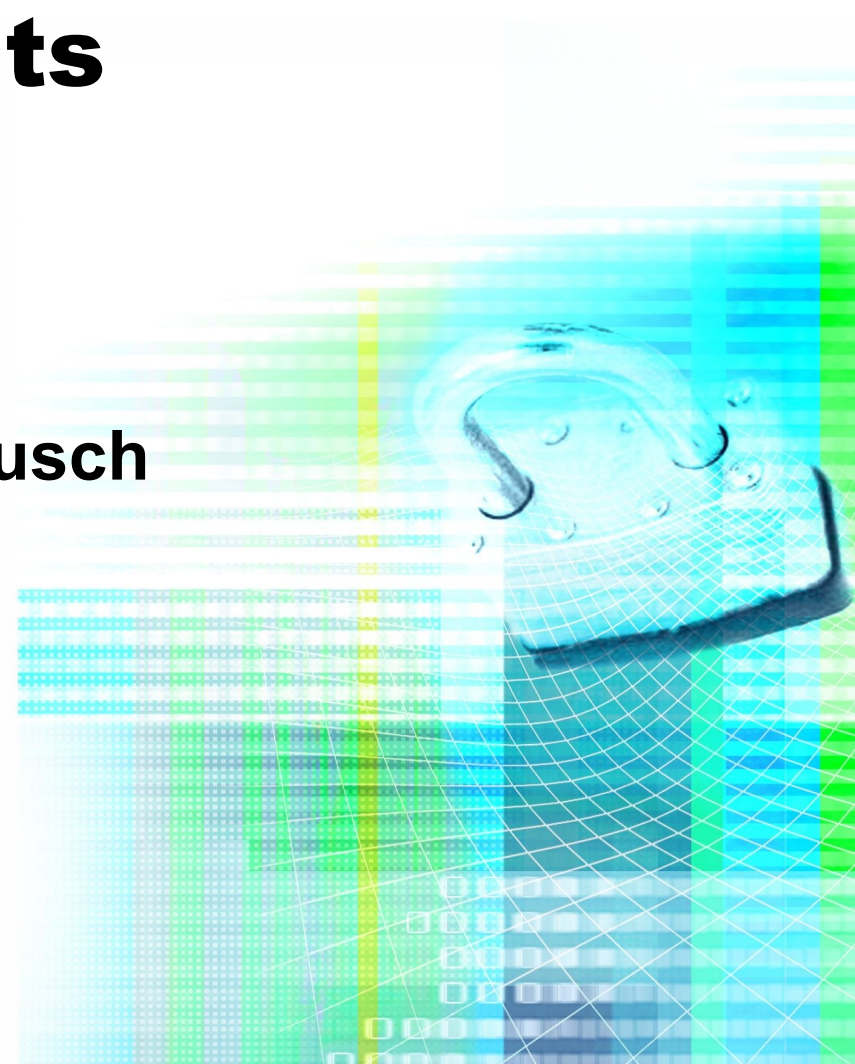


# **NoAH Developments**

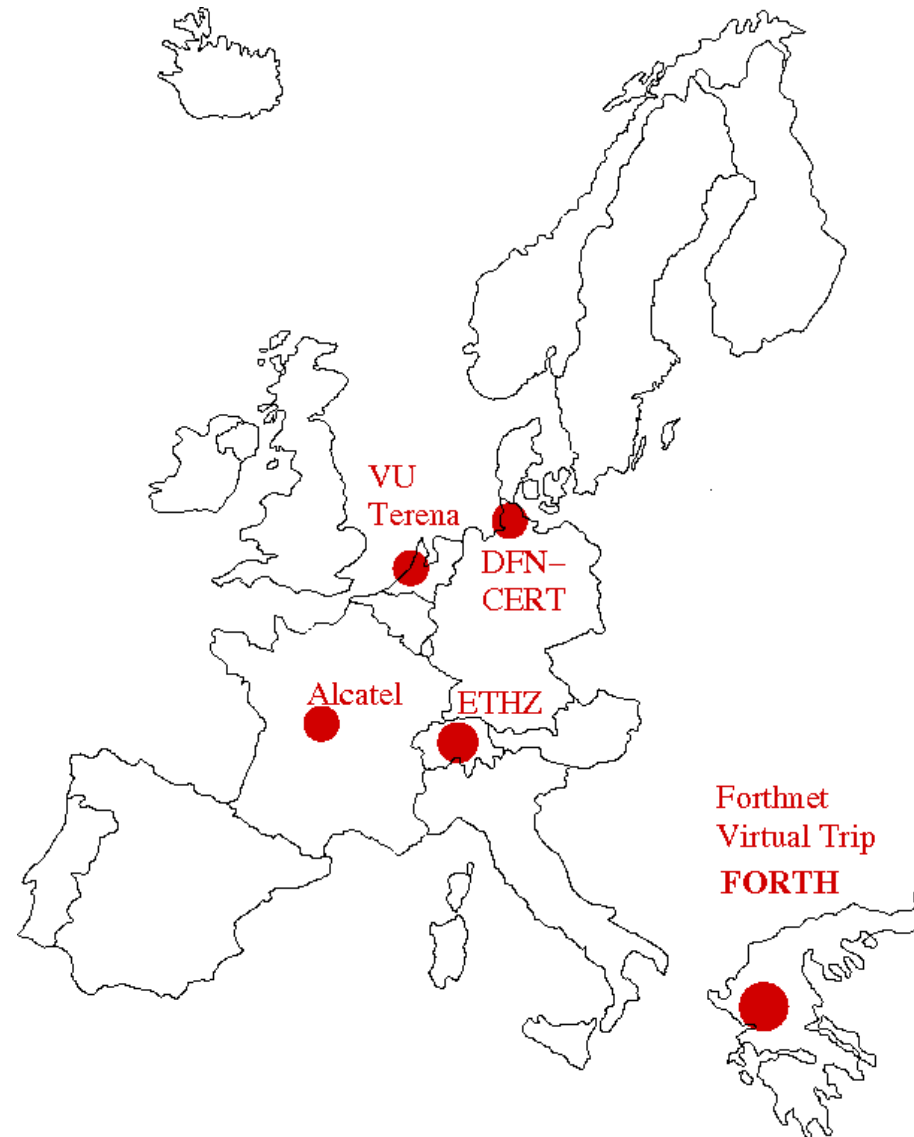
**Andreas Buntен / Jan Kohlrausch**

**DFN-CERT Services GmbH**  
[buntен|kohlrausch]@dfn-cert.de

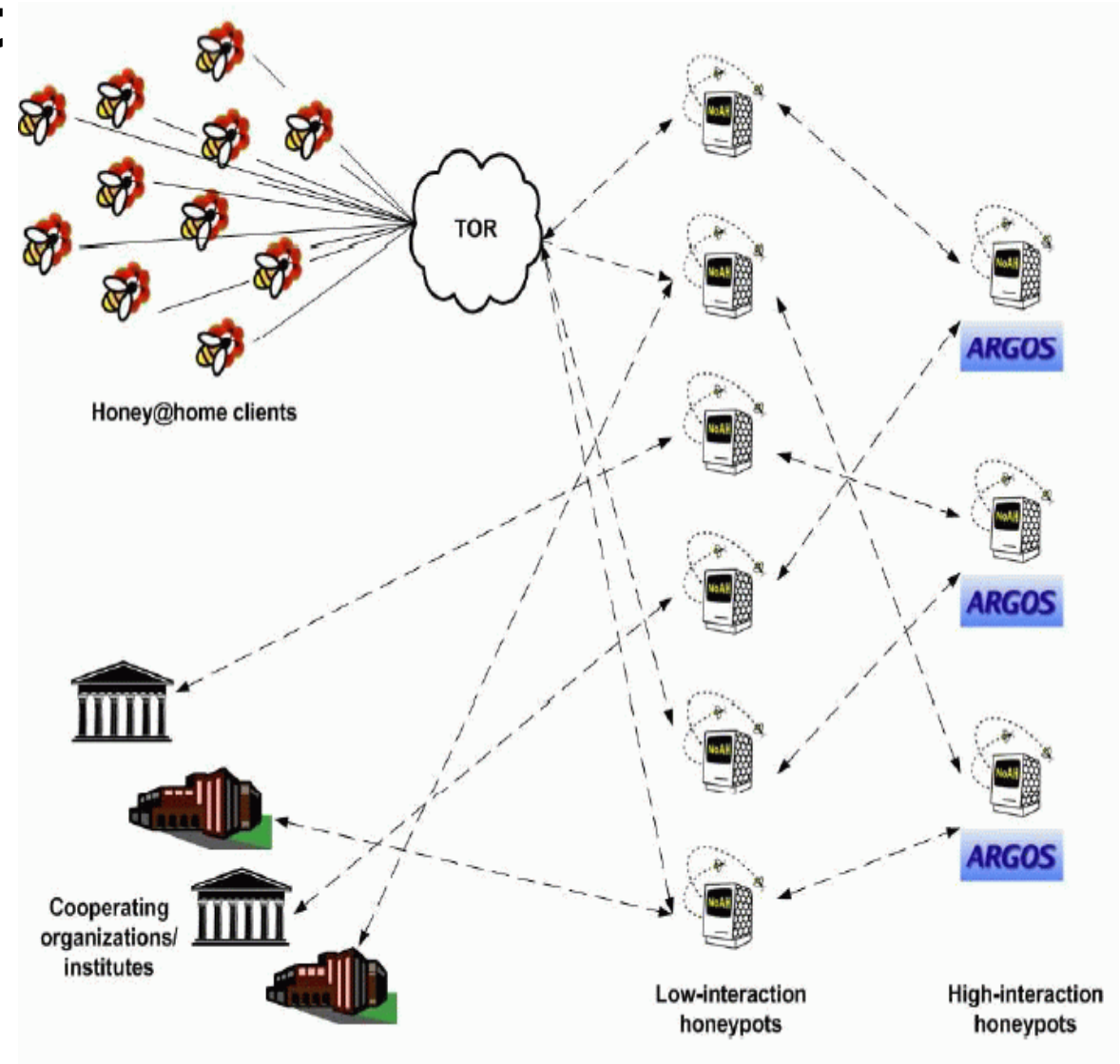


- **EU project of the 6th framework**

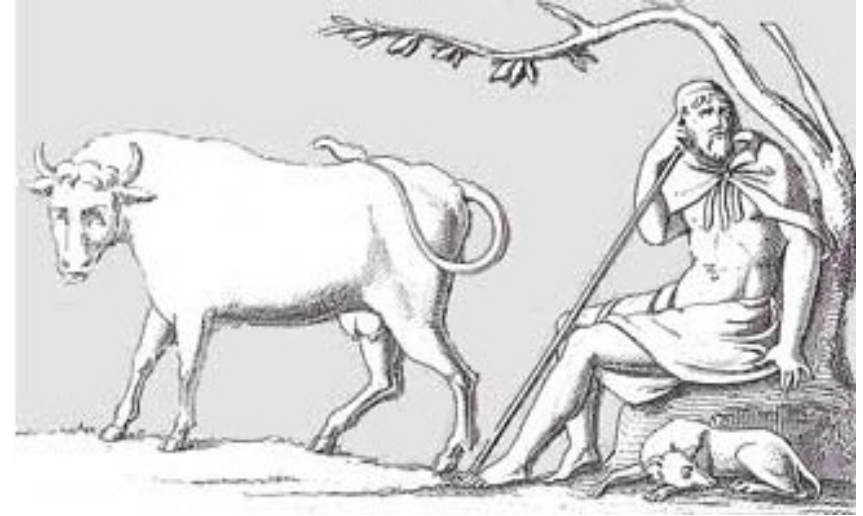
- Leader: FORTH
- Start April 2005
- End Sep 2008



- **Set-up of a honeynet**
- **Hybrid architecture**
  - Cooperation of:
    - low-interaction sensors
    - high-interaction (Argos-sensors)
- **Generation of attack signatures**



- High-interaction honeypot
  - Based on QEMU emulator
- Instrumented for dynamic taint analysis on network data
  - Designed to reliably detect buffer overflow and related attacks



# NoAH Project: Argos alert

```
kohlrausch@wayne:.../honey/qemu/alerts
carlog v0.1.2 Copyright(c) G Portokalidis

Net tracker data: YES Attack-packet available?

VERSION          ARCH          TYPE          Type of alert          TIMESTAMP
0x02             i386          RET           alert                  1194963783

EAX              ECX              EDX              EBX
0x00000000      0x000acdd0     0x00085aea      0x005bfd18
(0x00000000)    (0x00000000)   (0x00000000)    (0x00000000)
[ 637]         [ 637]         [ 637]         [ 637]

ESP              EBP              ESI              EDI
0x005bf7bc     0x19eb10eb     0x000bb310      0x000bc7fc
(0x00000000)   (0x067957ac)  (0x00000000)    (0x00000000)
[ 637]         [ 669]         [ 637]         [ 637]

EIP              Faulty EIP          EFLAGS
0x0018759f     0x75879a8d        0x00000202
(0x067957b0)
[673]          Address of RET assembly command

Program counter
BLOCK#  VERSION  TAINTED  SIZE  PADDR          VADDR
0       0x01    YES      4     0x06732028     0x00080028
1       0x01    YES      8     0x067b8b68     0x0008db68
2       0x01    YES     744   0x06d326b8     0x000946b8
lines 1-26
```

- **The demonstrator testbed is up**
- **Two sensors:**
  - Windows XP without any SP
    - Vulnerable Apache 1.3.24 webserver
    - A lot of other known vulnerabilities
  - SuSE 9.3
    - ssh server
    - vsftpd FTP server
    - Standard SuSE apache webserver

- **Data presentation service online**
  - Based on weasel presentation of Snort alerts
  - Extension for graphical data presentation
- **Two versions**
  - Project internal
  - Version for cooperating sites containing anonymized data

- Alerts in tabular form

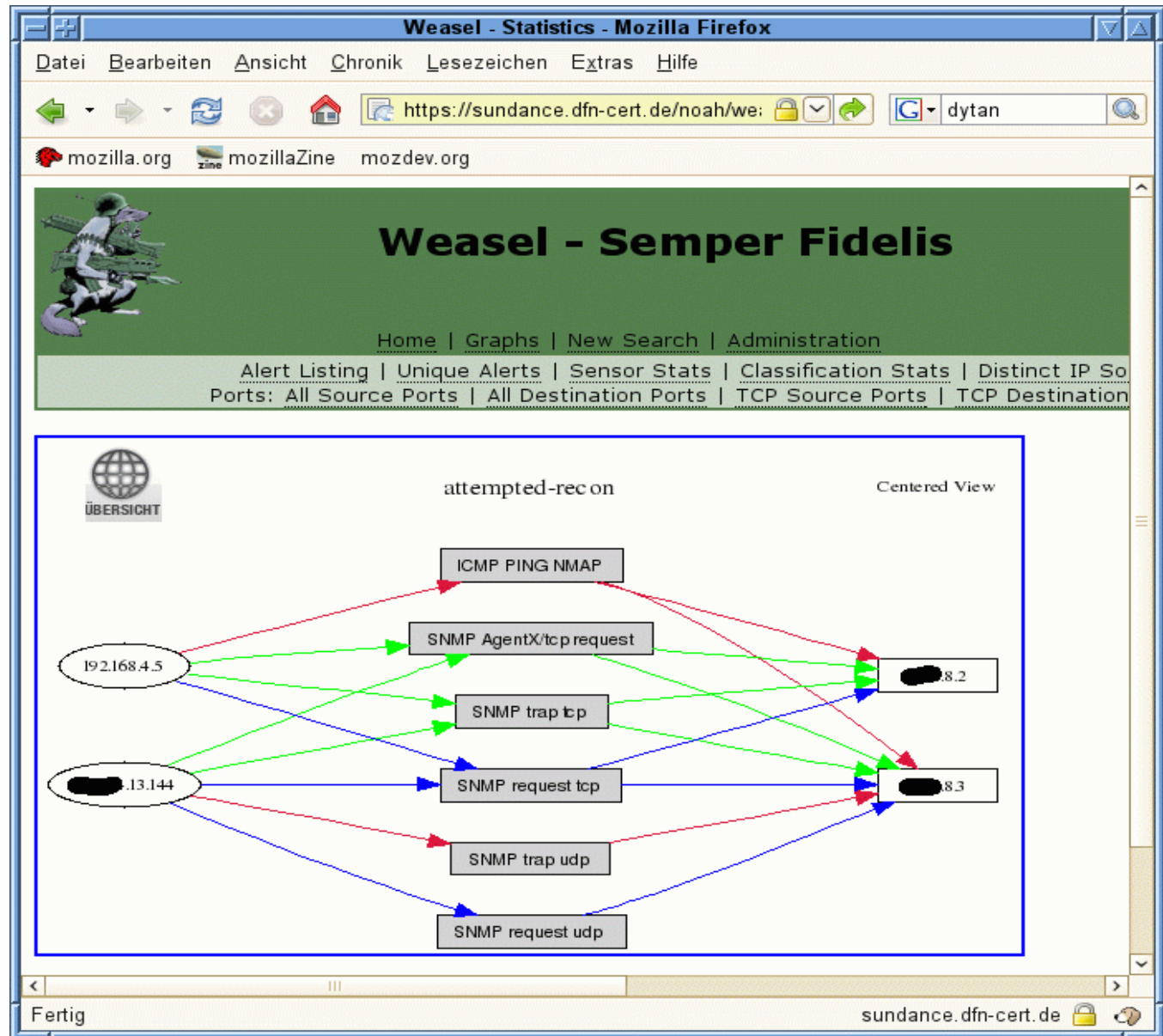
Weasel - Query Results - Mozilla Firefox

https://sundance.dfn-cert.de/noah

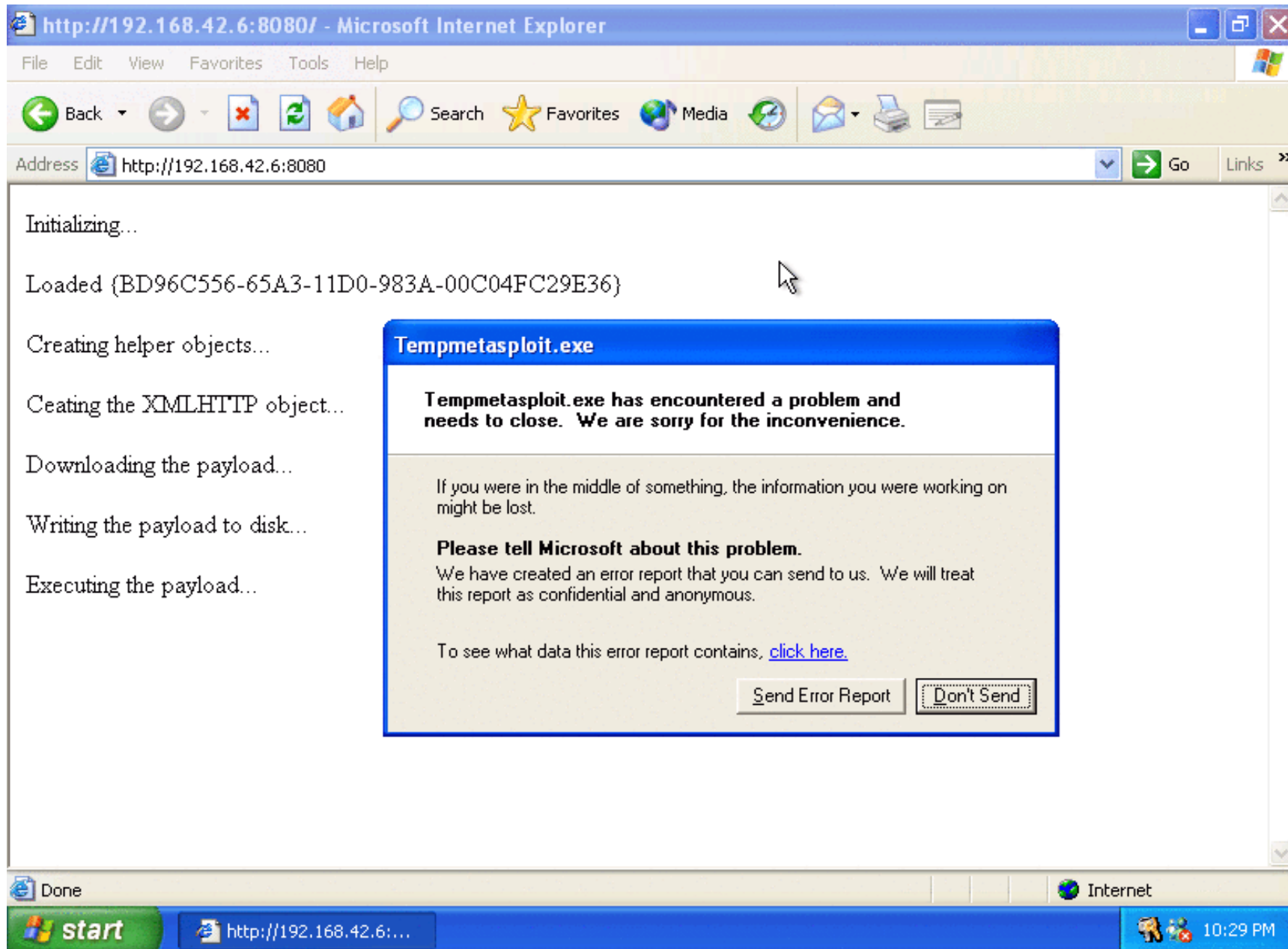
<input type="checkbox"/>	33-1997 MS-SQL Worm propagation attempt [Snort]	2008-05-06 11:15:46
<input type="checkbox"/>	34-1996 MS-SQL Worm propagation attempt OUTBOUND [Snort]	2008-05-06 11:15:46
<input type="checkbox"/>	35-1995 MS-SQL Worm propagation attempt [Snort]	2008-05-06 11:06:44
<input type="checkbox"/>	36-1994 MS-SQL Worm propagation attempt OUTBOUND [Snort]	2008-05-06 11:06:44
<input type="checkbox"/>	37-1993 MS-SQL Worm propagation attempt [Snort]	2008-05-06 06:28:30
<input type="checkbox"/>	38-1992 MS-SQL Worm propagation attempt OUTBOUND [Snort]	2008-05-06 06:28:30
<input type="checkbox"/>	39-1991 MS-SQL Worm propagation attempt [Snort]	2008-05-06 05:49:26
<input type="checkbox"/>	40-1990 MS-SQL Worm propagation attempt OUTBOUND [Snort]	2008-05-06 05:49:26
<input type="checkbox"/>	41-1989 BLEEDING-EDGE EXPLOIT NETBIOS SMB-DS DCERPC NetrpPathCanonicalize request (possible MS06-040) [Snort]	2008-05-06 02:11:11
<input type="checkbox"/>	42-1988 BLEEDING-EDGE EXPLOIT NETBIOS SMB-DS DCERPC NetrpPathCanonicalize request (possible MS06-040) [Snort]	2008-05-06 02:11:10
<input type="checkbox"/>	43-1987 MS-SQL Worm propagation attempt [Snort]	2008-05-06 01:31:42
<input type="checkbox"/>	44-1986 MS-SQL Worm propagation attempt OUTBOUND [Snort]	2008-05-06 01:31:42
<input type="checkbox"/>	45-1985 MS-SQL Worm propagation attempt [Snort]	2008-05-06 01:09:50
<input type="checkbox"/>	46-1984 MS-SQL Worm propagation attempt OUTBOUND [Snort]	2008-05-06 01:09:50
<input type="checkbox"/>	47-1983 MS-SQL Worm propagation attempt	2008-05-05 22:56:36

https://sundance.dfn-cert.de/noah/weasel004/index.php?action=stdstat&filt...

- **Attacks in graphical form**



- Very few attacks against SuSE linux
- MS-SQL worm is by far the most frequent attack detected by snort and Argos
- Many attacks exploiting known windows vulnerabilities
  - Not all succeed
  - Corresponding snort alert for each attack
  - However, not all are detected by snort as exploit
- No attacks against vulnerable apache server



- **Next steps will extend the demonstrator testbed**
- **Cooperating sites are welcome!**
  - Will be announced on the TF-CSIRT mailing-list

# Questions?

**Andreas Bunten / Jan Kohlrausch**  
**<https://www.dfn-cert.de/>**  
**[bunten|kohlrausch]@dfn-cert.de**