

# **Some Thoughts on Malicious Mobile Code**

**Panel at RAID 2003**

**Arno Wagner**

**Computer Engineering and Networking Laboratory**

**Swiss Federal Institute of Technology at Zurich**

# Background / Current Research

## Background:

- Security (some Crypto)
- Formal methods: Model Checking, specification, verification
- Some OO
- Some EE (digital only)

## Research: Massive malicious network events in Internet backbones:

- Worms
- (D)DoS

## Some Subjective Predictions

- **Worms will become irrelevant when**
  - **There are no large OS/application mono-cultures**
  - **OS and applications are designed with security in mind**

⇒ **Not anytime soon!**
- **Cleanup after worms will take longer and longer:**

**Months, years, ...**

  - **More and more always-on computers without competent administrators**
  - **Less intrusive worms**
  - **Worms that hide and sleep**

## **More Predictions**

**We will see more application worms:**

- **P2P filesharing**
- **Messaging**
- **(Mobile) Agents**
- **Email (classics never go out of fashion...)**

**ISPs seem not really be able/willing to handle the problem:**

**Could a legal solution work? Worldwide?**

**Will computer administrators become liable/need a licence/...???**

## Why Detect Malicious Mobile Code?

- **Quarantine: Not likely to work ...**
- **Understand what happened: Yes**
- **Damage assessment: Yes**
- **Cleanup: Definitely!**
- **Mitigate (side)effects (in RT?): Definitely!**
- **...**

# DDoSVax

<http://www.tik.ee.ethz.ch/~ddosvax> or google("ddosvax")

- **Focus: Detection and countermeasures for DDoS attacks on the backbone level**
- **(Fast) Worms: Preferred tool to acquire attacking hosts**
- **Start: Early 2003**
- **Partially funded by and in collaboration with SWITCH (Swiss Academic and Research Network, carried about 5% of Swiss Internet traffic in 2002)**

## **DDoSVax: Captured Data**

### **Cisco Netflow:**

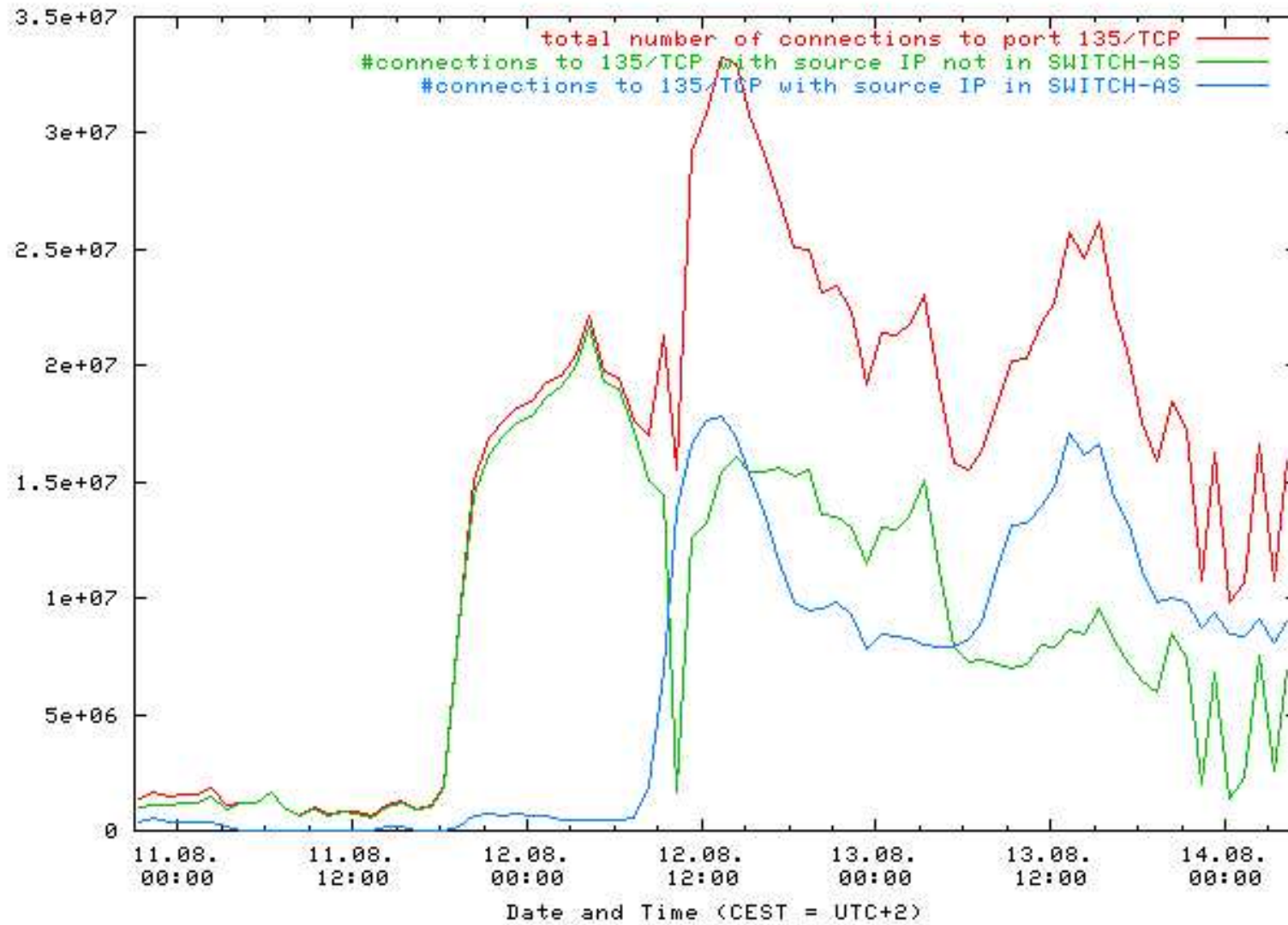
- **About 1.5GB/hour Netflow data (Nachia: 3GB/hour)**
- **Netflow is bursty  $\Rightarrow$  Logging is non-trivial**
- **Simple data processing: 20 CPU minutes/hour of data**
- **Storage: Currently several TBytes on tape**

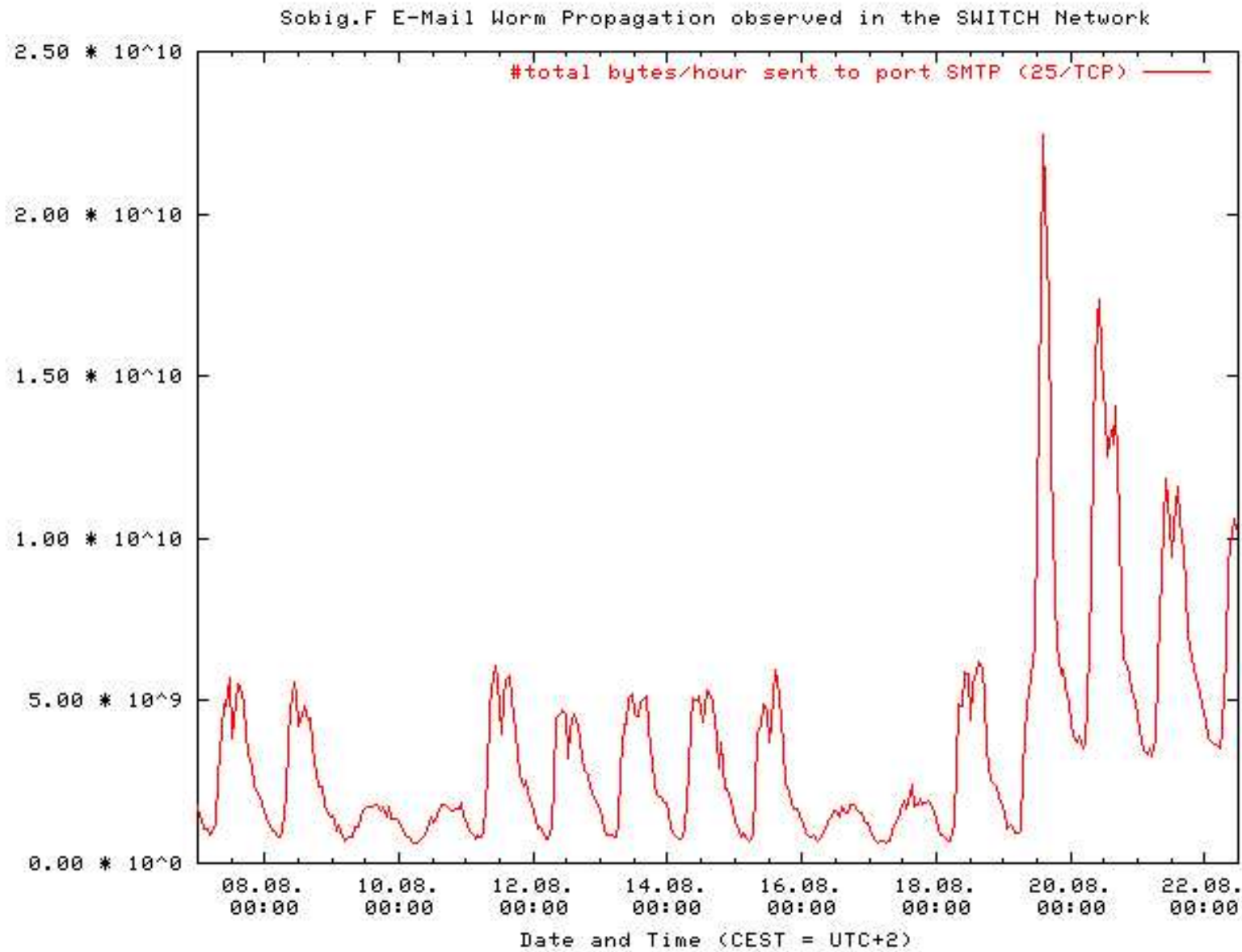
## **DDoSVax: Results**

- **Full capturing and storage of SWITCH Netflow data**
- **Manual analysis of W32.Blaster, Nachia, SoBig.F network data**
- **Simulator to predict (fast) worm behaviour (WORM 2003)**



W32.Blaster Worm Propagation observed in the SWITCH Network





## Applied Stupidity: Nachia

**”Counter-Worm” for W32.Blaster.**

- **Does not really work, W32.Blaster still active**
- **Side-Effect: Roughly 100% more Netflow data**
- **Side-Effect: Some ISPs have serious problems**

**August, 28th (Thursday), 6:21-7:21 :**

- **Flows: All: 60,134,084 ICMP: 905,411 (1.5%) Nachia: 28,264,392 (47%)**
- **Bytes: All: 290 GB Nachia: 2.6 GB (0.9%)**
- **Packets: All: 466,081,451 Nachia: 28,264,392 (6%)**

## DDoSVax: Next Steps

- **Test more detection algorithms on the data**
  - Graph-based
  - "Entropy"-based
  - ?
- **Acquire more CPU power**
- **Look at behaviour network applications, mostly P2P**

## **Even More Subjective Predictions**

**We will need router-integrated support for**

- **Logging network traffic with flexible level of abstraction**
- **Detection of Malicious Mobile Code**
- **Filtering of worms, scan-traffic, infection-attempts**
- **Filtering of large numbers of individual IP addresses**

**All of the above also for IPv6!**