Federal Office
for Information Security

Internet Analysis System (IAS)

Module of the German IT Early Warning System

Martin Bierwirth, André Vorbach
Federal Office for Information Security (BSI), Germany

21st Annual FIRST Conference, Kyoto June 28 – July 3 2009

Agenda

- BSI and CERT-Bund
- Situation center and situation awareness
- Internet-Analysis-System:
  - Concept / implementation
  - Sensor network
  - Examples, incident research, incident handling
  - Distinction from other systems
- Conclusion

Federal Office for Information Security

Federal Office for Information Security (BSI)

The national IT-Security authority

- High level federal public agency within the area of responsibility of the Federal Ministry for the Interior
- Independent and neutral authority for IT security in Germany
- Founded in 1991, ~ 500 employees, 64 Mio Budget
- Primary tasks:
  Internet security, Secure e-government, IT baseline protection, National / international security cooperation, Cryptographic innovation, Biometrics, Security from eavesdropping, Awareness campaign on IT security, Certification and approval, Protection of critical infrastructure
- Constituency: Federal administration, CI, citizen, partners
- **Responsible for IT-security of federal networks!**

Federal Office
for Information Security

CERT-Bund

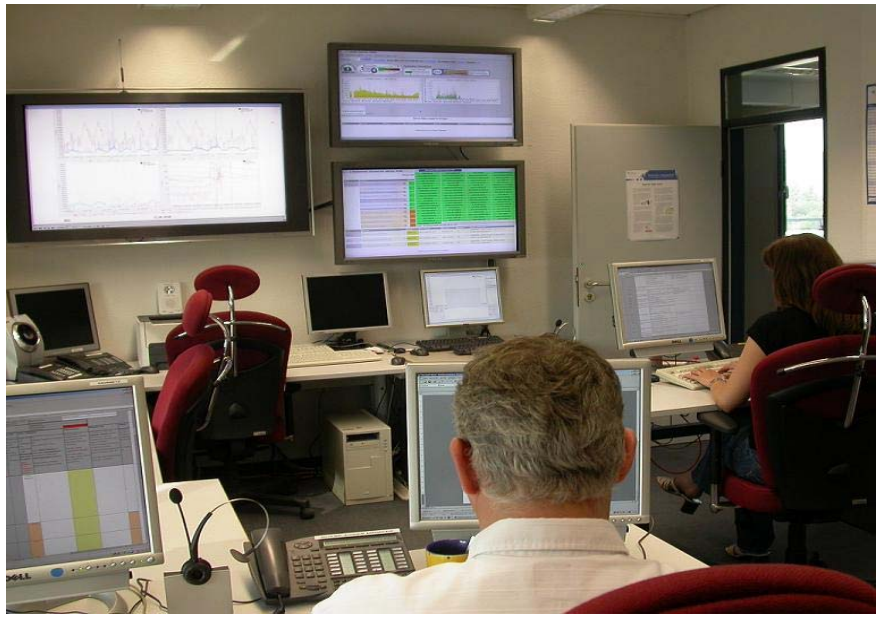
The Federal Incident Response Team

- Governmental CERT for the federal administration since 2001
- Provide central 24/7 PoC for national and international cooperation
- Analyze incoming incident reports and information about vulnerabilities and malware
- Publish advisories or information on counter measures and / or workarounds by running a *Warning & Information Service*
- Coordinate incident handling & malware reports
- Support the investigation of incidents and the recovery process
- **Run the *IT-Situation Centre* for monitoring sources and technical sensors**
- Run an alerting service for the federal administration
- Run the *National IT-Crisis Response Centre*

The National IT-Situation Centre

Generating Situation Awareness

- 24x7 availability, 8x7 staff on site
- Regular analysis of various sources and technical sensors
- Monitoring of the government networks using technical sensors
- Monitoring of availability of governmental web sites and services
- Close contact with national and international professional organizations
- Generating situation awareness
- Longterm monitoring generates situation reports for different levels
- Organizational and technical preparation for expansion to the IT Crisis Response Centre



Relevance of Sensor Networks

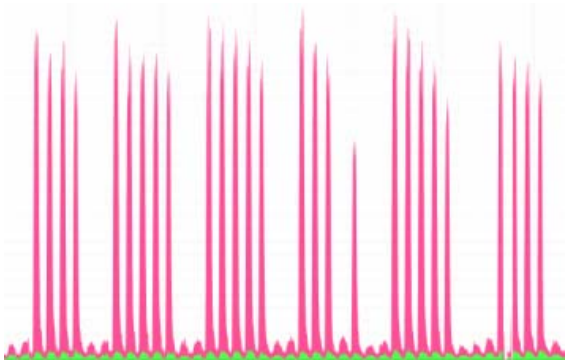
- Support analysts during research and the evaluation of incidents like
  - DDoS
  - Malware traffic, mass exploits
  - Spam and malware waves
- Extend and validate other sources
- Not necessarily „early warning capabilities“, but they can detect anomalies
  - caused by technical failures
  - caused by IT-attacks

- Deeper research after alerting of availability monitoring
- EVAA, CarmentiS, **Internet Analysis System (IAS)**

Internet-Analysis-System (IAS)

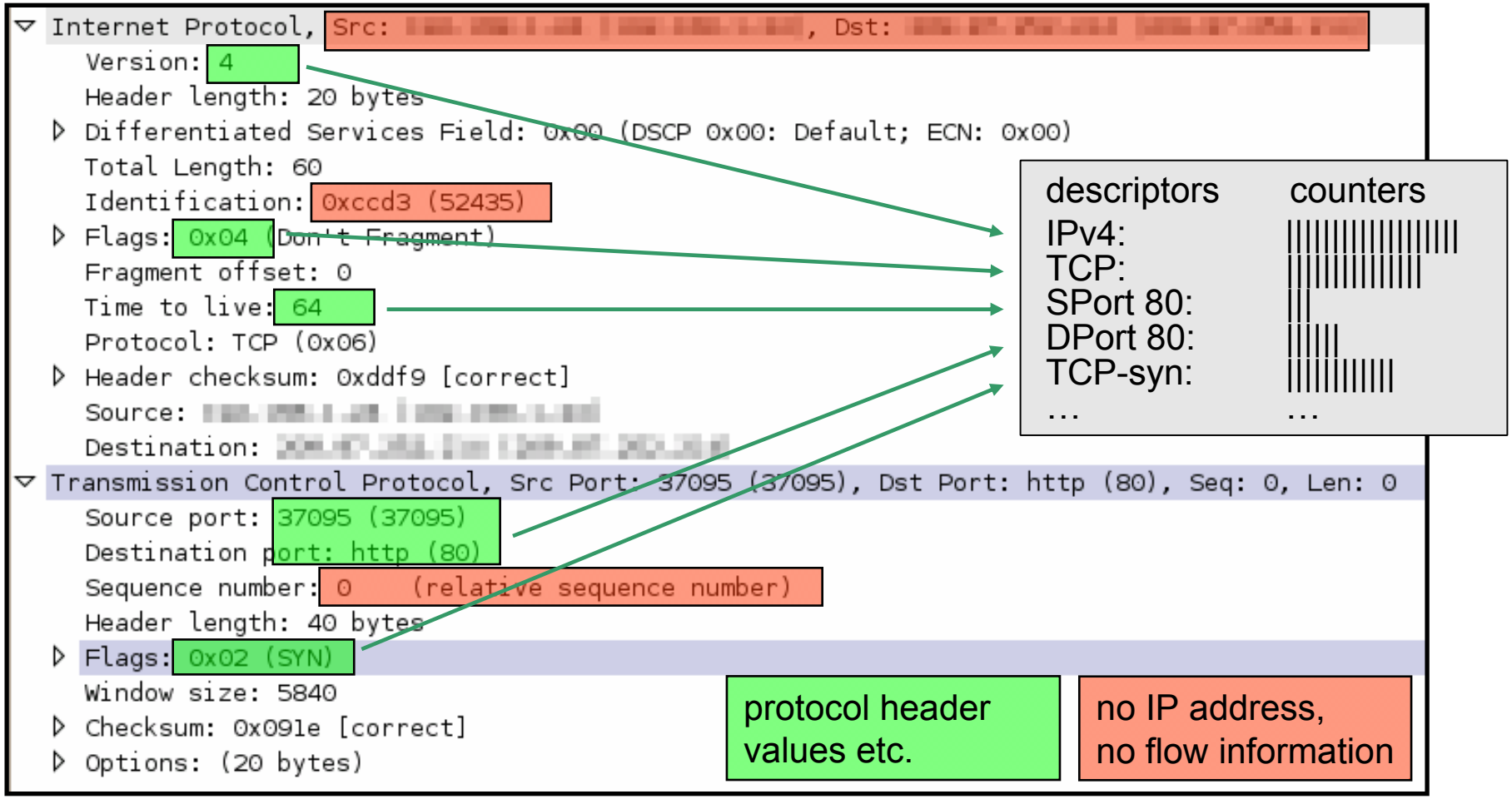
Motivation & background

- German government passed the „National plan for the protection of critical information infrastructures“ (2005).
  - Implementation plan for federal administration (2007).
  - Build a national IT early warning system.



- Among other aspects, one ambition was to
  - monitor statistical data in several networks of different authorities → find partners.
  - do not monitor data with personal reference (IP-address, content etc.) or flow information → implicit sanitization.
  - establish a central analysis station to gain a larger monitoring scope → compare data.

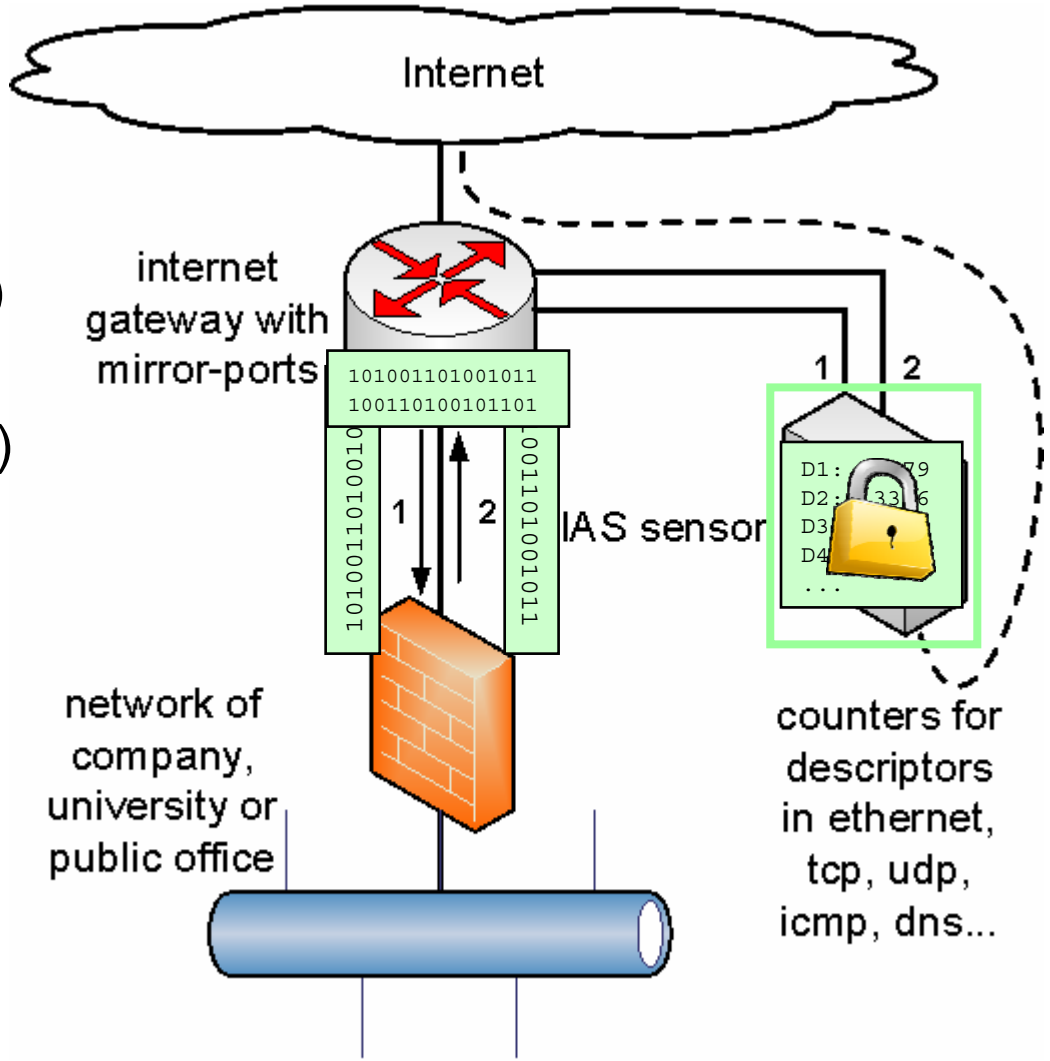
Monitoring concept of the IAS



Screenshot taken from Wireshark.

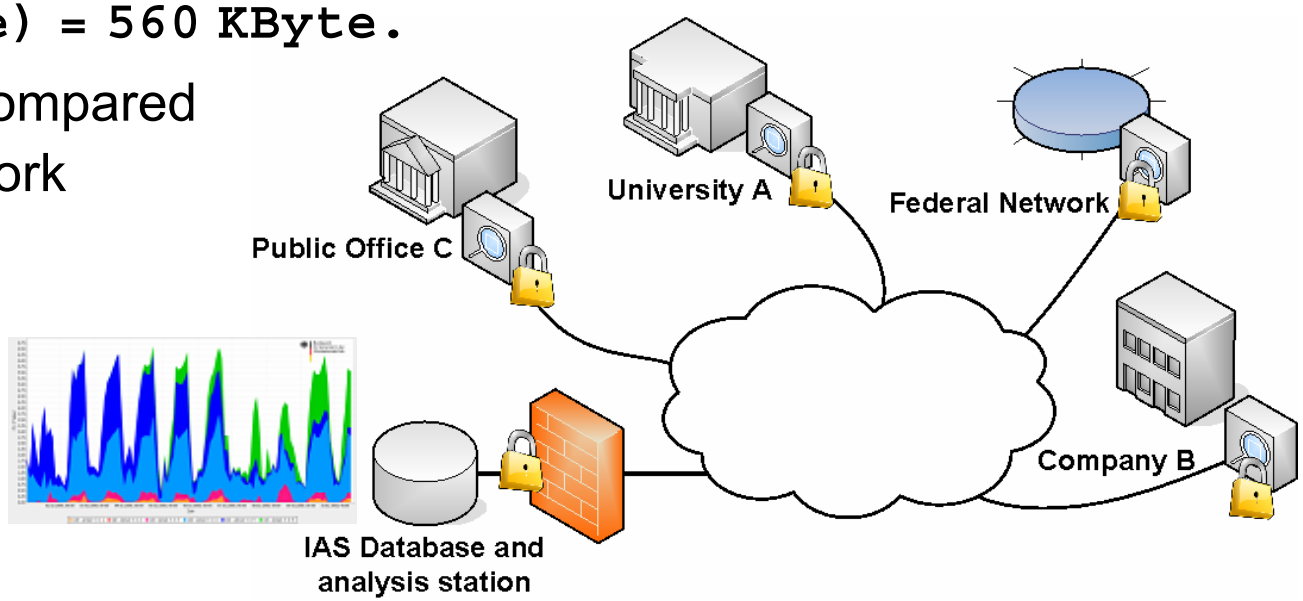
Functionality of an IAS sensor

- Passive sensor that receives the inbound / outbound traffic.
- Duplication by mirror (span) port or by network tap.
- Output (descriptor counters) is sent to analysis station every N seconds through a separate link (encrypted, usually + VPN tunnel).
- Hardware: 'small' server, xeon cpu, 1 GB RAM, 1U.



Sensor network, data aggregation

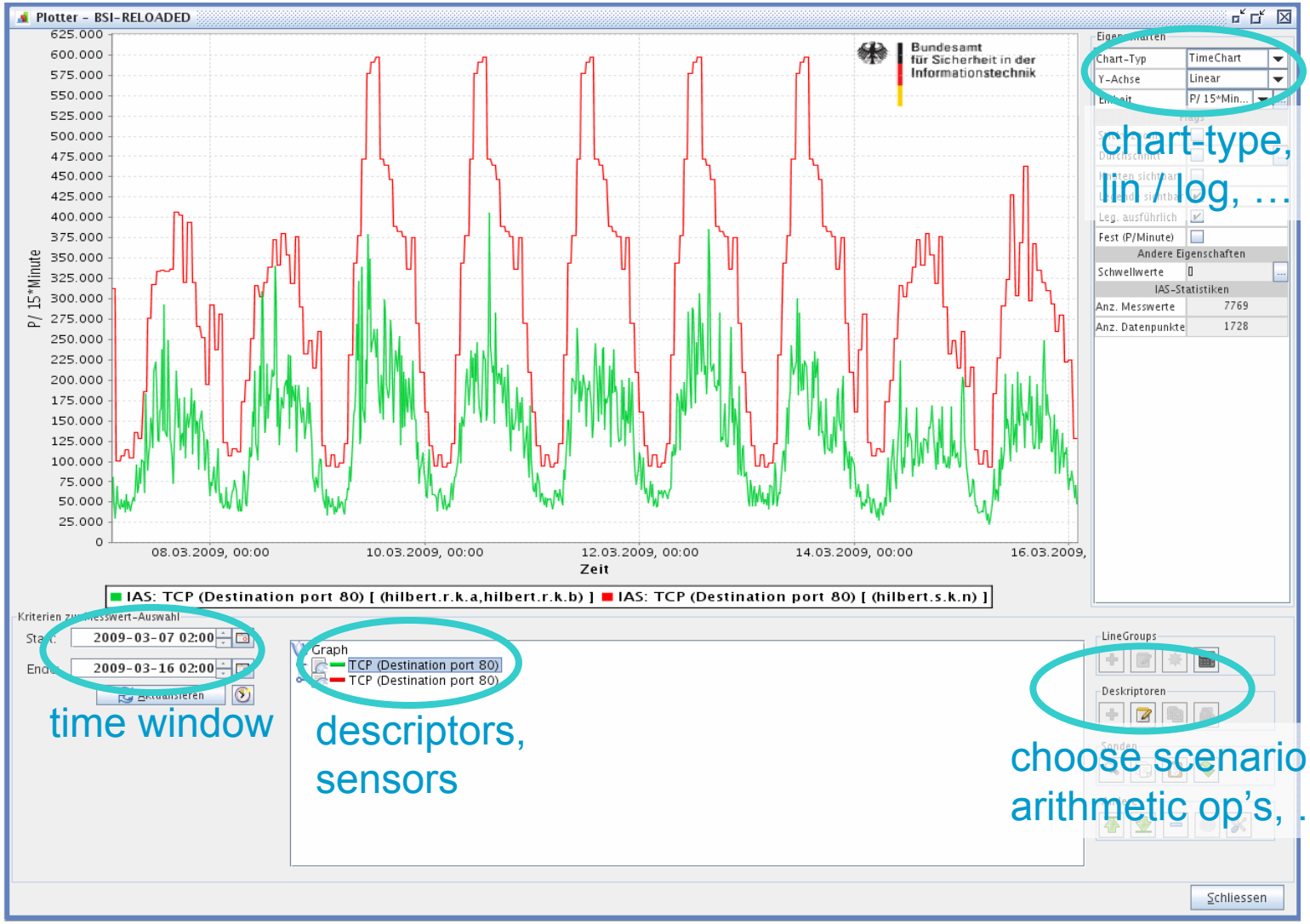
- Sensors in use: government networks + some partners.
- At each location one logical sensor per direction. In case of redundant internet links one logical sensor per link → up to 4 sensors.
- In one interval (N = 300 seconds), about 50K – 90K different attributes occur in network traffic. → Store counters and corresponding ID.
- Every five minutes, a sensor has to transmit about
  `70K * (4 + 4 Byte) = 560 KByte.`
- Extremely ‘small‘ compared to the original network throughput.



Federal Office
for Information Security

Accessing the IAS data

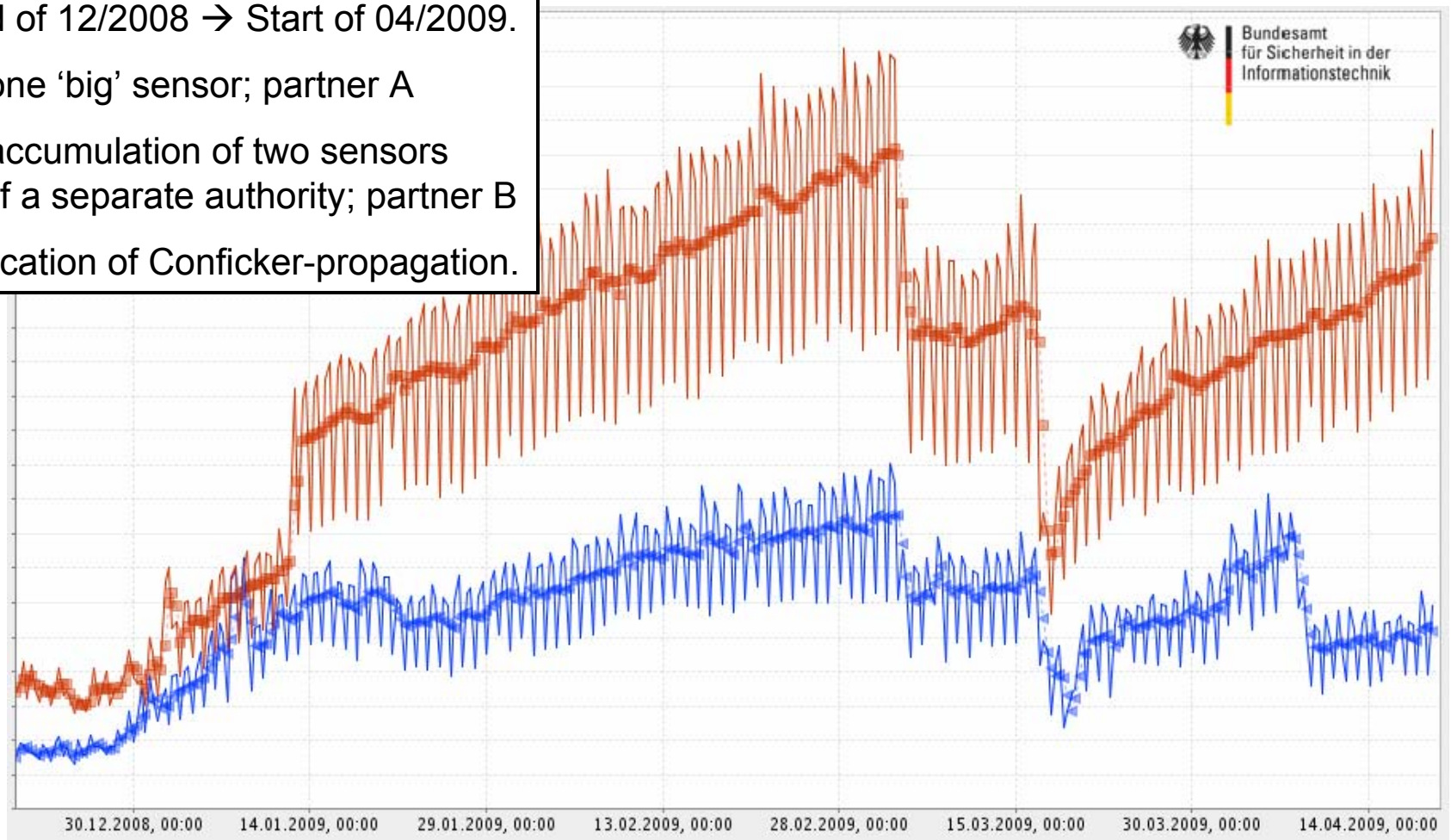
Client for manual research



Federal Office
for Information Security

IAS trend analysis
Example: Conficker

- Scans on port 445/tcp.
- End of 12/2008 → Start of 04/2009.
  - one ‘big’ sensor; partner A
  - accumulation of two sensors of a separate authority; partner B
- Indication of Conficker-propagation.

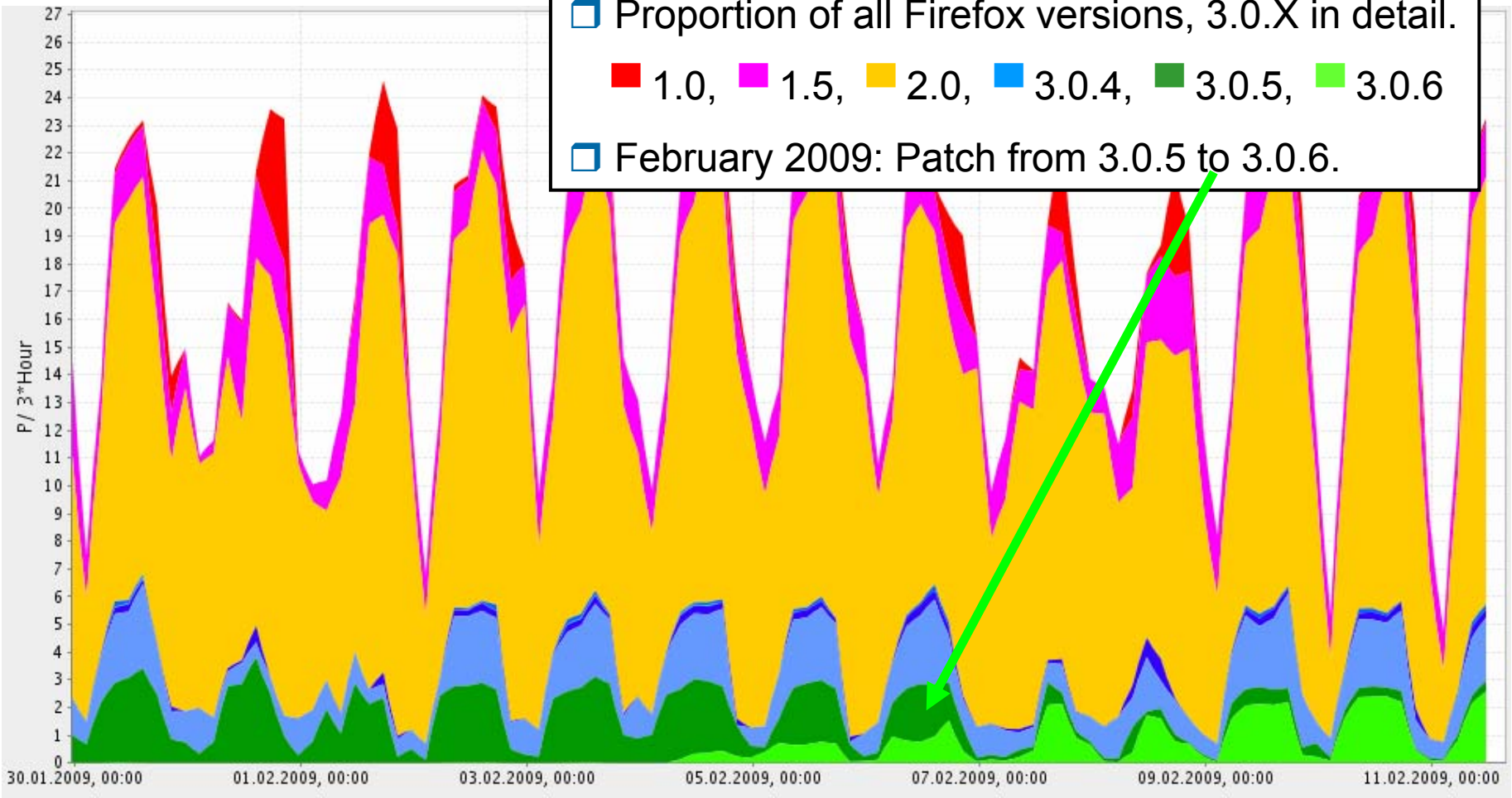


Federal Office
for Information Security

IAS trend analysis

Example: distribution of browser versions

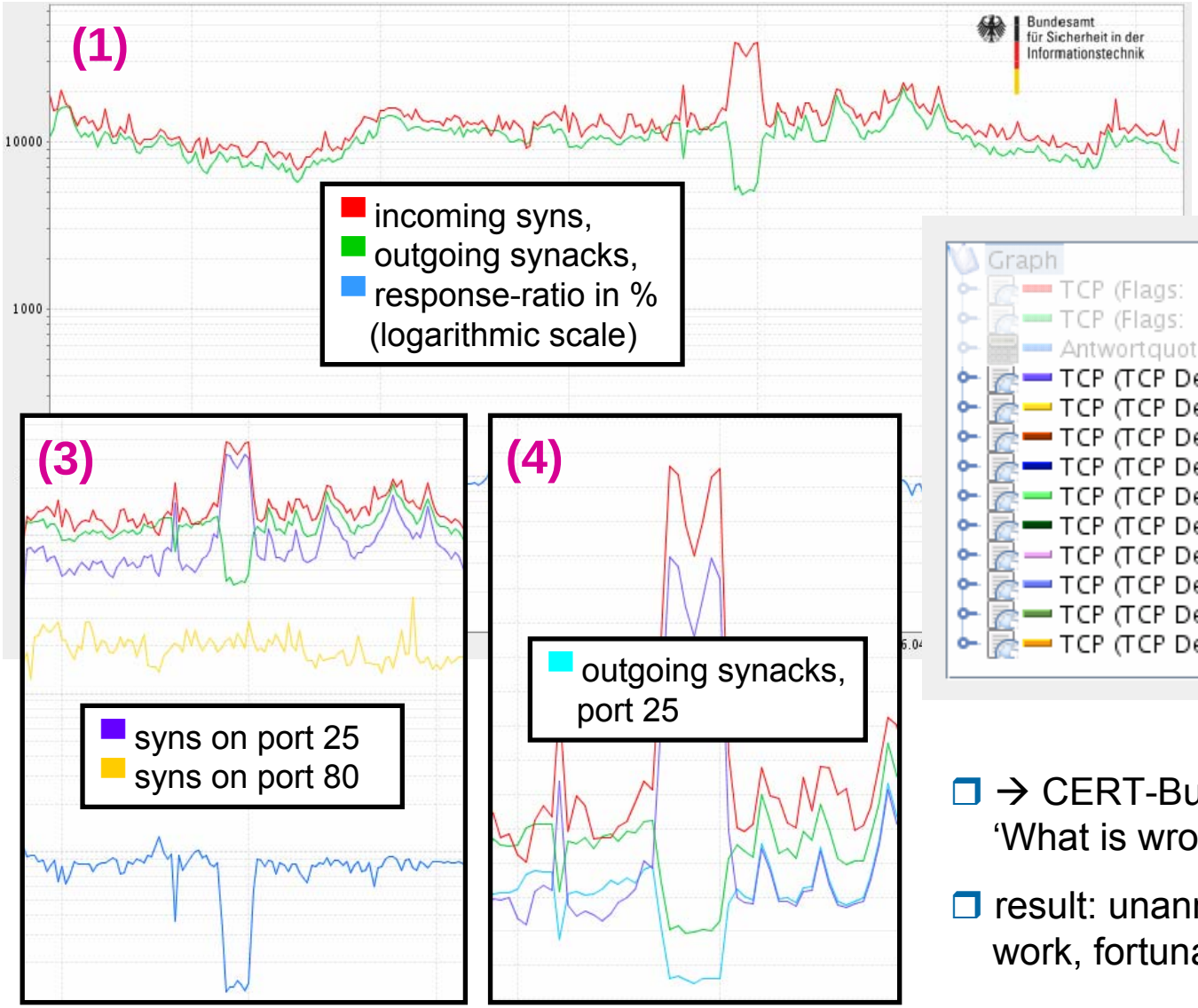
- Outgoing HTTP traffic, get-request user-agent.
- Proportion of all Firefox versions, 3.0.X in detail.
  - 1.0, 1.5, 2.0, 3.0.4, 3.0.5, 3.0.6
- February 2009: Patch from 3.0.5 to 3.0.6.



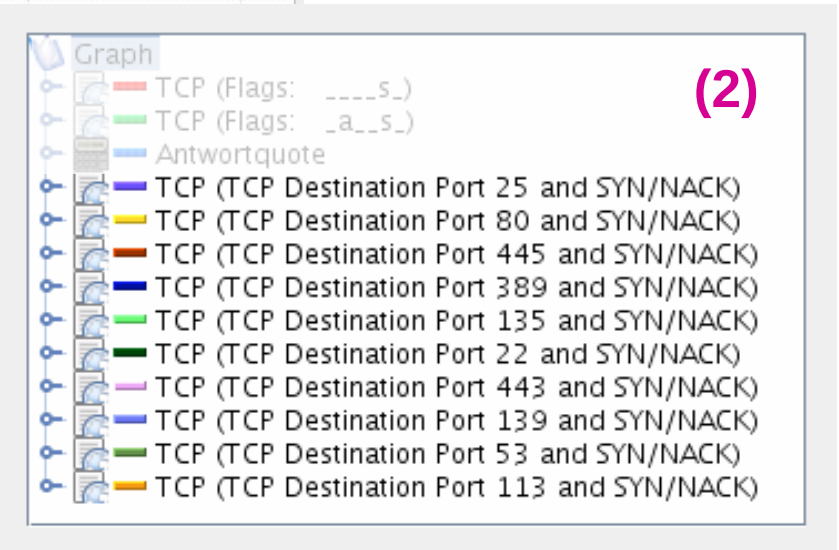
Federal Office for Information Security

Research in case of an incident

Example: TCP SYN ‘anomaly’



query-result:
top 10 ports

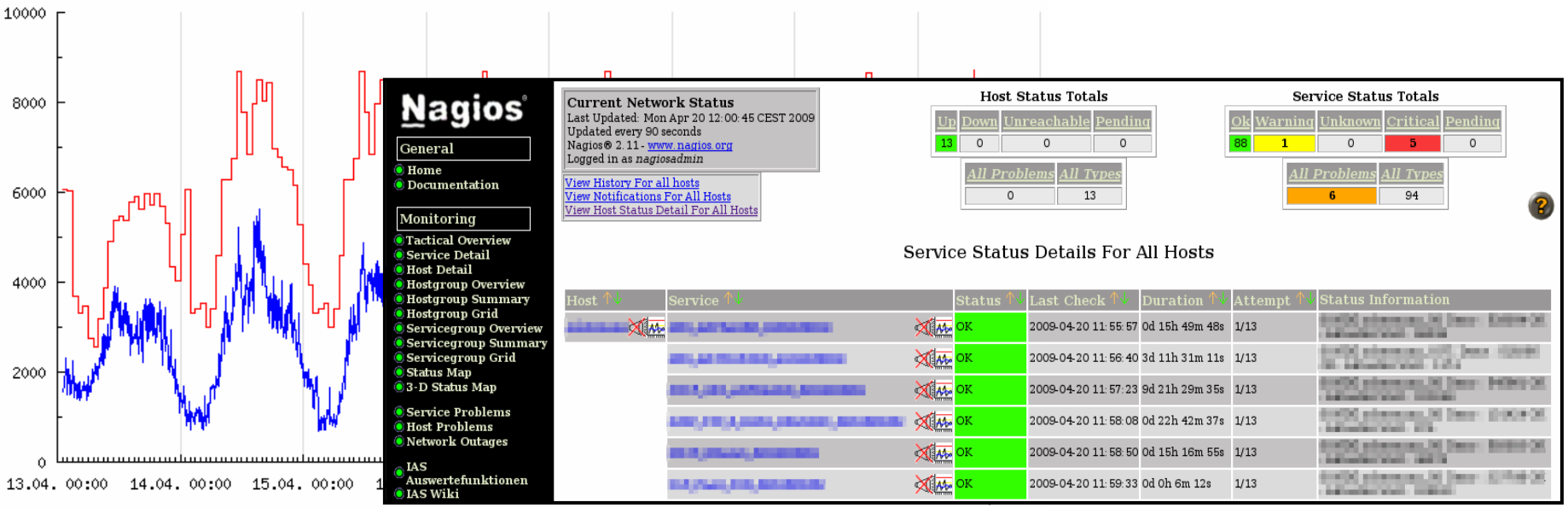


- → CERT-Bund, calling the operator: ‘What is wrong with the MTA?’
- result: unannounced maintenance work, fortunately no serious problem

Federal Office for Information Security

IAS anomaly detection

Profile generation, checking thresholds

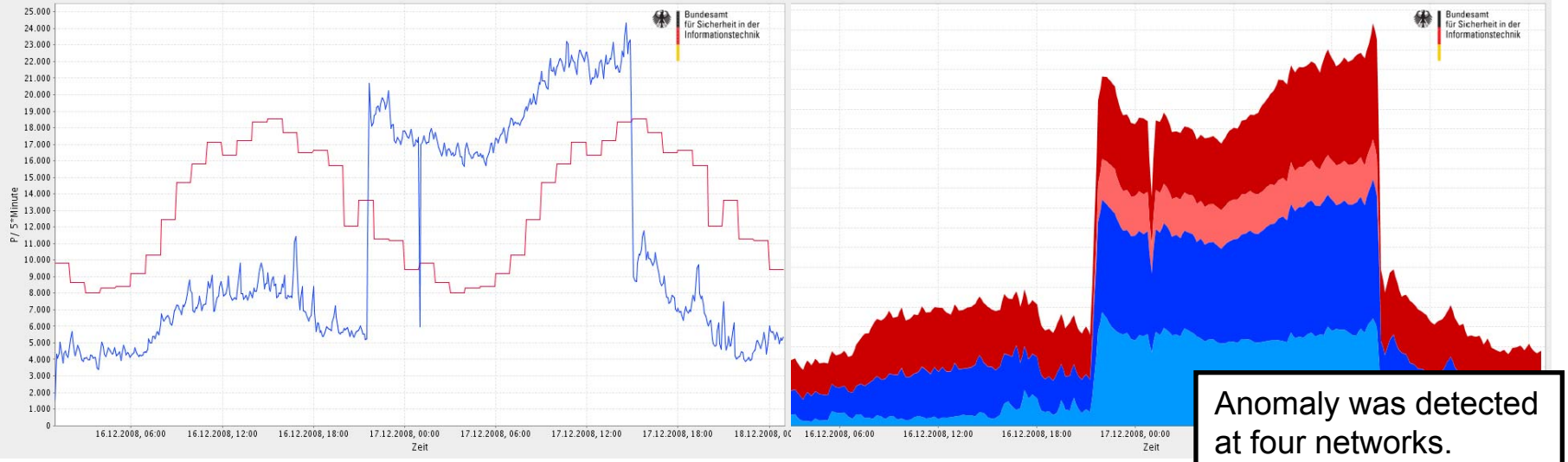


- Calculate ■ upper bound of ■ normal behavior periodically.
- This is done for a subset of the descriptor-set: important attributes like ICMP-ping, DNS-queries, TCP-SYN, SMTP-RCPT…
- Permanent checks: compare ‘fresh’ IAS-data with precalculated thresholds → NAGIOS http://www.nagios.org/

Federal Office
for Information Security

IAS-detected anomalies

Example: DNS anomaly, 12/2008

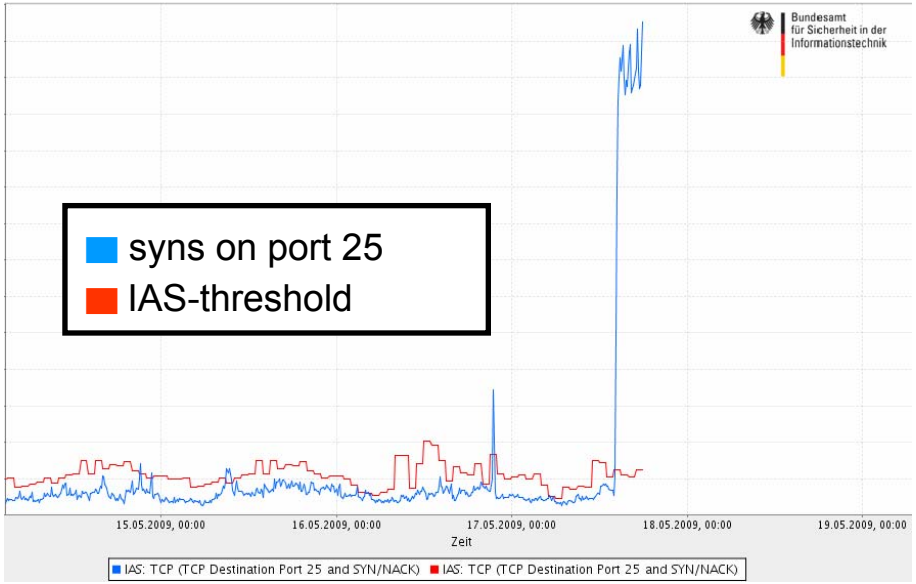


- Long-lasting peak in incoming DNS-queries, seen by several networks.
- IAS-analysis showed, that all queries asked for NS records.
  Some servers refused the queries.
- Calling operators & partners, asking for NetFlow & further info.
- Result: Queries for NS record ".", two source IPs in eastern Europe.
  Obviously source IPs had been spoofed, reflected DDoS-attack.
- ISC SANS, 2009-01-18: *DNS queries for "."*.

IAS-detected anomalies

Example: SMTP anomaly, 05/2009 1/2

- Spam…Have seen spam for many years now, have upgraded to bigger hardware, have deployed anti-spam-clusters…
- But in this case, operators said: “We are under attack, a DDoS!”

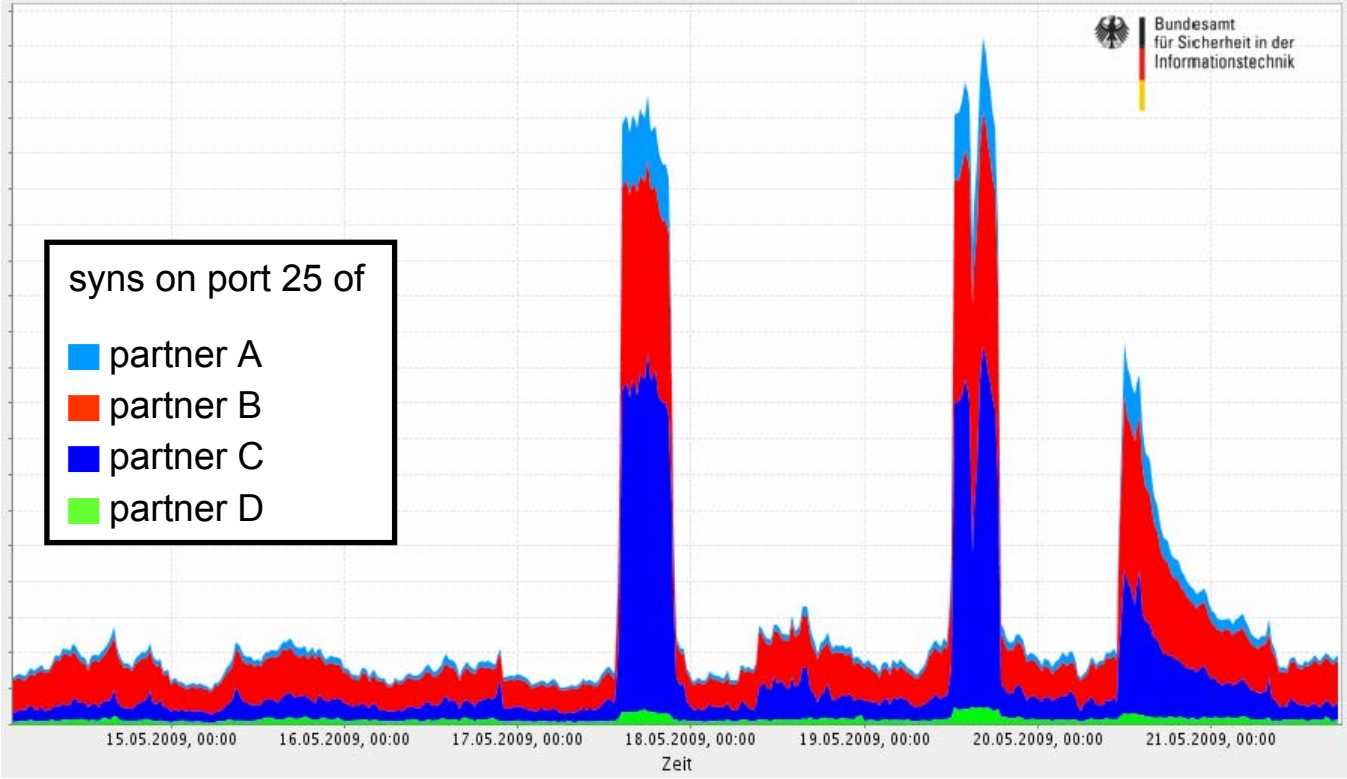


- Ratio of mails per SMTP session was very small, compared to ‘normal waves’.
  - More than 64.000 sessions at one MTA, 500 new per second.
  - Response-ratio of MTA dropped to ~60%, later on to ~30%.

Federal Office
for Information Security

IAS-detected anomalies

Example: SMTP anomaly, 05/2009 2/2



- IAS data analysis: all monitored networks saw the same behaviour.
  → No targeted DDoS-attack but rather a mass phenomena.
- EVAA showed: not a DDoS, transmission of a ‘regular’ mail with a casino-ad. → MTA had problems with large number of sessions.

Conclusion

Distinction from other systems

- IAS sensors
  - do not monitor data with personal reference,
  - do not reassemble TCP flows,
  - are independent of intrusion detection signatures,
  - revoke context of a packet after building its counters,
  - work passively, no impact on original network traffic.
- IAS cannot
  - detect targeted attacks or individual exploits,
  - protect networks actively like a firewall or an IPS,
  - provide attacker byte code,
  - give info for identifying source-IP or even targeted machine.

Conclusion
Benefits

- A sensor network of IAS-monitored authorities gives valuable information in terms of IT security.
- Aggregated data extends the perspective of individual networks.
- Manual analysis provides security-related trends.
- Anomaly detection shows indications of incidents.
- In case of incidents (detected by IAS or other sources), IAS provides nearly real-time monitoring of network traffic.
- ➢ Helpful to develop and evaluate counter measures.

Prospect:

- Automatic correlation with other systems.
- Deploy additional sensors.

Federal Office for Information Security

Thank you! - Questions?

Contact

Federal Office for Information Security (BSI)
Godesberger Alle 185-189
53175 Bonn, Germany

www.bsi.bund.de

Martin.Bierwirth@bsi.bund.de
Andre.Vorbach@bsi.bund.de

Tel: +49 (0)228 99 9582-5119
-5830