EGI CSIRT: Keeping EGI Secure

Vincent BRILLAULT
Federated e-infrastructure and security

- **EGI:**
  - ~300 sites, world-wide, various time-zone
  - variable local security expertise & capabilities
- **EGI CSIRT:**
  - Security officers & experts from NGIs
  - Partial time involvement, other duties
  - Activities: Prevention, Response & Training
EGI CSIRT
Activities & collaborations

Security Policy Group

Security Monitoring Group

Incident Response Task Force

Software Vulnerability Group

Security Drills Group

Training & Dissemination Group
Prevention

Vulnerability detected in software package X

Verify if vulnerability can affect the e-infra

Assess criticality and/or impact

Info is forwarded if the risk is critical or high

Software Vulnerability Group

Verify mitigation

Support data centres

Contact data centres

Incident Response Task Force

Handling

Update sensors and probes

Detect data centres running package X

Security Monitoring Group

Monitoring

Update on number of vulnerable data centres

Keeping EGI Secure
Prevention: Vulnerability reported
Prevention: Classifying vulnerabilities

- Advisories: Critical, High, Medium, Low, (Alert)
- Always to be patched, but with different priority & impact
- Only Critical is actively followed-up by the CSIRT
- Escalation possible (e.g. High -> Critical)
Prevention: Vulnerability hunt

Number of machines affected by selected vulnerabilities:

- CVE-2015-7547
- CVE-2016-1950
- EGI-SVG-2016-11476
- CVE-2016-5195

Graph showing the number of machines affected over time from April 2016 to July 2017, with a peak in October 2017.
Prevention:
Getting help from EGI Operation

- Following data centres vulnerabilities
  - Time consuming (esp. waves)
  - Requires almost no security knowledge
  - Requires good site contacts
- Currently evaluating involving EGI Operations
Response

- IRTF roles:
  - Coordinate response: contacts, overview, actions...
  - Help with forensics analysis, guide site admins
- 44 incidents since 2010:
  - 2010-2013: SSH bruteforce, trojans, bots
  - 2013-2014: AUP violations (Bitcoin mining)
  - 2014-2017: User VM compromise (basic errors)
Rootkit identified by an EGI site

IRTF and site expert analysis:
- Identify all persistence mechanisms → IoCs
- Reverse the backdoor protocols → remote scanner

Recursive take down possible:
- Collect network activity from compromised systems
- Remotely scan systems for the backdoor
- Contact owner with IoCs for confirmation
Response: VENOM – *takedown*

- Few systems in Europe
  - Contacted directly
  - Backdoor found but no network traces
- More cases in the US
  - Forwarded to colleagues
  - Partial follow-up: 25 server identified
- Criminals & goals still unknown...
Security Challenges

- Simulate incidents over several sites
- Test all links in the chain:
  - Site security: Communication, setup & response
  - IRTF: coordination & help
  - SPG: Policies
Security Challenges 2017: Federated Cloud

- Scenario: user VMs starts DDOS & Crypto-mining
- Response:
  - 2 sites reported DDOS within few hours
  - Most sites suspended VMs within a day
  - Many out-of-office contributions!
- Some issues identified (e.g. suspension)
  But also very good participation from sites!
Training

- Usually at conferences or dedicated for NGI/NREN
- Different session types:
  - Defensive
  - Offensive
  - Digital forensics
  - Roleplay
- Contact us for organizing trainings!
Ongoing Challenge: Federated Cloud Security

- EGI continues to develop Federated Cloud
- Cloud is difficult for users:
  - Full sysadmin, responsible for everything
  - Often directly exposed on the internet
- Most of recent incidents Cloud related

→ How to make the cloud *user-proof*?
Ongoing Challenge: Federated Identity

- Simpler access to the grid (home institute credentials)
- New participants in incident response:
  - Home institutes (compromised identities, AUP violation,...)
  - Token translation services, VO portals
- How to maintain security levels?
  - Emergency suspension?
  - Incident reporting?
Ongoing Challenge: Widening collaborations

- Collaboration with EUDAT, PRACE:
  - Mailing list cross-membership
  - F2F meetings (dedicated or conferences)
    → EOSC project/funding: even more integration
- WISE Community
- Collaboration with the US?
- Collaboration with other communities (see VENOM...)
Links to check

- EGI CSIRT Report, Venom Analysis:
  http://csirt.egi.eu/materials/

- Incident handling checklist:

- Report a vulnerability: report-vulnerability@egi.eu

- Check your site/NGI vulnerabilities:
  - https://operations-portal.egi.eu/csiDashboard/
  - https://pakiti.egi.eu/ (Pakiti v2)
  - https://pakiti.cesnet.cz/egi/ (Pakiti v3)