Operational Security
&
Dealing with Cyberthreats:

Looking at the future

Romain Wartel, CERN






WLCG
Worldwide LHC Computing Grid

Cybercriminals

- Profound changes in the underground economy and organised crime in the last years
  - Cybercrime highly profitable
  - Risks are minimum
  - Malware-as-a-service
- Interpol:
  - Cybercrime is bigger than cocaine, heroin and marijuana trafficking put together
- Typical features:
  - Custom 0-days, targeted phishing
  - Target end-users, administrators and organisations
    - GoZ, Dridex, etc.
  - Large distributed malicious infrastructure
- This has significant impacts for our community

Nation-states

…After all, we have only little money, and our work is public…

- Current main organisational targets:
  - Aerospace and Defence
  - Construction and Engineering
  - High Tech
  - Telecommunications
  - Transportation
  - Financial institutions
- Common known objectives of intrusions:
  - Politics
  - Strategy
  - Trends in a sector, tender purchasing strategy
  - Trade secrets, pricing discussions, competitor pricing information
  - Gain a competitive edge
  - Insider trading
- It used to be very risky, complex and expensive. Now affordable on a large scale.

Short answer: because they can and it makes economical/strategical sense

Nation-states

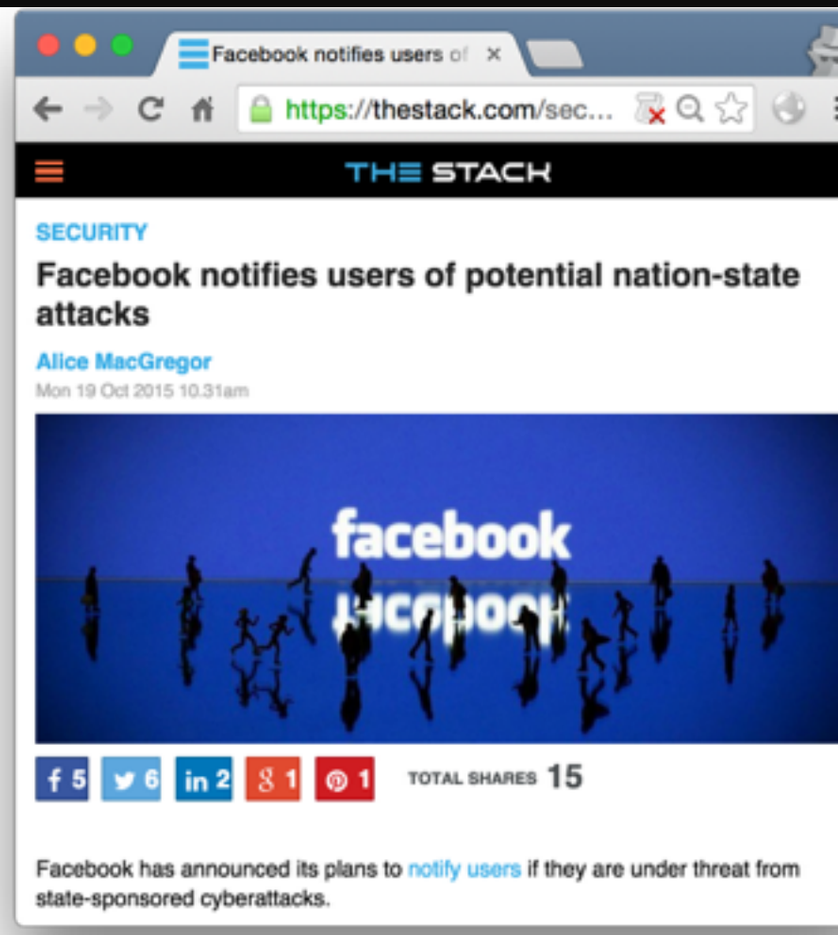
- Tools:
  - Custom attacks, aiming at exfiltrate specific data
  - Multiple 0-Days (in-house)
  - Targeted social engineering
  - Small distributed malicious infrastructure
  - Complex frameworks developed over the course of years (+ $ Millions)

- Cashing out:
  - Not interested in money, attribution extremely difficult

- According to Symantec, 70% APT victims profile:
  - Research, innovation, IT.
  - “forward looking technologies” highly sellable

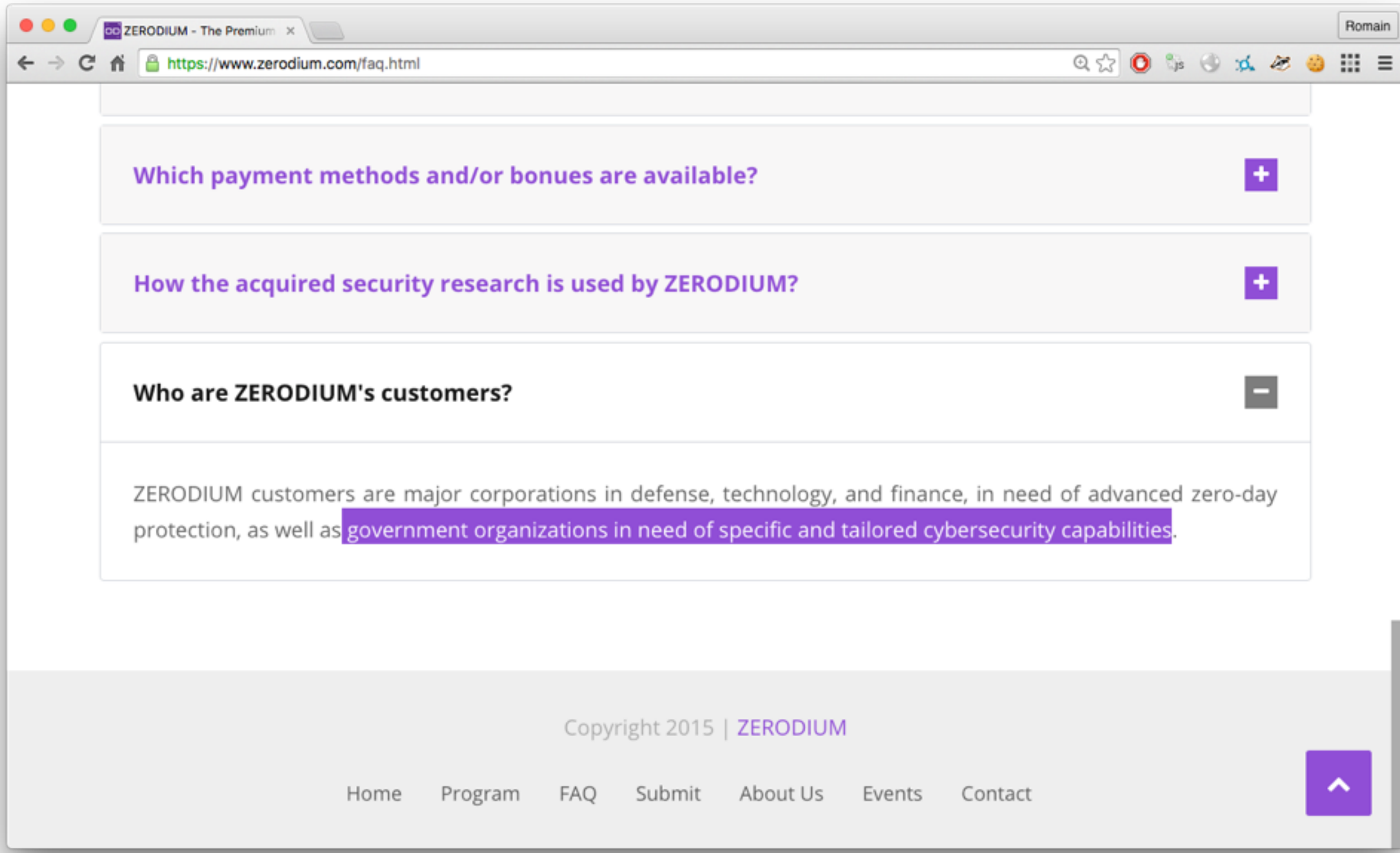
- Example: Stuxnet, Regin, Ukraine blackout in 2016

- Outsourcing to enable “plausible deniability”

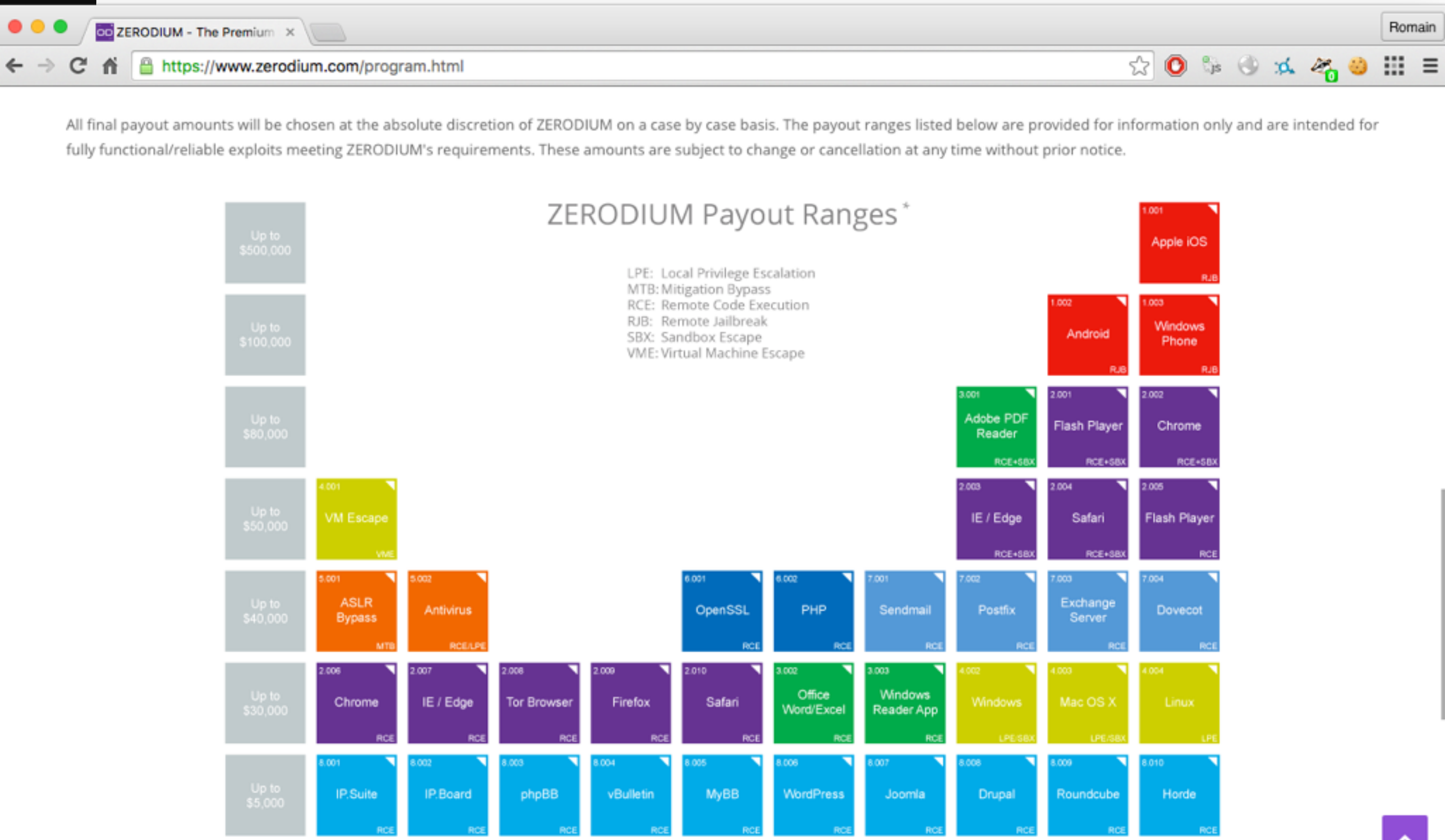


Outsourcing

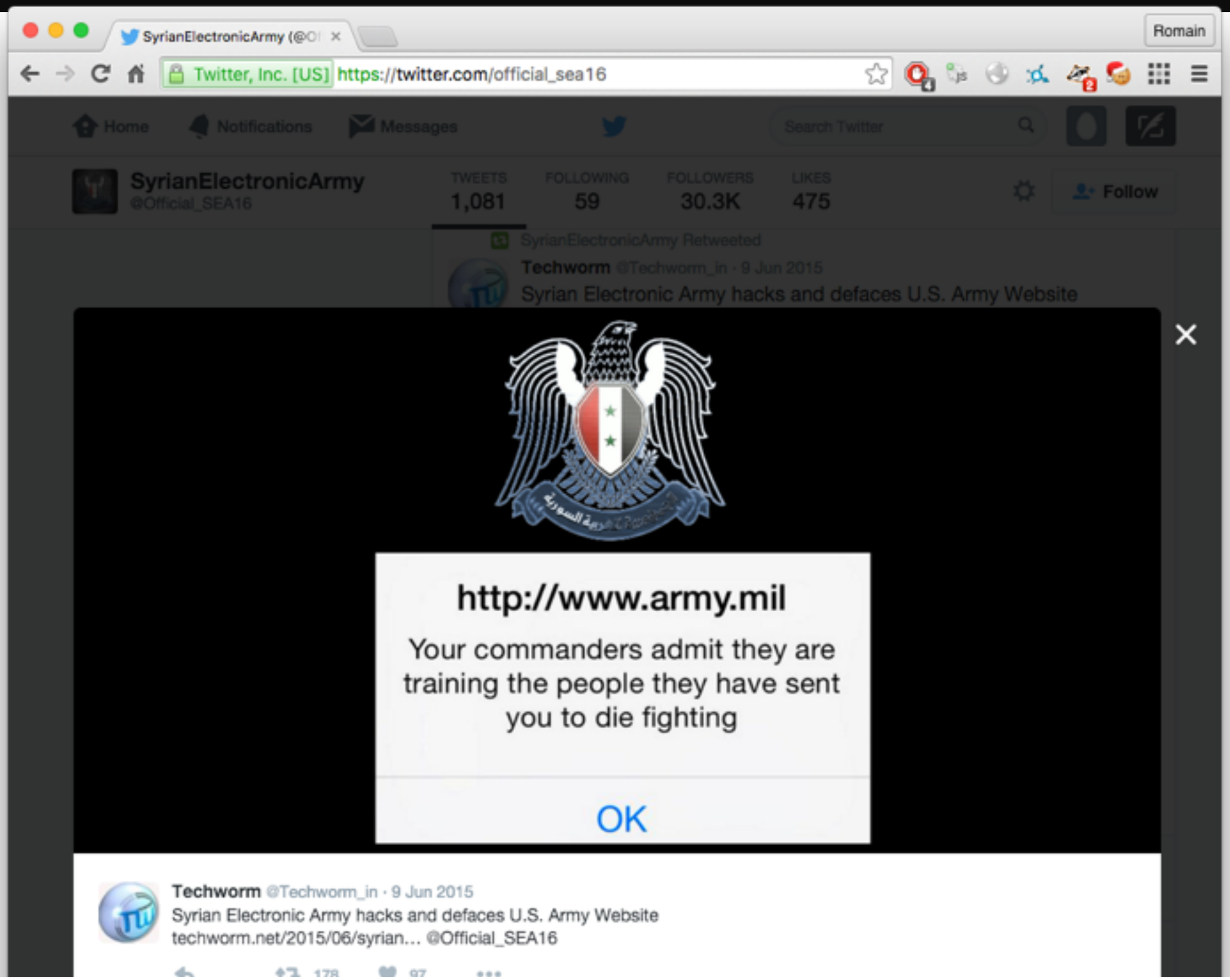
Outsourcing



Outsourcing



Hacktivists



- Goal:
  - Destruction for publicity
  - Concerns over SCADA capability

Response & strategy

- Treat security is a global issue
  - Not limited to WLCG/HEP
  - Including: operations, traceability, incident handling, policies
  - Continue to invest in global trust frameworks
  - Contribute to global efforts against cybercrime (Dridex, etc.)
- Main strategy for the VOs
  - Focus on traceability and controls in priority
  - Participate more actively in the incident response process
- Shift security emphasis from services to people
  - Next big breach likely via phishing, unlikely via SSH/grid 0-day
- “secure services” —> “defendable services”

Incident response

- Reinforce WLCG's incident response contacts globally
  - Not solely rely on EGI CSIRT and OSG Security team
  - Reinforce coordination role with federations, private sector, etc.
  - Propose/lead an academic security trust group to share threat intelligence
- Update WLCG's incident response workflow
  - Centrally manage forensics and analysis - *too few sites have sufficient expertise*
  - Sites will would simply fulfil "traceability" requests *(unless they have expertise to do more)*
    - Provide access to VM images, disk images, log files, etc.
    - How about private/commercial cloud providers?
  - Involve directly the WLCG/EGI operations team (already the case in OSG) and VOs
- Encourage the adoption of the three following incident response roles?
  1. Incident lead: Coordinator, process driver and responsible for the outcomes.
  2. Tactical analyst: The big picture person, setting the analytical course.
  3. Information manager: Managing the information flow/overload.

source: http://frodehommedal.no/presentations/first-tc-oslo-2015/#

- Prepare for possible funding for serious cases?
  - Security vendor
  - Travel expenses of WLCG experts, etc.

Response & strategy

WLCG participants and WLCG itself should consider a strategy addressing how to:

1. Involve security vendors in monitoring/incidents/forensics
   - Appliance? Service? Partnership?
     "We are keen on working with you guys, because you have large network and you are favorable target for advanced attackers."

2. Obtain indicators of compromise (threat intelligence)
   - Establish a solid network of security contacts?
   - Outsource and hire a security vendor (jointly or alone)?
   - Build the technical means to use them (SoC, etc.)
     - Do we need a working group for this?
     - Should we work on a "HEP appliance", like the NSF is the US?

3. Involve law enforcement for serious breaches
   - Attackers rarely decide they have had enough data/money…

4. Continue to raise the bar
   - Make it as difficult and expensive possible to break-in