HEPiX 2020 Short security message

Sebastian Lopiensky*, Liviu Vaalsan*, Romain Vartel*

(* allegedly)

Before ☕…one more thing!

- We work and collaborate in a different way this year
  - Teleworking, video-conferencing
- Attackers have adapted too
- 2019: 20% of attacks were linked to APT / Government actors
- Big Game Hunting Ransomware attacks on the rise.
  Our online events are perfect watering holes

- Teleworking also brings additional exposure
  - Reduced protection from campus security team (IDS logging, etc.)
  - Use your organisation's VPN or similar if you can! And avoid DNS-over-HTTPS.
  - Protection against malicious domains if your organisation has DNSFirewall-like mechanism

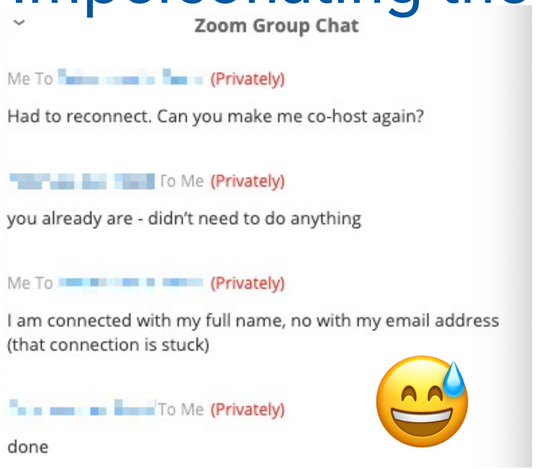
Fully online events like HEPiX 2020

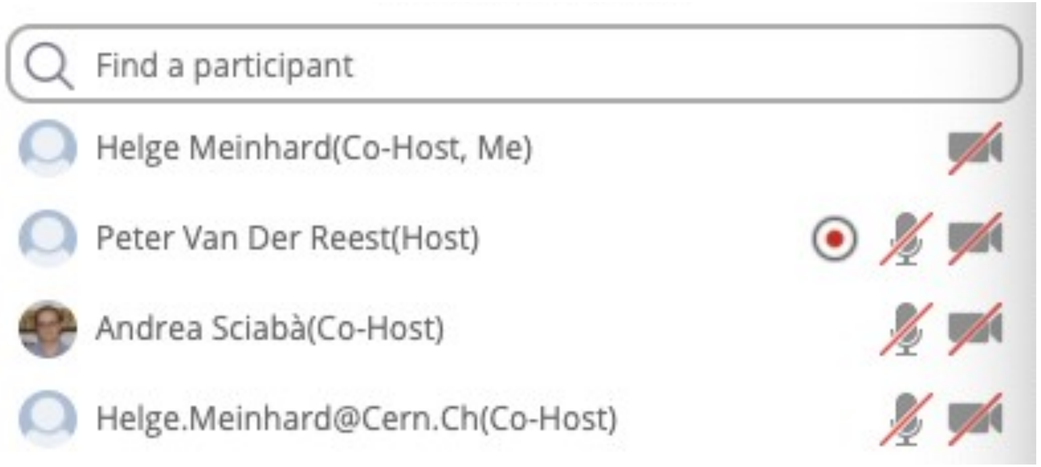
- Managed to register a totally fake, non-existing persona
- Worldwide community: Very easy, regardless of the vetting efforts in place
  - Impact? No confidentiality, meeting effectively public (to attackers too)
  - Can you spot them? First valid answer wins Swiss chocolate!

- Videoconferencing limitations / threats and “Zoom bombing”
  - Anyone can join your meeting (unless protected - not trivial if you don't know all participants)
  - Password hard to remember vs easy to guess
  - Anyone can unmute or share screen and disturb (unless that is disabled - but Q&A not easy)
  - Anyone can write on the chat (including malicious links)
  - Anyone can rename themselves to anyone else

Fully online events like HEPiX 2020

- Impersonating the host is possible





✅ (“sudo Zoom”)

- Beware of links or pointers or information requests! Do not trust.
- Indico slides public
  - >Anonymous access to the Google Doc: free unlimited phishing!
  - Exposes home teleworking IP, approximate location, browser + OS version, etc.

If you have Zoom video / audio quality issues here are some tips: https://bit.ly/34MQN5z

13 hits

(Dave K): When I see this kind of HEPiX group photo it makes me so downhearted

7 hits (in ~30 min)

Thanks for the great computer security update talk. Phishing is a major issue for our community as well, with dedicated campaigns targeting academia: https://bit.ly/2SPUORm

1 hit

(If you aren't so sure about where a Bitly link will direct to, it is possible to previ before clicking on it. To do this, simply add a + sign to the end of any link in your browser. For example, for https://bit.ly/2SPUORm just enter https://bit.ly/2SPUORm+ into your browser and you'll be sent to a preview page for the link.)

It's a hard game

- Organising an online conference is difficult, guidelines still needed
  - See talks from Graeme, Pepe etc.
  - Sebastian and Helge are preparing general guidelines
- Organising a "secure" online conference is very difficult
  - Security advice is being worked on