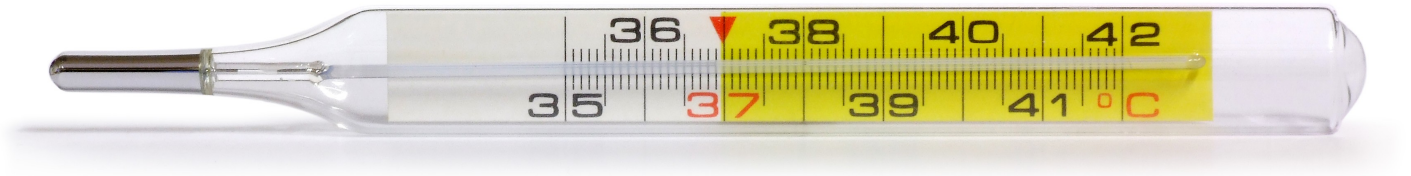
Network security monitoring working group



Jan Vykopal

39th TF-CSIRT meeting, Bucharest, Romania

May 24, 2013

Recapitulation

- September 2012 at the Ljubljana meeting:

  several teams interested in sharing and discussing methods and tools as a new TF-CSIRT activity
- May 2013 in tf-csirt@terena.org:

  several teams still interested
- Now:
  - discuss goals and format of the working group
  - demo presentation of CSIRT-MU infrastructure, used and developed tools and needs

Proposal

- Share best practices
- Inform about new tools
- Platform for closer cooperation

- Short updates by several teams (like Draw of Seven?)
- Collocated with TF-CSIRT meetings
- Keep it informal

CSIRT-MU

- Team of Masaryk University, located in Brno, Czech Republic
- Constituency: > 40 000 students, > 4 000 staff
- ~ 20 000 hosts online every day
- Four key services:
  - Incident handling
  - **Intrusion detection (incl. R&D)**
  - Alerts&warnings, announcements
  - Education and training

Monitoring infrastructure

- Based on **NetFlow** monitoring by stand-alone probes (no routers)
  - Two 10 GE probes at uplinks to NREN (CESNET)
  - ~ 20 1 and 10 GE probes within the network (incl. honeypots)
  - Probes connected by TAP (Test access ports)
  - Several NfSen collectors (production, development, for students)
  - ~5 kflows/s, 300 Mflows/day
  - In-house detection tools and plugins for NfSen (Perl, BASH)
  - Monitored by Nagios
- Low- and high-interaction **honeypots**
  - Honeyd and virtual machines (collect attempted passwords)
- Access to sendmail **logs**
- Mitigation using **Remotely Triggered Black Hole filtering**

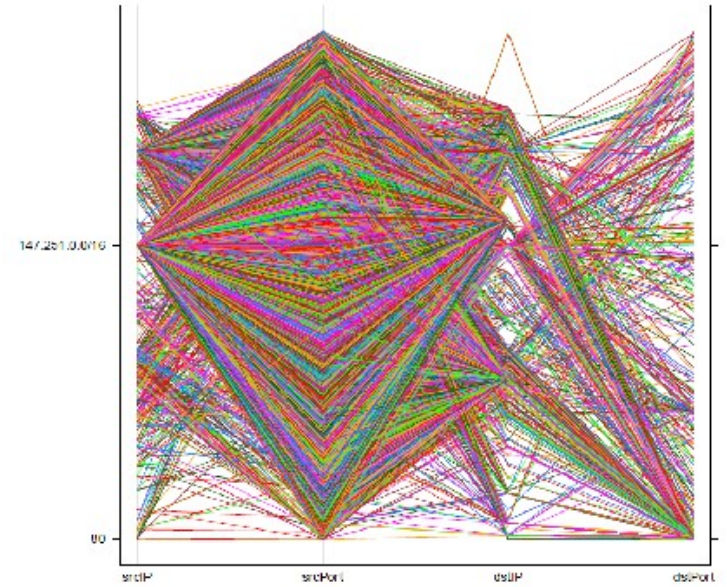
Developed and available tools

- NfSen plugins:
  - RDPMonitor – RDP brute-force attacks detection
  - SSHMonitor – SSH brute-force attacks detection
  - Honeyscan – honeynet monitoring plugin (feeds Team Cymru)

- Other tools:
  - NfPlugger – plugin template generator for NfSen
  - PhiGARo – for management and resolution of phishing incidents
  - NetFlow and IPFIX Geolocation Tools
  - Plugins for HTTP Monitoring
  - IPFIX Export Plugin
- Available at http://www.muni.cz/ics/services/csirt/tools/ and http://www.muni.cz/ics/920232/web/

Ongoing work

- Analysis of flow time series (Holt-Winters prediction)
- Deploy HTTP monitoring for precise detection of replies to phishing e-mails
- Visualization – IPv4 address space map, parallel coordinate plots
- DNS requests monitoring (IPFIX)
- Penetration testing based on NetFlow profiling



Known tools

- SSHCure – flow-based SSH IDS by University of Twente
  http://sourceforge.net/projects/sshcure/
- IPFIXcol – IPFIX flow data collector by CESNET
  https://www.liberouter.org/ipfixcol/
- SURFmap – visualizes a geographical dimension to network traffic using Google Maps API
  http://sourceforge.net/projects/surfmap/
- Netflow-indexer – indexes the flat file databases used by nfdump/flow-tools
  http://justinazoff.github.com/netflow-indexer/
- Other tools are available at http://sourceforge.net/apps/trac/nfsen-plugins/

Possible cooperation

- We offer:
  - anonymized flow samples for R&D
  - testing of NfSen plugins and other tools in our network

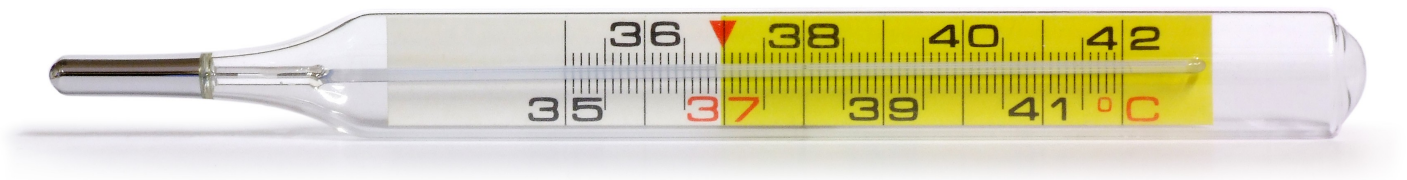
- We would like to:
  - test our tools in other networks
  - know about your tools and be inspired by your research

Back to working group

- What are your **expectations and needs**?
  - Share best practices
  - Inform about new tools
  - Platform for closer cooperation

- What is your opinion on the proposed **format**?
  - Short updates by several teams (like Draw of Seven?)
  - Collocated with TF-CSIRT meetings
  - Keep it informal

Network security monitoring working group



Jan Vykopal

http://muni.cz/csirt

vykopal@ics.muni.cz