycorp today.
- Windows XP based ICS controllers are still safely in operation behind ZTc.

After 3.5 years we've tracked over 5000 re-infection attempts.
All are still neutralized by adam:ONE® ZTc.

Protecting the people and systems you care about. ™

contact@adamnet.works

See adam:ONE® in action:
adamnet.io/C2begone

For a more detailed case description: adamnet.io/IR

All items © 2024: Adam Networks Inc. USA, Canada and Other Countries.