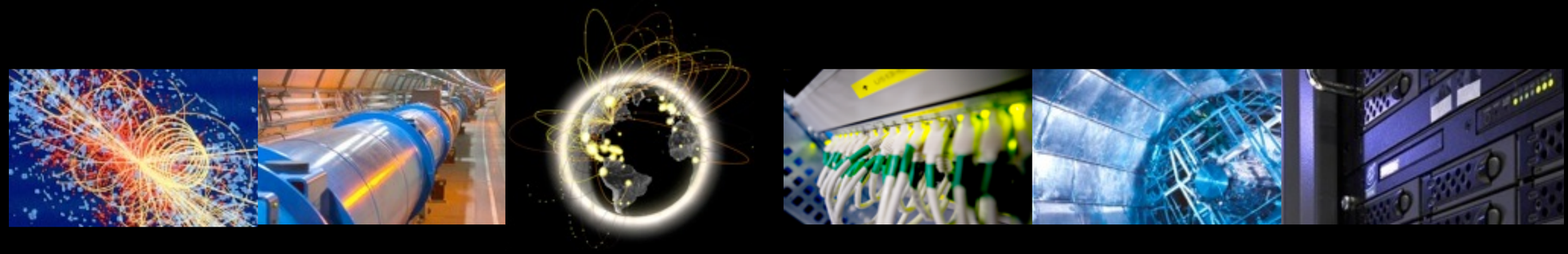
OSG-EGI Security drill

Romain Wartel, 11 March 2020



WLCG
Worldwide LHC Computing Grid

Background

- HOW2019: “Addressing the OSG - EGI security cooperation issues”
  - https://indico.cern.ch/event/759388/contributions/3324318/
  - “Collaboration between OSG and EGI security teams is too weak”

- Both teams physically met at CERN in Q4 2019:
  - Organise a “security drill” as a trust building exercise and situation review
  - Test the cooperation between both teams
  - Teams elected to choose Signal as a joint communication channel

- Scope of the security drill limited to:
  - EGI: CERN, STFC, NIKHEF
  - OSG: FNAL, IU

Statement

Additional caveats from the “Game Master” WLCG Security Officer

The drill was badly designed and poor communication was used to prepare, announce and run the exercise.

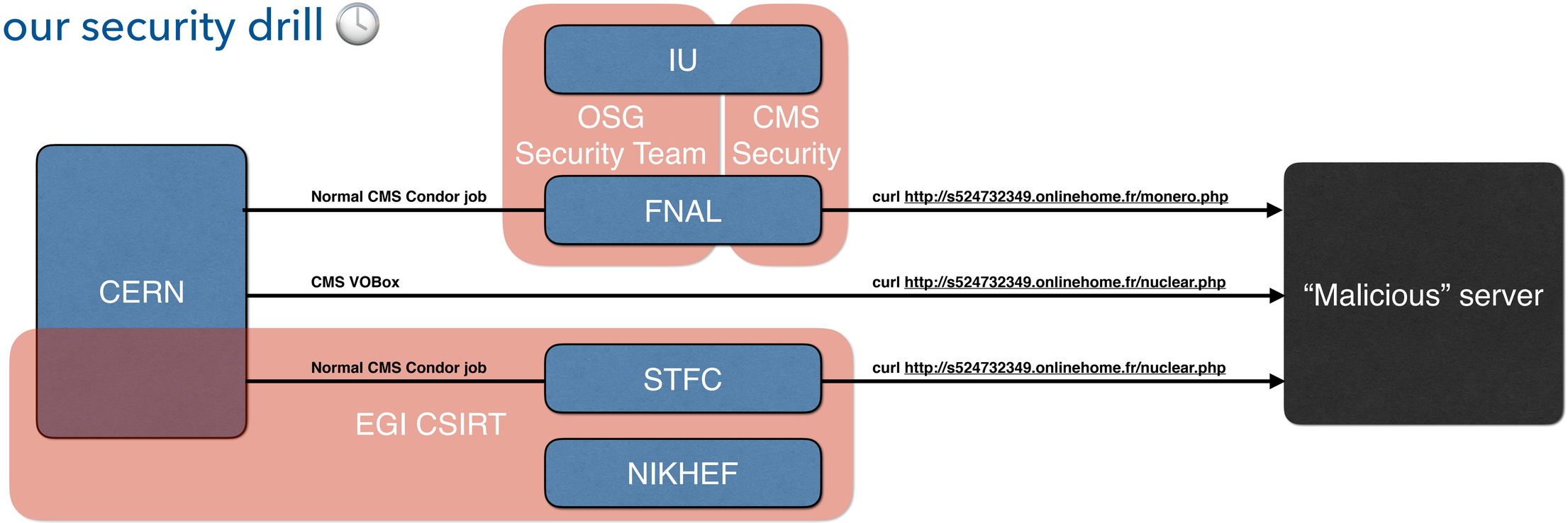
The initial triggers were misleading, the scope unclear and guidance of the so-called “game-master” was of no help throughout the challenge.

In fact, under no circumstance the drill would represent a credible intrusion scenario, and the organiser set unrealistic expectations on both teams and unhealthy amounts of effort to prevent them to solve the challenge.

Actions from all involved teams were adequate, timely and according to procedure – Any deviation would complete misinterpretation of the data.

Preparation

- 4-hour security drill 🕓

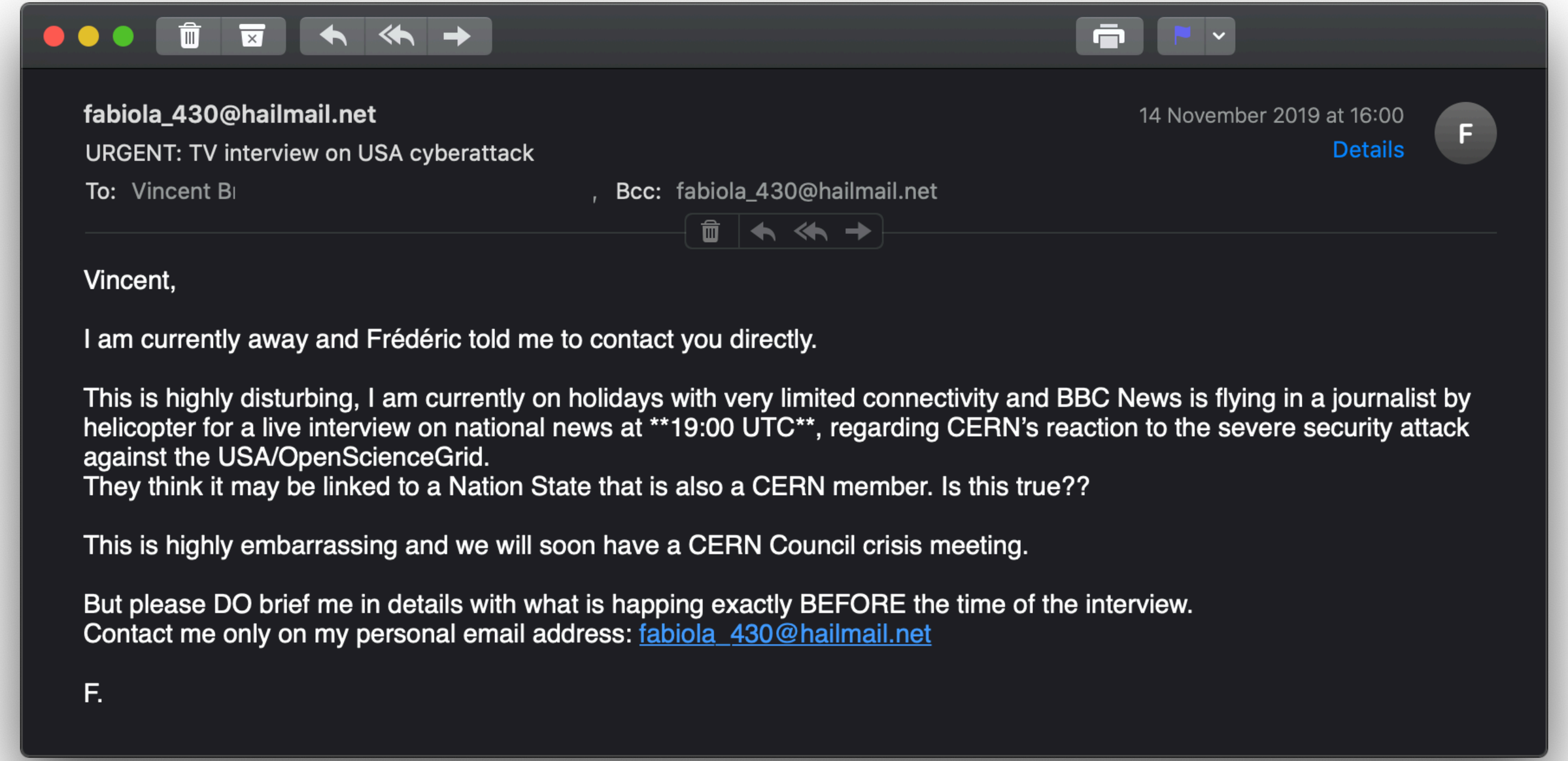


- Goals:
  - *Investigate both the extent and the likely source (attribution) of a possible attack, within the realm of the organizations represented in the exercise*
- Drill is based on real attacks that affected WLCG resources providers
  - No identity blocking: this is a EGI CSIRT - OSG Security Team communication exercise

Drill objectives

- Network traceability
  - The two “malicious” jobs perform a single, trivial task: download a text file over HTTP
  - This should provide a highly visible network trace
- Job traceability
  - The two “malicious” jobs are standard CMS condor jobs and should provide a highly visible log trace
  - Leading to the identity of the job submitter
    (The same CMS identity has been used for both jobs)
- Investigative skills and communication
  - The content of the downloaded files enable the OSG and EGI investigator to uncover additional evidence.
  - Upon sharing information, infer the root cause of the simulated intrusion

EGI CSIRT…Go !



fabiola_430@hailmail.net

14 November 2019 at 16:00

Details

URGENT: TV interview on USA cyberattack

To: Vincent B , Bcc: fabiola_430@hailmail.net

Vincent,

I am currently away and Frédéric told me to contact you directly.

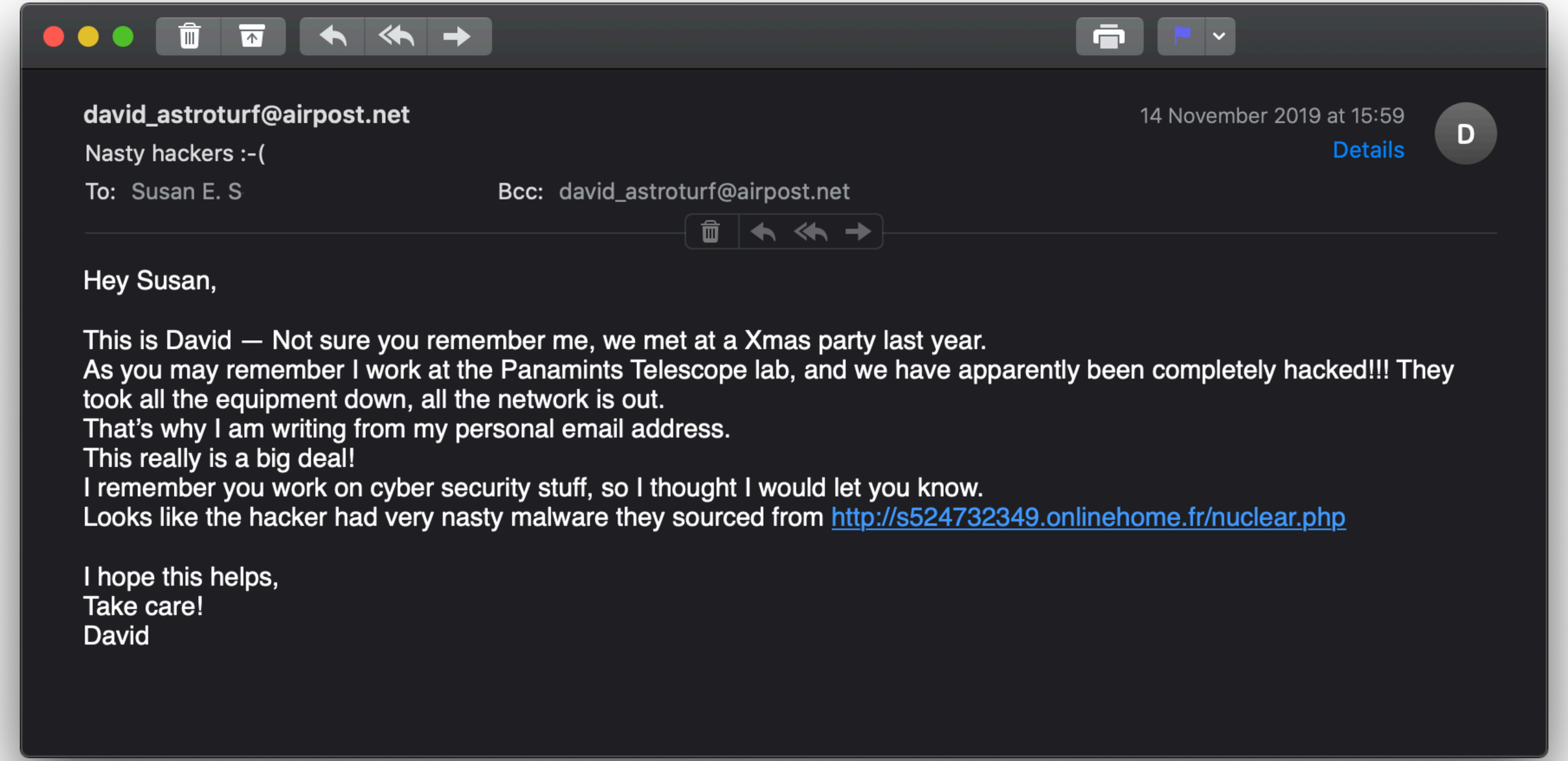
This is highly disturbing, I am currently on holidays with very limited connectivity and BBC News is flying in a journalist by helicopter for a live interview on national news at **19:00 UTC**, regarding CERN's reaction to the severe security attack against the USA/OpenScienceGrid.
They think it may be linked to a Nation State that is also a CERN member. Is this true??

This is highly embarrassing and we will soon have a CERN Council crisis meeting.

But please DO brief me in details with what is happing exactly BEFORE the time of the interview.
Contact me only on my personal email address: fabiola_430@hailmail.net

F.

OSG Security Team…Go !



david_astroturf@airpost.net

14 November 2019 at 15:59

Details

D

Nasty hackers :-(

To: Susan E. S

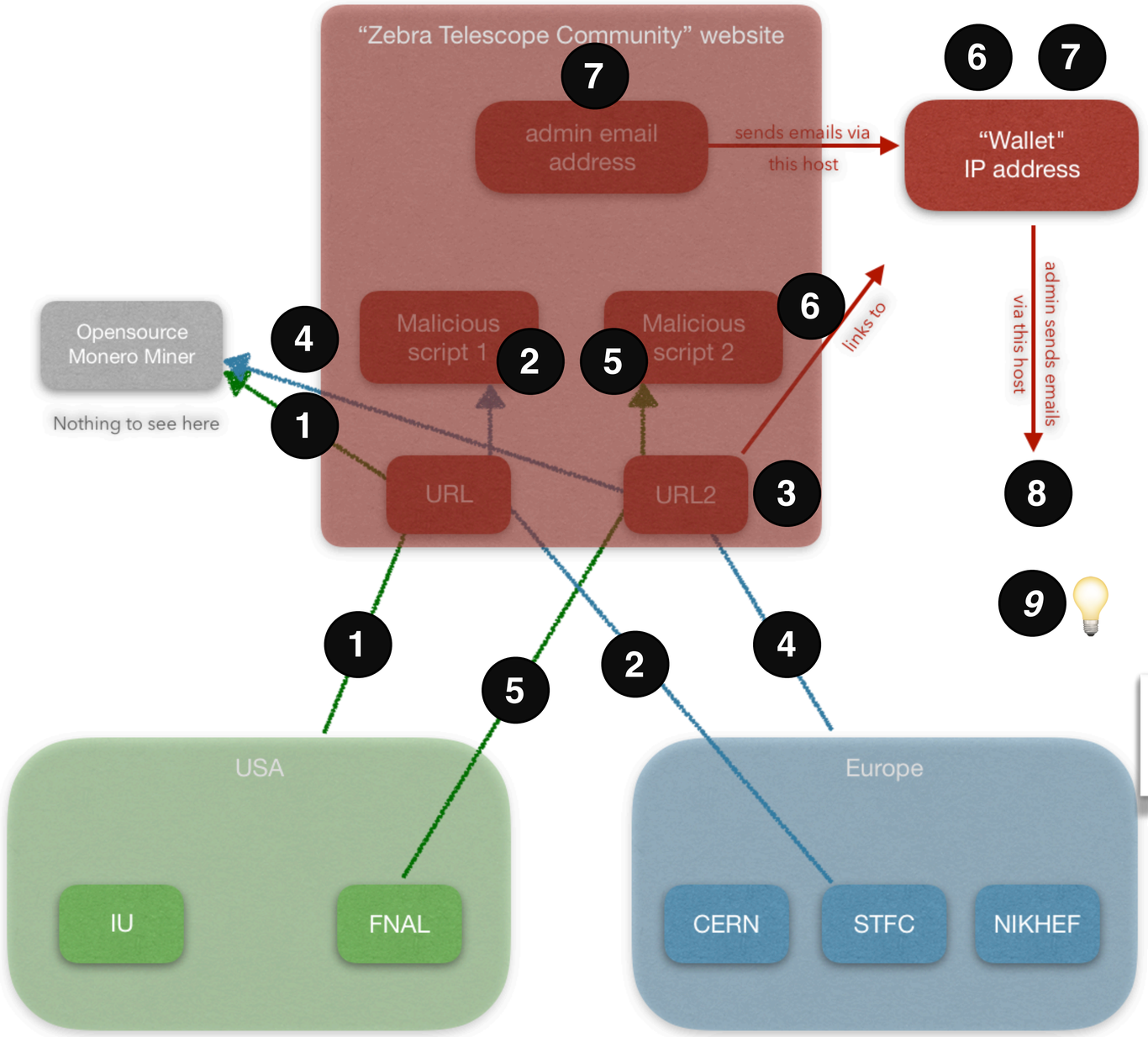
Bcc: david_astroturf@airpost.net

Hey Susan,

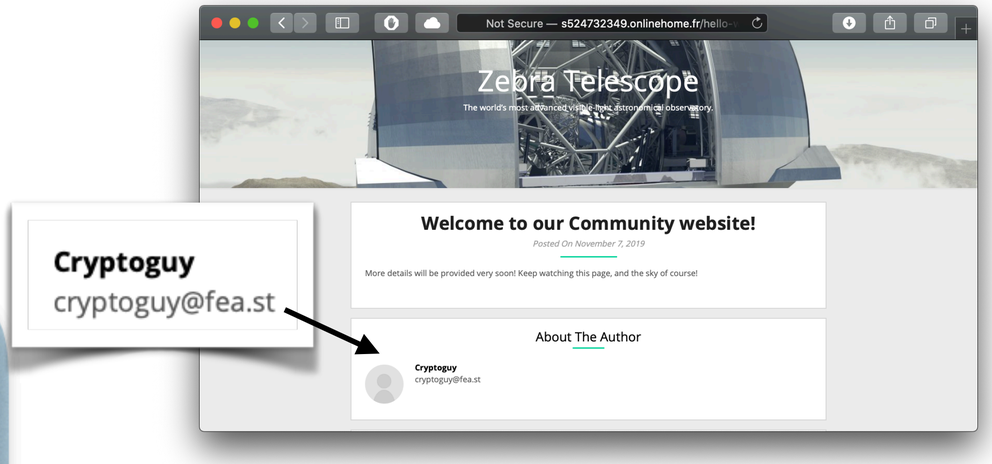
This is David — Not sure you remember me, we met at a Xmas party last year.
As you may remember I work at the Panamints Telescope lab, and we have apparently been completely hacked!!! They took all the equipment down, all the network is out.
That's why I am writing from my personal email address.
This really is a big deal!
I remember you work on cyber security stuff, so I thought I would let you know.
Looks like the hacker had very nasty malware they sourced from http://s524732349.onlinehome.fr/nuclear.php

I hope this helps,
Take care!
David

Cooperation is paramount



1. **URL** given to OSG points to OSS *from the US*…
2. But *from the EU*… **URL** points to **Script 1**
   STFC should find this too in their logs
3. **Script 1** reveals a message and new **URL2**
4. If accessed *from the EU*, **URL2** points to OSS…
5. But *from the US*, like at FNAL, **URL2** points to **Script 2**
6. **Script 2** reveals a new "**Wallet IP**"
7. Meanwhile, the website yields an email address:



8. If contacted, an reply will be sent from "**Wallet IP**"
9. *Sec teams should suspect the attack is about crypto, and attacker is behind the email address*

Overall results

- Both teams: excellent technical skills
  - Operate very well within the incident response procedures in their respective e-infras
  - OSG in particular was very quick to investigate the attacker infrastructure and tools

- However, despite the challenge being extend from 4 hours to 7 days:
  - EGI/STFC was unable to track the malicious job (detection took 3 days)
  - OSG/FNAL did not detect the malicious HTTP download or track the related job
  - CMS did not manage to track down the jobID or user DN of the malicious job at FNAL (based on a malicious URL)
  - CMS did not manage to track down the jobID or user DN of the malicious job at STFC (based on malicious URL, timestamps, and WN details)
  - The investigation stalled with no conclusion regarding the source or nature of the attack

Leading causes of failure

- No EGI-OSG central incident response coordination
  - No goals definition and tasks sharing, status synchronisation or assigned roles in the investigation, and incomplete information sharing
- This lead to incorrect assumptions, erroneous actions by involved participants and victims, massively increased delays, poor operational security practices, and eventually failure to resolve the case (both on the victims and attacker side)
- Interesting facts as example:
  - 2 hours in the challenge, number of downloads for Script 1:
    - **27** times by OSG (including 9 from non-anonimized IU IP addresses)
    - **0** by EGI
  - Nobody contacted the Zebra telescope website owner, where the malware was hosted
  - Time needed to ask the other team about their original notification and a summary of their technical findings: 3h for OSG, 2 days for EGI
  - EGI stopped using Signal and fell back to Keybase after 4 min in the challenge

Human factor

- The “human factor” played a crucial role thorough the incident

- The lack of coordination, communication and leadership is a natural phenomenon and the reason security drills are conducted
  - These central tasks are everybody’s job, which effectively means nobody’s job
  - All participants were working under pressure with limited information and could assume that they thought someone would take care of the the group responsibility

- Vital lessons to be learnt here to reveal the full potential of our security experts
  - Goal: achieve a truly global successful incident response

Recommendations

- Define a joint incident response workflow or model
  - to ensure roles, leadership and expectations on each team are explicitly defined
- Better access to traceability information (logs, etc.) at the sites
  - Gap between “grid" and campus security teams crippled OSG/EGI’s capabilities
- Face-to-face and virtual team meetings
  - Improve the cooperation between the teams, building trust, etc.
- Defined, practical communication channels
  - Ensure smooth and direct communication between team members (Signal did not work)
- Collaborative tool(s) to jointly investigate and share a live “view” or dashboard
  - Allow clear and immediate communication, respective current status, etc.
- Cross-membership of the teams
  - Ensure a better information flow, cooperation and trust
- Dynamic sharing of indicators of compromise using industry-standard tools (MISP)

Conclusion

- Collaboration is not easy!
- OSG and EGI security teams, as well as CMS, have indisputable technical skills
- But jointly, they failed to:
  - Track a trivial HTTP malicious download
  - Identify the related grid job and user DN
- The affected sites were both very experienced and playing a key role in CMS, EGI, and OSG's respective e-infrastructure security teams
- Both teams are supportive of improving the situation and taking necessary steps
  - Stay tuned for a follow up presentation