CERT-EU'S PERSPECTIVE

TLP:AMBER / SENSITIVE

GRID ATTACKS IN EUROPE

GEORGE KOUTEPAS, CYBER THREAT INTELLIGENCE

October 21, 2021 / v 1.0

KNOWNS AND UNKNOWNS

- Difficult to have an exact picture of threats to the grid.
  - Only a limited number of attacks have been reported publicly.
  - What we don't know is how many attacks have remained undetected or unreported
- Several factors for that…
  - Reluctance to report
  - Need to restrict public knowledge of incidents
  - Minor impact, late impact, indirect impact

WHAT DOES IT MEAN ATTACKING THE GRID?

- Limited reporting – limited experience
- Based on actual incidents:
  - Disabling grid control equipment
  - Disabling safeguard equipment
  - Disabling computer systems that interface to the OT
  - Hijacking control systems and controlling them remotely
  - Hijacking control systems and providing false status reports
  - Ransomware/mineware, yes we've seen that too…
  - IT side of the organisation - may impact OT, or just induce panic
    - Ransomware, DDoS attacks, defacements
    - Reconnaissance

RECENT INCIDENTS (1)

- October 2020: Italian energy firm compromised by the Netwalker ransomware.
- June 2020: France attributes 2018 cyberattack on the country's power grid to a Russia-based threat actor.
- May 2020: Berserk Bear actively targeting critical infrastructure in Europe and the US.
- April 2020: At least 8 major energy firms (including EU ones) hit by big game hunting ransomware attacks.
- March 2020: Disruptive attacks against European energy firms (not grid related) .
- March 2019: Norwegian aluminium and renewable energy company, Norsk Hydro became victim of a ransomware attack.

RECENT INCIDENTS (2)

- 2019: Strategic web compromise activity against Ukraine's largest power and coal producer.
- October 2017: Dragonfly 2.0 (Berserk Bear) - strong indications of attacker activity in the US, Switzerland, and Turkey.
- April 2017: EirGrid (Ireland) affected by mobile network attack.
- December 2016: Attack on Ukrainian electricity transmission system
- April 2016: Malware at a German Nuclear Plant
- December 2015: Attack on Ukrainian electricity distribution system

MALWARE

- BlackEnergy – since 2007 – Russian underground, Sandworm, Berserk Bear, APT29 (Russia)
  - + destructive Trojan KillDisk
- StuxNet – 2010 – US, Israel
- Shamoon – since 2012 - APT33 (Iran)
  - Wiper
- CrashOverride (Industroyer) - since 2016 - Russia
  - Modular, highly customizable
  - Uses industrial communication protocols
- Triton – since 2017 – TEMP.Veles (Russia-research institute)
  - Can purportedly manipulate industrial safety systems, cause physical accidents and shut down operations
  - an attack framework built to interact with the Triconex Safety Instrumentation System (SIS) developed by Schneider Electric

SOME OBSERVATIONS ON INCIDENTS (1)

- Degree of uncertainty over the actual threat, the actual attacks
- Attacks on OT require significant engineering skill and resources to develop and deploy, but…
  - once demonstrated, TTPs are used widely
- Combination of skills / cooperation between teams
  - specialists in cyber intrusion (breach cyber defences, gaining foothold in the system)
  - specialists in "grid" (understand specialised technologies and processes)
- Requirement for reconnaissance, mapping of victim infrastructure

SOME OBSERVATIONS ON INCIDENTS (2)

- OT is not the only vulnerable point for energy organisations
  - Several IT processes need to be maintained for the normal functioning (billing, customer data, "smart" meters, public web-site access)
- Energy companies make for enticing cybercrime targets
  - Size, critical infrastructure framework, liability to customers, public interest
  - Ransomware/DDoS

10 years

CERT-EU

THINK CONSTITUENT
CREATE VALUE

https://cert.europa.eu

secretariat@cert.europa.eu

@CERTEU