EGI-CSIRT – Operational Security

EGI-20141024-01 FedCloud incident at CESNET

EGI-CSIRT

sveng@nikhef.nl, Nikhef, EGI-CSIRT

EGI-20141024-01 FedCloud incident

Outline

- What happened / Status
- Which Problems were found during incident handling
- Summary / Next steps

EGI-20141024-01 FedCloud incident

What happened

- FedCloud VM client has been remotely compromised and used for dDOS attacks
- Affected System: 2 VM images available from App-DB
- Vulnerability/Attack vector: Tomcat server with the Manager servlet was active. The default credentials "admin:admin" were unchanged giving manager level access to Tomcat. Attackers are constantly scanning for this misconfiguration.
- Site security team found that the attacker(s) deployed malware on the machine, which seems to be based on the Bill Gates trojan family
- VMs were controlled from a CnC and used for ddos attacks

EGI-20141024-01 FedCloud incident

What happened / timeline / status

- 15/16 Oct 2014 ddos attack originating from fedcloud site
- Fr Oct 24 22:22:11 details reported to irtf (not really an advanced attack)
- Sat Oct 25 12:05:41 2014 fedcloud informed, request to remove vulnerable images from App-db
- Sat Oct 25 12:28:24 2014 feedback / Ack from fedcloud
- Some operational issues found with removing VMs from App-DB, addressed over the weekend
- All 4 affected sites replied till Mon Oct 27 10:30 2014 that the vulnerable VMs were removed locally
- No other site reported network connections as found by the reporting site / Incident is contained / Investigation on going

EGI-20141024-01 FedCloud incident

Which Problems were found during incident handling, very prelim. list

- Unclear communications/reporting: Always use **abuse at egi.eu**
- Operational issues in VM handling (Very vital discussions via e-mail/meeting)
- Missing fedcloud tech expert in IRTF
- Unclear (for IRTF) which information about VMs is available where
- Unclear how to operate on known bad VMs
- Unclear security model in fedcloud
- Unclear how the policy on VM endorsement is in effect

EGI-20141024-01 FedCloud incident

Summary / Next Steps

- Endorsement is a crucial step in providing VM images / qualified endorsers needed. Take the policy serious.
- Framework for Incident Response for VMs has to be developed (Low level incident response plan)
- Fedcloud Tech expert in irtf needed.
- Evaluation of the fedcloud meeting 28. Oct will reveal some action items, not done yet
- Grid Incident Response has a focus on DNs/VOs, to be translated to fedcloud.
- ”Useful” incident, probably no big impact, revealed a lot of IR issues.
- Major effort for EGI-CSIRT to provide Operational Security for Cloud Infrastructure, funding?