Security Drill Group: Security Service Challenges

Oscar Koeroo

Together with:
- Intro
- Why an SSC?
- SSC{1,2,3,4}
- SSC5
- Future
acknowledgements

• NON INTRUSIVE
• DO NOT affect actual production
• FULL control of the distributed infection
• Detailed LOGGING of all infection activity
• Have an emergency FULL STOP of the drill
Who am I

• Work at NIKHEF

• Security (grid middleware) expert, 2003-
  • Multiple EU FP7 projecten
  • Account mapping framework (LCMAPS)
  • Standardization (Open Grid Forum)
  • Security training for grid infra (SSC)
  • Risk Analysis Team (EGI-SVG)
European Grid Infrastructure

372 sites globally
10 – 40 Gbps network
296 000 CPU cores
140 000 TByte storage

09:26:06 UTC
Why perform security drills?

• Our own research infrastructure
  • with small and large data centers
  • Non-standard/custom/special software stack
• Distributed skill levels
• Training and learn from doing
Objectives

• Goal
  • Investigate whether sufficient information is available to be able conduct an audit trace as part of an incident response
  • and to ensure that appropriate communications channels are available
Objectives

- SSC Addresses
  - Compliance with audit requirements
  - Understanding of the incident handling and response guide
  - The overall execution of the incident handling procedures
Compute workflow analyses

• Functional email address
  • Registered in a central database

• Responsive email address
  • Send a reply within 4 hours (SLA-test)
Identities on the Grid

- Authentication using PKI
  - International Grid Trust Federation - www.igtf.net
  - Globally unique name - users and hosts
  - Traceable to a real person

- Virtual Organisation membership
  - Registration based on the unique name
  - Membership can grant access to resources
  - Group and role based
Storage challenge

- Regional operation center were targeted
  - File stored on the mass storage system
  - Who stored/ transferred a file?

- Revealed limitations in log file quality
  - Missing features in the storage solutions
Workflow: Storage access

Role: Scientist / end-user

Internet

Storage headnode

Authentication

Authorisation: Subject + VO

Enforce: Storage pool selection

Storage pool
Security Service Challenge 3

Operational diligence challenge

• Submitting a grid job to various sites
  • First friendly malware
  • Malware tested site setup and revealed problems
  • Admins & security contacts are forced to track down the malware on their cluster

• Revealed problematic cluster setups
Role: Scientist / end-user

Workflow: Compute with regular job

Internet → Gatekeeper → Authentication

Authorisation: Subject + VO → Enforce: Account mapping

Batch system scheduler → Cluster node

www.egi.eu

EGI-InSPIRE RI-261323
Challenging a sites and a VO (LHC: ATLAS)

- Job submission now using pilot jobs
  - Mimicking physics analyses jobs
  - Malware tested site setup and revealed problems
  - Admins are forced to track down the malware on their cluster

- Forced distributed teams to communicate
  - Result: ATLAS now has a formal CSIRT
Workflow: Compute with Pilot Job

Role: Production Manager

Role: Scientist / end-user

Internet

Gatekeeper

Authentication

Authorisation: Subject + VO

Enforce: Account mapping

Batch system scheduler

Cluster node

VO task queue
Workflow: Compute with Pilot Job

Role: Production Manager

Role: Scientist / end-user

Internet

Gatekeeper

Authentication

Authorisation: Subject + VO

Enforce: Account mapping

Batch system scheduler

Cluster node

VO task queue
Security Service Challenge 4

• SysAdmins see the regular grid job
  • Log: “This job is from the production manager”
  • Need to dig into the analyses framework
  • Expose the real “scientist” ==> Requires help

• Forced to contact CERN-IT and Atlas
  • Learn what to look for
  • Mapping of PanDa-ID <-> Rogue Scientist
  • Follow regular procedures & contain the IRC bot
SSC5: a Multi Site Security Drill
code name: “World Domination”
Goal

- Simulate a grid wide security incident
  - Means: ~40 sites, globally, all at once
- Challenge the procedures on IR handling
- Focus on the communication channel capabilities
Workflow: Pilot jobs and storage
Architecting the attack
t0: Initial tickets

The diagram shows the flow of initial tickets from T1 NGI CSIRT to T2, with additional tickets T4, T5, and T6. The process starts with an initial ticket to T2 and includes interactions with EGI CSIRT and Pilot CSIRT.
t1: Informing NGI and EGI teams

Informing NGI and EGI CSIRT teams

Pilot CSIRT

EGI CSIRT

T1
NGI CSIRT

T2_1

T2_2

T2_3

T2_4

T2_5

T2_6
t2: Checking the logs

Looking for certificate and VO involvement

T1
NGI CSIRT

T2

T3

T4

T5

T6

Pilot CSIRT

EGI CSIRT

www.egi.eu
t3: Contacting the VO

- Notify Pilot CSIRTs
  - Request Job/Site list

- EGI CSIRT
- Pilot CSIRT

- T1 NGI CSIRT
  - T2₁
  - T2₂
  - T2₃
  - T2₄
  - T2₅
  - T2₆
t4: EGI informs T1 & T2

Inform T1s and T2s about job/site information

Pilot CSIRT

T1 NGI CSIRT

T1 NGI CSIRT

T2₁

T2₂

T2₃

T2₄

T2₅

T2₆
t5: NGI containment

Containment by T1 and T2s

T1 NGI CSIRT

Pilot CSIRT

EGI CSIRT

T1 NGI CSIRT

T21 - T23

T24 - T26
t6: Forensics & Reporting

Diagram:

- **T1 NGI CSIRT**
  - Connected to **T2_1**, **T2_2**, and **T2_3**
  - Connected to **T2_4**
  - Connected to **T2_5** and **T2_6**
- **T2_1**
- **T2_2**
- **T2_3**
- **T2_4**
- **T2_5**
- **T2_6**

Nodes labeled with initials and numbers, connected with arrows indicating relationships.

Labeled sections include:
- Forensics and Reporting
- Pilot CSIRT
Problems to solve

• SysAdmins need to keep production up
• Security contacts need to communicate
• Don’t DDoS the pan-EU coordinators with email
• Seek help & share data
• Find the rogue identity
• Hunt on all other services for similar activity
  • Storage
  • Other grid infrastructure systems
Coordinating our quest for ‘World Domination’

• Malware
  • Friendly malware
  • Pakiti tool
• C’n’C service
• Embedded RT-IR service
  • Templated ticket generation
• Grid MW installed User-Interface
• Django-based webportal
  • Google Maps themed after Wargames
• External: a Jabber room
SSC-Monitor: the coordination hub
Build-in features in the bot

• Use plain HTTP as the C&C protocol
  • Packing libevent for HTTP

• Encrypt the HTTP JSON payload with AES
  • Packing libjson, AES and SHA1/SHA256

• Fake (deadcode) for cron/atd tests & others

• Search for writeable file locations
  • and leave files

• Command set through JSON
  • incl arbitrary command execution

• “Look busy”
  • Calculate SHA256 hashes and create 70% load on a Core i7
Bot kill switches

- Through a command; HTTP/JSON-AES
- Time based; two weeks
- DNS
  - A specific return value was expected from a DNS service; otherwise stop
Anti-debugging features

• Used:
  • GDB detection
  • ptrace detection

• Not used:
  • encrypted binary; Not open sourced
The challenge viewed from our side
• Regional
  • Latest news is that the Spanish NGI is being challenged right now
  • Challenge-as-a-Service portal
    • Disclaimer: Exclusively for grid resources

• SSC6
  • Same concept, different bot, new VO

• Outreach
  • Sharing our ideas into other communities
Questions?

Oscar Koeroo
okoeroo@nikhef.nl

@okoeroo