S4x20

RYUK
OT Incidents

A Case Study From the Responders

Clint Bodungen

ThreatGEN

BACKGROUND

- We responded to 2 incidents (MTSA regulated)
- We know of at least 3 others (MTSA regulated)
- All within ~2 months of each other
- Same TTPs

THE COAST GUARD ALERTS

- https://www.bleepingcomputer.com/news/security/us-coast-guard-says-ryuk-ransomware-took-down-maritime-facility/
- https://www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/us-coast-guard-discloses-ryuk-ransomware-infection-at-maritime-facility/
- https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf

ThreatGEN

THE COAST GUARD ALERTS

- Recent reports on Coast Guard alerts aren’t completely accurate
  (at least not from what we saw at the incidents we responded to and/or have information on)

  - RYUK did not exactly effect or shut down ICS
  - Upon discovery, operations were switched over to manual
  - Loss of physical access control and camera monitoring was not caused directly by RYUK
  - RYUK did not disrupt the business internet/network communication

TTPs

- Ryuk is not “spray and pray”
- Gained initial entry using phishing emails
- Remained in network for a while (weeks/months)
- Lateral movement was facilitated by insecure RDP
- Weaponized Active Directory
- Could this be a diversion tactic?
- IOCs?

SO WAS THIS A TARGETED CAMPAIGN?

- Timing and similar TTPs would suggest so
- I’ve had one IC source and one source close to the IC tell me it was
- Waiting on information regarding depth and specifics of targeting

WHERE IS THE COMMUNICATION?

- No industry operators that we spoke with (outside of these incidents) have heard anything throughout the available channels
  - It’s not the ISAC’s fault if they aren’t getting the info
  - Why aren’t operators communicating?
  - Why aren’t responders communicating?
  - Why didn’t we communicate?
- The Coast Guard Alert was vague, void of details, and inaccurate (if related to one or more of the incidents we responded to)