The Honeynet

PROJECT

HonEeeBox – Rapid Deployment of Many Distributed Low Interaction Malware Collectors

AusCERT 2009

David Watson david@honeynet.org.uk

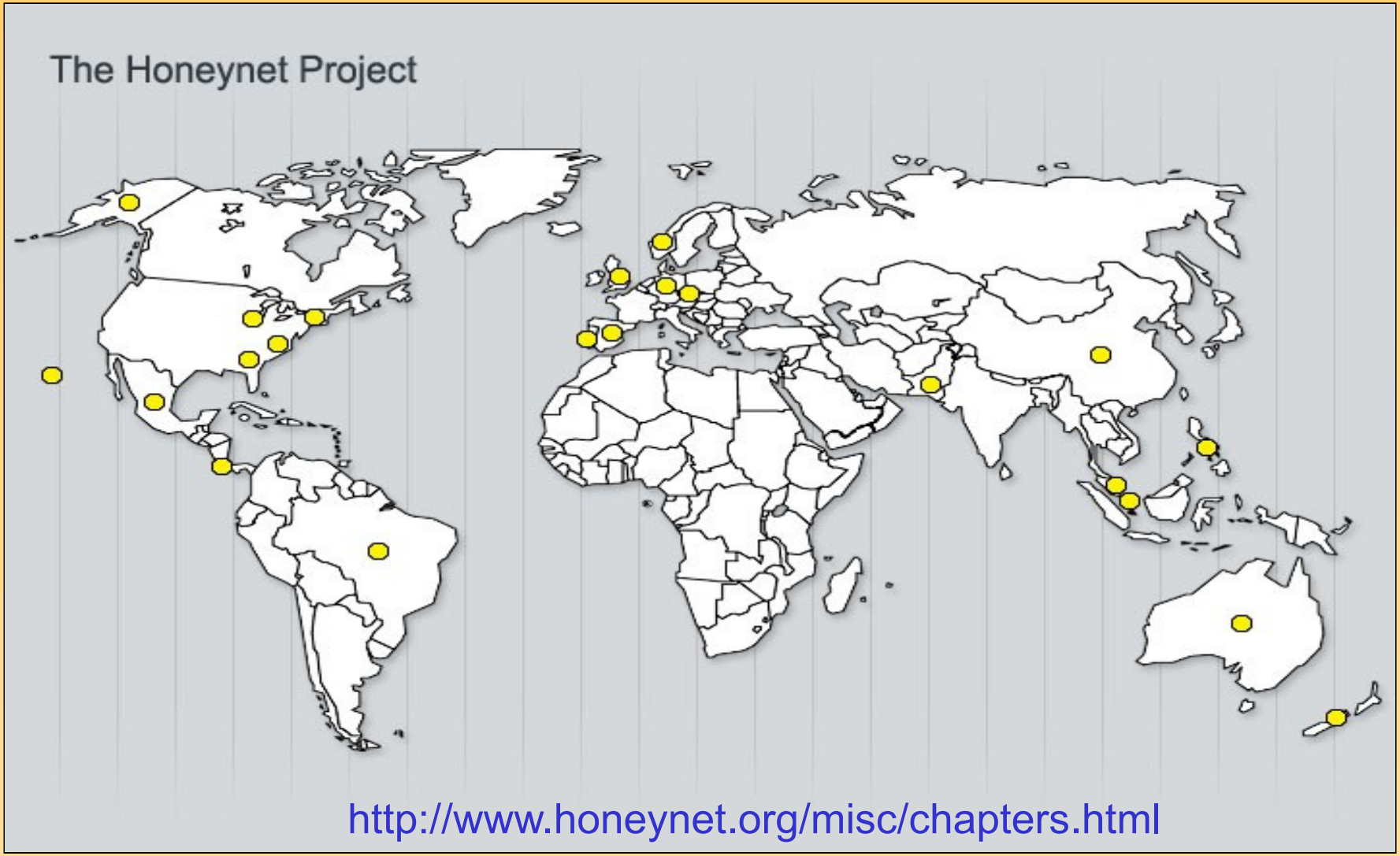
The Honeynet PROJECT®

Speaker

shadowserver

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

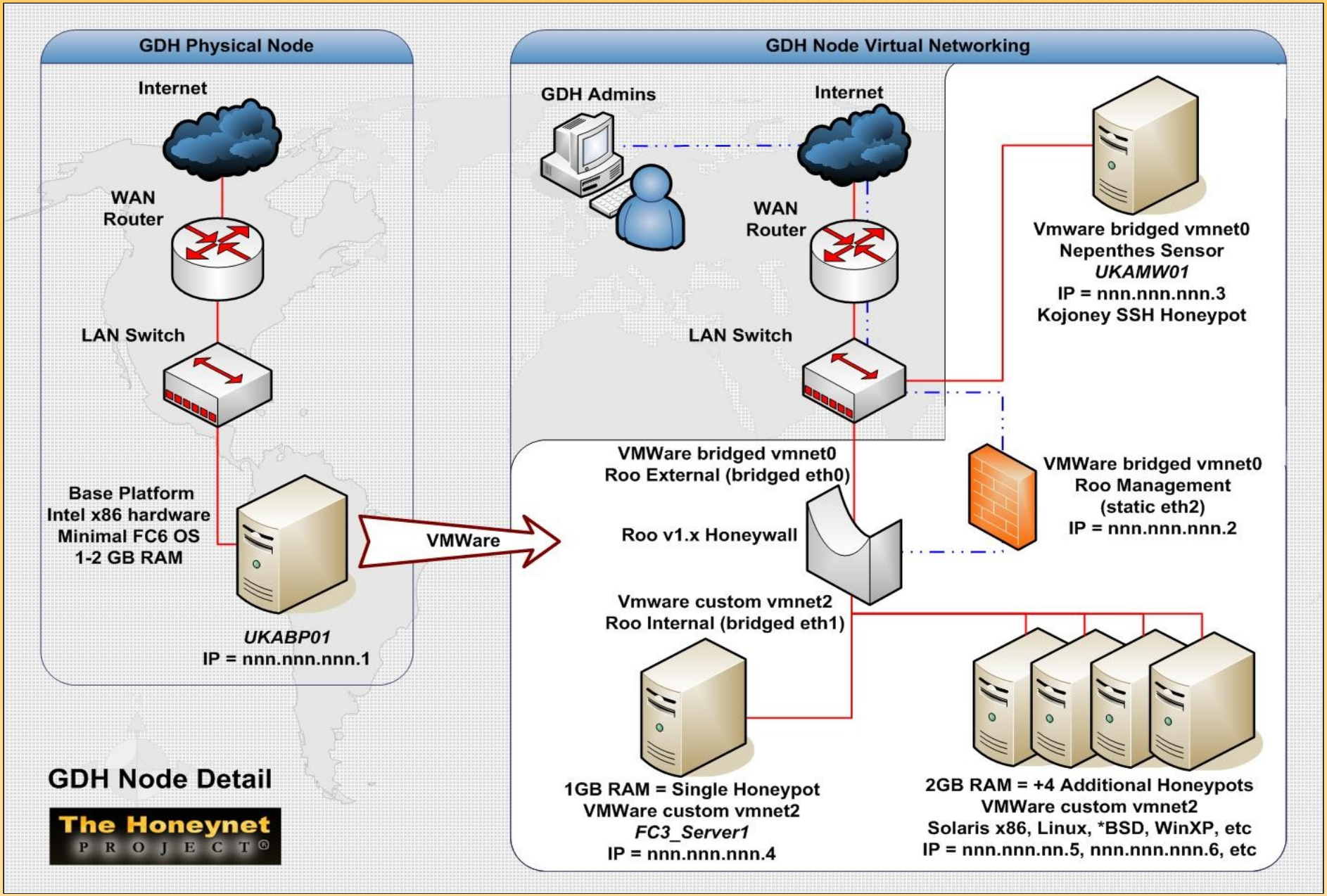
25 International Chapters

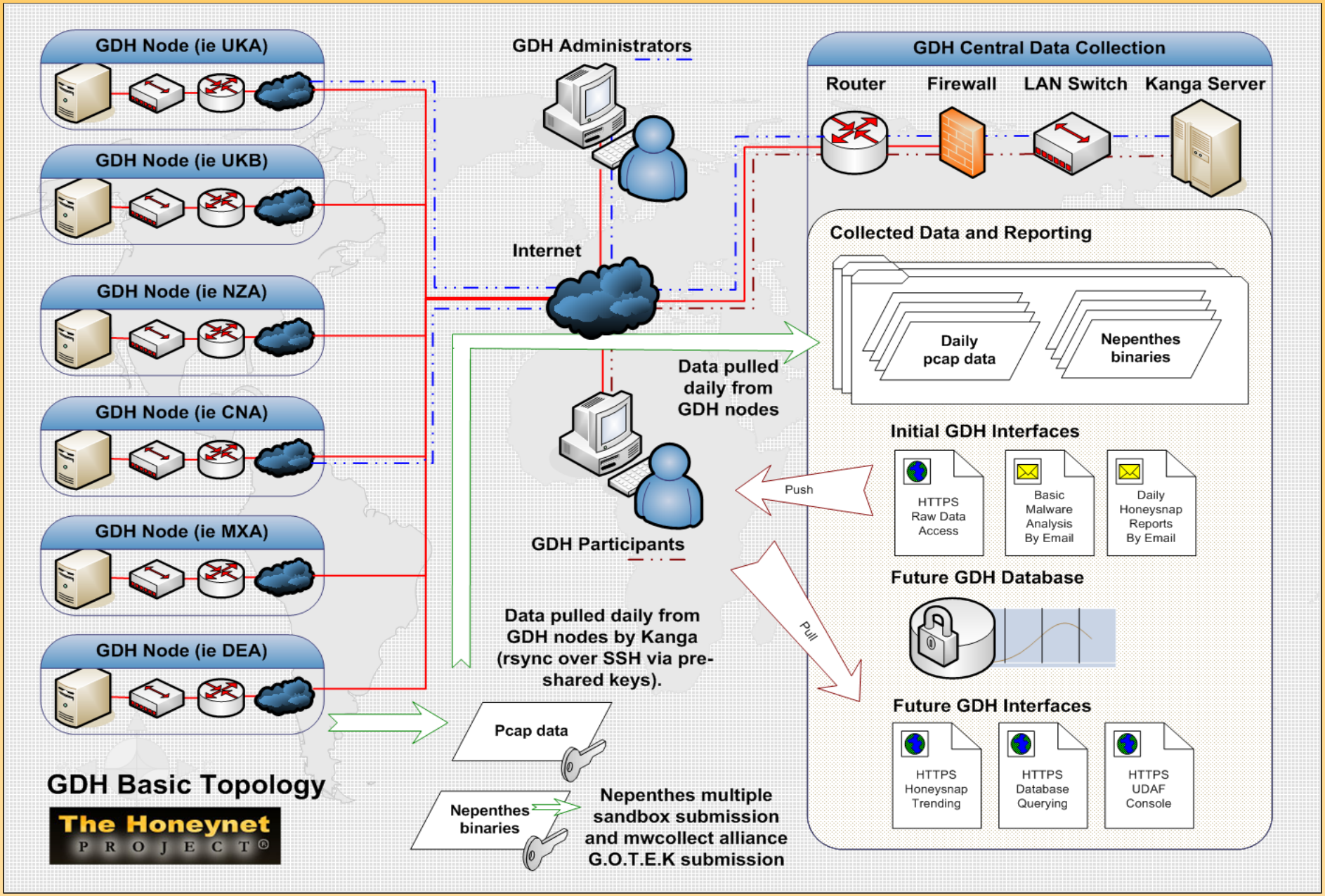


GDH Phases 1 and 2

- Global Distributed Honeynet (GDH)
- Previous efforts to deploy and operate long running standardised low and high interaction virtual honeynets
- Multiple identical international nodes
- Centralised data collection and analysis (DA)
- Human analysts responding to incidents
- GDH1 voted best talk at PacSec 2007
- Ongoing R&D effort, continuing in 2009/2010

http://www.ukhoneynet.org/PacSec07_David_Watson_Global_Distributed_Honeynet.pdf


GDH Physical Node
Internet
WAN Router
LAN Switch
Base Platform
Intel x86 hardware
Minimal FC6 OS
1-2 GB RAM
UKABP01
IP = nnn.nnn.nnn.1
VMWare
GDH Node Virtual Networking
GDH Admins
Internet
WAN Router
LAN Switch
Vmware bridged vmnet0
Nepenthes Sensor
UKAMW01
IP = nnn.nnn.nnn.3
Kojoney SSH Honeypot
VMWare bridged vmnet0
Roo External (bridged eth0)
Roo v1.x Honeywall
VMWare bridged vmnet0
Roo Management
(static eth2)
IP = nnn.nnn.nnn.2
Vmware custom vmnet2
Roo Internal (bridged eth1)
1GB RAM = Single Honeypot
VMWare custom vmnet2
FC3_Server1
IP = nnn.nnn.nnn.4
2GB RAM = +4 Additional Honeypots
VMWare custom vmnet2
Solaris x86, Linux, *BSD, WinXP, etc
IP = nnn.nnn.nn.5, nnn.nnn.nnn.6, etc
GDH Node Detail
The Honeynet PROJECT®

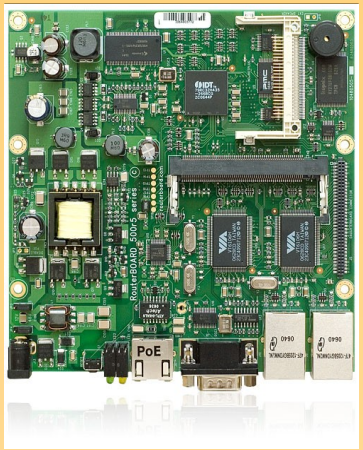

GDH Node (ie UKA)
GDH Node (ie UKB)
GDH Node (ie NZA)
GDH Node (ie CNA)
GDH Node (ie MXA)
GDH Node (ie DEA)
GDH Administrators
Internet
GDH Central Data Collection
Router
Firewall
LAN Switch
Kanga Server
Collected Data and Reporting
Daily pcap data
Nepenthes binaries
Data pulled daily from GDH nodes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

New “HonEeeBox” Project

- Build small, cheap, highly portable low interaction honeypots for distributed malware collection to a central location
- Deploy widely and internationally (100's)
- Anonymous central sample submission
- 'Outsource' malware binary analysis to Shadowserver, VirusTotal, etc
- Focus development on reporting and analysis UI, then improving data analysis
- Also add netflow and p0f data recording

Embedded Nepenthes

- Spent a fair bit of time building embedded Nepenthes sensors on many platforms



OpenWrt
Wireless Freedom

vmware

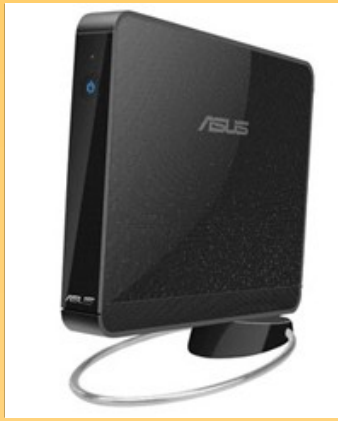
http://www.ukhoneynet.org/category/howto

Embedded Sensors Pros/Cons

- ✔ Consumer hardware
- ✔ Cheap
- ✔ Small
- ✔ Quiet
- ✔ Low power
- ✔ Reliable
- ✔ Easy to ship
- ✔ Minimal footprint

- ✗ Cross compiling
- ✗ Slow development
- ✗ Endian-ness
- ✗ Capacity
- ✗ Performance
- ✗ Poor console / UI
- ✗ Upgrade re-flash
- ✗ Making bricks!

Asus Eee PC Box (B202)



- Best of both worlds
- Intel Atom x86 CPU
- 1.6 GHz HT
- 1GB RAM
- 160GB hard disk
- Standard PC I/O
- Hardware warranty
- Comparable price

- Still small, quiet, low power, easy to ship
- Normal Linux distros
- Simple to reinstall
- Update from image
- Upgrade from repos

HonEeeBox

- Scripts to build a bootable ISO or USB image:
  - Live CD sensor
  - Live CD sensor with disk persistence
  - Live USB sensor
  - Live USB sensor with disk persistence
  - Virtual appliance
  - Hard disk installation (ideally to Eee Box PC)
  - SHDC card installation, no moving parts

HonEeeBox

- Minimal Debian-Live system (Lenny 5.0)
- Custom Nepenthes .deb created from the current Nepenthes release in svn
- DHCP plus automatic live CD login
- Patch and upgrade on the fly via apt
- Permanent installation prompts for locale, network configuration, etc as normal
- Basic anonymous HTTPS submission

```
egin: Setting up locales ... Generating locales (this might take a while)...
 en_US.UTF-8... done
eneration complete.
one.
egin: Setting up automatic login ... done.
egin: Setting up console keyboard ... done.
egin: Configuring gnome-panel-data ... done.
egin: Configuring screensaver ... done.
egin: Preconfiguring /etc/modules ... done.
egin: Preconfiguring networking ... done.
egin: Running /scripts/init-bottom ... done.
NIT: version 2.86 booting
tarting the hotplug events dispatcher: udevd[    8.512504] udevd version 125 s
rted

ynthesizing the initial hotplug events...done.
aiting for /dev to be fully populated...[    8.873512] Linux agpgart interface
0.103
    8.876631] agpgart: Detected an Intel 440BX Chipset.
    8.876706] agpgart: AGP aperture is 256M @ 0x0
    8.884715] pci_hotplug: PCI Hot Plug PCI Core version: 0.5
    8.884984] shpchp: Standard Hot Plug PCI Controller Driver version: 0.4
                                                        as /class/input/input1
                                                        [PWRF]
```

```
Press F1 for help, or ENTER to boot: _
admin@debian: $ ps -ef ; grep nepen
101       2612     1  0 08:28 ?        00:00:00 /opt/nepenthes/bin/nepenthes --
ser=nepenthes --group=nepenthes
admin     2703  2667  0 08:31 tty1     00:00:00 grep nepen
admin@debian:~$
admin@debian:~$
admin@debian:~$ tail /opt/nepenthes/var/log/nepenthes.log
26022009 08:28:07 info sc module] Loading signatures from file
nes/signatures/shellcode-signatures.sc
26022009 08:28:08 debug info fixme] Logfile var/log/nepenthes.
now 101:103 (nepenthes:nepenthes)
26022009 08:28:08 crit mgr] Compiled without support for capab
 run capabilities
26022009 08:28:08 info mgr] Process groupid 103
26022009 08:28:08 info mgr] Process userid 101
admin@debian:~$ _
```

```
[!!] Choose language

Please choose the language used for the installation process. This
language will be the default language for the final system.

Choose a language:

        C                    -  No localization
        Albanian             -  Shqip
        Arabic               -  عربي
        Basque               -  Euskara
        Belarusian           -  Беларуская
        Bosnian              -  Bosanski
        Bulgarian            -  Български
        Catalan              -  Català
        Chinese (Simplified) -  中文(简体)
        Chinese (Traditional) -  中文(繁體)
        Croatian             -  Hrvatski
        Czech                -  Čeština
        Danish               -  Dansk
        Dutch                -  Nederlands
        English              -  English
        Esperanto            -  Esperanto

    <Go Back>

<Tab> moves between items; <Space> selects; <Enter> activates buttons
```

HonEeeBox Participation

- 1+ public IP addresses (more is better)
- 1+ networked x86 PC/server(s) to boot ISO or USB key **or** space to host HonEeeBox sensor hardware
- Be willing to submit basic attack data

  (SRC IP, download URL, MD5, timestamp, binary, etc)
- Be willing to share collected malware samples with all participants and project sponsors
- Submissions from existing Nepenthes sensors
- Funding for additional sensor deployment
  - Regional, CERT, industry, academic, etc
- Sponsorship ;-)

HonEeeBox Summary

Total Attacks: 56 | Total Source IPs: 6 | Total Target IPs: 1 | Total MD5sums: 7

Attacks

ID	Time	Attacker IP	Victim IP	MD5sum	Download
1	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243
2	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.18
3	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.5
4	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.
5	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73
6	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	creceive://87.17.73
7	20 Mar 2009 17:22:37	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.165.4
8	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243
9	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.18
10	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.5
11	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.
12	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73
13	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	creceive://87.17.73
14	20 Mar 2009 17:22:37	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.165.4
15	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243
16	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.18
17	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.5
18	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.
19	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73

Page 1 of 3 IP: MD5: Rows 1 - 20 of 56

Attack Detail

ID:	2
Time:	1235924337
Sensor:	64.236.114.1
Download:	ftp://1:1@88.204.183.126:7293/netlibrary.exe
Trigger:	ftp://1:1@88.204.183.126:7293/netlibrary.exe
MD5sum:	e399196c959235c23f71ac2c5ab1192d
SHA512:	d41821a576642131e32645afc3d531dca5f6d4a09a76ad0ce71a7d49021c6906
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Attacker IP:	1089237505
Victim IP:	1089237505
Filename:	netlibrary.exe
Country:	FR
ISP:	Vodafone FR
ASN:	5142

Google Map | Google Earth | Sandbox | Anti-Virus | Graphs | PicViz | Heatmap | Cuttlefish

HonEeeBox Summary

Total Attacks: 56 | Total Source IPs: 6 | Total Target IPs: 1 | Total MD5sums: 7

Attacks

ID	Time	Attacker IP	Victim IP	MD5sum	Download
1	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
2	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.183.126:7293/netlibrary.exe
3	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.58.187:4652
4	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.220.64:3647
5	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73.69:43074
6	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	creceive://87.17.73.69:59800
7	20 Mar 2009 17:22:37	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.165.49.147:2866/iqxdfdfds.com
8	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
9	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.183.126:7293/netlibrary.exe
10	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.58.187:4652
11	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.220.64:3647
12	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73.69:43074
13	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	creceive://87.17.73.69:59800
14	20 Mar 2009 17:22:37	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.165.49.147:2866/iqxdfdfds.com
15	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
16	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.183.126:7293/netlibrary.exe
17	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.58.187:4652
18	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.220.64:3647
19	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73.69:43074

Page 1 of 3 IP: MD5: Rows 1 - 20 of 56

Attack Detail

ID:	3
Time:	1236003748
Sensor:	64.236.114.1
Download:	creceive://87.175.58.187:4652
Trigger:	creceive://87.175.58.187:4652
MD5sum:	3875b6257d4d21d51ec13247ee4c1cdb
SHA512:	5e60dd302d73e64b2a4c7e3d7e22b684028a6d5a719c7869891783f5f86e2cf3
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Attacker IP:	1471101627
Victim IP:	1089237505
Filename:	index.html
Country:	BR
ISP:	Centrica Internet
ASN:	3310

Google Map | Google Earth | Sandbox | **Anti-Virus** | Graphs | PicViz | Heatmap | Cuttlefish

File **Sasser.B.exe.vir** received on **02.16.2009 14:12:41 (CET)**
Current status: **finished**
Result: **38/39 (97.44%)**

Compact | Print results

Antivirus	Version	Last Update	Result
a-squared	-	-	Net-Worm.Win32.Sasser!IK
AhnLab-V3	-	-	Win32/Sasser.worm.15872.B
AntiVir	-	-	Worm/Sasser.B
Authentium	-	-	W32/IRCBotX.BRM
Avast	-	-	Win32:Sasser-N
AVG	-	-	Obfustat.KWY
BitDefender	-	-	Win32.Worm.Sasser.B
CAT-QuickHeal	-	-	W32.Sasser.B
ClamAV	-	-	Worm.Sasser.B
Comodo	-	-	Worm.Win32.Sasser.B
DrWeb	-	-	Win32.HLLW.Jobaka
eSafe	-	-	-
eTrust-Vet	-	-	Win32/Sasser.B
F-Prot	-	-	W32/IRCBotX.BRM
F-Secure	-	-	Net-Worm:W32/Sasser.A
Fortinet	-	-	W32/Sasser.B
GData	-	-	Win32.Worm.Sasser.B
Ikarus	-	-	Net-Worm.Win32.Sasser
K7AntiVirus	-	-	Net-Worm.Win32.Sasser.a
Kaspersky	-	-	Net-Worm.Win32.Sasser.a
McAfee	-	-	W32/Sasser.worm.b
McAfee+Artemis	-	-	W32/Sasser.worm.b
Microsoft	-	-	Worm:Win32/Sasser.dam
NOD32	-	-	Win32/Sasser.B
Norman	-	-	Sasser.B
nProtect	-	-	Win32.Worm.Sasser.B

HonEeeBox Summary

Total Attacks: 56 Total Source IPs: 6 Total Target IPs: 1 Total MD5sums: 7

Attacks

ID	Time	Attacker IP	Victim IP	MD5sum	Download
1	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243
2	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.18
3	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.5
4	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.
5	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73
6	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	creceive://87.17.73
7	20 Mar 2009 17:22:37	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.165.4
8	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243
9	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.18
10	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.5
11	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.
12	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73
13	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	creceive://87.17.73
14	20 Mar 2009 17:22:37	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.165.4
15	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243
16	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.18
17	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.5
18	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.
19	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73

Page 1 of 3 IP: MD5: Rows 1 - 20 of 56

Attack Detail

ID:	15
Time:	1235801109
Sensor:	64.236.114.1
Download:	ftp://70.232.61.243:5554/16745_up.exe
Trigger:	ftp://anonymous:bin@192.168.1.64:5554/16745_up.exe
MD5sum:	1a2c0e6130850f8fd9b9b5309413cd00
SHA512:	8e1e40dedb4aa57ae5c89a75aca26a813ce5622e371049ddbc916552d1c00b48
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Attacker IP:	1189625331
Victim IP:	1089237505
Filename:	16745_up.exe
Country:	US
ISP:	AOL
ASN:	1331

Google Map | Google Earth | **Sandbox** | Anti-Virus | Graphs | PicViz | Heatmap | Cuttlefish

Scan Summary | File Changes | Reg

Technical Details

Analysis Number	1
Parent ID	0
Process ID	1340
Filename	H:\EuTeAmo.exe
Filesize	222720 bytes
MD5	79e2133fcc5b201b89a6680a7d289f6f
Start Reason	AnalysisTarget
Termination Reason	NormalTermination
Start Time	00:00.750
Stop Time	00:54.453
Detection	OK (ClamAV)
COM	COM Create Instance: H:\WINDOWS\system32\ieframe.dll, ProgID: (), Interface ID: {{000214E6-0 COM Create Instance: H:\WINDOWS\system32\urlmon.dll, ProgID: (), Interface ID: {{886D8EEB-8C
DLL-Handling	**Loaded DLLs** H:\WINDOWS\system32\ntdll.dll H:\WINDOWS\system32\kernel32.dll H:\WINDOWS\system32\advapi32.dll H:\WINDOWS\system32\RPCRT4.dll H:\WINDOWS\system32\Secur32.dll H:\WINDOWS\system32\comctl32.dll H:\WINDOWS\system32\GDI32.dll H:\WINDOWS\system32\USER32.dll H:\WINDOWS\system32\oleaut32.dll H:\WINDOWS\system32\msvcrt.dll H:\WINDOWS\system32\ole32.dll H:\WINDOWS\system32\shell32.dll H:\WINDOWS\system32\SHLWAPI.dll H:\WINDOWS\system32\version.dll H:\WINDOWS\system32\IMM32.DLL H:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.260 H:\WINDOWS\system32\pstorec.dll H:\WINDOWS\system32\ATL.DLL H:\EuTeAmo.DEU H:\EuTeAmo.DE H:\WINDOWS\system32\uxtheme.dll H:\WINDOWS\system32\msctfime.ime H:\WINDOWS\system32\msctfime.ime H:\WINDOWS\system32\WS2_32.DLL H:\WINDOWS\system32\netapi32.dll H:\WINDOWS\system32\appHelp.dll H:\WINDOWS\system32\urlmon.dll H:\WINDOWS\system32\ieframe.dll H:\WINDOWS\system32\MSCTF.dll
	New Files

HonEeeBox Summary

Total Attacks: 56 | Total Source IPs: 6 | Total Target IPs: 1 | Total MD5sums: 7

Attacks

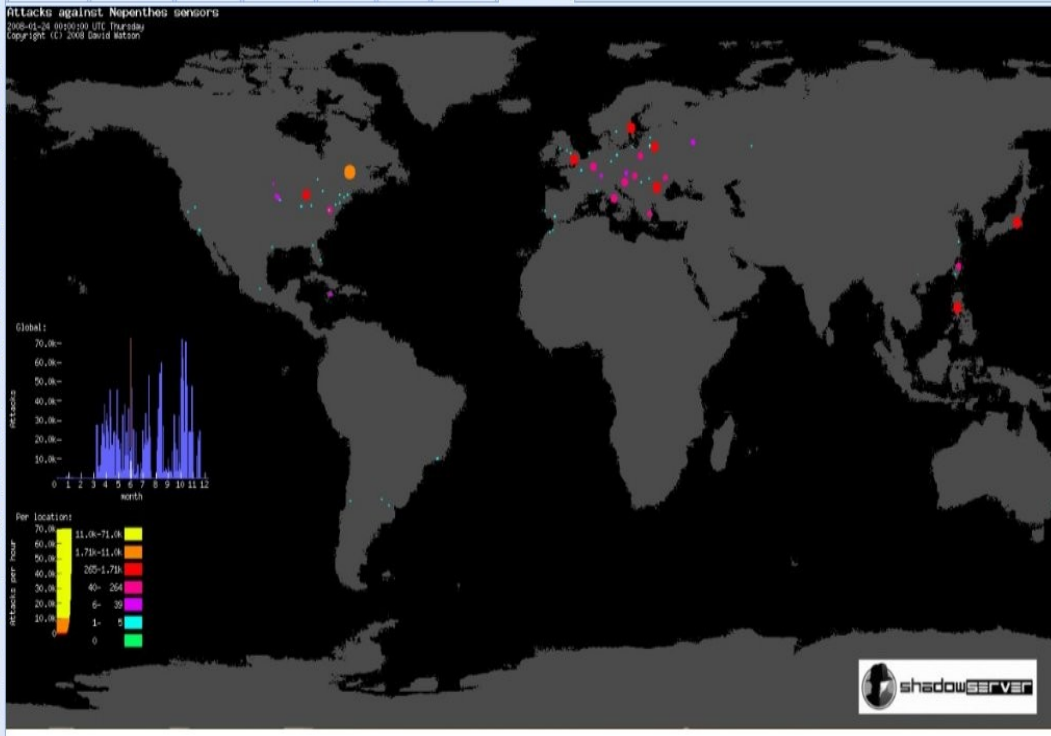
ID	Time	Attacker IP	Victim IP	MD5sum	Download
1	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243
2	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.18
3	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.5
4	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.
5	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73
6	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	creceive://87.17.73
7	20 Mar 2009 17:22:37	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.165.4
8	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243
9	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.18
10	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.5
11	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.
12	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73
13	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	creceive://87.17.73
14	20 Mar 2009 17:22:37	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.165.4
15	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243
16	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.18
17	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.5
18	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.
19	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73

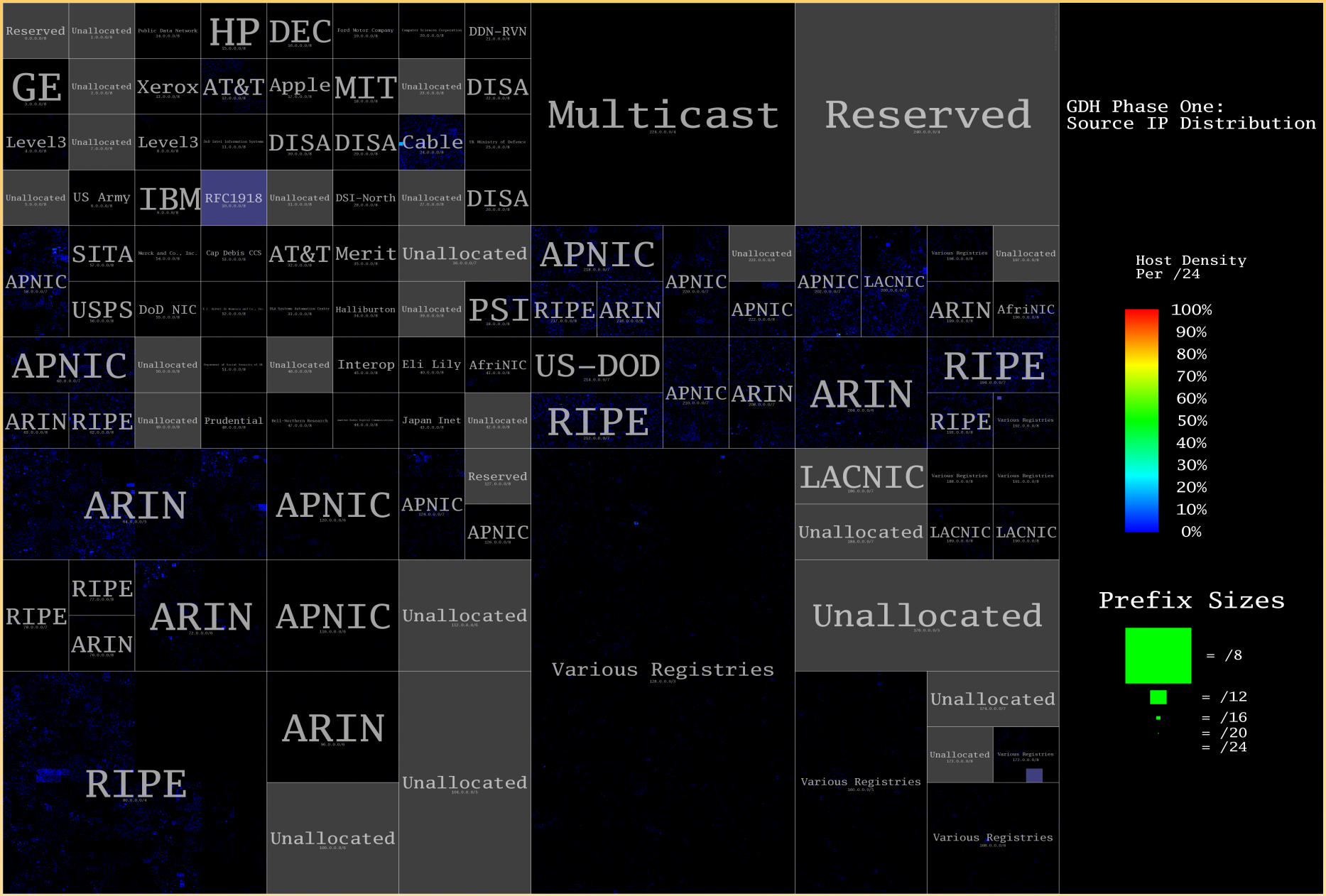
Page 1 of 3 IP: MD5: Rows 1 - 20 of 56

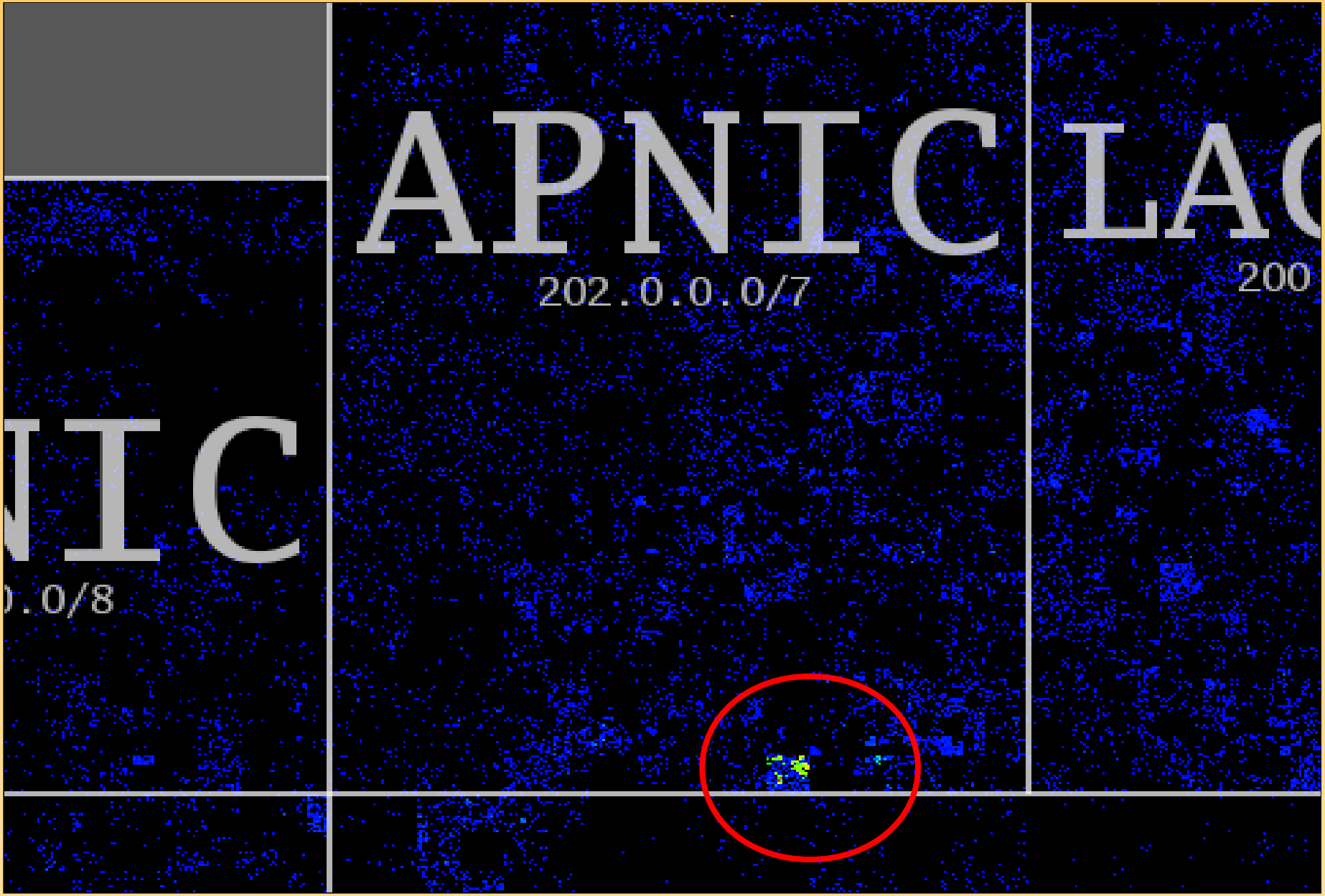
Attack Detail

ID:	16
Time:	1235924337
Sensor:	64.236.114.1
Download:	ftp://1:1@88.204.183.126:7293/netlibrary.exe
Trigger:	ftp://1:1@88.204.183.126:7293/netlibrary.exe
MD5sum:	e399196c959235c23f71ac2c5ab1192d
SHA512:	d41821a576642131e32645afc3d531dca5f6d4a09a76ad0ce71a7d49021c6906
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Attacker IP:	1089237505
Victim IP:	1089237505
Filename:	netlibrary.exe
Country:	FR
ISP:	Vodafone FR
ASN:	5142

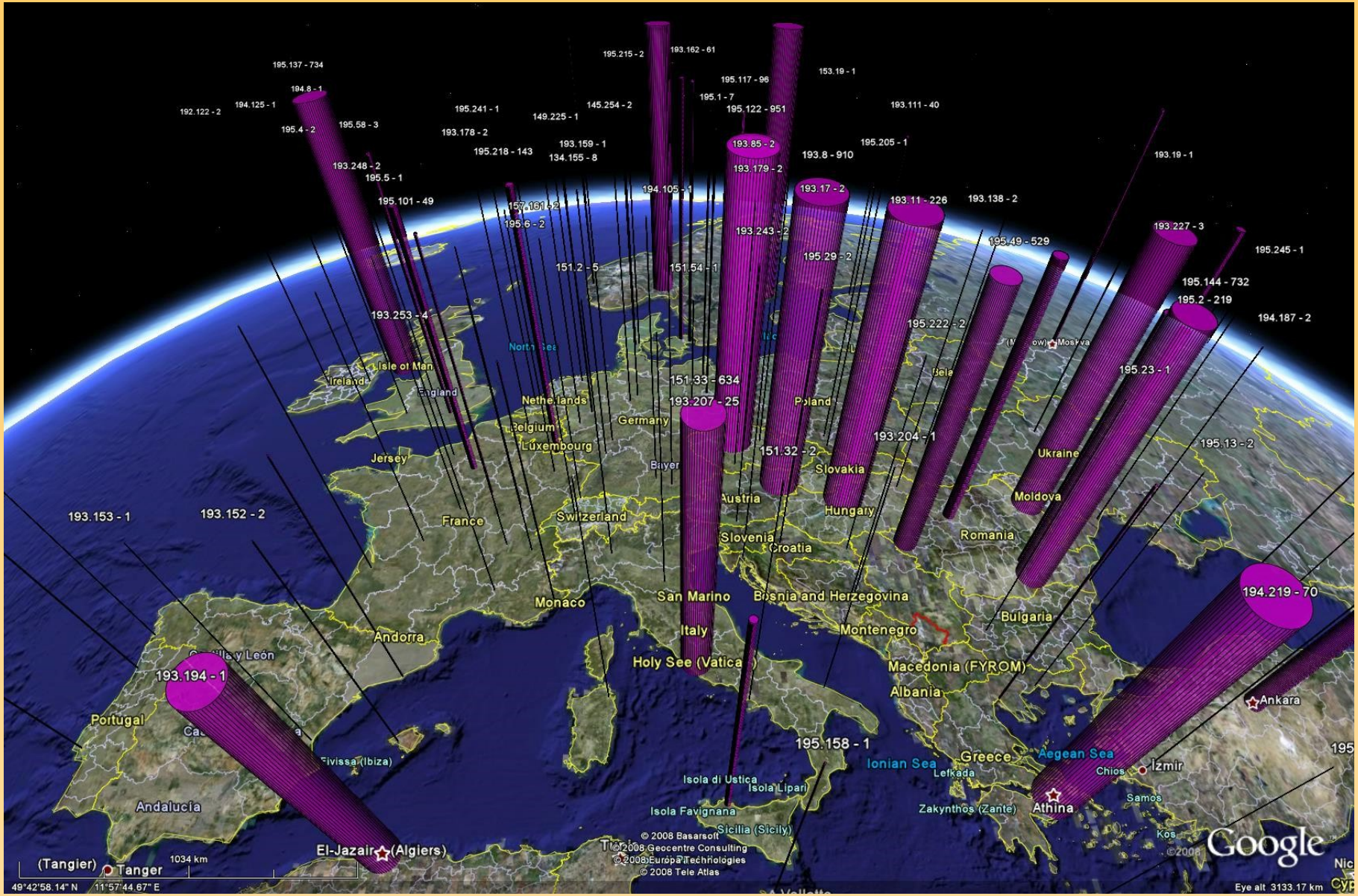
Google Map | Google Earth | Sandbox | Anti-Virus | Graphs | PicViz | Heatmap | **Cuttlefish**

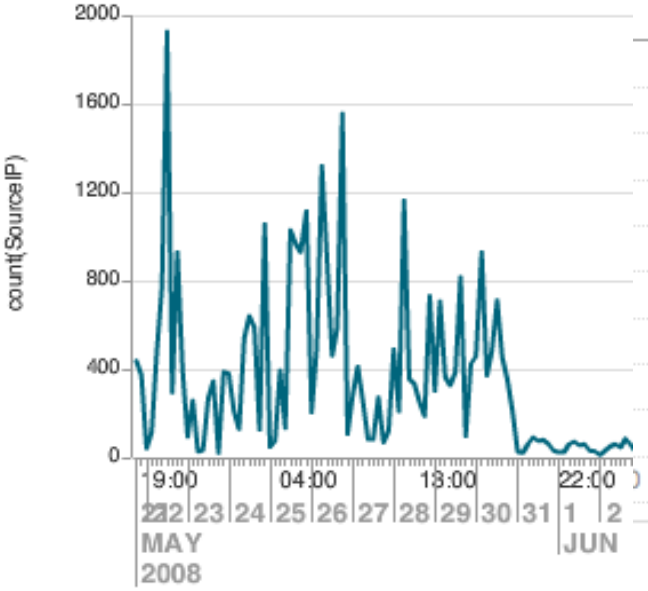



GDH Phase One:
Source IP Distribution
Host Density
Per /24
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Prefix Sizes
= /8
= /12
= /16
= /20
= /24
Reserved
Unallocated
HP
DEC
DDN-RVN
GE
Xerox
AT&T
Apple
MIT
DISA
Level3
Cable
IBM
US Army
RFC1918
DSI-North
Multicast
Reserved
APNIC
SITA
USPS
DoD NIC
Merit
PSI
RIPE
ARIN
LACNIC
AfriNIC
US-DOD
Interop
Eli Lily
Prudential
Japan Inet
Various Registries

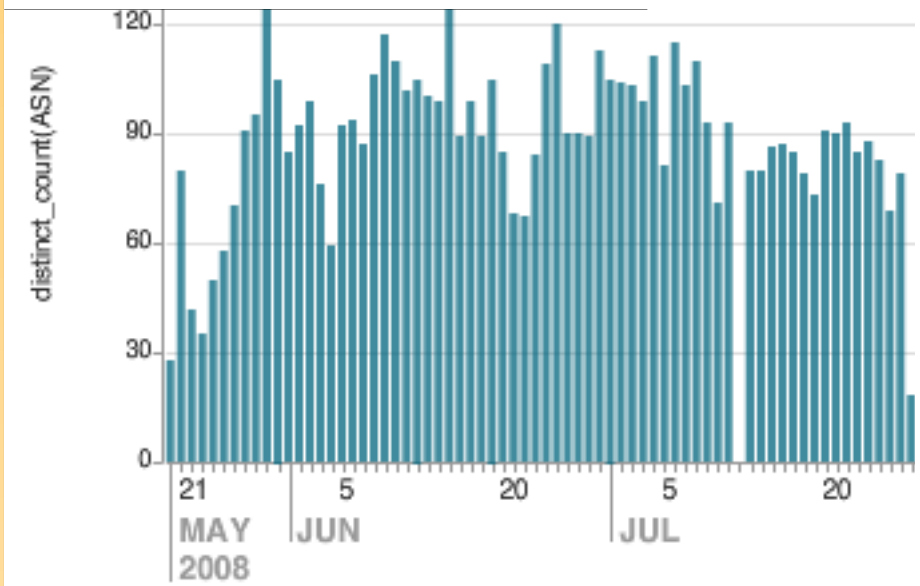


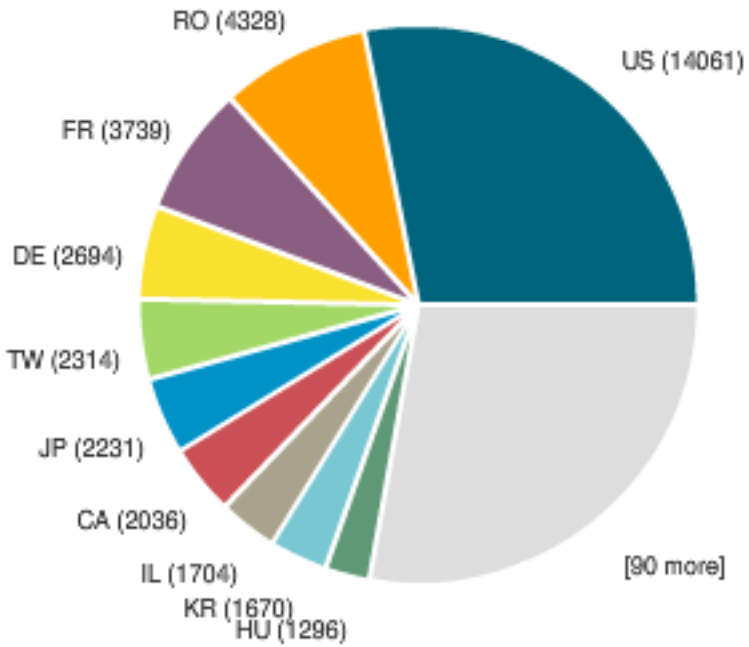
David Watson (david@honeynet.org.uk)


195.137 - 734
194.8 - 1
192.122 - 2
194.125 - 1
195.4 - 2
195.58 - 3
193.248 - 2
195.5 - 1
195.101 - 49
195.241 - 1
193.178 - 2
195.218 - 143
149.225 - 1
145.254 - 2
193.159 - 1
134.155 - 8
195.215 - 2
193.162 - 61
195.117 - 96
195.1 - 7
195.122 - 951
153.19 - 1
193.111 - 40
193.85 - 2
193.179 - 2
193.8 - 910
195.205 - 1
193.17 - 2
194.105 - 1
193.11 - 226
193.138 - 2
193.19 - 1
193.227 - 3
195.245 - 1
195.49 - 529
195.29 - 2
193.243 - 2
151.2 - 5
151.54 - 1
195.144 - 732
195.2 - 219
194.187 - 2
193.253 - 4
195.222 - 2
195.23 - 1
151.33 - 634
193.207 - 25
193.204 - 1
151.32 - 2
195.13 - 2
193.153 - 1
193.152 - 2
194.219 - 70
195.158 - 1
193.194 - 1
Isle of Man
Ireland
England
Netherlands
Belgium
Luxembourg
Germany
Jersey
France
Switzerland
Austria
Slovakia
Poland
Hungary
Ukraine
Moldova
Romania
Slovenia
Croatia
Bosnia and Herzegovina
Montenegro
Bulgaria
Macedonia (FYROM)
Albania
Greece
Monaco
San Marino
Italy
Holy See (Vatica
Andorra
Portugal
Andalucía
Ionian Sea
Aegean Sea
Lefkada
Zakynthos (Zante)
Athina
Chios
İzmir
Samos
Kos
Ankara
Isola di Ustica
Isola Lipari
Isola Favignana
Sicilia (Sicily)
Ibiza (Ibiza)
El-Jazair (Algiers)
(Tangier)
Tanger
1034 km
© 2008 Basarsoft
© 2008 Geocentre Consulting
© 2008 Europa Technologies
© 2008 Tele Atlas
Google
49°42'58.14" N 11°57'44.67" E
Eye alt 3133.17 km

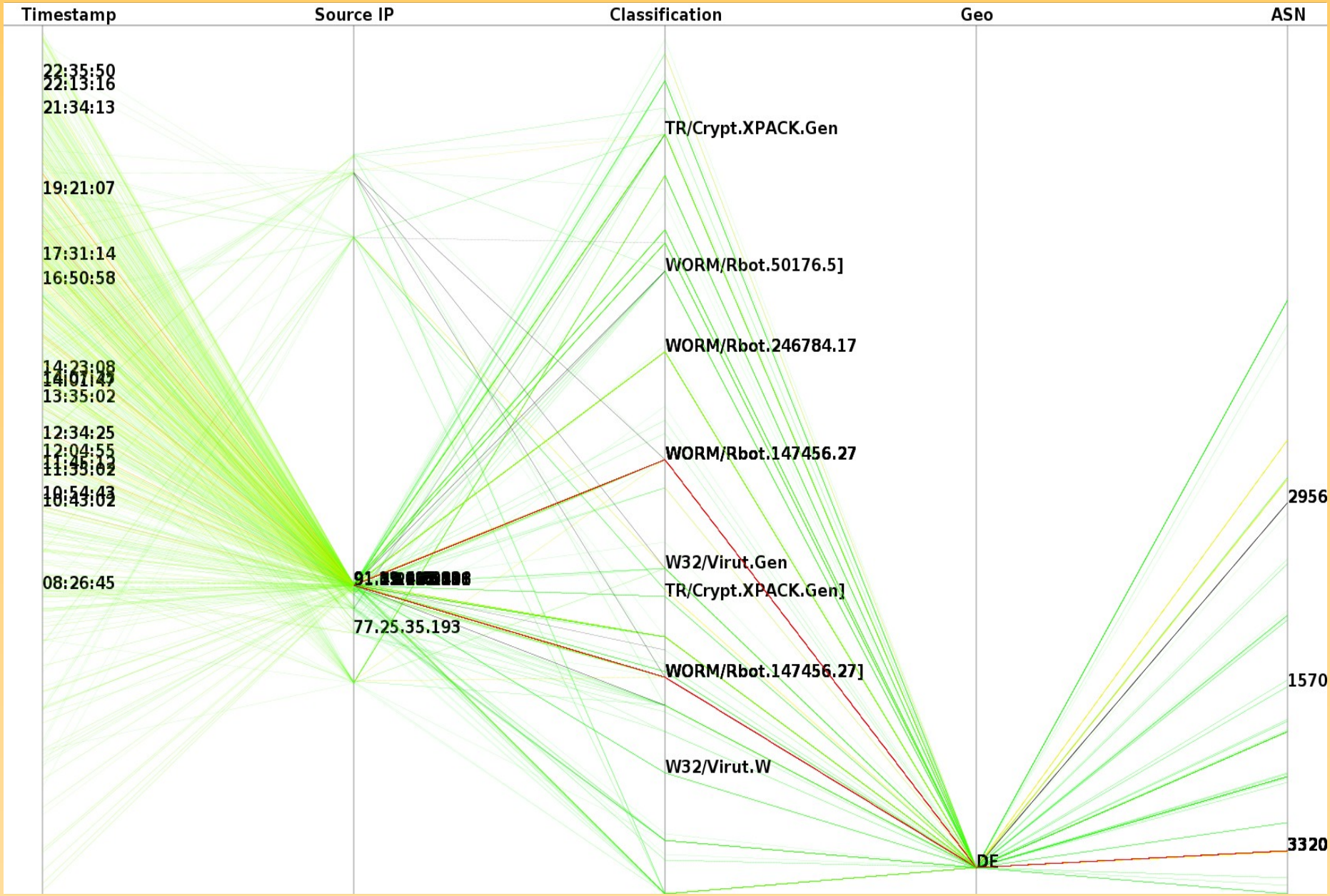


Classification	count	percent
WORM/Allaple.Gen	14228	28.951063
TR/Crypt.XPACK.Gen	9021	18.355886
TR/Crypt.NSPM.Gen	5059	10.294028
WORM/Allaple.Damaged.Gen	2700	5.493946
W32/Virut.N.DR	2375	4.832638
WORM/Rbot.147456.27	1830	3.723675
WORM/Rbot.147456.27]	1774	3.609726
W32/Virut.Gen	1550	3.153932
WORM/Rbot.50176.5	975	1.983925
W32/Virut.W	975	1.983925

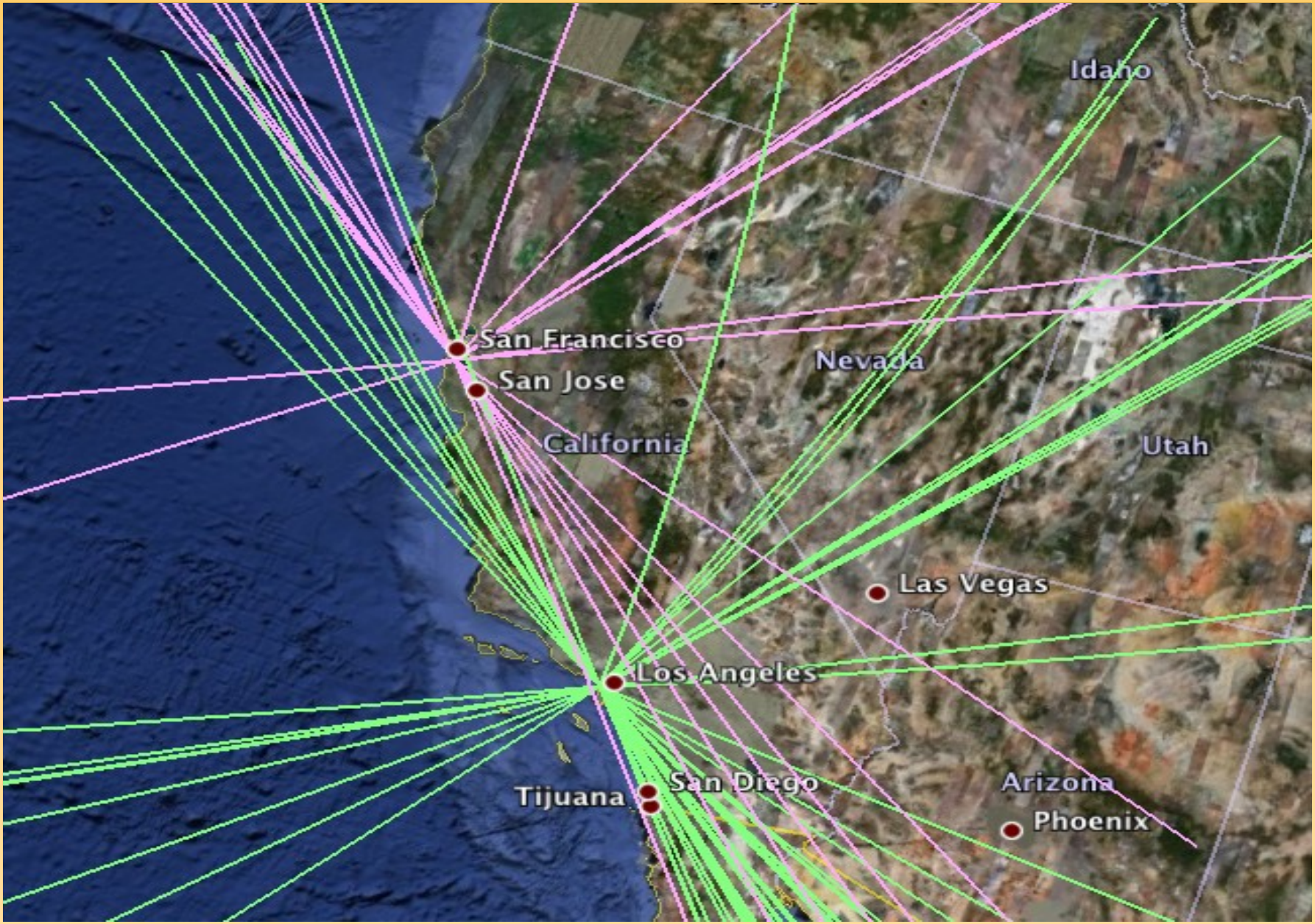




David Watson (david@honeynet.org.uk)



David Watson (david@honeynet.org.uk)



David Watson (david@honeynet.org.uk)

David Watson (david@honeynet.org.uk)

The Honeynet

PROJECT

HonEeeBox – Rapid Deployment of Many Distributed Low Interaction Malware Collectors

AusCERT 2009

Any Questions?

David Watson david@honeynet.org.uk