EDINBURGH
JUNE 16-21
2019

Defending the Dutch Healthcare Sector

Jasper Hupkens
Z-CERT

About Z-CERT

- Sectoral CERT for healthcare in the Netherlands
- Incident response
- Facilitate collaboration across the sector
- Not-for-profit organization, funded by constituency
- FIRST member since May 23th!

Healthcare in the Netherlands

- Private sector
- Fragmented
  - Not one electronic patient file system
  - No dedicated network
- Complex, diverse IT landscape
- Not considered vital/critical infrastructure

Threats we see

- Mostly opportunistic attacks
- Lets have some examples

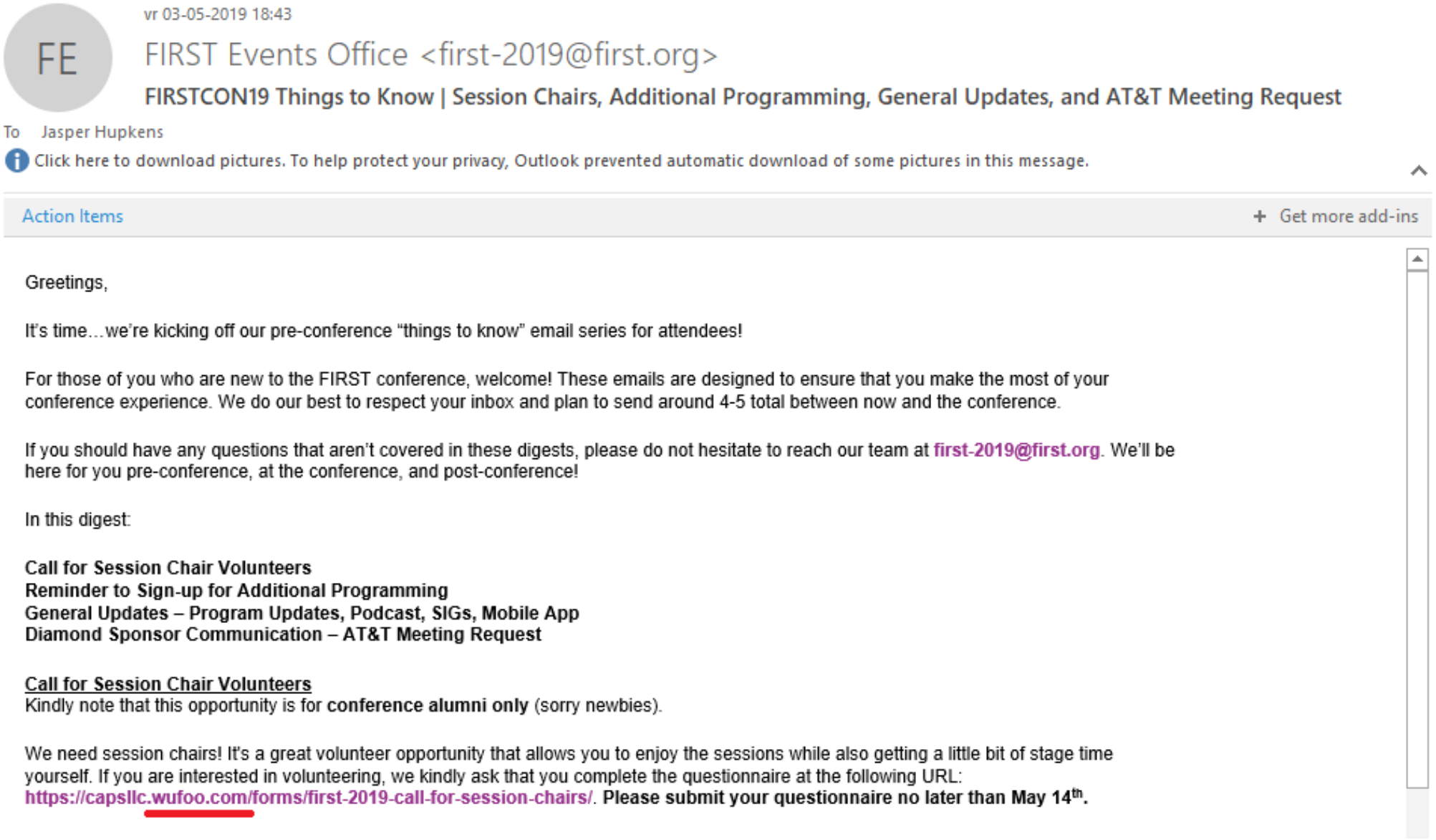
Phishing

- Phishing, phishing and more phishing
- About half of our registered incidents involve phishing
- We see all forms (sextortion, CEO fraud, etc.)

Phishing using free hosters

- Victim receives an email containing a URL to a party were e.g. a form can be hosted for free
- We made a list of all the domains encountered and advised our constituency to block them all
- There is no good reason to allow such domains

Right?



vr 03-05-2019 18:43

FE

FIRST Events Office <first-2019@first.org>

FIRSTCON19 Things to Know | Session Chairs, Additional Programming, General Updates, and AT&T Meeting Request

To Jasper Hupkens

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Action Items + Get more add-ins

Greetings,

It's time…we're kicking off our pre-conference "things to know" email series for attendees!

For those of you who are new to the FIRST conference, welcome! These emails are designed to ensure that you make the most of your conference experience. We do our best to respect your inbox and plan to send around 4-5 total between now and the conference.

If you should have any questions that aren't covered in these digests, please do not hesitate to reach our team at **first-2019@first.org**. We'll be here for you pre-conference, at the conference, and post-conference!

In this digest:

Call for Session Chair Volunteers
Reminder to Sign-up for Additional Programming
General Updates – Program Updates, Podcast, SIGs, Mobile App
Diamond Sponsor Communication – AT&T Meeting Request

Call for Session Chair Volunteers
Kindly note that this opportunity is for **conference alumni only** (sorry newbies).

We need session chairs! It's a great volunteer opportunity that allows you to enjoy the sessions while also getting a little bit of stage time yourself. If you are interested in volunteering, we kindly ask that you complete the questionnaire at the following URL: **https://capsllc.wufoo.com/forms/first-2019-call-for-session-chairs/**. **Please submit your questionnaire no later than May 14th.**

Data breach through old domain names

- Healthcare institution suffered from a data breach because they changed their name and let their old domain expire

- An automated system was still sending email to that domain

And now for something completely different

- Various healthcare institution received phone calls from “Hans”
- Posing various threats and connecting to hospitals to each other
- No real motive found but very annoying

Medical Device security

- Operation Technology vs IT
- Rapid digitalization
  - Remote patient monitoring
  - Biomedical devices
  - eHealth
- Slowly getting more attention
  - DefCon, Hack in the Box Medical Device Village
  - FDA / EU regulation on safety moving to include security

Challenges

- Legacy systems everywhere – think BlueKeep
- Wide range of maturity levels
- Organizations not in control
  - No/Not enough resources
  - No (combined) overview
  - Vendor lockdowns
- Collaboration
  - Vendors
  - MSP’s
  - Inter-sector
  - International

Collaboration

- We’re not the only healthcare sectoral CERT
- Work together with manufacturers
- Opportunities within FIRST?

Moving forward

- Expand the community
  - TheHive/MISP
  - TechOps - Facilitate communication on operational level within constituency
- Explore options for Medical Device security testing
- Continue efforts to increase maturity level within the sector
  - Factsheets
  - Training
  - Awareness

Questions?

- Key take-aways:
  - Healthcare not deemed vital/critical infrastructure in The Netherlands
  - Wide range of maturity levels
  - Do **not** let old domains where email was sent to expire
  - Looking for organizations to collaborate with!