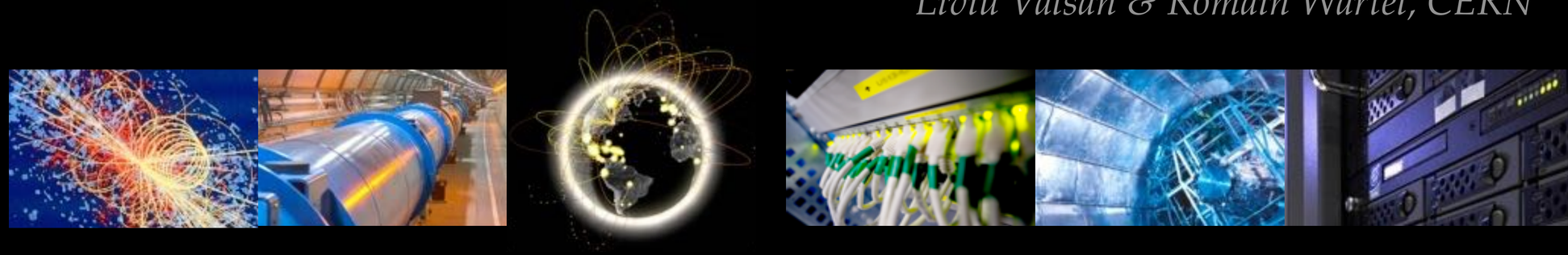
Facilitating campus and grid security teams working on the same threats

Liviu Valsan & Romain Wartel, CERN



WLCG Worldwide LHC Computing Grid

…Continued from the WLCG workshop

- Academia is a viable market for cybercriminals
  - Ransomware, finance fraud, etc.
  - Actors have started specifically targeting Research & Education
  - Some attacks are no longer opportunistic
- Nation-states target us as well and use similar infection vectors
- In the past, attackers would mostly target Linux/SSH/etc.
  - However, the next major grid disaster may come from an email to the site administrator
- Crucial to closely cooperate or merge operations
- Complementary strengths:
  - Campus has controls and monitoring in place
  - Science / cloud has a strong community + indicators of compromise
  - Both have limited efforts!

…But how?

- Teams are already busy with “other things”
- Highlighting new threats is seen as creating extra work
- Level of maturity is a critical aspect
  - Better response from exposed or well connected partners
- Pushing for something people do not want will fail

Ways forward

- Lots of relevant data within the WLCG collaboration
  - Engage in discussions with campus, share experience from WLCG
  - Explore existing threat intelligence in the CERN MISP instance
    - Around 60 000 indicators available now
  - CERN MISP instance mostly containing threat intel aimed at campus

- Challenge your email system
  - How hard is it to sent malware to your team?

Ways forward

- Raise awareness on ongoing security events
  - Ignorance makes attacks cheaper and easier
  - Well documented nation-states and for-profit attacks on the Web
  - Expose how public universities and national labs are targeted

- Readiness against attacks coming propagating via campus
  - What happens with incidents spanning across campus + grid?
  - Is access to needed traceability information available?

A malspam day at CERN

- Initial emails difficult to filters
  - From, to, subject, body and attachments different for every message
  - Attachments all unique
    - Sometimes encrypted (password in the body of the email)
    - Sometimes obfuscated, like a zip containing xxxxx.pdf.wsf
    - Sometimes no attachment, just a malicious random URL
- Once opened, further challenges
  - Obfuscated macro will conduct multiple checks (ever increasing evasion techniques)
  - PowerShell is spawned and payload fetched from URIs
- Even with the payload, there is more
  - Payload needs decrypting, then there are more challenges before contacting the real Command & Control and config file…
- Behaviour-based analysis helps

A malspam day at CERN

- Initial heads-up (trust group, MISP or security monitoring)
- Obtain sample (e.g. Microsoft Word file) and extra payload URIs
- Try and block further malspam emails (difficult!)
- Determine the nature of the malware and its target
  - If CERN's reputation/finance is at risk in any way: block payload URIs (sometimes dozens) + check whether someone clicked
  - If opportunistic or targets individuals, decide on a per-case basis
- Share back our findings with relevant trust group(s)
- Note: APTs/Nation-states use very identical techniques