Research and Development
Czech Cyber Crime Centre of Excellence

Jan Vykopal
Masaryk university

September 27, 2013
40th TF-CSIRT meeting, London, UK
Joint effort of a wide spectrum of Czech experts:
- academia,
- Police,
- private digital forensic labs,
- National Security Authority,
- justice, prosecution.

**Goal:** create single point of contact in the Czech Rep. for expert advices and know-how in the investigation of cyber crime.
Funded by EU (HOME/2012/ISEC/AG/INT/4000003882).
Start: May 2013
End: May 2015

Other related projects:
• 2CENTRE – network of national centres + Irish and French national centre,
• B-CCENTRE – Belgian national centre,
• B2CENTRE – Bulgarian centre,
• ECENTRE – English centre,
• and other national centres.
• Other centers develop tools for host forensics.
• We are experienced in **network monitoring** and operation of, and participation in **TI-accredited CSIRTs** (university and grid infrastructure).
• LE agencies **lack know-how** in the network traffic analysis.

**Our focus:** network forensics
NetFlow + DPI
• Shift from (near) real-time detection and prevention to post-mortem analysis and tracking.
• Real-life problems:
  1. Common tools for processing PCAP dumps do not work for huge amounts of data.
  2. How to trace back attackers? Using high-interaction honeypots (Sebek for recent kernels).

New task requires new tools (available on request).
Tools are not enough.
We seek for best practices in communication of CSIRTs and police:
  - What kind of incidents is reasonable to report?
  - What is helpful for police and national CSIRT?
Q&A

Jan Vykopal
vykopal@ics.muni.cz

September 27, 2013
40th TF-CSIRT meeting, London, UK