Security operations

Sven Gabriel, Nikhef, EGI CSIRT

June 2022

Security operations

Sven Gabriel, Nikhef, EGI CSIRT

June 2022

Overview

Some aspects of Operational Security

CSIRT Organisation and provided Services

Drivers for CSIRT Evolution

Security Operations

Lessons learned from Incidents

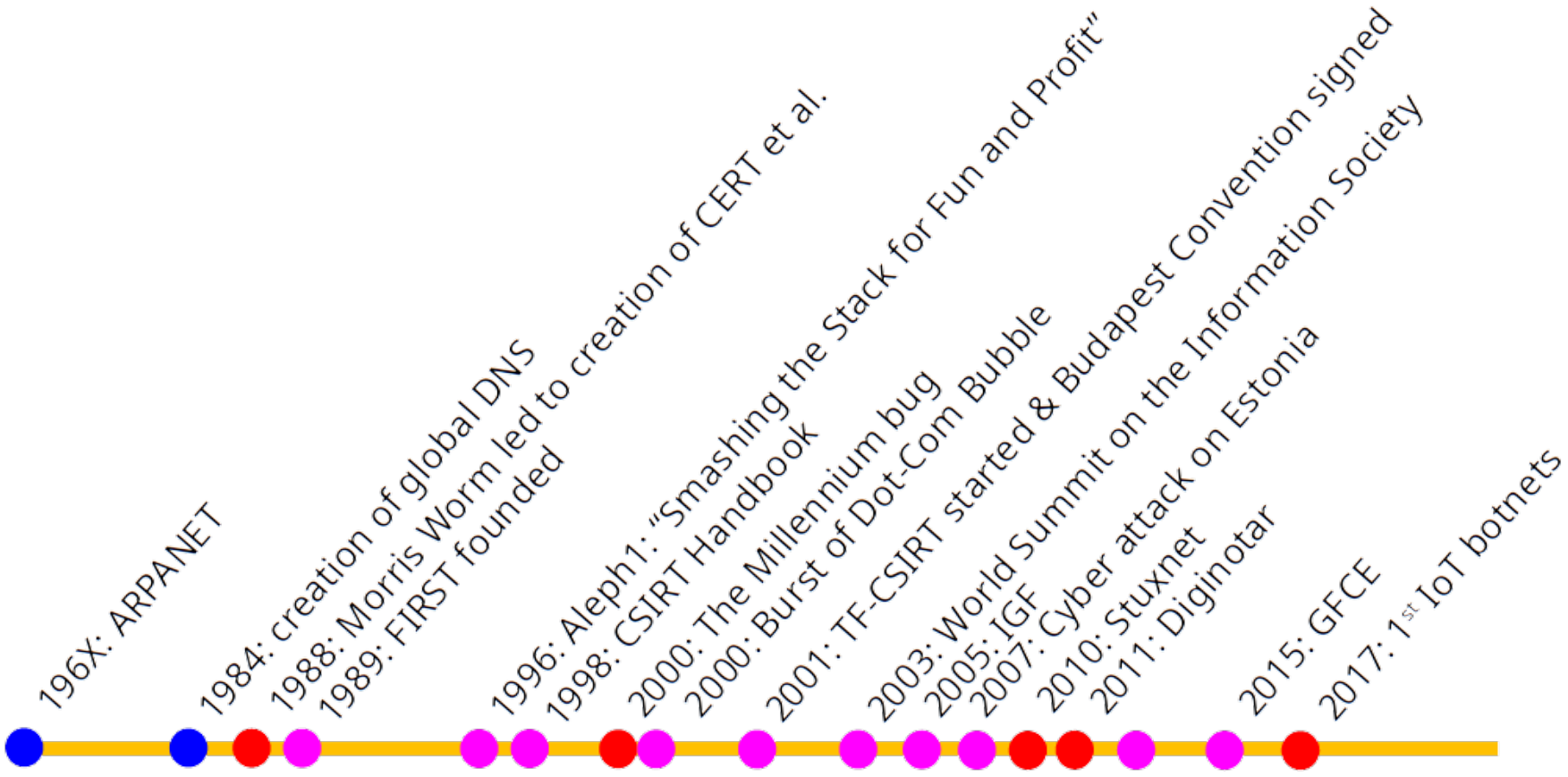
- Attack on EGI Conflence
- Highly Sensitive Incidents
- Maastricht University Ransom attack
- Security exercises

Some aspects of Operational Security

Reliable Systems

- Threat to reliability (availability).
  - Bad software update
  - Hardware failures
  - Issues tracked with a Ticket-System
- Threat to security
  - Vulnerabilities
  - Adversary actively exploiting the system, affecting CIA triad.
  - Issues tracked with a Ticket-System (the same as above?)

Security Teams, . . . a look back [1]



[1] Timeline courtesy FIRST

additional "entertaining" reads

- https://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg_(book)
- https://en.wikipedia.org/wiki/23_(film)
- https://www.youtube.com/watch?v=fj8S6Hd-5bk

Security Teams and Incident Management

Terminology:

- CERT: Computer Emergency Response Team
  - Origin 1988, later trademarked
  - CERT Coordination Center (CERT/CC)
  - Permission to use: http://www.sei.cmu.edu/legal/permission/index.cfm
- CSIRT: Computer Security Incident Response Team
  - Origin 1998: http://www.cert.org/archive/pdf/csirt-handbook.pdf
  - Free to use !
- IHT, SIRT, CIRT, IHC, SOC (a story in itself), etc. etc.

CSIRT Organisation and provided Services

CSIRT Management

Managerial and technical aspects of CSIRT Management are topics in TRANSITS I trainings.

- Organisational and Technical module are half day courses.
- check https://tf-csirt.org/transits/transits-events/transits-i/
- Here we will cover just a subset of the topics.

CSIRT Services I

The services a CSIRT should provide and the needed tooling depends on the mandate of the CSIRT, examples.

- Coordinating CSIRT
  - eduGAIN CSIRT, needs a communication infrastructure to coordinate incident response activities among the participants (see Hannahs talk)
  - EGI CSIRT, coordinating security activities for EGI. In addition to the communications infra, + a lot more
- Organisation/Company CSIRT
  - Constituency is defined easier.
  - Stronger mandate, organisation can more easily decide on policies.

Talking to a CSIRT

Trust, Transparency, What to expect from a CSIRT $\rightarrow$

- RFC-2350.
- TermsOfReference (TOR): Mandate/Authority given to the CSIRT, Responsibilities of the CSIRT.
- Responsible disclosure: RFC-9116 (security.txt).

CSIRT Services revisited, EGI

- Incident Management (tested and maintained Communications infra)
- Forensics support (malware analysis)
- Vulnerability Management (separate talk)
- Trainings (see Intro to forensics)
- Intel sharing, WLCG-SOC (more in the SOC session)
- Security Challenges (sort of pentests, rather an assessment of the security situation).

CSIRT Communities

- Now, that you have a CSIRT with a mandate, public contact info for reporting security issues, you now would need to collaborate with other CSIRTs. For example participating in:
- TF-CSIRT https://tf-csirt.org/
- FIRST https://www.first.org/
- Sectoral Communities (PSIRTs, Critical Infra, National CSIRTs, etc)
- Trust Groups (based on personal peer-to-peer trust relations)

Drivers for CSIRT Evolution

CSIRT Evolution

Drivers for Security Initiatives:

- (External, or self) Audit of the security framework (ISO 27k, SIM3i[2])
- Compliance: Information Security regulations have to be met, for example in call for tenders [3]
- Risk Management (see later talk)

[2] https://opencsirt.org/csirt-maturity/sim3-and-references/

[3] https://www.surf.nl/en/stitch-a-short-checklist-for-application-security

Assessment of Incident Response readiness

Layout:

- Realistic Simulation of an Incident involving CSIRTS at 40 sites in 20 countries and a VO
- Malware (Bot-Net) was deployed with help of a VO-Job-Submission Framework
- Alerts have been sent out to 2 affected sites

Assessment of Incident Response readiness

Targets/Expected Results:

- Project wide incident response capabilities.
- Trigger ad hoc Collaboration (EGI-CSIRT, VO-CSIRTS, CAs, ...).
- How long does it take to get the incident contained?
- Efficiency of security operations?
- Effects on the resource availability?
- Operational Problems in Incident Handling?
- Identify Experts: Forensics, Network-Analysis
- Assessment of tools used

Security Operations

Incident Response, get prepared

- Have your Infra ready. Network segmentation. Can you find and isolate systems on your network, can you act on any user account. Can you trace activities (on systems and network) back to accounts.

Incident Response, get prepared

- Security Monitoring, do you have a baseline of normal system behaviour? Do you monitor the patch status of your systems?
- Have your Infra ready. Network segmentation. Can you find and isolate systems on your network, can you act on any user account. Can you trace activities (on systems and network) back to accounts.

Incident Response, get prepared

- Have your communications ready (users, management, legal, press). Update stakeholders frequently. (Crisis communication as a course in itself, you would need to deal with social media.)
- Security Monitoring, do you have a baseline of normal system behaviour? Do you monitor the patch status of your systems?
- Have your Infra ready. Network segmentation. Can you find and isolate systems on your network, can you act on any user account. Can you trace activities (on systems and network) back to accounts.

Incident Response, prepare to fail

- Every Incident Response is challenging your CSIRT set-up, **Use Them!**
- You will find weak points in:
  - Tooling (Communication Infra (ticket system etc) and all other services you provide.
  - Policies
  - Procedures
- All the above are subject to constant review and development, start from a decent environment and evolve.

Lessons learned from Incidents

Examples why to prepare to fail

The incidents and Security Challenges discussed in this section are not limited to incidents handled by EGI CSIRT. i

- Attack on EGI Confluence . . . and then the documentation and mail infra went dark
- . . . and then the other end got silent
- Crypto Currency mining using grid technology . . . and then an insider thought he could smart out the forensics team.

Subsection 1

Attack on EGI Conflence

EGI-20190411-01

To understand the impact of this incident better, lets look at the services EGI CSIRTs Incident Response Task Force uses:

- Mail: Communication to Resource Centres
- Ticket system: RT-IR
- Private Wiki

Atlassian Confluence attack

- March 20^{th}: Critical vulnerability published
- Week of April 8^{th}: Multiple Confluence attacks: EGI and at least two close organizations affected
- At least two confirmed different attackers:
  - One had the exact same methodology as Jenkins

$\rightarrow$ Wide-scale successful attack within 3 weeks!

EGI services compromise
Timeline (April 2019)

- 4^{th}: Very first attempt to use the vulnerability
- 8^{th} afternoon: First confirmed attack
- 9^{th} and 10^{th}: Further attack activities
- 10^{th} lunch time: Attack detected
  - Malicious processes quickly isolated
- 10^{th} evening: Vulnerability patched
- 17^{th}: Servers rolled-back to safe backup

EGI services compromise

Impact

- Confluence co-hosted with various services
  $\rightarrow$ all co-hosted services affected
- Forensics analysis shows no sign of data exfiltration
- LDAP service not hosted on same service
  - LDAP passwords (hashed) not directly affected
  - Password of users who logged in on services with password potentially leaked (but no evidence)
- Forceful backup roll-back to safe backup
  - Data from April 3^{rd} to 17^{th} initially *lost*
  - Ongoing efforts to re-inject all data

Who is actually handling this incident?

- EGI CSIRT provides Operational Security for the Grid Sites in goc-db
- EGI CSIRT relies on services operated in EGI Back-Office
- A good example for legacy infra (10 years). Admin task was handed over multiple times, Experience, documentation lost. The last one who took this job had the hot potato, and some sleepless nights.
- Unclear responsibilities, who handles the incident, now sorted.
- Secure system operation will be discussed later this week.
- Risk Assessment: the risk from this set up would probably not been accepted.

Always have a fallback

- Standard communications were not available.
- Have multiple alternatives (IM like signal, keybase, mattermost) for trusted team communications.
- Collaboration tools not available (Wiki)
- Here we could move to gitlab (hosted elsewhere)
- Don't have all eggs in one basket

Subsection 2

Highly Sensitive Incidents

No slides here

Intentionally left blank

Subsection 3

Maastricht University Ransom attack

Uni Maastricht, Ransom Attackd

- Uni Maastricht was very open about the incident
- 2h of public(recorded (in Dutch)) debriefing Youtube https://www.youtube.com/watch?v=ik-ZVvZ2-xU, here also payment of ransom is discussed! including the process on how to pay via bitcoin, proof that data can be decrypted.
- FOX-IT called in for support.
- Debriefing also has a report from FOX-IT including how they organised Incident Response, and what actions the victim should take to prevent future incidents. https://www.maastrichtuniversity.nl/file/49750/download?token=cT_19j-W

How it began . . .

- Night 23rd - 24th Dec. 2019 Uni Maastricht calls FOX IT.
- Intrusion (via phishing) happend on Oct. 15, various activities of the attackers could be reconstructed.
- Some Servers not reachable because of an ransomware attack.
- On 24th Dec 16:00 FOX IT starts assisting in the incident response process.
- 1st Phase support of Crisis management, start forensic investigation, goal: find out how the attack was done.

Uni Giessen, Response and Media attention

Bei der Ausgabe der neuen Passwörter kommt es zum Teil zu langen Schlangen. FOTO: LKL © Lena Karber

. . . oh, and is the response really targeted/balanced? [4] [5]

[4] https://www.degruyter.com/document/doi/10.1515/abitech-2022-0005/html

[5] https://www.bbc.com/news/technology-50838673

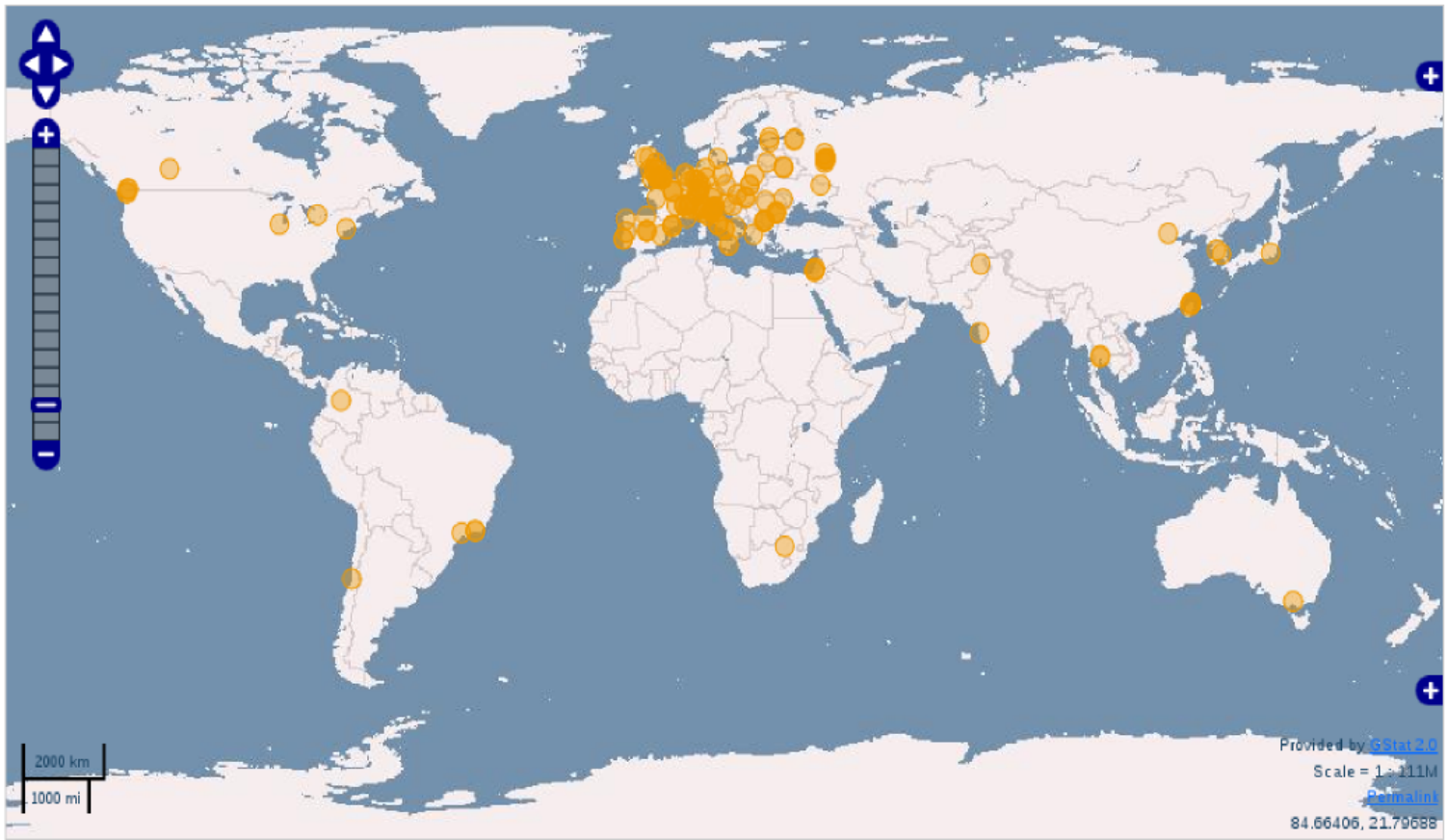
Subsection 4

Security exercises

Results from earlier exercises

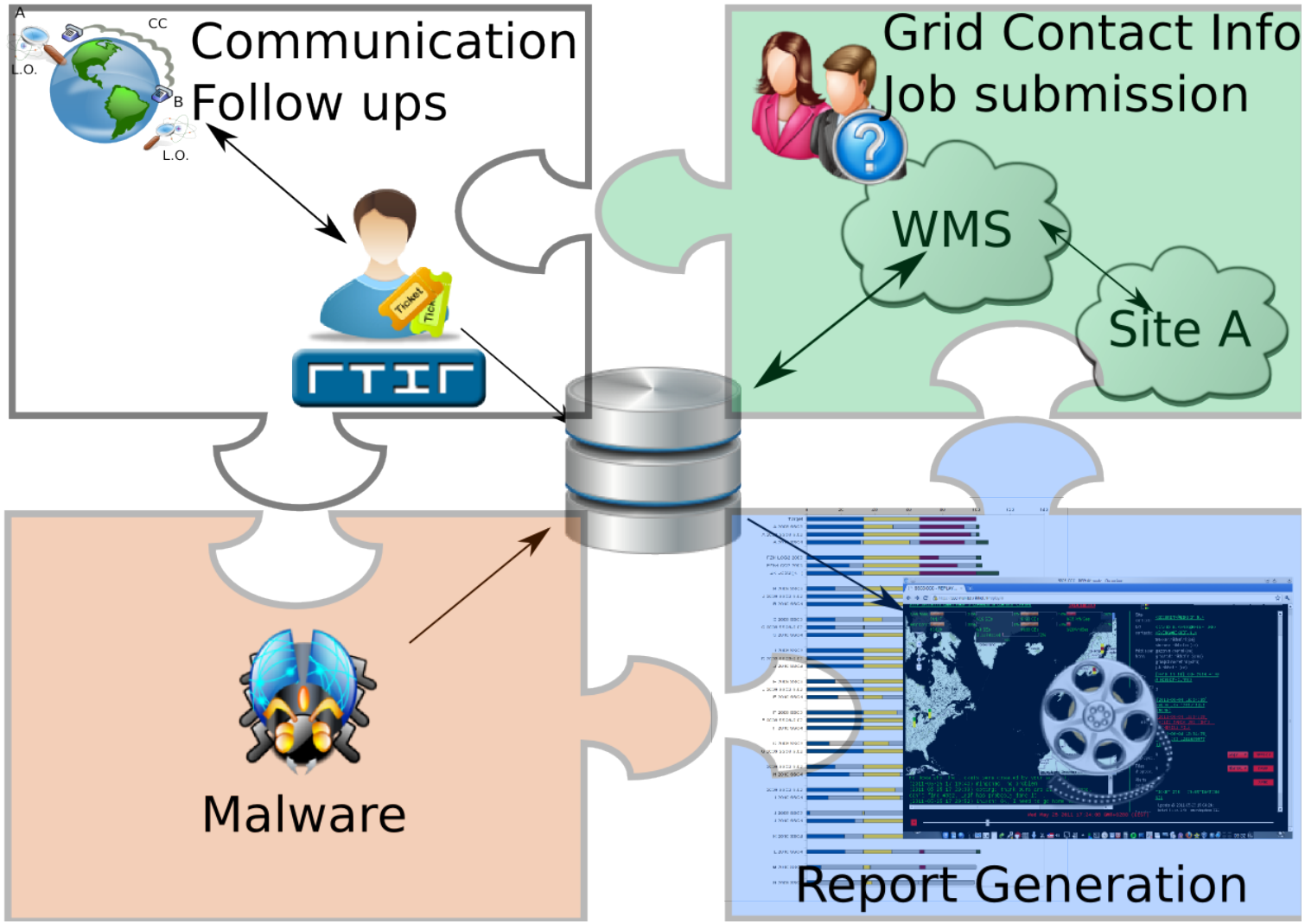
- Outdated contact data → Run Communication Challenges
- Poor quality of report's → Provide Communication templates
- Slow responses → Response times covered in Incident Response procedures
- Insufficient knowledge in forensics → Provide Instructions, Trainings

Exercise playground: EGI (2011)



Exercise playground: EGI (2011)

Assessment Framework Components



48h IR in 5min

Demo Movie 48h of incident response in 5 minutes

Results

- Response time improved (within procedure boundaries).
- Quality of reports improved.e
- Completeness and Format of the reports improved.

Mail: E Ryabinkin

It turns out that ATLAS Pilot framework
us a malicious Grid jobs that initiated IR
able to run the commands that are give
wunderbar.geenstijl.de:35443.

It turns out that the following list of sit
this bot too:
{{{
Bot sits at eio64.weizmann.ac.il (192.114
Bot sits at 193.109.175.80 ([unknown])
Bot sits at lap-210.nikhef.nl (192.16.192.
Bot sits at td044.pic.es (193.109.173.44)
Bot sits at wn-204-11-33-01-b.cr.cnaf.inf
Bot sits at eio64.weizmann.ac.il (192.114
}}}
I am attaching bot detection script; you
in order to run it.