Overview of incidents we are dealing with and how to improve the response readiness

EGI CSIRT

About this presentation

- Only high-level information will be provided as case details are sensitive
- Analysis from personal perspective

Cases: initial foothold

- Two ways to gain the initial foothold for resent severe cases:
  - The service is abused using a valid but possibly hacked account
  - The service is compromised using a weakness

Attack goals

- Run cryptominers
- Spread illicit material

What we've learned so far

- Threat actors are (still) sneaky and hard to catch.
- Complexity in infrastructure increases various aspect of incident handling.

Global trends and EGI

- Ransomware-as-a-service, crime-as-a-service bring advanced tools to hands of anyone → complexity of attacks likely not going to decrease
- Money is the main motivator → EGI related infrastructure is interesting to malicious actors: computing power, bandwidth...

Recommendations

- Ensure that proper evidence is gathered (and secured + preserved!) all over the infrastructure.
- Early detection and well-defined processes help minimizing the damage. Processes only work if people master them.
- Ensure that your infrastructure has the ability to recover.

Recommendations

- Keep your systems healthy, under your control and apply principle of least privilege.
- Improve logging and monitoring across the entire infrastructure and dependencies.
- Know your most valuable assets, know your infrastructure’s value.
- Share knowledge with the community – IoCs

EGI CSIRT

- https://csirt.egi.eu/
- abuse@egi.eu