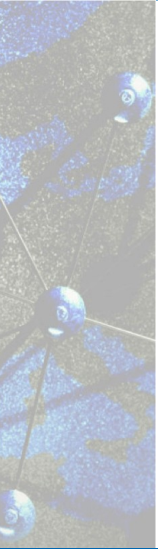


Security in EGI FedCloud

Incident Response / Security Challenges

Sven Gabriel, sveng@nikhef.nl

Nikhef http://nikhef.nl

EGI-CSIRT https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page

SSCs in EGI-FedCloud

Security Service Challenges

Security Drills / EGI

Until SSC4 (2010) “per site security drills”

- Script based malware deployment.
- Evaluation based on:
    - Manually processing response mails (extracting times).
    - Digging for related information (forensics part).
    - ”malware” logs.
    - Scoring schema in a spreadsheet.
    - ... quite a human factor ... time consuming.

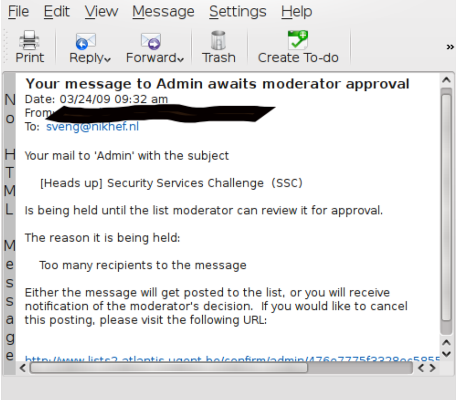
Security Drills / EGI

- Communication:
  - Endpoints valid?
  - Form/Content OK ?

- Problems: Drill-Alarm ignored, contact address wrong, outdated, ...
- ....Unfortunately all the people involved in the incident response at Site XXXX were off-line on Monday ...
- .... I've received both messages. As our site YYYY does not provide any interactive access to the grid users, I developed a bad habit of not paying much attention to the security alerts.

Security Drills / EGI

- Communication:
  - Endpoints valid?
  - Form/Content OK ?



Your message to Admin awaits moderator approval

Date: 03/24/09 09:32 am
From: [redacted]
To: sveng@nikhef.nl

Your mail to 'Admin' with the subject

[Heads up] Security Services Challenge (SSC)

Is being held until the list moderator can review it for approval.

The reason it is being held:

Too many recipients to the message

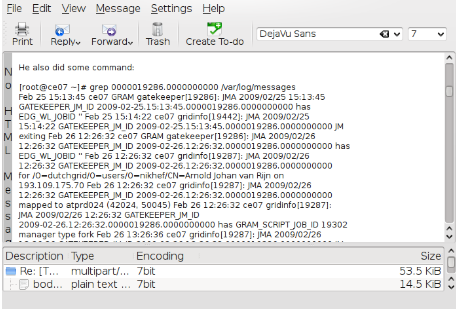
Either the message will get posted to the list, or you will receive notification of the moderator's decision. If you would like to cancel this posting, please visit the following URL:

http://www.lists2.atlantic.ugent.be/confirm/admin/476e7775f3328ec5855

Security Drills / EGI

- Communication:
  - Endpoints valid?
  - Form/Content OK ?

Format / Content of the received mails



He also did some command:

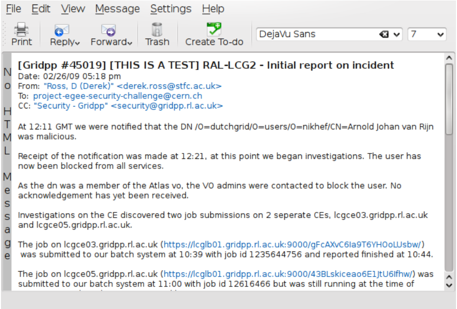
```
[root@ce07 ~]# grep 0000019286.0000000000 /var/log/messages
Feb 25 15:13:45 ce07 GRAM gatekeeper[19286]: JMA 2009/02/25 15:13:45
GATEKEEPER_JM_ID 2009-02-25.15:13:45.0000019286.0000000000 has
EDG_WL_JOBID '' Feb 25 15:14:22 ce07 gridinfo[19442]: JMA 2009/02/25
15:14:22 GATEKEEPER_JM_ID 2009-02-25.15:13:45.0000019286.0000000000 JM
exiting Feb 26 12:26:32 ce07 GRAM gatekeeper[19286]: JMA 2009/02/26
12:26:32 GATEKEEPER_JM_ID 2009-02-26.12:26:32.0000019286.0000000000 has
EDG_WL_JOBID '' Feb 26 12:26:32 ce07 gridinfo[19287]: JMA 2009/02/26
12:26:32 GATEKEEPER_JM_ID 2009-02-26.12:26:32.0000019286.0000000000
for /O=dutchgrid/O=users/O=nikhef/CN=Arnold Johan van Rijn on
193.109.175.70 Feb 26 12:26:32 ce07 gridinfo[19287]: JMA 2009/02/26
12:26:32 GATEKEEPER_JM_ID 2009-02-26.12:26:32.0000019286.0000000000
mapped to atprd024 (42024, 50045) Feb 26 12:26:32 ce07 gridinfo[19287]:
JMA 2009/02/26 12:26:32 GATEKEEPER_JM_ID
2009-02-26.12:26:32.0000019286.0000000000 has GRAM_SCRIPT_JOB_ID 19302
manager type fork Feb 26 13:26:36 ce07 gridinfo[19287]: JMA 2009/02/26
```

Description	Type	Encoding	Size
Re: [T...	multipart/...	7bit	53.5 KiB
bod...	plain text ...	7bit	14.5 KiB

Security Drills / EGI

- Communication:
  - Endpoints valid?
  - Form/Content OK ?

Format / Content of the received mails



[Gridpp #45019] [THIS IS A TEST] RAL-LCG2 - Initial report on incident
Date: 02/26/09 05:18 pm
From: "Ross, D (Derek)" <derek.ross@stfc.ac.uk>
To: project-egee-security-challenge@cern.ch
CC: "Security - Gridpp" <security@gridpp.rl.ac.uk>

At 12:11 GMT we were notified that the DN /O=dutchgrid/O=users/O=nikhef/CN=Arnold Johan van Rijn was malicious.

Receipt of the notification was made at 12:21, at this point we began investigations. The user has now been blocked from all services.

As the dn was a member of the Atlas vo, the VO admins were contacted to block the user. No acknowledgement has yet been received.

Investigations on the CE discovered two job submissions on 2 seperate CEs, lcgce03.gridpp.rl.ac.uk and lcgce05.gridpp.rl.ac.uk.

The job on lcgce03.gridpp.rl.ac.uk (https://lcglb01.gridpp.rl.ac.uk:9000/gFcAXvC6Ia9T6YHOoLUsbw/) was submitted to our batch system at 10:39 with job id 1235644756 and reported finished at 10:44.

The job on lcgce05.gridpp.rl.ac.uk (https://lcglb01.gridpp.rl.ac.uk:9000/43BLskiceao6E1JtU6Ifhw/) was submitted to our batch system at 11:00 with job id 12616466 but was still running at the time of

Security Drills / EGI

- Communication:
  - Endpoints valid?
  - Form/Content OK ?
- Containment
  - Ban ”malicious” users
  - Find/Stop malicious processes
  - Find submission IP

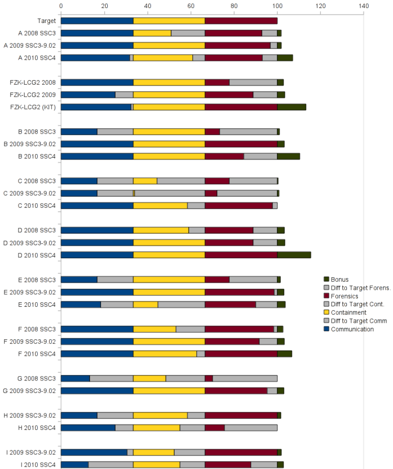
- Access Control
- X.509 based Authentication
- Definitive access control at the sites. (DN in Textfiles)
- User-certificate information gets mapped to a unix account

Security Drills / EGI

- Communication:
  - Endpoints valid?
  - Form/Content OK ?
- Containment
  - Ban ”malicious” users
  - Find/Stop malicious processes
  - Find submission IP
- Forensics
  - Basic Forensics on Binary
  - Network traffic

Security Drills / EGI

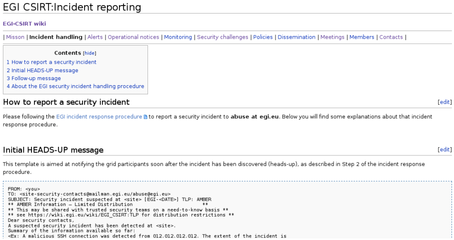
- Communication:
  - Endpoints valid?
  - Form/Content OK ?
- Containment
  - Ban ”malicious” users
  - Find/Stop malicious processes
  - Find submission IP
- Forensics
  - Basic Forensics on Binary
  - Network traffic



Sites got Supporting Material

Lessons Learned, Supporting material provided by EGI-CSIRT to the sites.

- Communication Templates



EGI CSIRT:Incident reporting

EGI-CSIRT wiki

| Misson | **Incident handling** | Alerts | Operational notices | Monitoring | Security challenges | Policies | Dissemination | Meetings | Members | Contacts |

Contents [hide]

How to report a security incident [edit]

Please following the EGI incident response procedure to report a security incident to **abuse at egi.eu**. Below you will find some explanations about that incident response procedure.

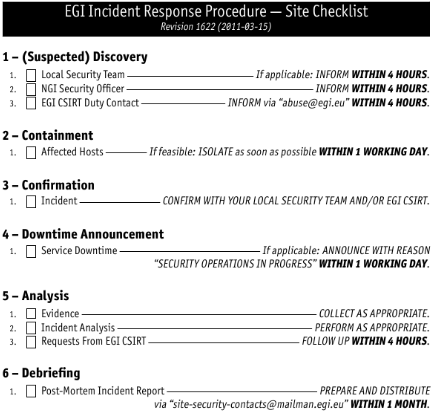
Initial HEADS-UP message [edit]

This template is aimed at notifying the grid participants soon after the incident has been discovered (heads-up), as described in Step 2 of the incident response procedure.

```
FROM: <you>
TO: <site-security-contacts@mailman.egi.eu/abuse@egi.eu>
SUBJECT: Security incident suspected at <site> [EGI-<DATE>] TLP: AMBER
** AMBER Information – Limited Distribution                        **
** This may be shared with trusted security teams on a need-to-know basis **
** see https://wiki.egi.eu/wiki/EGI_CSIRT:TLP for distribution restrictions **
Dear security contacts,
A suspected security incident has been detected at <site>.
Summary of the information available so far:
<Ex: A malicious SSH connection was detected from 012.012.012.012. The extent of the incident is
```

Sites got Supporting Material

- Communication Templates
- Generic Incidence Response Procedure



EGI Incident Response Procedure — Site Checklist

Revision 1622 (2011-03-15)

1 – (Suspected) Discovery

1. □ Local Security Team ——— *If applicable: INFORM* ***WITHIN 4 HOURS***.
2. □ NGI Security Officer ——— *INFORM* ***WITHIN 4 HOURS***.
3. □ EGI CSIRT Duty Contact ——— *INFORM via "abuse@egi.eu"* ***WITHIN 4 HOURS***.

2 – Containment

1. □ Affected Hosts ——— *If feasible: ISOLATE as soon as possible* ***WITHIN 1 WORKING DAY***.

3 – Confirmation

1. □ Incident ——— *CONFIRM WITH YOUR LOCAL SECURITY TEAM AND/OR EGI CSIRT.*

4 – Downtime Announcement

1. □ Service Downtime ——— *If applicable: ANNOUNCE WITH REASON "SECURITY OPERATIONS IN PROGRESS"* ***WITHIN 1 WORKING DAY***.

5 – Analysis

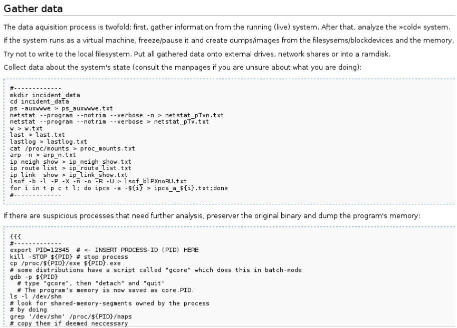
1. □ Evidence ——— *COLLECT AS APPROPRIATE.*
2. □ Incident Analysis ——— *PERFORM AS APPROPRIATE.*
3. □ Requests From EGI CSIRT ——— *FOLLOW UP* ***WITHIN 4 HOURS***.

6 – Debriefing

1. □ Post-Mortem Incident Report ——— *PREPARE AND DISTRIBUTE via "site-security-contacts@mailman.egi.eu"* ***WITHIN 1 MONTH***.

Sites got Supporting Material

- Communication Templates
- Generic Incidence Response Procedure
- Forensics guidelines



Gather data

The data aquisition process is twofold: first, gather information from the running (live) system. After that, analyze the »cold« system.

If the system runs as a virtual machine, freeze/pause it and create dumps/images from the filesysems/blockdevices and the memory.

Try not to write to the local filesystem. Put all gathered data onto external drives, network shares or into a ramdisk.

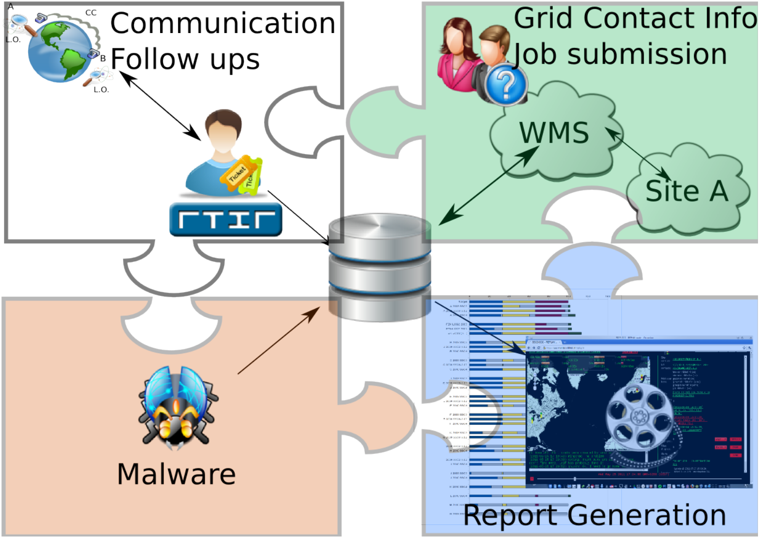
Collect data about the system's state (consult the manpages if you are unsure about what you are doing):

```
#-------------
mkdir incident_data
cd incident_data
ps -auxwwwe > ps_auxwwwe.txt
netstat --program --notrim --verbose -n > netstat_pTvn.txt
netstat --program --notrim --verbose > netstat_pTv.txt
w > w.txt
last > last.txt
lastlog > lastlog.txt
cat /proc/mounts > proc_mounts.txt
arp -n > arp_n.txt
ip neigh show > ip_neigh_show.txt
ip route list > ip_route_list.txt
ip link  show > ip_link_show.txt
lsof -b -l -P -X -n -o -R -U > lsof_blPXnoRU.txt
for i in t p c t l; do ipcs -a -${i} > ipcs_a_${i}.txt;done
#-------------
```

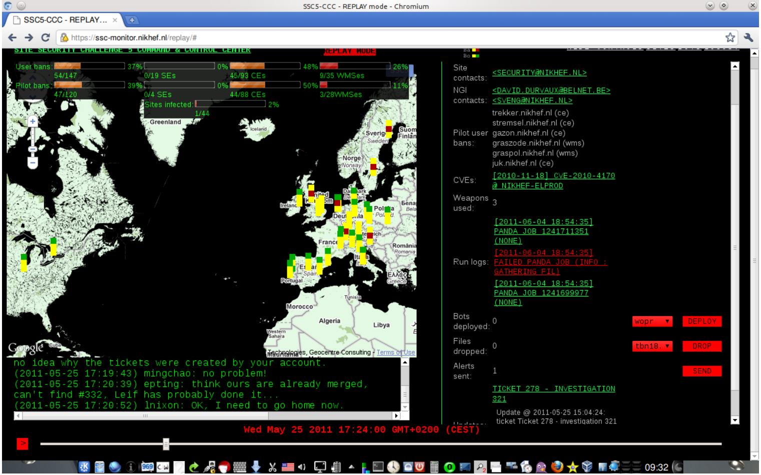
If there are suspicious processes that need further analysis, preserver the original binary and dump the program's memory:

```
{{{
#-------------
export PID=12345  # <- INSERT PROCESS-ID (PID) HERE
kill -STOP ${PID} # stop process
cp /proc/${PID}/exe ${PID}.exe
# some distributions have a script called "gcore" which does this in batch-mode
gdb -p ${PID}
  # type "gcore", then "detach" and "quit"
  # The program's memory is now saved as core.PID.
ls -l /dev/shm
# look for shared-memory-segments owned by the process
# by doing
grep '/dev/shm' /proc/${PID}/maps
# copy them if deemed neccessary
```

SSC-Monitor Components



SSC-Monitor Components



SSC5-CCC - REPLAY mode - Chromium
SSC5-CCC - REPLAY...
https://ssc-monitor.nikhef.nl/replay/#

SITE SECURITY CHALLENGE 5 COMMAND & CONTROL CENTER

REPLAY MODE

User bans: 37% 54/147 | 0% 0/19 SEs | 48% 45/93 CEs | 26% 9/35 WMSes

Pilot bans: 39% 47/120 | 0% 0/4 SEs | 50% 44/88 CEs | 11% 3/28WMSes

Sites infected: 2% 1/44

```
no idea why the tickets were created by your account.
(2011-05-25 17:19:43) mingchao: no problem!
(2011-05-25 17:20:39) epting: think ours are already merged,
can't find #332, Leif has probably done it...
(2011-05-25 17:20:52) lnixon: OK, I need to go home now.
```

Site contacts: <SECURITY@NIKHEF.NL>

NGI contacts: <DAVID.DURVAUX@BELNET.BE> <SVENG@NIKHEF.NL>

Pilot user bans:
trekker.nikhef.nl (ce)
stremsel.nikhef.nl (ce)
gazon.nikhef.nl (ce)
graszode.nikhef.nl (wms)
graspol.nikhef.nl (wms)
juk.nikhef.nl (ce)

CVEs: [2010-11-18] CVE-2010-4170 @ NIKHEF-ELPROD

Weapons used: 3

Run logs:
[2011-06-04 18:54:35] PANDA JOB 1241711351 (NONE)
[2011-06-04 18:54:35] FAILED PANDA JOB (INFO : GATHERING FIL)
[2011-06-04 18:54:35] PANDA JOB 1241699977 (NONE)

Bots deployed: 0 — wopr ▾ DEPLOY

Files dropped: 0 — tbn18. ▾ DROP

Alerts sent: 1 — SEND

TICKET 278 - INVESTIGATION 321

Update @ 2011-05-25 15:04:24:
ticket Ticket 278 - investigation 321

Wed May 25 2011 17:24:00 GMT+0200 (CEST)

SSC-Monitor Components

- SSC in FedCloud: What would be important for you to look at?
- Who would be willing to collaborate on a scenario
- Who would be willing to collaborate on a **” image ”**