THE HONEYNET PROJECT

PARIS 2011

The Honeynet PROJECT

HonEeeBox – Lessons Learned and Plan For 2011

Annual Workshop Private Day 22/03/11

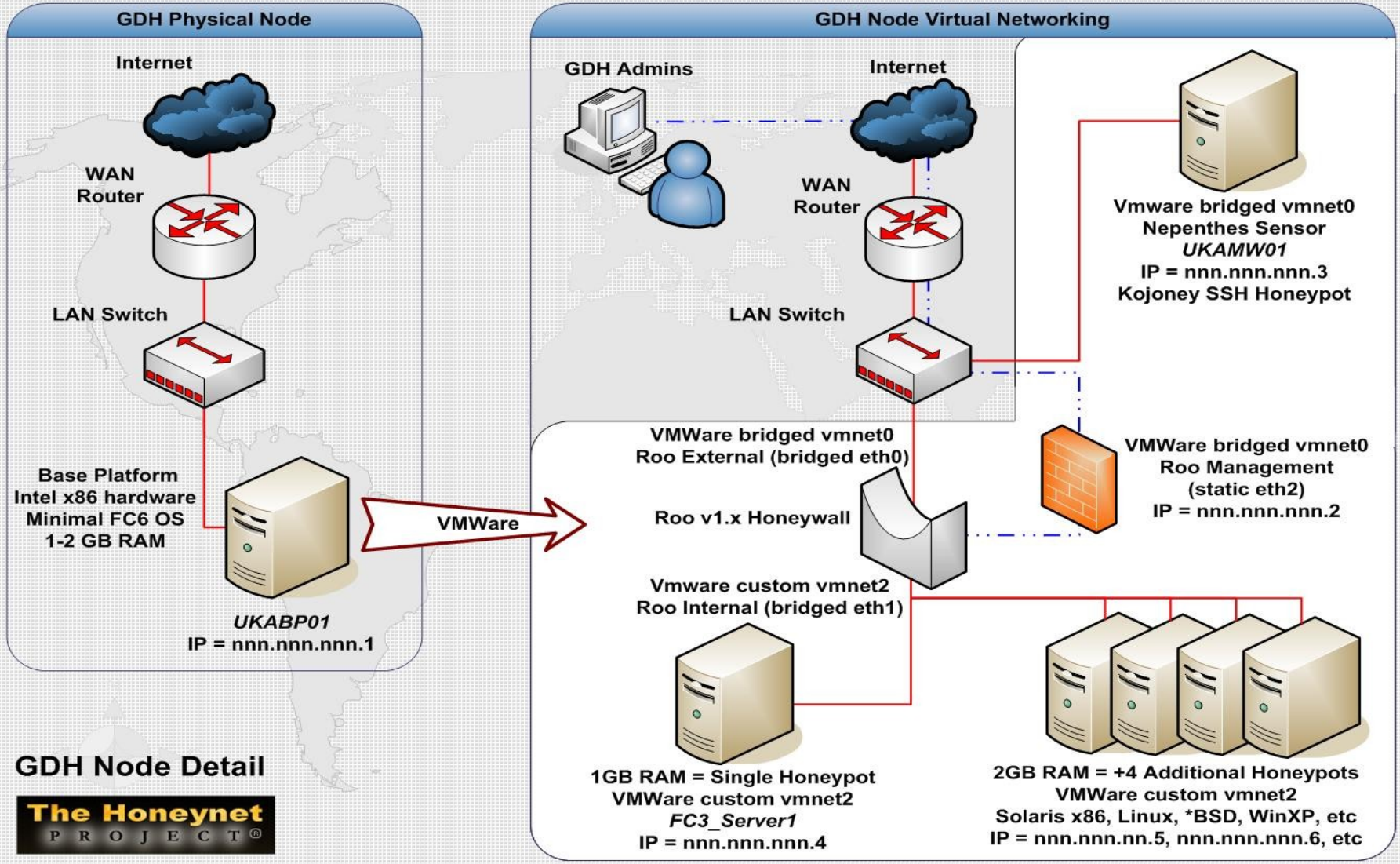
David Watson david@honeynet.org.uk

Speaker

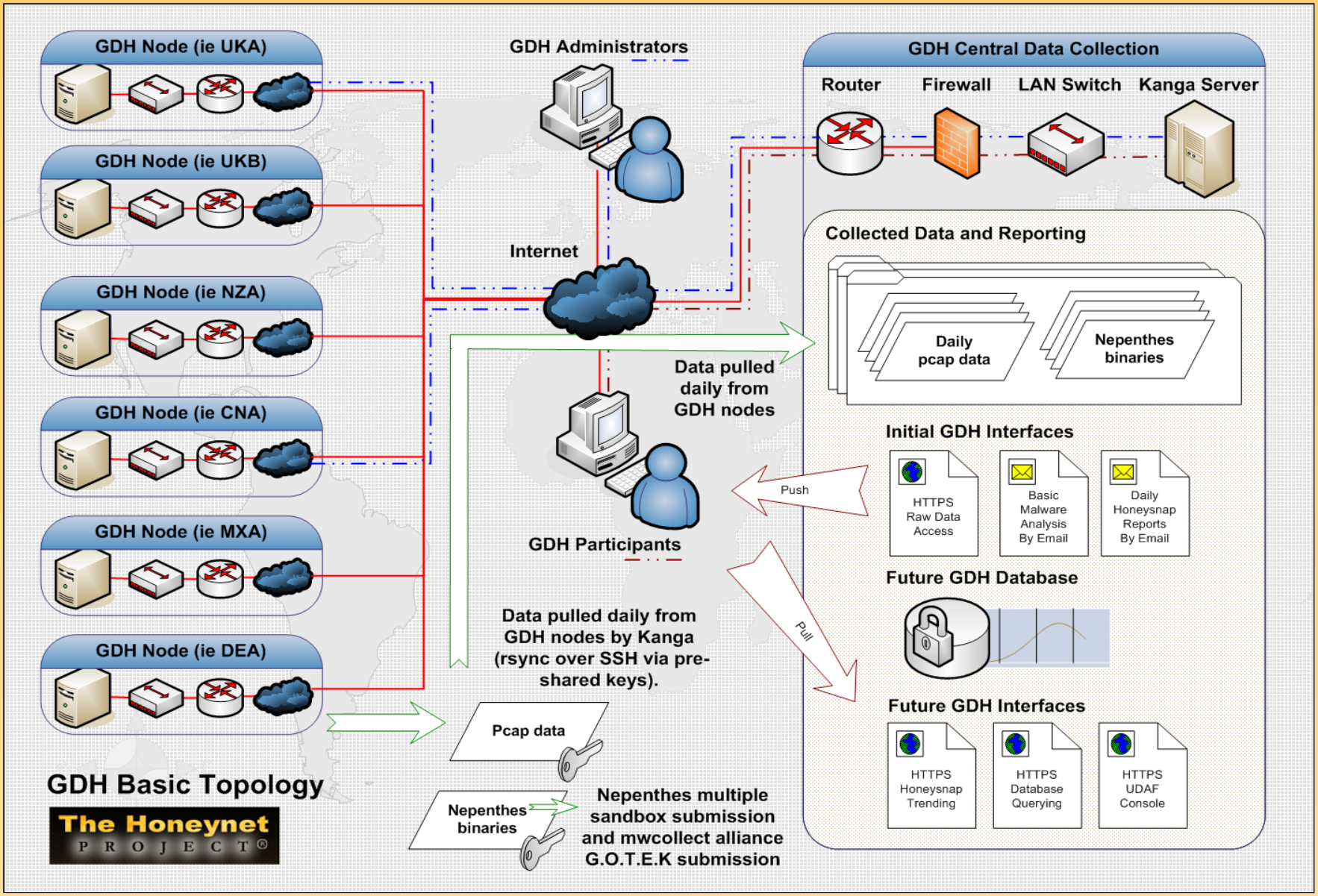
- **David Watson** (UK)
  - 14 years managed services industry and consultancy
  - Solaris, IP Networking, Firewalls, PenTest background
  - Led the UK Honeynet Project since 2003
  - Honeynet Project Chief Research Officer / Director
  - Bootable systems, Honeystick, Honeysnap analysis tool, co-authored “KYE: Phishing”, KYE reviewer / editor
  - GDH and HonEeeBox lead developer & project manager
  - GSoC org admin, Conficker Working Group
  - Shadowserver Foundation member
  - Director of UK open source consultancy Isotoma Ltd.

The Honeynet PROJECT®

Global Distributed Honeynets (GDH1) (2006-2008)



http://www.honeynet.org/speaking/PacSec07_David_Watson_Global_Distributed_Honeynet.pdf



http://www.honeynet.org/speaking/PacSec07_David_Watson_Global_Distributed_Honeynet.pdf

THE HONEYNET PROJECT

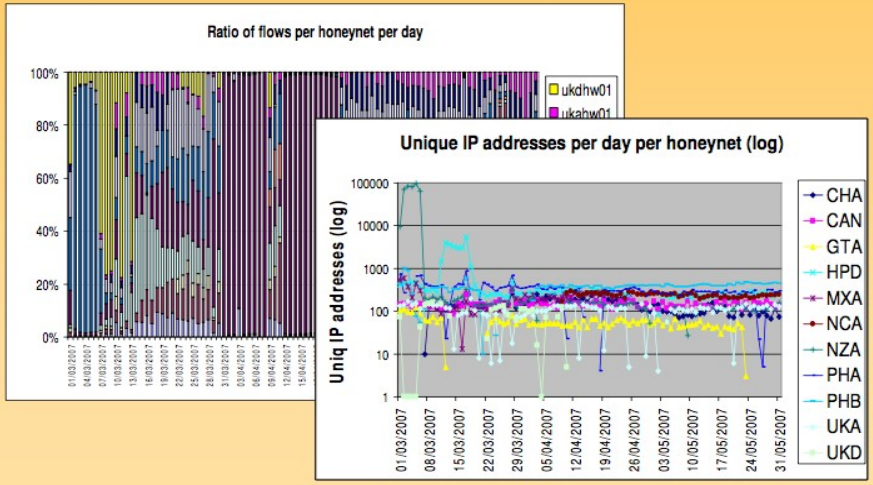
GDH: Top Level Statistics

- 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

David Watson (david@honeynet.org.uk)

THE HONEYNET PROJECT

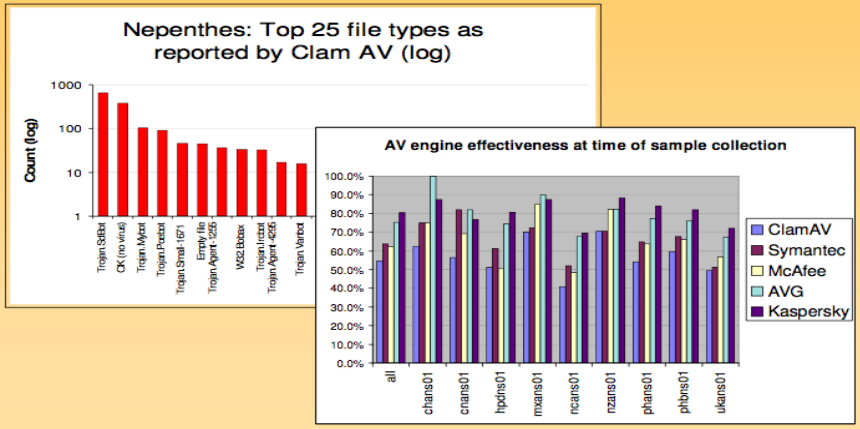
GDH: Sample Data Summaries 2



David Watson (david@honeynet.org.uk)

THE HONEYNET PROJECT

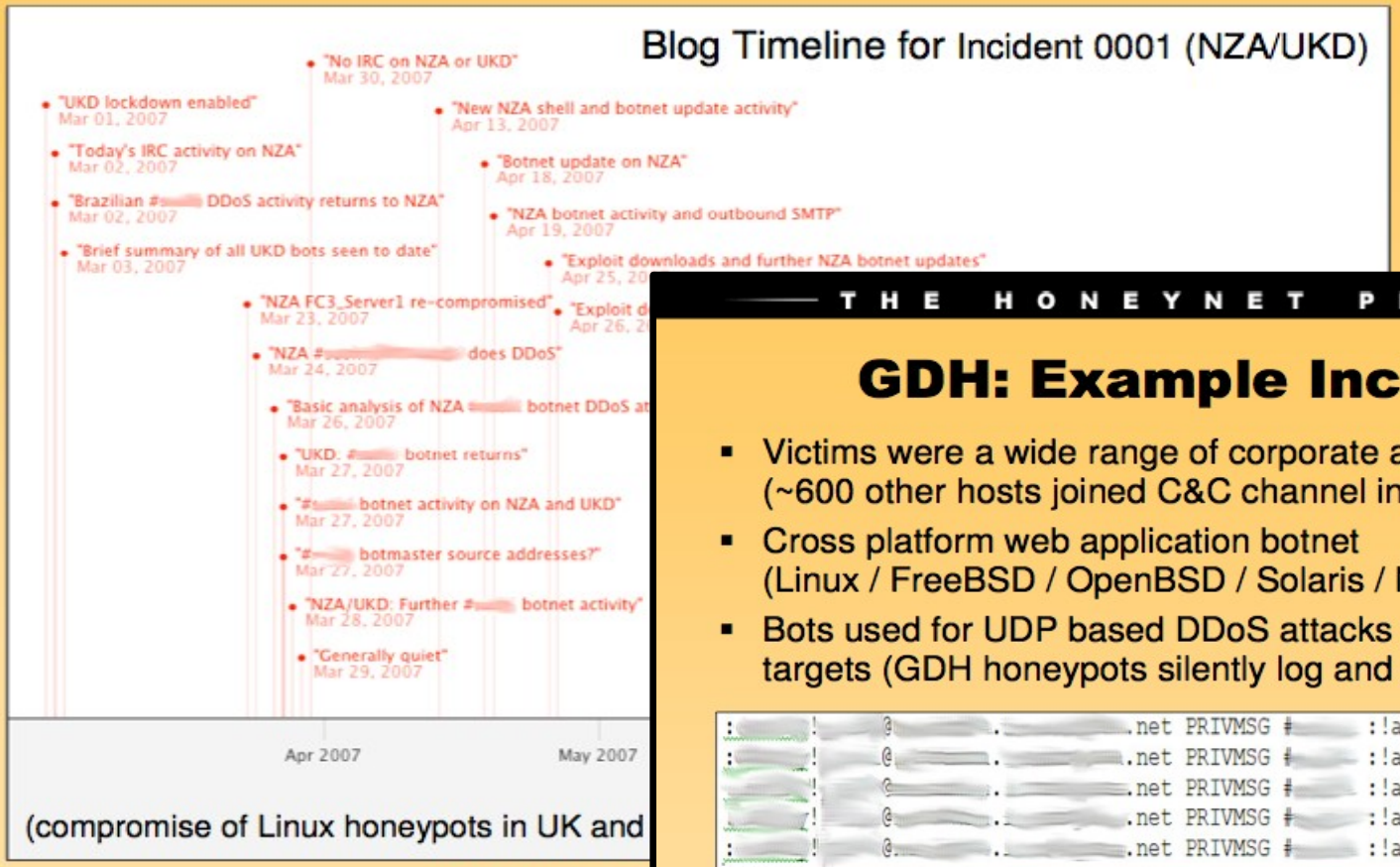
GDH: Nepenthes Malware Analysis



David Watson (david@honeynet.org.uk)

http://www.honeynet.org/speaking/PacSec07_David_Watson_Global_Distributed_Honeynet.pdf

THE HONEYNET PROJECT



David Watson (

THE HONEYNET PROJECT

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

http://www.honeynet.org/speaking/PacSec07_David_Watson_Global_Distributed_Honeynet.pdf

The Honeynet PROJECT®

Global Distributed Honeynets (GDH2) (2008-2009)

Motivation

- GDH2 gives members a shared project
- Tools available as open source
- Data available only to participants
- Continues honeynet R&D plus testing

BUT

- Big, complex, development dependencies, manual, time consuming, resource intensive
- Significant funding to really be successful
- On hold, but still want to find full time funding

The Honeynet PROJECT®

HonEeeBox v1: Rapid Deployment of Many Distributed Low Interaction Malware Collectors (2009-2010)

David Watson (david@honeynet.org.uk)

Motivation

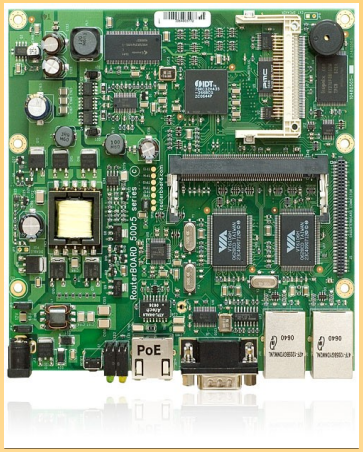
- Do something simple, then more funded GDH2
- Reduce amount of new development required
- Minimise operational support and DA effort
- Keep up momentum from annual workshop
- Start project immediately (June 2009)
- Quickly provide a live shared data feed
- Involve as many members as possible
- Kick start development of analysis tools that will be useful when GDH2 does restart

Proposed Approach

- Build small, cheap, highly portable low interaction honeypots for distributed malware collection to a central location
- Deploy widely and internationally (100+)
- Anonymous central sample submission
- 'Outsource' malware binary analysis to Shadowserver, VirusTotal, etc
- Focus development on reporting and analysis UI, then 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 disk image**:
  - Live CD sensor
  - Live CD sensor with disk persistence
  - Live USB sensor
  - Live USB sensor with disk persistence
  - Virtual appliance (including cloud nodes, AWS)
  - Hard disk installation (ideally to Eee Box PC)
  - SHDC card installation, no moving parts

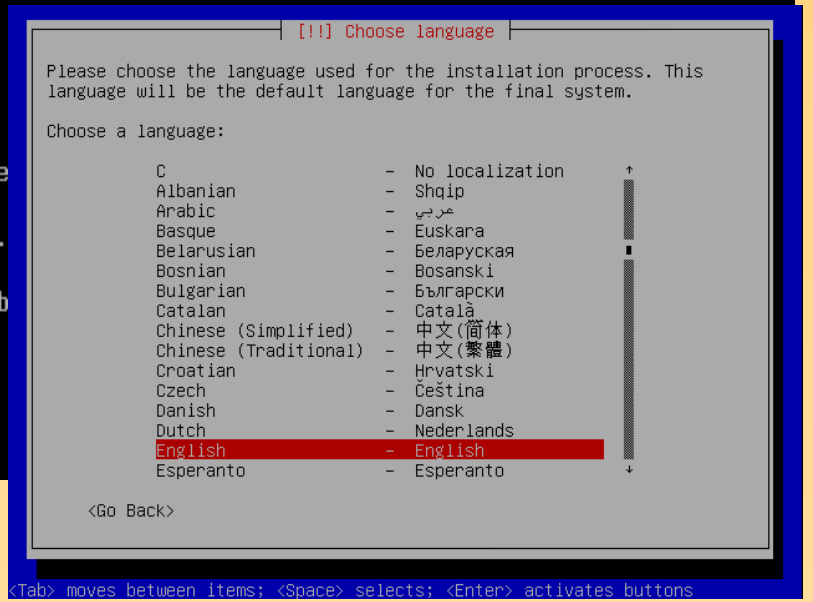
HonEeeBox v1

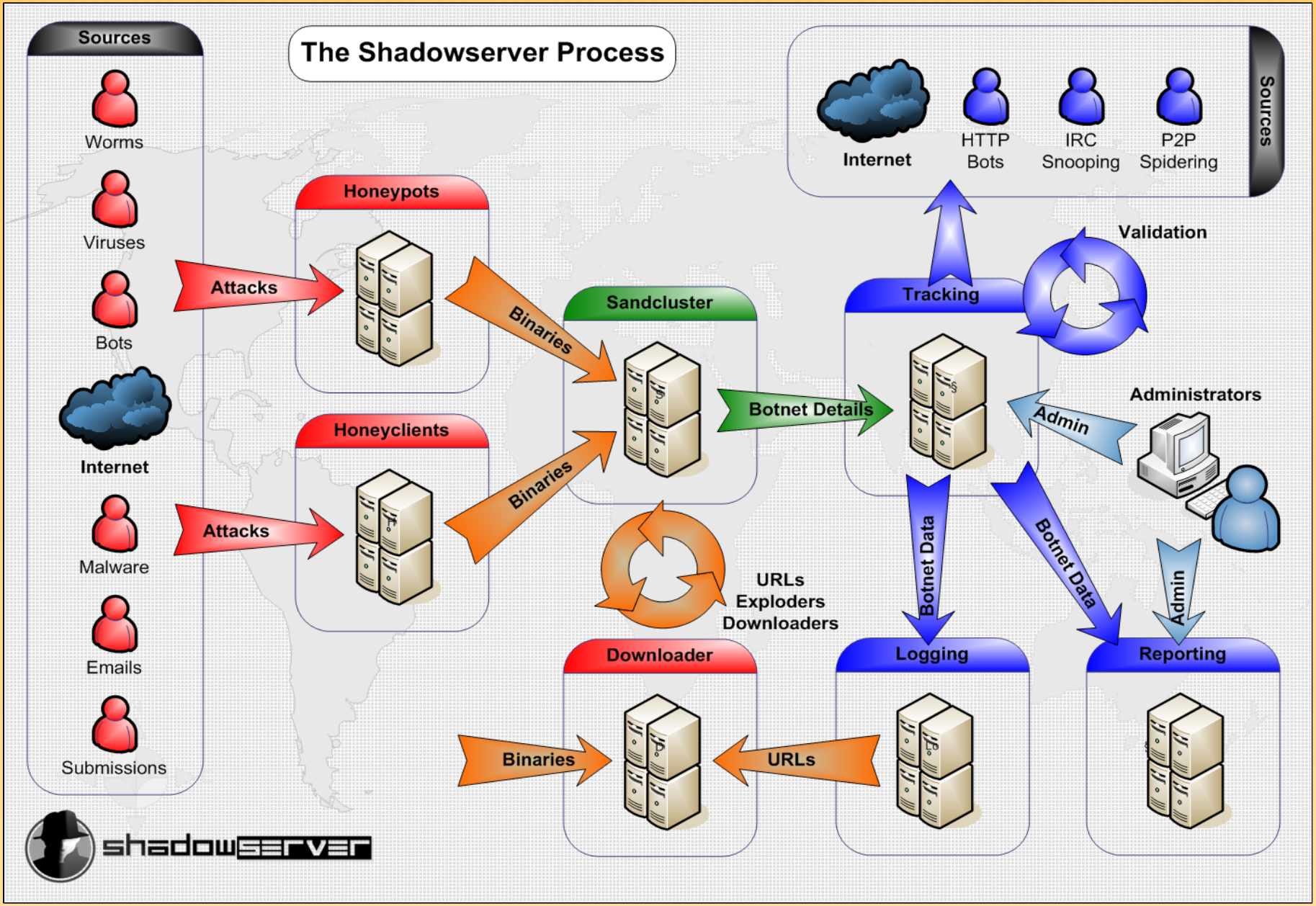
- Minimal **Debian-Live** system (Lenny 5.0)
- Custom **Nepenthes** .deb created from the current Nepenthes release in svn
- DHCP plus automatic live CD login
- Patch and upgrade on the fly via apt
- Permanent installation prompts for locale, network configuration, etc as normal
- HTTPS data submission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


```
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]
```

```
dmin@debian:~$ ps -ef | grep nepen
101       2612     1  0 08:28 ?        00:00:00 /opt/nepenthes/bin/nepenthes --
ser=nepenthes --group=nepenthes
dmin      2703  2667  0 08:31 tty1     00:00:00 grep nepen
dmin@debian:~$
dmin@debian:~$
dmin@debian:~$ tail /opt/nepenthes/var/log/nepenthes.log
26022009 08:28:07 info sc module] Loading signatures from file
es/signatures/shellcode-signatures.sc
26022009 08:28:08 debug info fixme] Logfile var/log/nepenthes.
ow 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
dmin@debian:~$ _
```

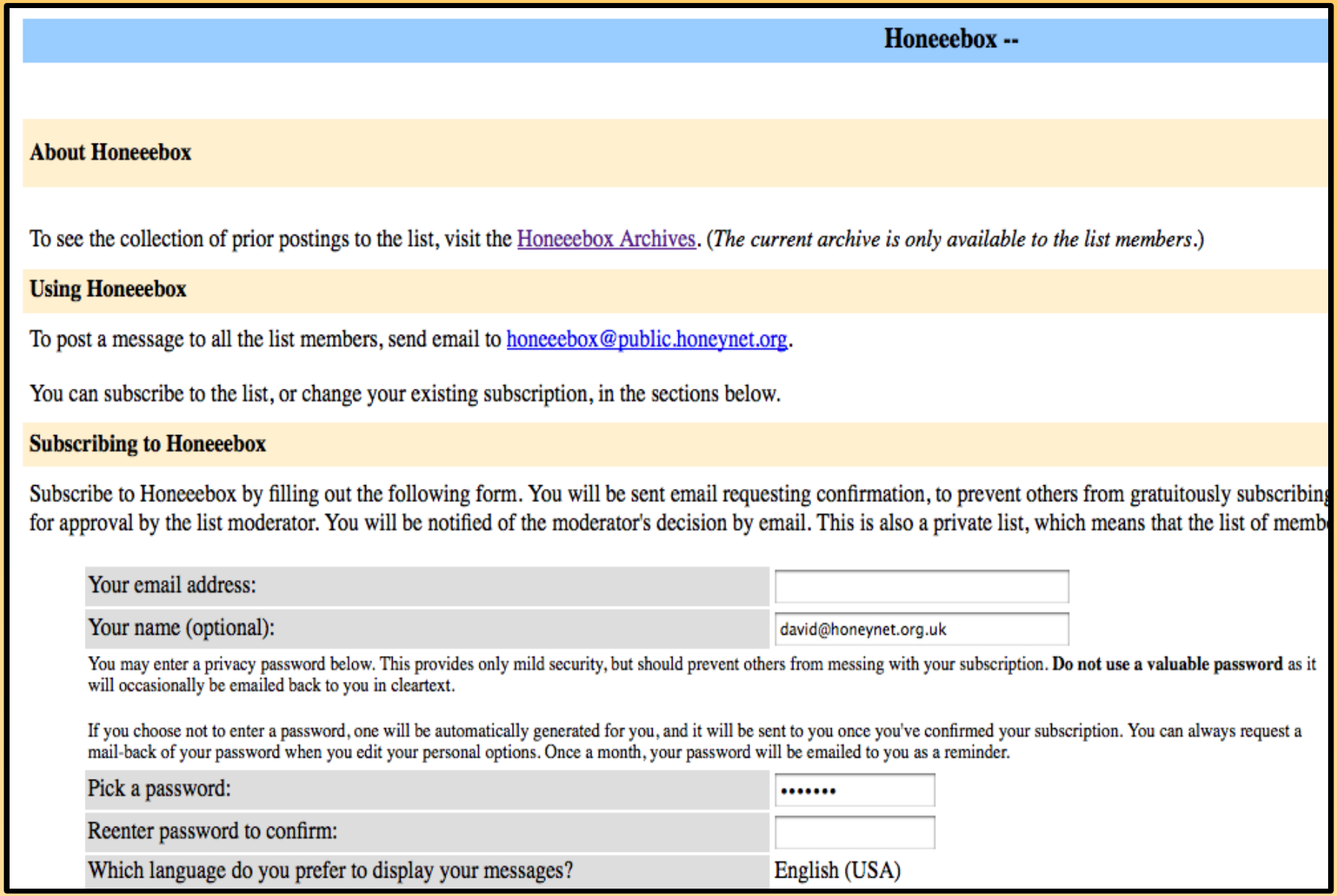



The Shadowserver Process
Sources
Worms
Viruses
Bots
Internet
Malware
Emails
Submissions
Attacks
Attacks
Honeypots
Honeyclients
Binaries
Binaries
Sandcluster
Botnet Details
URLs
Exploders
Downloaders
Downloader
Binaries
URLs
Tracking
Validation
Internet
HTTP Bots
IRC Snooping
P2P Spidering
Sources
Administrators
Admin
Botnet Data
Botnet Data
Admin
Logging
Reporting
shadowserver

HonEeeBox Participation

- 1+ public **static** 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
- Tried to find sponsorship (NIC $40k, Symantec $10k)
- Potential funding for additional sensor deployment
  - Regional, CERT, industry, academic, etc



Honeeebox --

About Honeeebox

To see the collection of prior postings to the list, visit the Honeeebox Archives. (*The current archive is only available to the list members.*)

Using Honeeebox

To post a message to all the list members, send email to honeeebox@public.honeynet.org.

You can subscribe to the list, or change your existing subscription, in the sections below.

Subscribing to Honeeebox

Subscribe to Honeeebox by filling out the following form. You will be sent email requesting confirmation, to prevent others from gratuitously subscribing for approval by the list moderator. You will be notified of the moderator's decision by email. This is also a private list, which means that the list of memb

Your email address:	
Your name (optional):	david@honeynet.org.uk

You may enter a privacy password below. This provides only mild security, but should prevent others from messing with your subscription. **Do not use a valuable password** as it will occasionally be emailed back to you in cleartext.

If you choose not to enter a password, one will be automatically generated for you, and it will be sent to you once you've confirmed your subscription. You can always request a mail-back of your password when you edit your personal options. Once a month, your password will be emailed to you as a reminder.

Pick a password:	•••••••
Reenter password to confirm:	
Which language do you prefer to display your messages?	English (USA)

https://public.honeynet.org/mailman/private/honeeebox/

HonEeeBox Operational Blog

Discussion about HonEeeBox operational events and data analysis

« HonEeeBox Sensor Added (HK002)

HonEeeBox Sensor Added (NO002) »

Good day for sensor deployments and attack data

As you may have noticed from the recent posts, we've recently added our first HonEeeBox nodes in the far east (Hong Kong nodes HK001 and HK002), Asia (Pakistan node PK001) and mainland Europe (NO001 in Norway and FR001 in France). There are also a number more in the pipeline. The good news is that we've seen attack data from many of these sensors today, such as:

Attacks 1409 and 1410 = HK001

Attacks 1436 to 1438 = FR001

And hopefully we'll start to lose our UK data bias quite soon.

However, our friends in Norway set a new record today: their sensor somehow managed to submit 20 attacks in ~1 second (attacks 1411-1435), most of which somehow created a new sensor record each time (race condition?), hence the summary report now showing 28 active sensors with 23 submitting data in the past 24 hours! Obviously something is broken somewhere, but it is nice to have this kind of submission bug to deal with finally. Congratulations Einar!

Many thanks for everyone who has been an early beta tester, your involvement is much appreciated.

isotoma

log

Wiki | Timeline | Roadmap | Browse Source

Honeeebox Sensors

The goal of the sensor stream within the Honeeebox project is to build small, cheap, easily portable low interaction honeypots for distributed malware collectio point Honeeebox uses Nepenthes to collect malware, with samples being submitted anonymously to a central server for offline analysis. The target hardware p (http://www.asus.com/products.aspx?modelmenu=1&model=2289&l1=24&l2=165&l3=0&l4=0 - hence the dodgy project name!), but the software compor compatible with Debian linux.

The Honeeebox sensor codebase is a set of scripts to build a bootable ISO or USB image using Debian Live. The resulting image can be used as:

- A live CD sensor
- A live CD sensor with persistence (via an additional USB or HDD)
- A live USB sensor
- A live USB sensor with persistence (to the USB device)
- A pre-built virtual appliance
- A means to install the same disk image to a local hard disk and make it permanently bootable
- A means to install the same disk image to a local media device (such as an SHDC card) and make it permanently, for solid state operation and people n

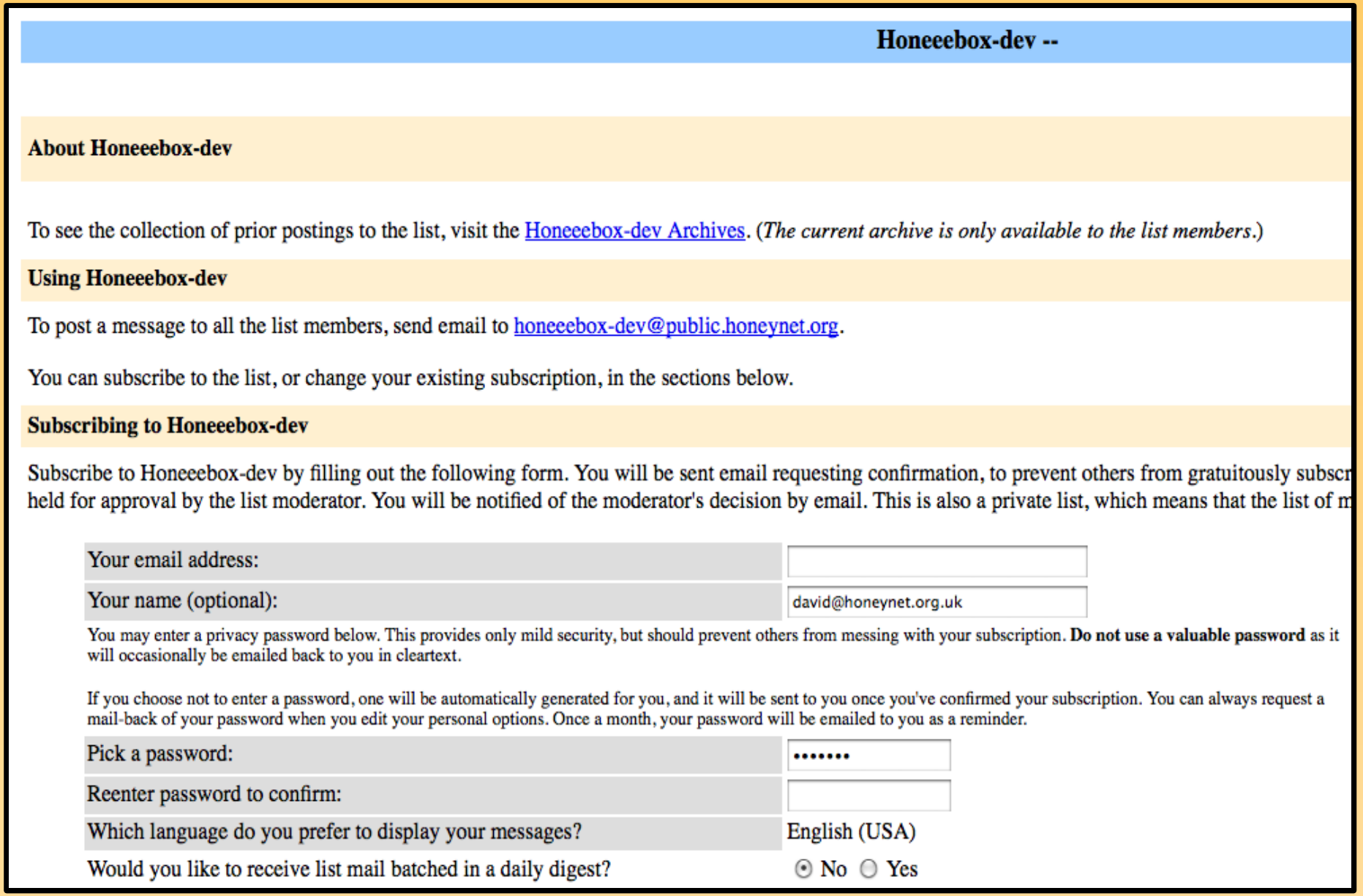
The generated image is a minimal Debian Lenny Linux system, with a custom Nepenthes build (via a .deb created from the current release in svn) with autom upgraded on the fly using aptitude/apt and can be permanently installed to local hard drives, prompting for locale, network configuration, etc details as per a easily be changed from a command line menu by running `sudo ceni` (or using vi).

Testing Pre-built Sensor Images

You can find instructions for downloading and testing a pre-build Honeeebox sensor image here:

- HoneeeboxSensorTesting

Building A Sensor Image



Honeeebox-dev --

About Honeeebox-dev

To see the collection of prior postings to the list, visit the Honeeebox-dev Archives. (*The current archive is only available to the list members.*)

Using Honeeebox-dev

To post a message to all the list members, send email to honeeebox-dev@public.honeynet.org.

You can subscribe to the list, or change your existing subscription, in the sections below.

Subscribing to Honeeebox-dev

Subscribe to Honeeebox-dev by filling out the following form. You will be sent email requesting confirmation, to prevent others from gratuitously subscr
held for approval by the list moderator. You will be notified of the moderator's decision by email. This is also a private list, which means that the list of m

Your email address:	
Your name (optional):	david@honeynet.org.uk

You may enter a privacy password below. This provides only mild security, but should prevent others from messing with your subscription. **Do not use a valuable password** as it will occasionally be emailed back to you in cleartext.

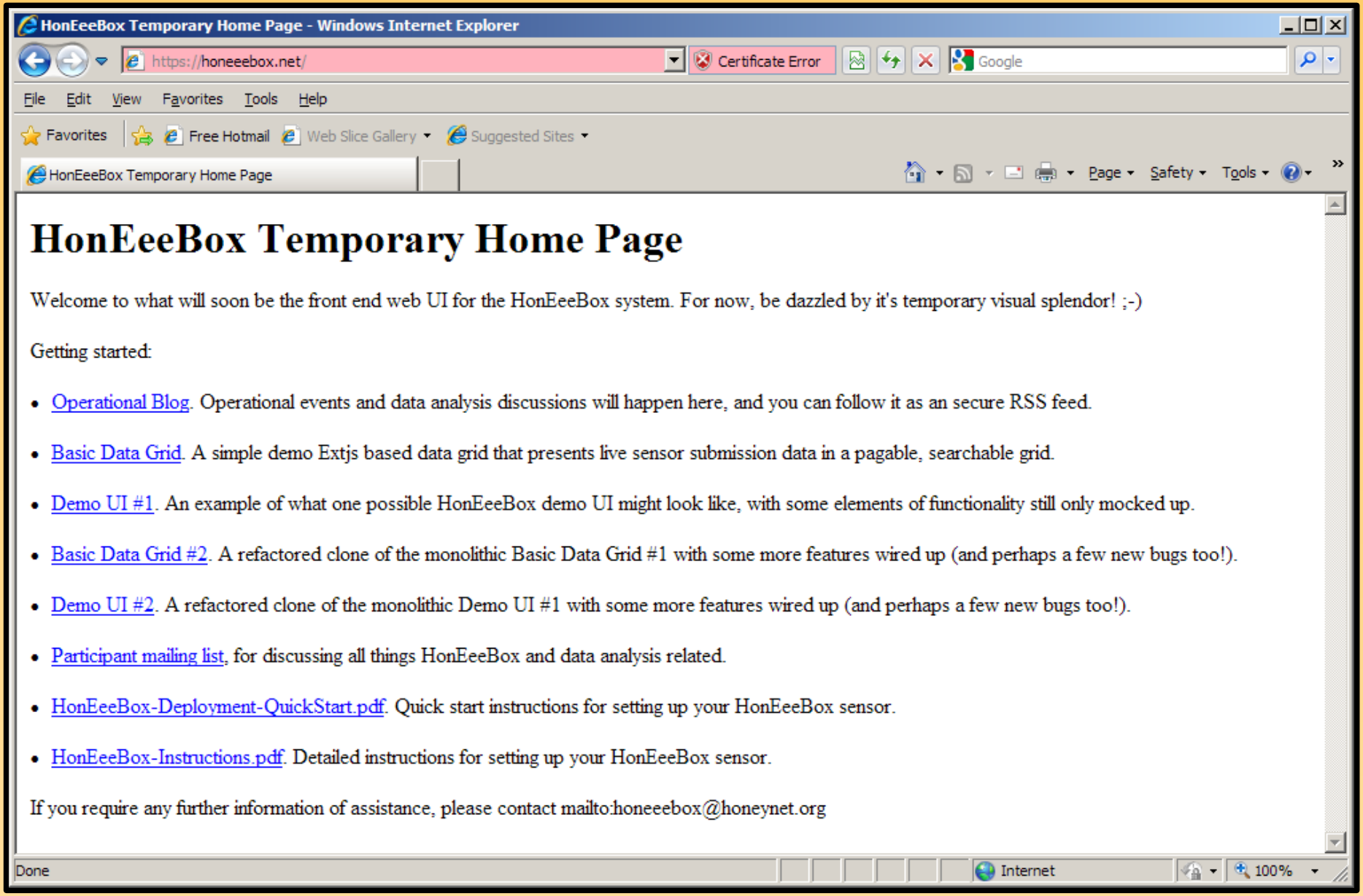
If you choose not to enter a password, one will be automatically generated for you, and it will be sent to you once you've confirmed your subscription. You can always request a mail-back of your password when you edit your personal options. Once a month, your password will be emailed to you as a reminder.

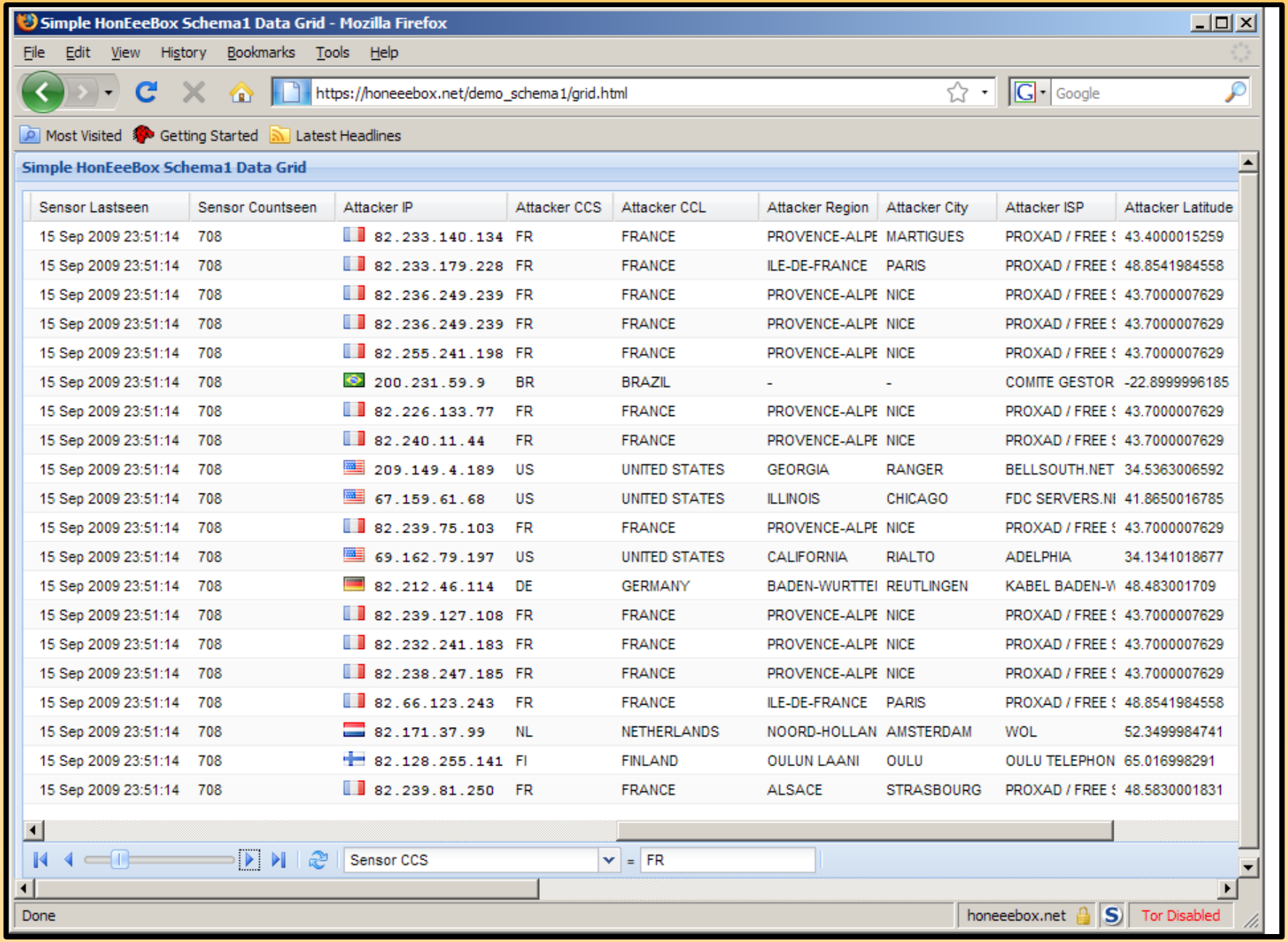
Pick a password:	•••••••
Reenter password to confirm:	
Which language do you prefer to display your messages?	English (USA)
Would you like to receive list mail batched in a daily digest?	◉ No ○ Yes

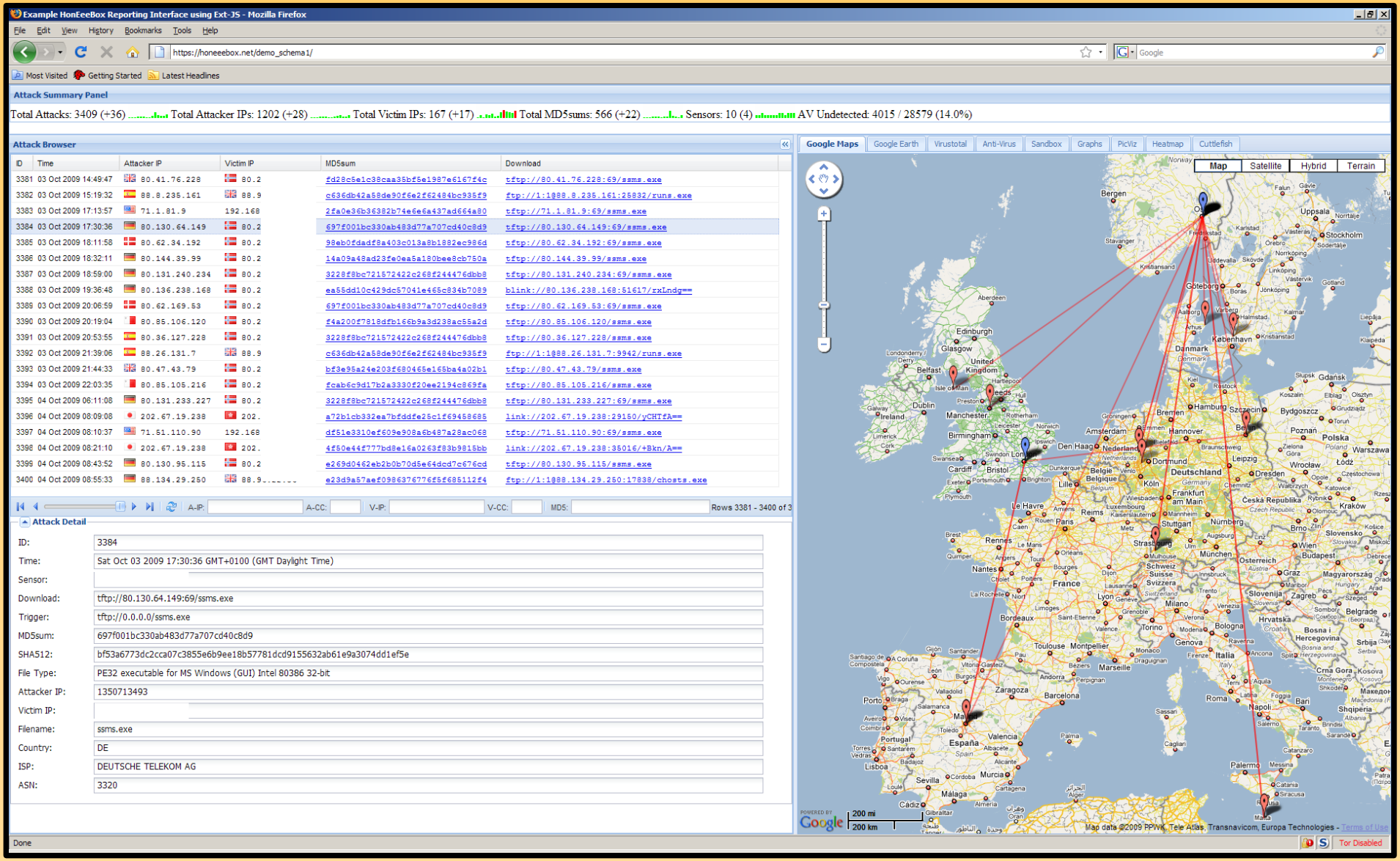
https://public.honeynet.org/mailman/private/honeeebox-dev/

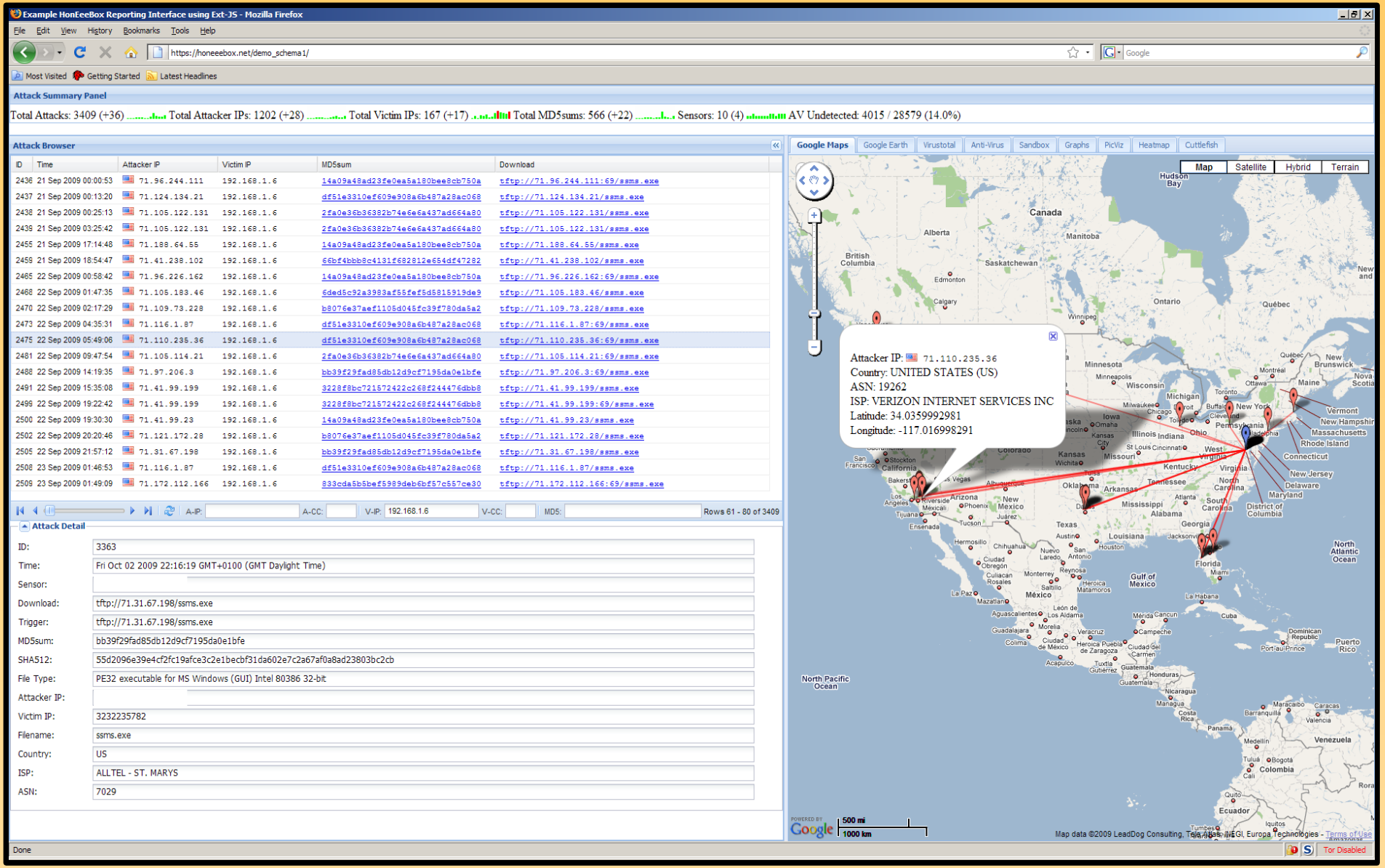
The Honeynet PROJECT®

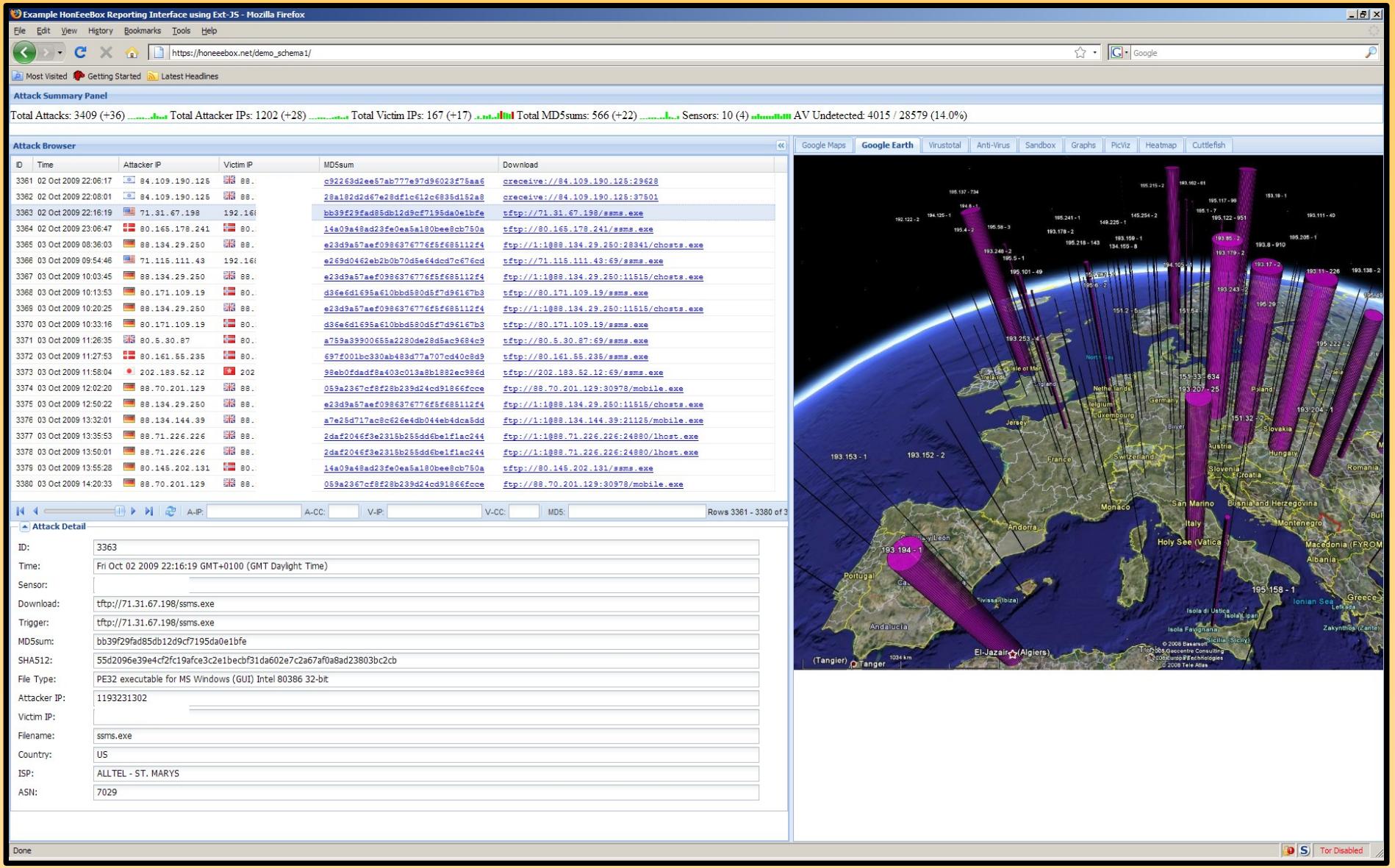
Prototype HonEeeBox v1 UI and Basic Example Visualisations

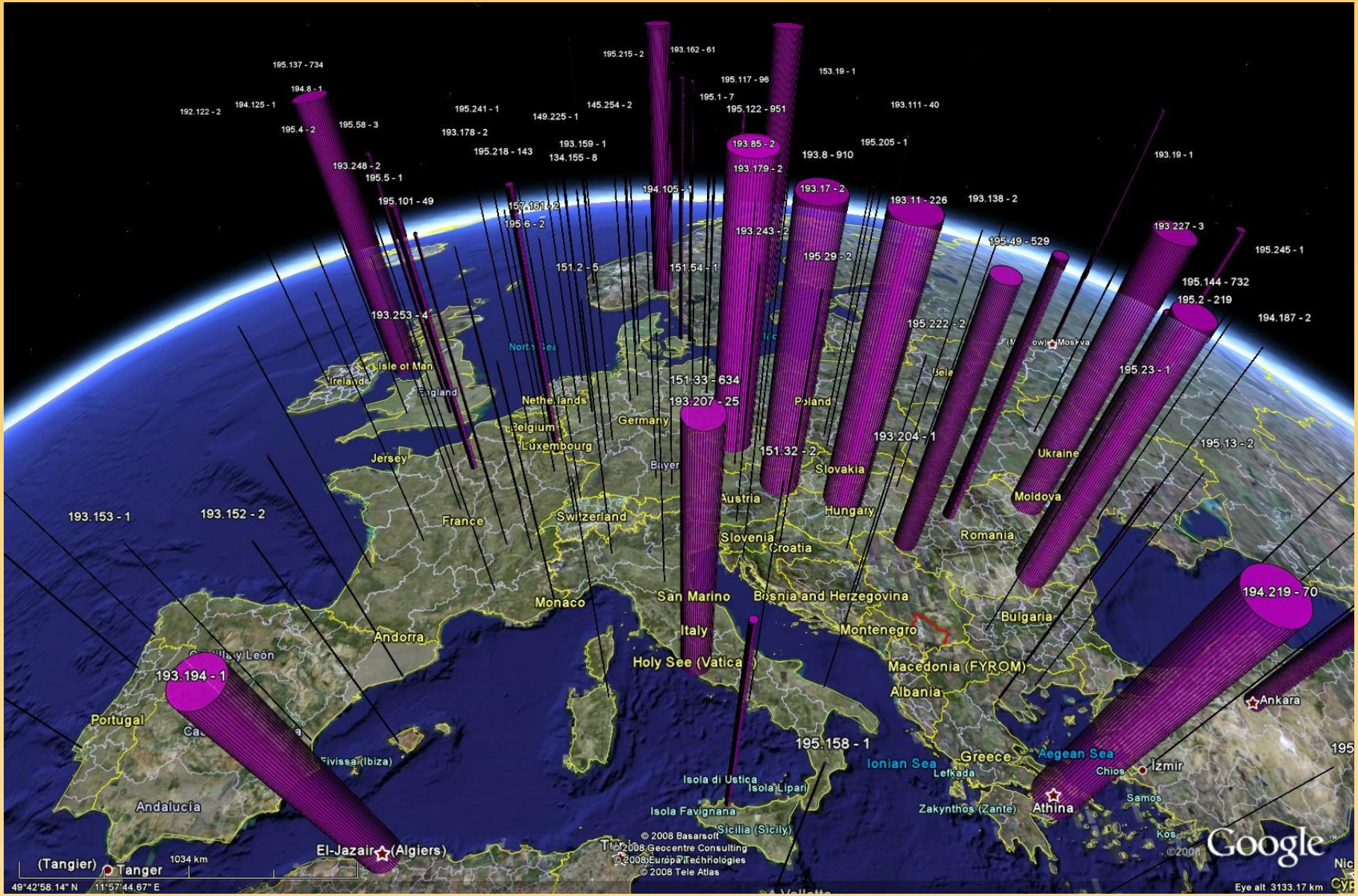

HonEeeBox Temporary Home Page - Windows Internet Explorer
https://honeeebox.net/
Certificate Error
Google
File Edit View Favorites Tools Help
Favorites
Free Hotmail
Web Slice Gallery
Suggested Sites
HonEeeBox Temporary Home Page
Page
Safety
Tools
HonEeeBox Temporary Home Page
Welcome to what will soon be the front end web UI for the HonEeeBox system. For now, be dazzled by it's temporary visual splendor! ;-)
Getting started:
Operational Blog. Operational events and data analysis discussions will happen here, and you can follow it as an secure RSS feed.
Basic Data Grid. A simple demo Extjs based data grid that presents live sensor submission data in a pagable, searchable grid.
Demo UI #1. An example of what one possible HonEeeBox demo UI might look like, with some elements of functionality still only mocked up.
Basic Data Grid #2. A refactored clone of the monolithic Basic Data Grid #1 with some more features wired up (and perhaps a few new bugs too!).
Demo UI #2. A refactored clone of the monolithic Demo UI #1 with some more features wired up (and perhaps a few new bugs too!).
Participant mailing list, for discussing all things HonEeeBox and data analysis related.
HonEeeBox-Deployment-QuickStart.pdf. Quick start instructions for setting up your HonEeeBox sensor.
HonEeeBox-Instructions.pdf. Detailed instructions for setting up your HonEeeBox sensor.
If you require any further information of assistance, please contact mailto:honeeebox@honeynet.org
Done
Internet
100%

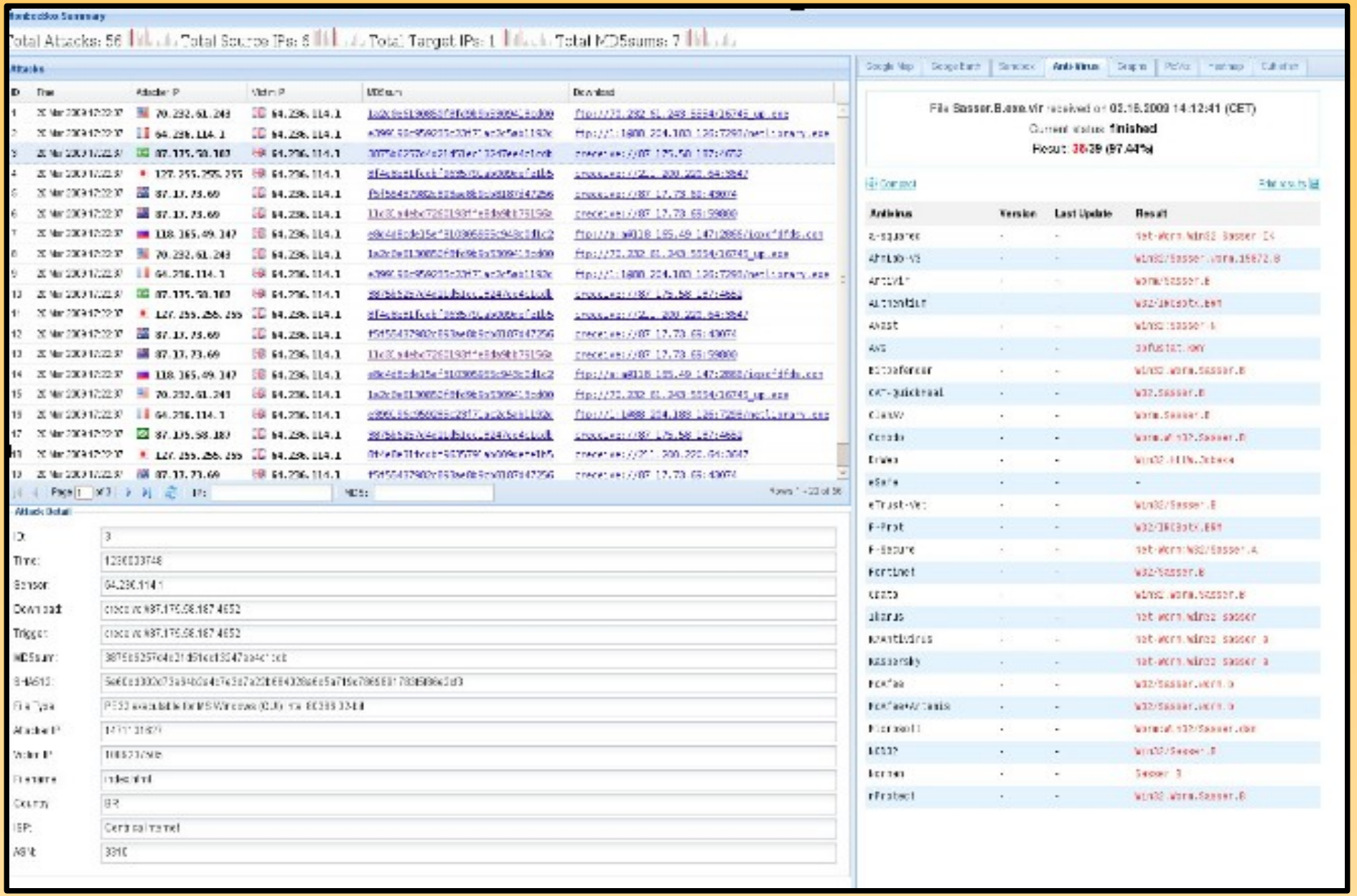

Simple HonEeeBox Schema1 Data Grid - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://honeeebox.net/demo_schema1/grid.html
Google
Most Visited Getting Started Latest Headlines
Simple HonEeeBox Schema1 Data Grid
Sensor Lastseen | Sensor Countseen | Attacker IP | Attacker CCS | Attacker CCL | Attacker Region | Attacker City | Attacker ISP | Attacker Latitude
15 Sep 2009 23:51:14 | 708 | 82.233.140.134 | FR | FRANCE | PROVENCE-ALPE | MARTIGUES | PROXAD / FREE S | 43.4000015259
15 Sep 2009 23:51:14 | 708 | 82.233.179.228 | FR | FRANCE | ILE-DE-FRANCE | PARIS | PROXAD / FREE S | 48.8541984558
15 Sep 2009 23:51:14 | 708 | 82.236.249.239 | FR | FRANCE | PROVENCE-ALPE | NICE | PROXAD / FREE S | 43.7000007629
15 Sep 2009 23:51:14 | 708 | 82.236.249.239 | FR | FRANCE | PROVENCE-ALPE | NICE | PROXAD / FREE S | 43.7000007629
15 Sep 2009 23:51:14 | 708 | 82.255.241.198 | FR | FRANCE | PROVENCE-ALPE | NICE | PROXAD / FREE S | 43.7000007629
15 Sep 2009 23:51:14 | 708 | 200.231.59.9 | BR | BRAZIL | - | - | COMITE GESTOR | -22.8999996185
15 Sep 2009 23:51:14 | 708 | 82.226.133.77 | FR | FRANCE | PROVENCE-ALPE | NICE | PROXAD / FREE S | 43.7000007629
15 Sep 2009 23:51:14 | 708 | 82.240.11.44 | FR | FRANCE | PROVENCE-ALPE | NICE | PROXAD / FREE S | 43.7000007629
15 Sep 2009 23:51:14 | 708 | 209.149.4.189 | US | UNITED STATES | GEORGIA | RANGER | BELLSOUTH.NET | 34.5363006592
15 Sep 2009 23:51:14 | 708 | 67.159.61.68 | US | UNITED STATES | ILLINOIS | CHICAGO | FDC SERVERS.NI | 41.8650016785
15 Sep 2009 23:51:14 | 708 | 82.239.75.103 | FR | FRANCE | PROVENCE-ALPE | NICE | PROXAD / FREE S | 43.7000007629
15 Sep 2009 23:51:14 | 708 | 69.162.79.197 | US | UNITED STATES | CALIFORNIA | RIALTO | ADELPHIA | 34.1341018677
15 Sep 2009 23:51:14 | 708 | 82.212.46.114 | DE | GERMANY | BADEN-WURTTEI | REUTLINGEN | KABEL BADEN-W | 48.483001709
15 Sep 2009 23:51:14 | 708 | 82.239.127.108 | FR | FRANCE | PROVENCE-ALPE | NICE | PROXAD / FREE S | 43.7000007629
15 Sep 2009 23:51:14 | 708 | 82.232.241.183 | FR | FRANCE | PROVENCE-ALPE | NICE | PROXAD / FREE S | 43.7000007629
15 Sep 2009 23:51:14 | 708 | 82.238.247.185 | FR | FRANCE | PROVENCE-ALPE | NICE | PROXAD / FREE S | 43.7000007629
15 Sep 2009 23:51:14 | 708 | 82.66.123.243 | FR | FRANCE | ILE-DE-FRANCE | PARIS | PROXAD / FREE S | 48.8541984558
15 Sep 2009 23:51:14 | 708 | 82.171.37.99 | NL | NETHERLANDS | NOORD-HOLLAN | AMSTERDAM | WOL | 52.3499984741
15 Sep 2009 23:51:14 | 708 | 82.128.255.141 | FI | FINLAND | OULUN LAANI | OULU | OULU TELEPHON | 65.016998291
15 Sep 2009 23:51:14 | 708 | 82.239.81.250 | FR | FRANCE | ALSACE | STRASBOURG | PROXAD / FREE S | 48.5830001831
Sensor CCS = FR
Done
honeeebox.net
Tor Disabled

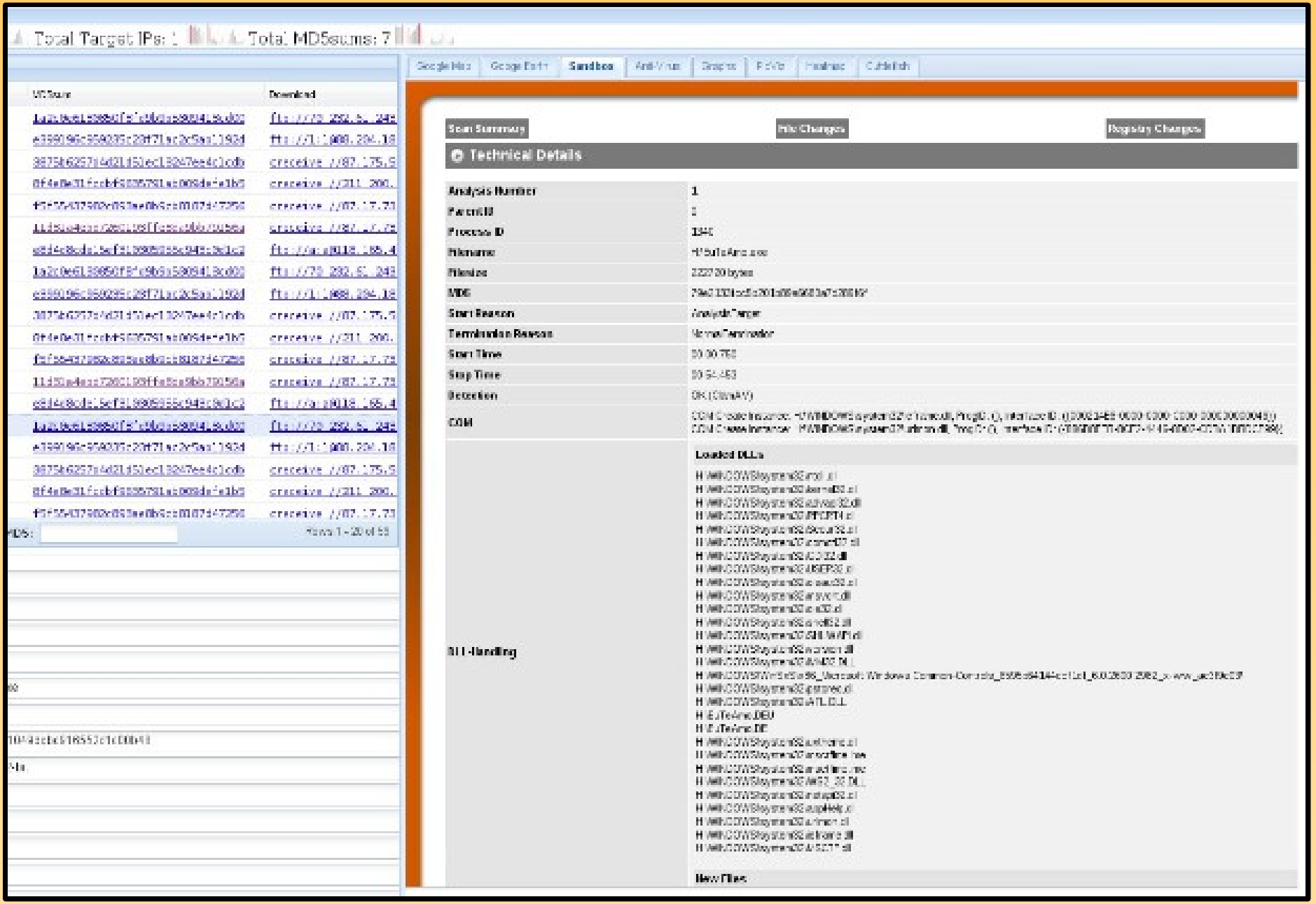

Example HonEeeBox Reporting Interface using Ext-JS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://honeeebox.net/demo_schema1/
Most Visited Getting Started Latest Headlines
Attack Summary Panel
Total Attacks: 3409 (+36) Total Attacker IPs: 1202 (+28) Total Victim IPs: 167 (+17) Total MD5sums: 566 (+22) Sensors: 10 (4) AV Undetected: 4015 / 28579 (14.0%)
Attack Browser
ID Time Attacker IP Victim IP MD5sum Download
3381 03 Oct 2009 14:49:47 80.41.76.228 80.2 fd28c5e1c38caa35bf5e1987e6167f4c tftp://80.41.76.228:69/ssms.exe
3382 03 Oct 2009 15:19:32 88.8.235.161 88.9 c636db42a58de90f6e2f62484bc935f9 ftp://1:1@88.8.235.161:25832/runs.exe
3383 03 Oct 2009 17:13:57 71.1.81.9 192.168 2fa0e36b36382b74e6e6e437ad664a80 tftp://71.1.81.9:69/ssms.exe
3384 03 Oct 2009 17:30:36 80.130.64.149 80.2 697f001bc330ab483d77a707cd40c8d9 tftp://80.130.64.149:69/ssms.exe
3385 03 Oct 2009 18:11:58 80.62.34.192 80.2 98eb0fdadf8a403c013a8b1882ec986d tftp://80.62.34.192:69/ssms.exe
3386 03 Oct 2009 18:32:11 80.144.39.99 80.2 14a09a48ad23fe0ea5a180bee8cb750a tftp://80.144.39.99/ssms.exe
3387 03 Oct 2009 18:59:00 80.131.240.234 80.2 3228f8bc721572422c268f244476dbb8 tftp://80.131.240.234:69/ssms.exe
3388 03 Oct 2009 19:36:48 80.136.238.168 80.2 ea55dd10c429dc57041e465c834b7089 blink://80.136.238.168:51617/rxLndg==
3389 03 Oct 2009 20:06:59 80.62.169.53 80.2 697f001bc330ab483d77a707cd40c8d9 tftp://80.62.169.53:69/ssms.exe
3390 03 Oct 2009 20:19:04 80.85.106.120 80.2 f4a200f7818dfb166b9a3d238ac55a2d tftp://80.85.106.120/ssms.exe
3391 03 Oct 2009 20:53:55 80.36.127.228 80.2 3228f8bc721572422c268f244476dbb8 tftp://80.36.127.228/ssms.exe
3392 03 Oct 2009 21:39:06 88.26.131.7 88.9 c636db42a58de90f6e2f62484bc935f9 ftp://1:1@88.26.131.7:9942/runs.exe
3393 03 Oct 2009 21:44:33 80.47.43.79 80.2 bf3e95a24e203f680465e165ba4a02b1 tftp://80.47.43.79/ssms.exe
3394 03 Oct 2009 22:03:35 80.85.105.216 80.2 fcab6c9d17b2a3330f20ee2194c869fa tftp://80.85.105.216/ssms.exe
3395 04 Oct 2009 06:11:08 80.131.233.227 80.2 3228f8bc721572422c268f244476dbb8 tftp://80.131.233.227:69/ssms.exe
3396 04 Oct 2009 08:09:08 202.67.19.238 202. a72b1cb332ea7bfddfe25c1f69458685 link://202.67.19.238:29150/yCHTfA==
3397 04 Oct 2009 08:10:37 71.51.110.90 192.168 df51e3310ef609e908a6b487a28ac068 tftp://71.51.110.90:69/ssms.exe
3398 04 Oct 2009 08:21:10 202.67.19.238 202. 4f50e44f777bd8e16a0263f83b9815bb link://202.67.19.238:35016/+Bkn/A==
3399 04 Oct 2009 08:43:52 80.130.95.115 80.2 e269d0462eb2b0b70d5e64dcd7c676cd tftp://80.130.95.115/ssms.exe
3400 04 Oct 2009 08:55:33 88.134.29.250 88.9 e23d9a57aef0986376776f5f685112f4 ftp://1:1@88.134.29.250:17838/chosts.exe
Rows 3381 - 3400 of 3
Attack Detail
ID: 3384
Time: Sat Oct 03 2009 17:30:36 GMT+0100 (GMT Daylight Time)
Sensor:
Download: tftp://80.130.64.149:69/ssms.exe
Trigger: tftp://0.0.0.0/ssms.exe
MD5sum: 697f001bc330ab483d77a707cd40c8d9
SHA512: bf53a6773dc2cca07c3855e6b9ee18b57781dcd9155632ab61e9a3074dd1ef5e
File Type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Attacker IP: 1350713493
Victim IP:
Filename: ssms.exe
Country: DE
ISP: DEUTSCHE TELEKOM AG
ASN: 3320
Google Maps
Google Earth
Virustotal
Anti-Virus
Sandbox
Graphs
PicViz
Heatmap
Cuttlefish
Map
Satellite
Hybrid
Terrain
Map data ©2009 PPWK, Tele Atlas, Transnavicom, Europa Technologies - Terms of Use
Done
Tor Disabled

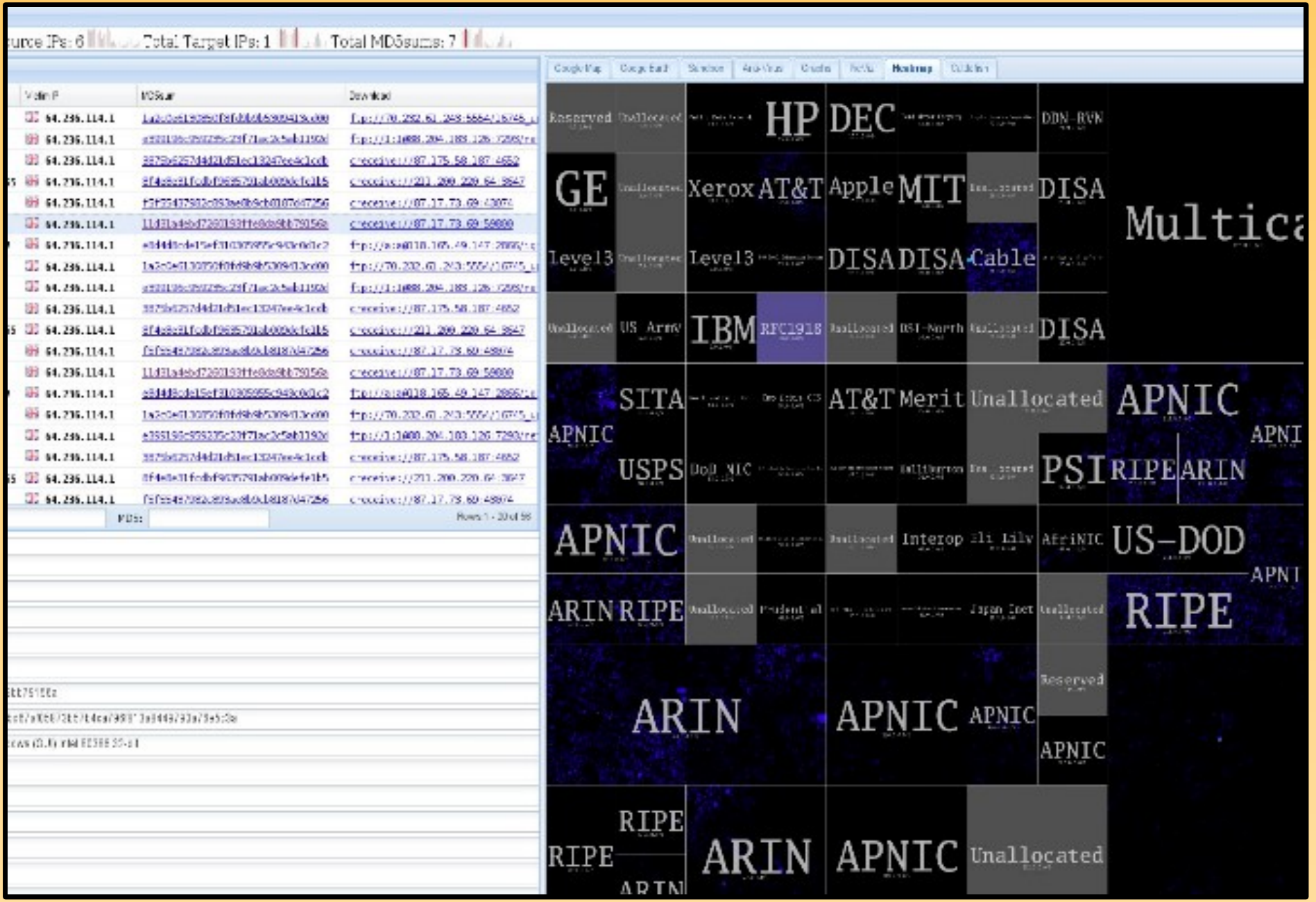

Example HonEeeBox Reporting Interface using Ext-JS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://honeeebox.net/demo_schema1/
Most Visited Getting Started Latest Headlines
Attack Summary Panel
Total Attacks: 3409 (+36) Total Attacker IPs: 1202 (+28) Total Victim IPs: 167 (+17) Total MD5sums: 566 (+22) Sensors: 10 (4) AV Undetected: 4015 / 28579 (14.0%)
Attack Browser
ID Time Attacker IP Victim IP MD5sum Download
2436 21 Sep 2009 00:00:53 71.96.244.111 192.168.1.6 14a09a48ad23fe0ea5a180bee8cb750a tftp://71.96.244.111:69/ssms.exe
2437 21 Sep 2009 00:13:20 71.124.134.21 192.168.1.6 df51e3310ef609e908a6b487a28ac068 tftp://71.124.134.21/ssms.exe
2438 21 Sep 2009 00:25:13 71.105.122.131 192.168.1.6 2fa0e36b36382b74e6e6a437ad664a80 tftp://71.105.122.131/ssms.exe
2439 21 Sep 2009 03:25:42 71.105.122.131 192.168.1.6 2fa0e36b36382b74e6e6a437ad664a80 tftp://71.105.122.131/ssms.exe
2455 21 Sep 2009 17:14:48 71.188.64.55 192.168.1.6 14a09a48ad23fe0ea5a180bee8cb750a tftp://71.188.64.55/ssms.exe
2459 21 Sep 2009 18:54:47 71.41.238.102 192.168.1.6 66bf4bbb8c4131f682812e654df47282 tftp://71.41.238.102/ssms.exe
2465 22 Sep 2009 00:58:42 71.96.226.162 192.168.1.6 14a09a48ad23fe0ea5a180bee8cb750a tftp://71.96.226.162:69/ssms.exe
2468 22 Sep 2009 01:47:35 71.105.183.46 192.168.1.6 6ded5c92a3983af55fef5d5815919de9 tftp://71.105.183.46/ssms.exe
2470 22 Sep 2009 02:17:29 71.109.73.228 192.168.1.6 b8076e37aef1105d045fc39f780da5a2 tftp://71.109.73.228/ssms.exe
2473 22 Sep 2009 04:35:31 71.116.1.87 192.168.1.6 df51e3310ef609e908a6b487a28ac068 tftp://71.116.1.87:69/ssms.exe
2475 22 Sep 2009 05:49:06 71.110.235.36 192.168.1.6 df51e3310ef609e908a6b487a28ac068 tftp://71.110.235.36:69/ssms.exe
2481 22 Sep 2009 09:47:54 71.105.114.21 192.168.1.6 2fa0e36b36382b74e6e6a437ad664a80 tftp://71.105.114.21:69/ssms.exe
2488 22 Sep 2009 14:19:35 71.97.206.3 192.168.1.6 bb39f29fad85db12d9cf7195da0e1bfe tftp://71.97.206.3:69/ssms.exe
2491 22 Sep 2009 15:35:08 71.41.99.199 192.168.1.6 3228f8bc721572422c268f244476dbb8 tftp://71.41.99.199/ssms.exe
2499 22 Sep 2009 19:22:42 71.41.99.199 192.168.1.6 3228f8bc721572422c268f244476dbb8 tftp://71.41.99.199:69/ssms.exe
2500 22 Sep 2009 19:30:30 71.41.99.23 192.168.1.6 14a09a48ad23fe0ea5a180bee8cb750a tftp://71.41.99.23/ssms.exe
2502 22 Sep 2009 20:20:46 71.121.172.28 192.168.1.6 b8076e37aef1105d045fc39f780da5a2 tftp://71.121.172.28/ssms.exe
2505 22 Sep 2009 21:57:12 71.31.67.198 192.168.1.6 bb39f29fad85db12d9cf7195da0e1bfe tftp://71.31.67.198/ssms.exe
2508 23 Sep 2009 01:46:53 71.116.1.87 192.168.1.6 df51e3310ef609e908a6b487a28ac068 tftp://71.116.1.87/ssms.exe
2509 23 Sep 2009 01:49:09 71.172.112.166 192.168.1.6 833cda5b5bef5989deb6bf57c557ce30 tftp://71.172.112.166:69/ssms.exe
A-IP: A-CC: V-IP: 192.168.1.6 V-CC: MD5: Rows 61 - 80 of 3409
Attack Detail
ID: 3363
Time: Fri Oct 02 2009 22:16:19 GMT+0100 (GMT Daylight Time)
Sensor:
Download: tftp://71.31.67.198/ssms.exe
Trigger: tftp://71.31.67.198/ssms.exe
MD5sum: bb39f29fad85db12d9cf7195da0e1bfe
SHA512: 55d2096e39e4cf2fc19afce3c2e1becbf31da602e7c2a67af0a8ad23803bc2cb
File Type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Attacker IP:
Victim IP: 3232235782
Filename: ssms.exe
Country: US
ISP: ALLTEL - ST. MARYS
ASN: 7029
Google Maps Google Earth Virustotal Anti-Virus Sandbox Graphs PicViz Heatmap Cuttlefish
Map Satellite Hybrid Terrain
Attacker IP: 71.110.235.36
Country: UNITED STATES (US)
ASN: 19262
ISP: VERIZON INTERNET SERVICES INC
Latitude: 34.0359992981
Longitude: -117.016998291
Canada
Alberta
Manitoba
Saskatchewan
British Columbia
Ontario
Québec
Minnesota
Wisconsin
Michigan
New York
Texas
Florida
Louisiana
Mississippi
Alabama
Georgia
Gulf of Mexico
North Atlantic Ocean
North Pacific Ocean
Cuba
Venezuela
Colombia
Ecuador
Map data ©2009 LeadDog Consulting, Tele Atlas, IGI, Europa Technologies - Terms of Use
Done
Tor Disabled

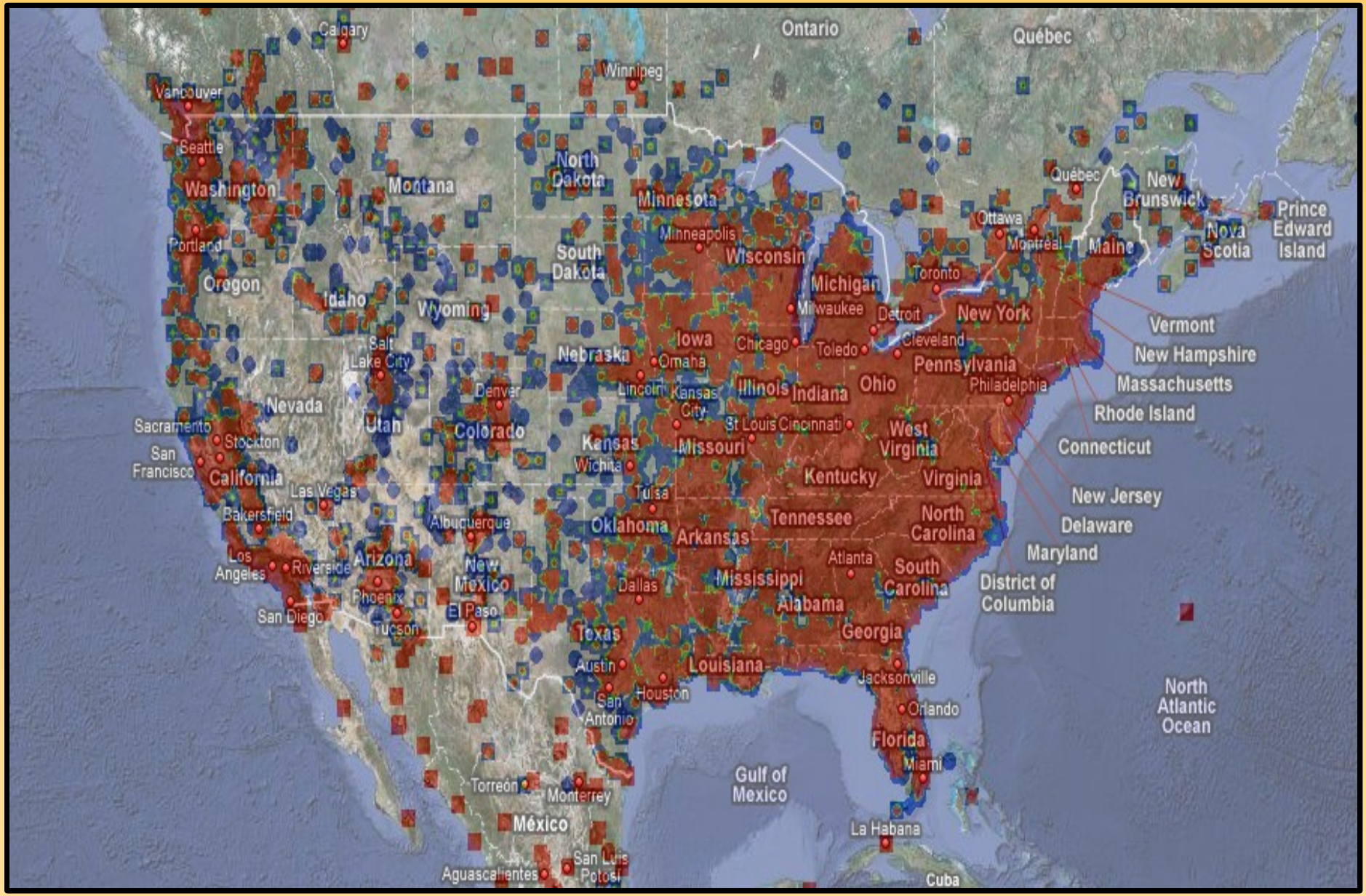

Example HonEeeBox Reporting Interface using Ext-JS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://honeeebox.net/demo_schema1/
Most Visited Getting Started Latest Headlines
Attack Summary Panel
Total Attacks: 3409 (+36) Total Attacker IPs: 1202 (+28) Total Victim IPs: 167 (+17) Total MD5sums: 566 (+22) Sensors: 10 (4) AV Undetected: 4015 / 28579 (14.0%)
Attack Browser
ID Time Attacker IP Victim IP MD5sum Download
3361 02 Oct 2009 22:06:17 84.109.190.125 88. c92263d2ee57ab777e97d96023f75aa6 creceive://84.109.190.125:29628
3362 02 Oct 2009 22:08:01 84.109.190.125 88. 28a182d2d67e28df1c612c6835d152a8 creceive://84.109.190.125:37501
3363 02 Oct 2009 22:16:19 71.31.67.198 192.168 bb39f29fad85db12d9cf7195da0e1bfe tftp://71.31.67.198/ssms.exe
3364 02 Oct 2009 23:06:47 80.165.178.241 80. 14a09a48ad23fe0ea5a180bee8cb750a tftp://80.165.178.241/ssms.exe
3365 03 Oct 2009 08:36:03 88.134.29.250 88. e23d9a57aef0986376776f5f685112f4 ftp://1:1@88.134.29.250:28341/chosts.exe
3366 03 Oct 2009 09:54:46 71.115.111.43 192.168 e269d0462eb2b0b70d5e64dcd7c676cd tftp://71.115.111.43:69/ssms.exe
3367 03 Oct 2009 10:03:45 88.134.29.250 88. e23d9a57aef0986376776f5f685112f4 ftp://1:1@88.134.29.250:11515/chosts.exe
3368 03 Oct 2009 10:13:53 80.171.109.19 80. d36e6d1695a610bbd580d5f7d96167b3 tftp://80.171.109.19/ssms.exe
3369 03 Oct 2009 10:20:25 88.134.29.250 88. e23d9a57aef0986376776f5f685112f4 ftp://1:1@88.134.29.250:11515/chosts.exe
3370 03 Oct 2009 10:33:16 80.171.109.19 80. d36e6d1695a610bbd580d5f7d96167b3 tftp://80.171.109.19/ssms.exe
3371 03 Oct 2009 11:26:35 80.5.30.87 80. a759a39900655a2280de28d5ac9684c9 tftp://80.5.30.87:69/ssms.exe
3372 03 Oct 2009 11:27:53 80.161.55.235 80. 697f001bc330ab483d77a707cd40c8d9 tftp://80.161.55.235/ssms.exe
3373 03 Oct 2009 11:58:04 202.183.52.12 202 98eb0fdadf8a403c013a8b1882ec986d tftp://202.183.52.12:69/ssms.exe
3374 03 Oct 2009 12:02:20 88.70.201.129 88. 059a2367cf8f28b239d24cd91866fcce ftp://88.70.201.129:30978/mobile.exe
3375 03 Oct 2009 12:50:22 88.134.29.250 88. e23d9a57aef0986376776f5f685112f4 ftp://1:1@88.134.29.250:11515/chosts.exe
3376 03 Oct 2009 13:32:01 88.134.144.39 88. a7e25d717ac8c626e4db044eb4dca5dd ftp://1:1@88.134.144.39:21125/mobile.exe
3377 03 Oct 2009 13:35:53 88.71.226.226 88. 2daf2046f3e2315b255dd6be1f1ac244 ftp://1:1@88.71.226.226:24880/lhost.exe
3378 03 Oct 2009 13:50:01 88.71.226.226 88. 2daf2046f3e2315b255dd6be1f1ac244 ftp://1:1@88.71.226.226:24880/lhost.exe
3379 03 Oct 2009 13:55:28 80.145.202.131 80. 14a09a48ad23fe0ea5a180bee8cb750a tftp://80.145.202.131/ssms.exe
3380 03 Oct 2009 14:20:33 88.70.201.129 88. 059a2367cf8f28b239d24cd91866fcce ftp://88.70.201.129:30978/mobile.exe
A-IP: A-CC: V-IP: V-CC: MD5: Rows 3361 - 3380 of 3
Attack Detail
ID: 3363
Time: Fri Oct 02 2009 22:16:19 GMT+0100 (GMT Daylight Time)
Sensor:
Download: tftp://71.31.67.198/ssms.exe
Trigger: tftp://71.31.67.198/ssms.exe
MD5sum: bb39f29fad85db12d9cf7195da0e1bfe
SHA512: 55d2096e39e4cf2fc19afce3c2e1becbf31da602e7c2a67af0a8ad23803bc2cb
File Type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Attacker IP: 1193231302
Victim IP:
Filename: ssms.exe
Country: US
ISP: ALLTEL - ST. MARYS
ASN: 7029
Google Maps Google Earth Virustotal Anti-Virus Sandbox Graphs PicViz Heatmap Cuttlefish
Done
Tor Disabled


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
193.253 - 4
195.241 - 1
149.225 - 1
145.254 - 2
193.178 - 2
195.218 - 143
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
193.19 - 1
194.105 - 1
193.17 - 2
193.11 - 226
193.138 - 2
193.227 - 3
195.49 - 529
195.245 - 1
195.144 - 732
195.2 - 219
194.187 - 2
195.222 - 2
195.23 - 1
195.29 - 2
193.243 - 2
157.161 - 2
195.6 - 2
151.2 - 5
151.54 - 1
151.33 - 634
193.207 - 25
193.204 - 1
151.32 - 2
195.13 - 2
193.153 - 1
193.152 - 2
193.194 - 1
194.219 - 70
195.158 - 1
Ireland
England
Isle of Man
Netherlands
Belgium
Luxembourg
Germany
Poland
Jersey
France
Switzerland
Austria
Slovakia
Hungary
Ukraine
Moldova
Romania
Slovenia
Croatia
Bosnia and Herzegovina
Montenegro
Bulgaria
Macedonia (FYROM)
Albania
Greece
Italy
San Marino
Monaco
Andorra
Holy See (Vatica
Portugal
Andalucía
Ionian Sea
Aegean Sea
Lefkada
Zakynthos (Zante)
Athina
Chios
İzmir
Ankara
Samos
Kos
Isola di Ustica
Isola Lipari
Isola Favignana
Sicilia (Sicily)
Ibiza
El-Jazair (Algiers)
(Tangier)
Tanger
1034 km
49°42'58.14" N
11°57'44.67" E
Eye alt 3133.17 km
© 2008 Basarsoft
© 2008 Geocentre Consulting
© 2008 Europa Technologies
© 2008 Tele Atlas
Google

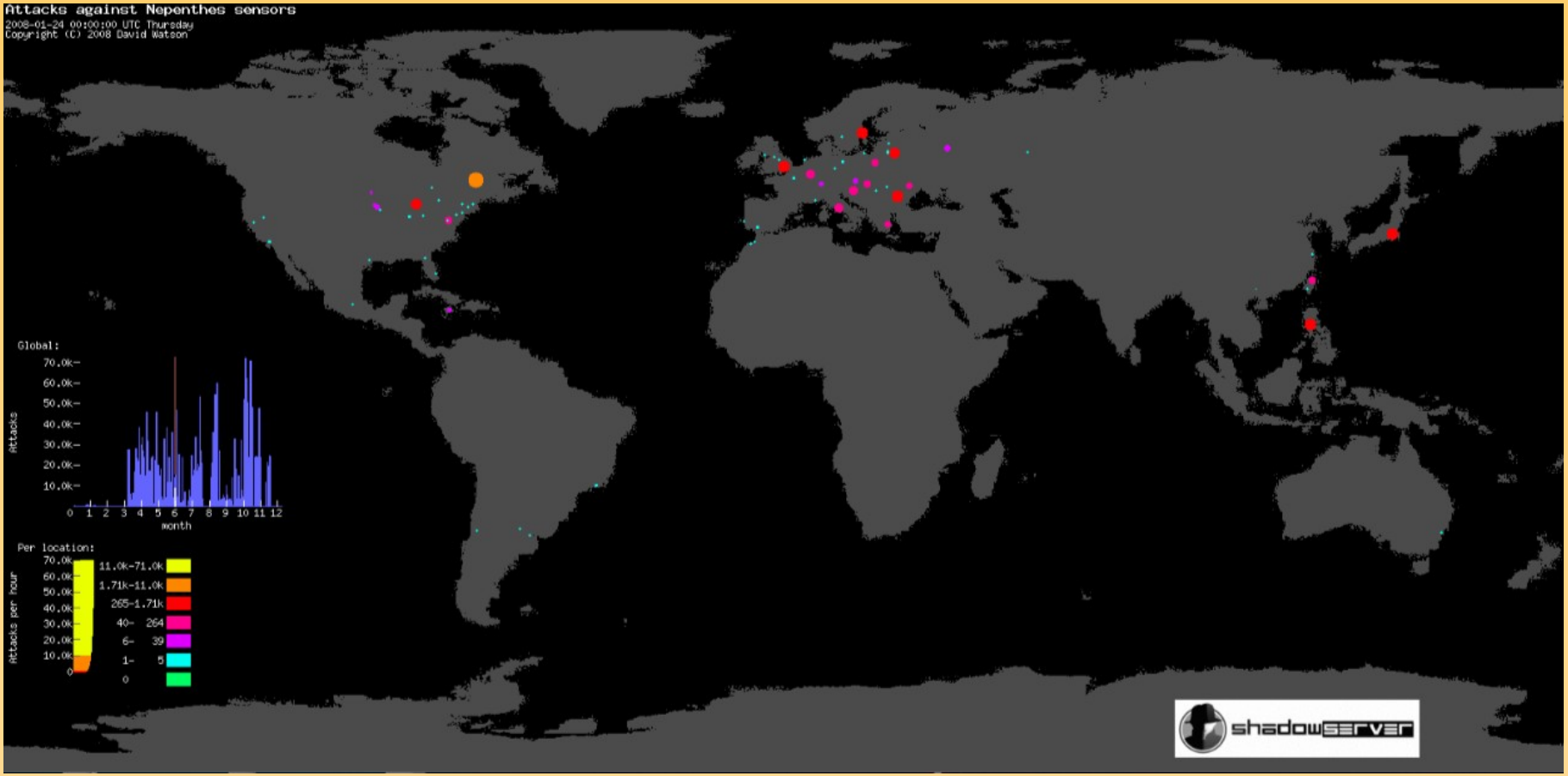

Total Attacks: 56
Total Source IPs: 8
Total Target IPs: 1
Total MD5sums: 7
Attacks
ID
Time
Attacker IP
Victim IP
MD5sum
Download
Attack Detail
Sophos
Result: 38/39 (97.44%)

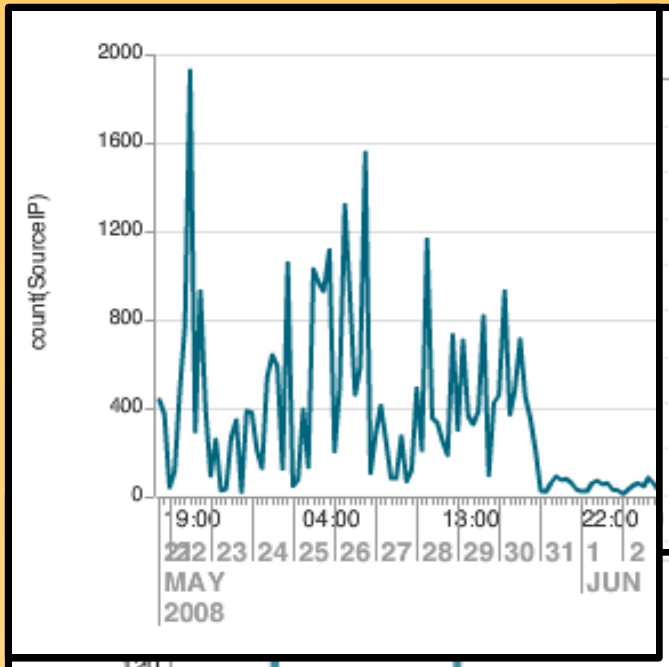

Total Target IPs:
Total MD5sums: 7
Scan Summary
File Changes
Registry Changes
Technical Details
Analysis Number
1
Process ID
Filename
Filesize
MD5
Start Reason
Termination Reason
Start Time
Stop Time
Detection
COM
DLL Handling
Loaded DLLs
New Files


Total Target IPs: 1
Total MD5sums: 7
Reserved
HP
DEC
DDN-RVN
GE
Xerox
AT&T
Apple
MIT
DISA
Multica
Level3
DISA
Cable
IBM
RFC1918
SITA
APNIC
USPS
AT&T
Merit
Unallocated
APNIC
PSI
RIPE
ARIN
US-DOD
RIPE
ARIN
APNIC

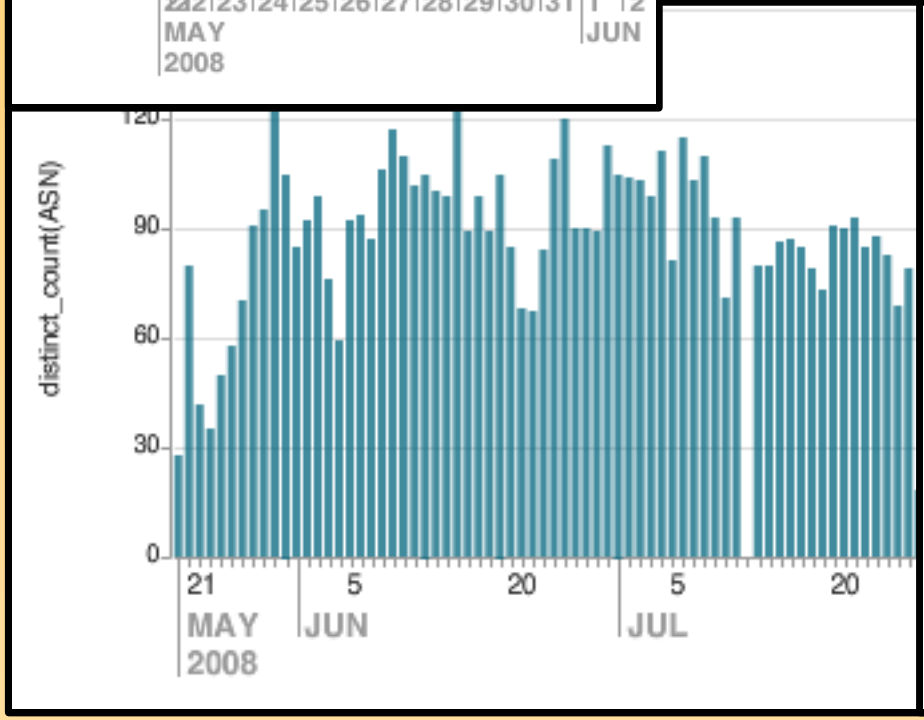


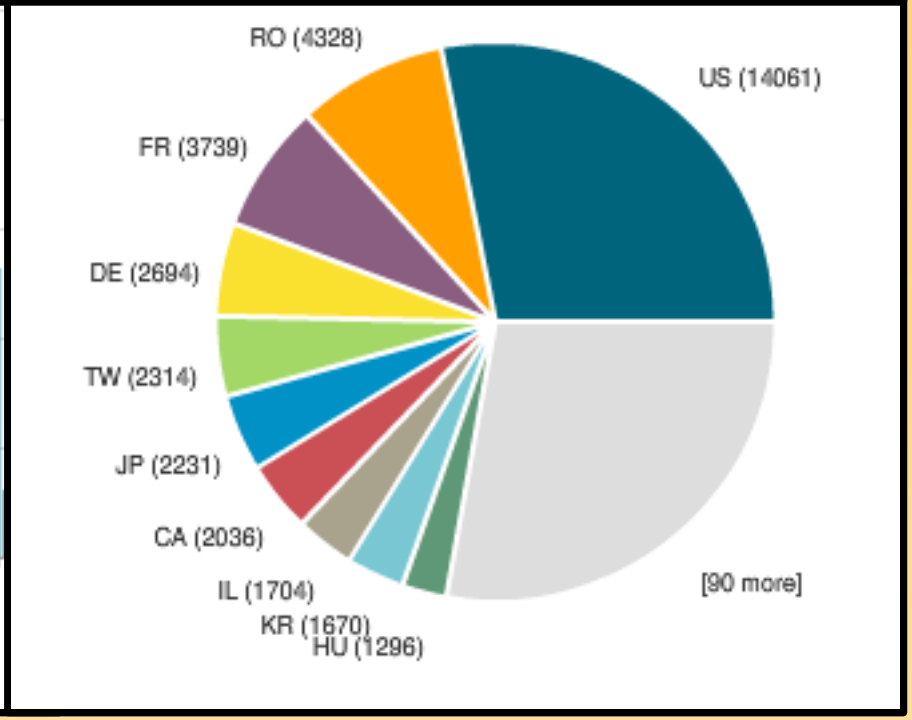
David Watson (david@honeynet.org.uk)


Attacks against Nepenthes sensors
2008-01-24 00:00:00 UTC Thursday
Copyright (C) 2008 David Watson
Global:
Attacks
70.0k
60.0k
50.0k
40.0k
30.0k
20.0k
10.0k
0 1 2 3 4 5 6 7 8 9 10 11 12
month
Per location:
Attacks per hour
11.0k-71.0k
1.71k-11.0k
265-1.71k
40- 264
6- 39
1- 5
0
shadowserver

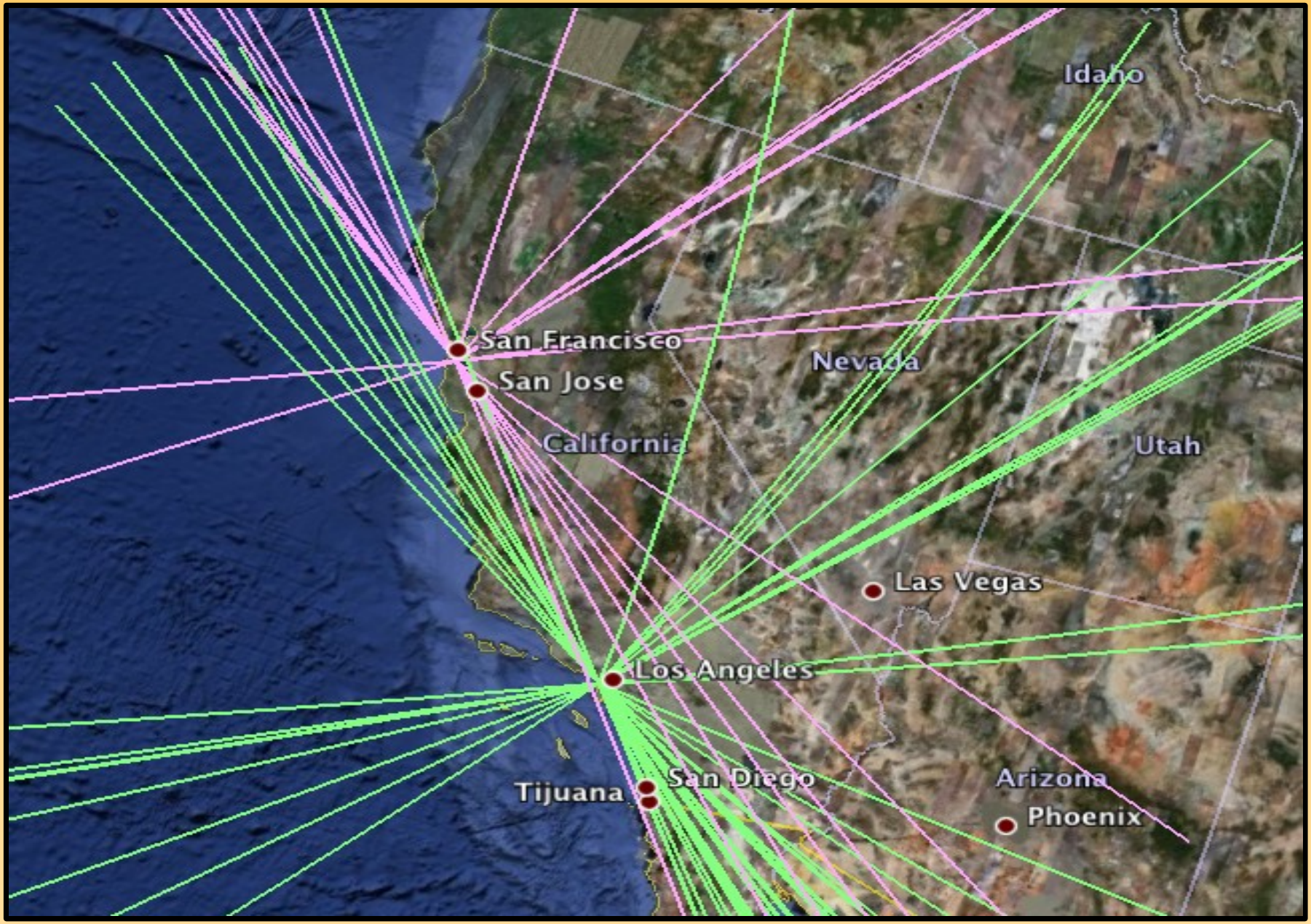


Classification	count	percent
WORM/Allaple.Gen	14228	28.951063
TR/Crypt.XPACK.Gen	9021	18.355886
TR/Crypt.NSPM.Gen	5059	10.294028
WORM/Allaple.Damaged.Gen	2700	5.493946
W32/Virut.N.DR	2375	4.832638
WORM/Rbot.147456.27	1830	3.723675
WORM/Rbot.147456.27]	1774	3.609726
W32/Virut.Gen	1550	3.153932
WORM/Rbot.50176.5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

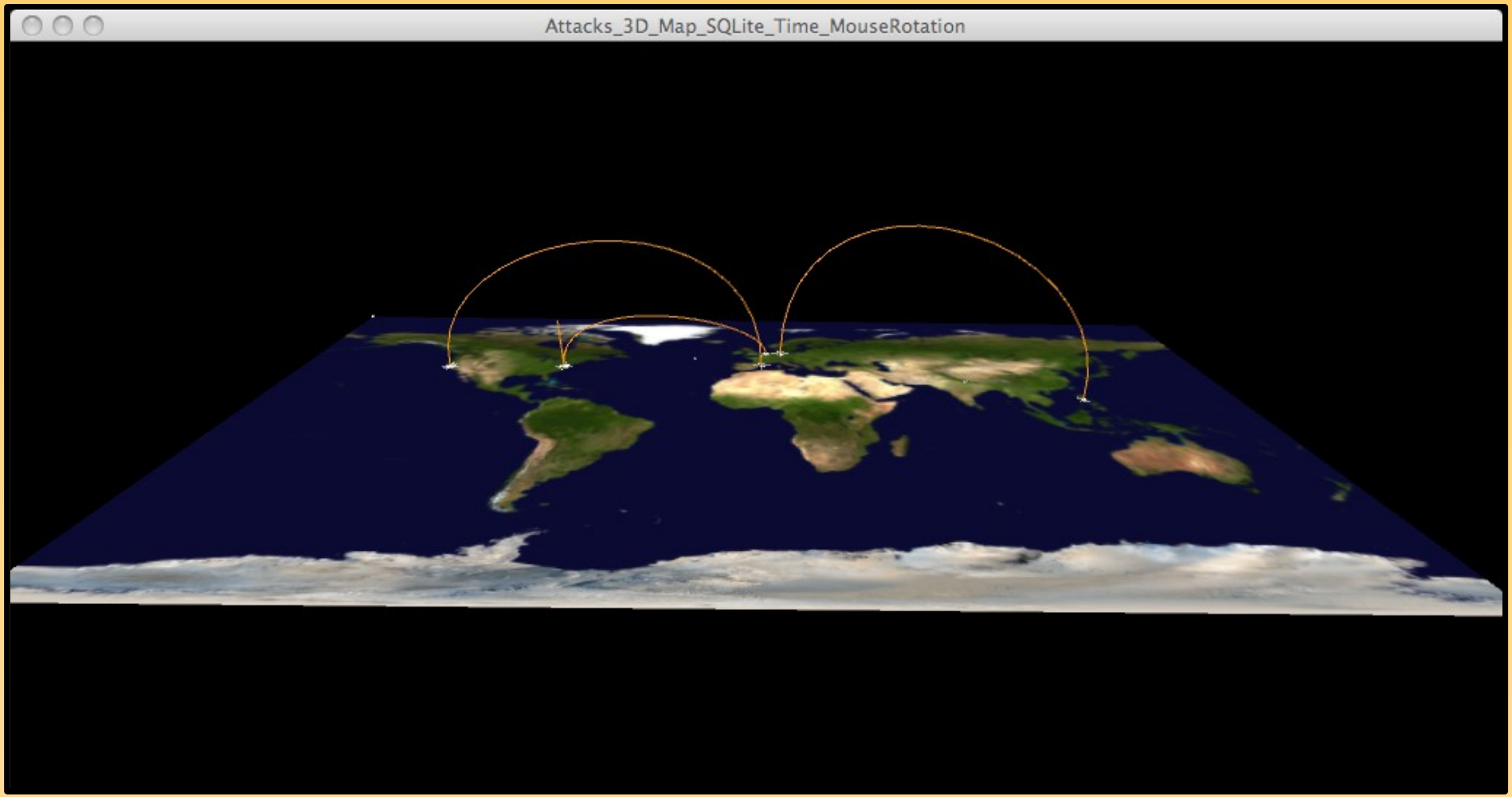




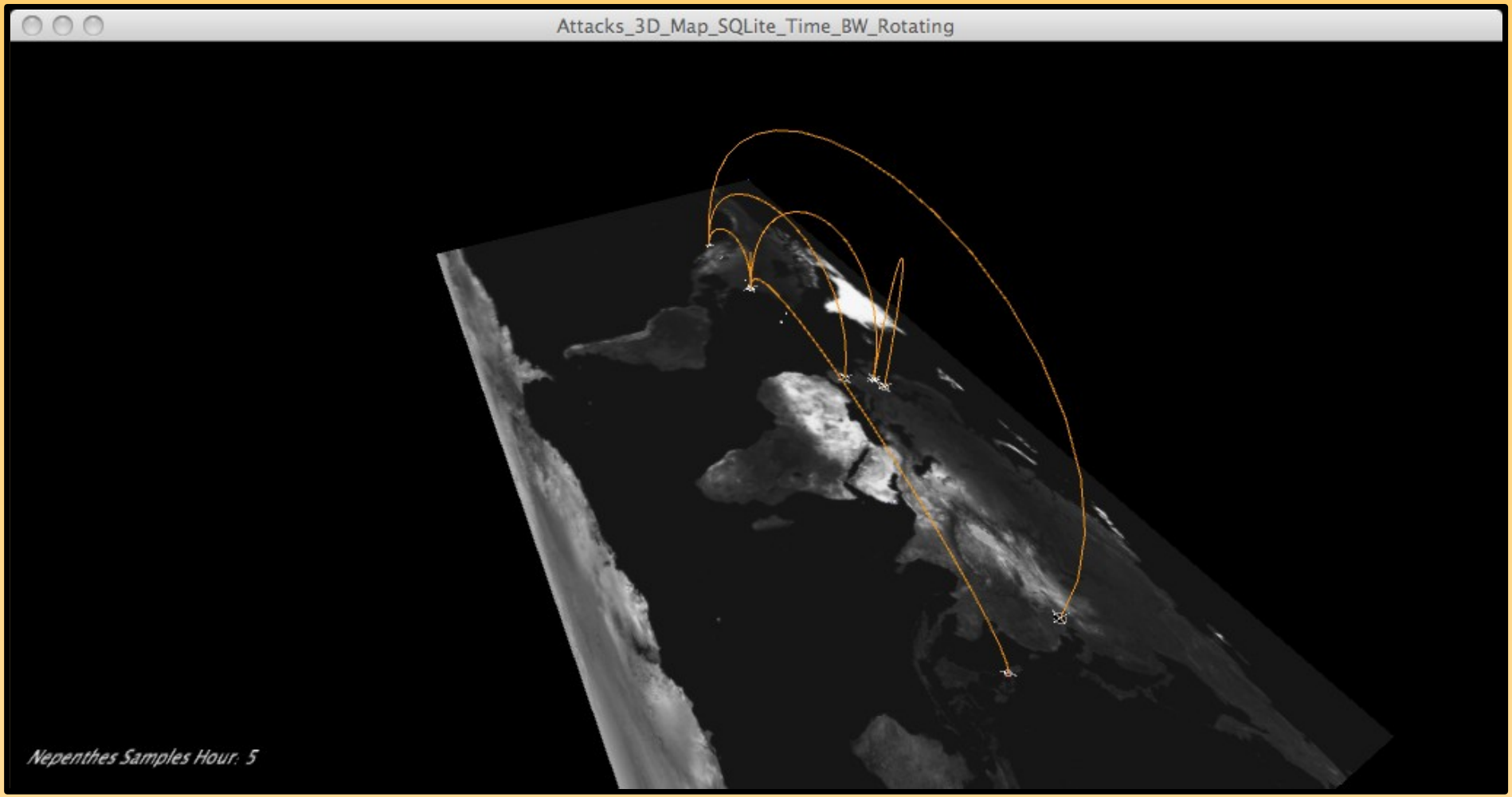
David Watson (david@honeynet.org.uk)



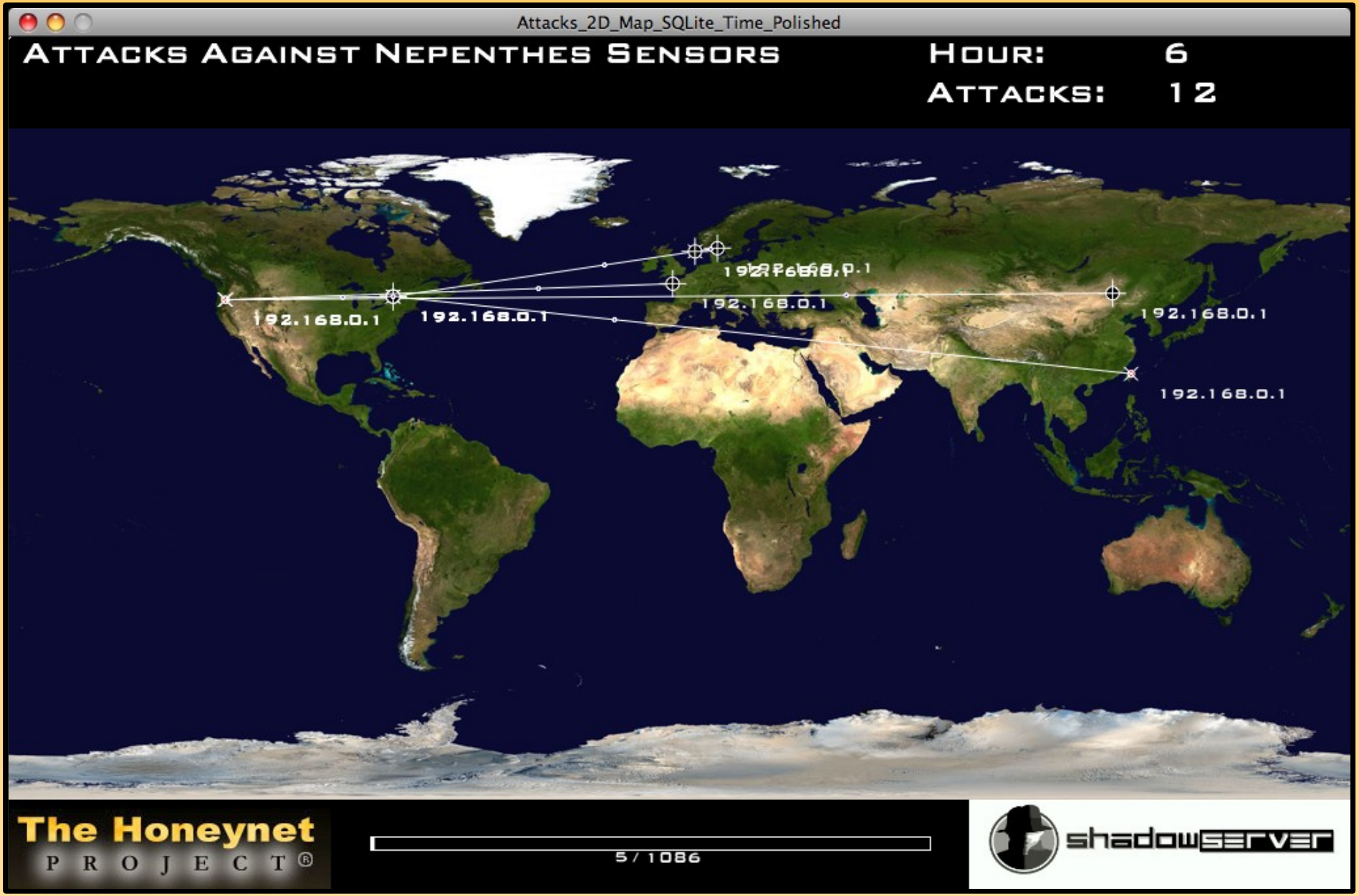
David Watson (david@honeynet.org.uk)



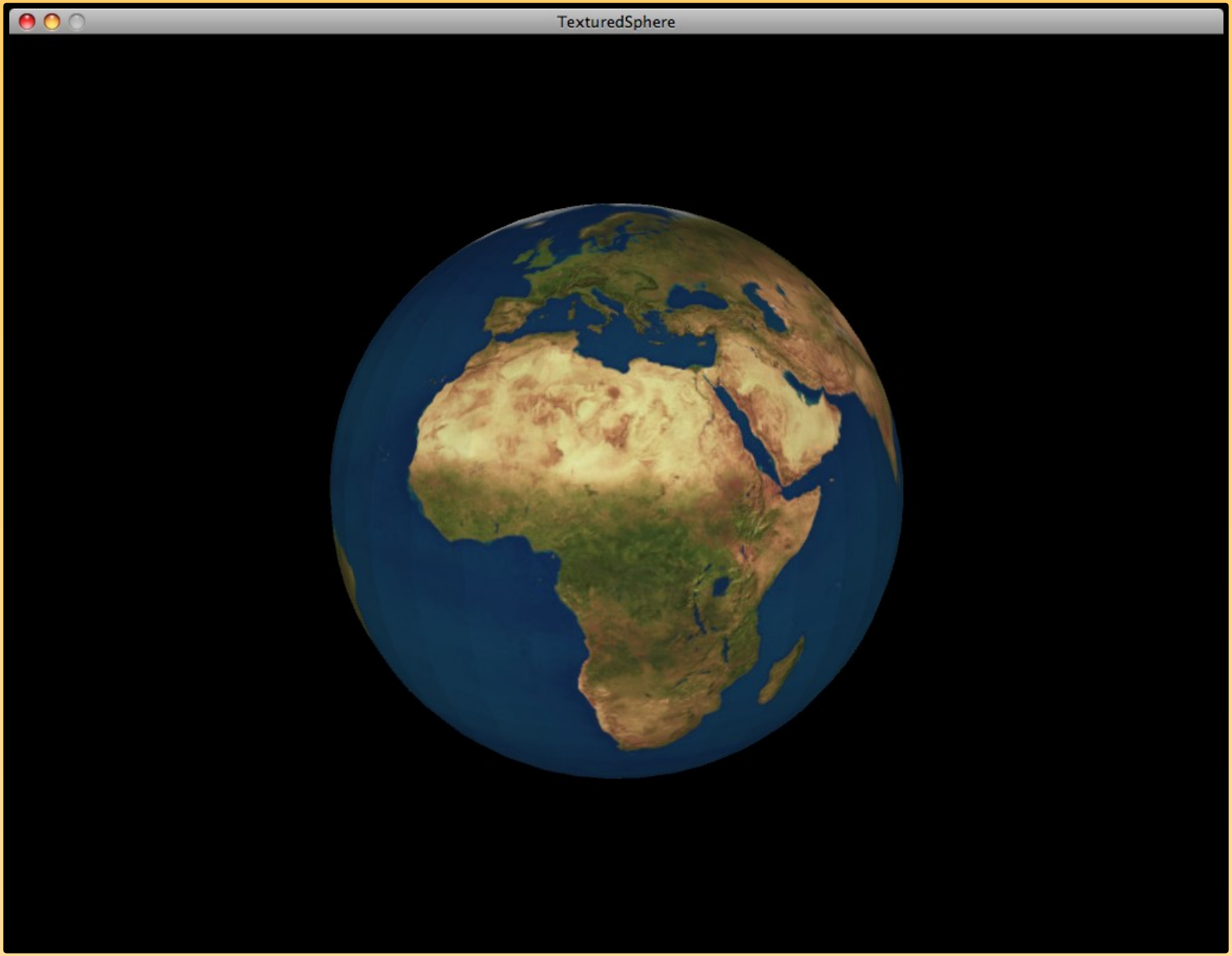
David Watson (david@honeynet.org.uk)



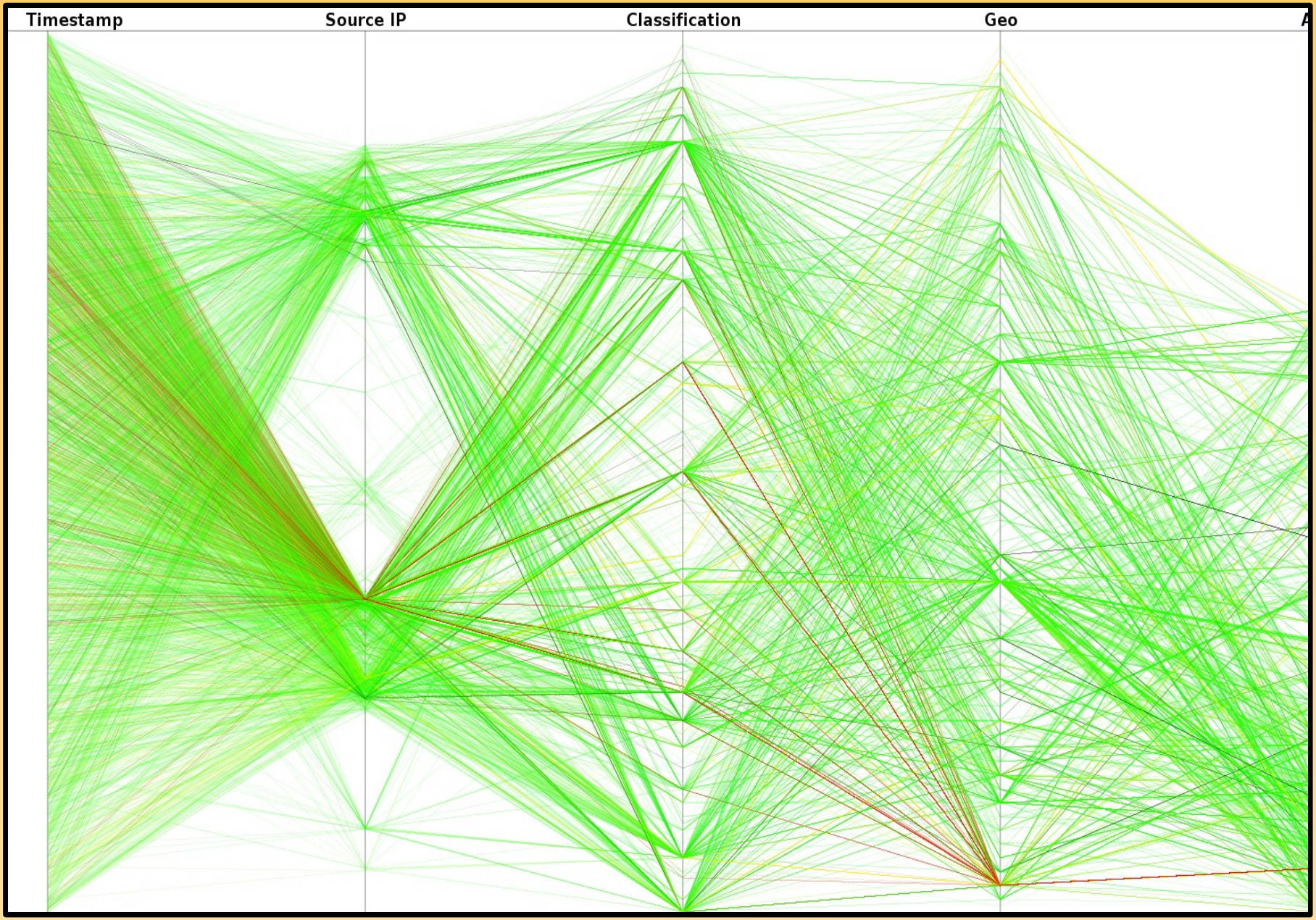
David Watson (david@honeynet.org.uk)



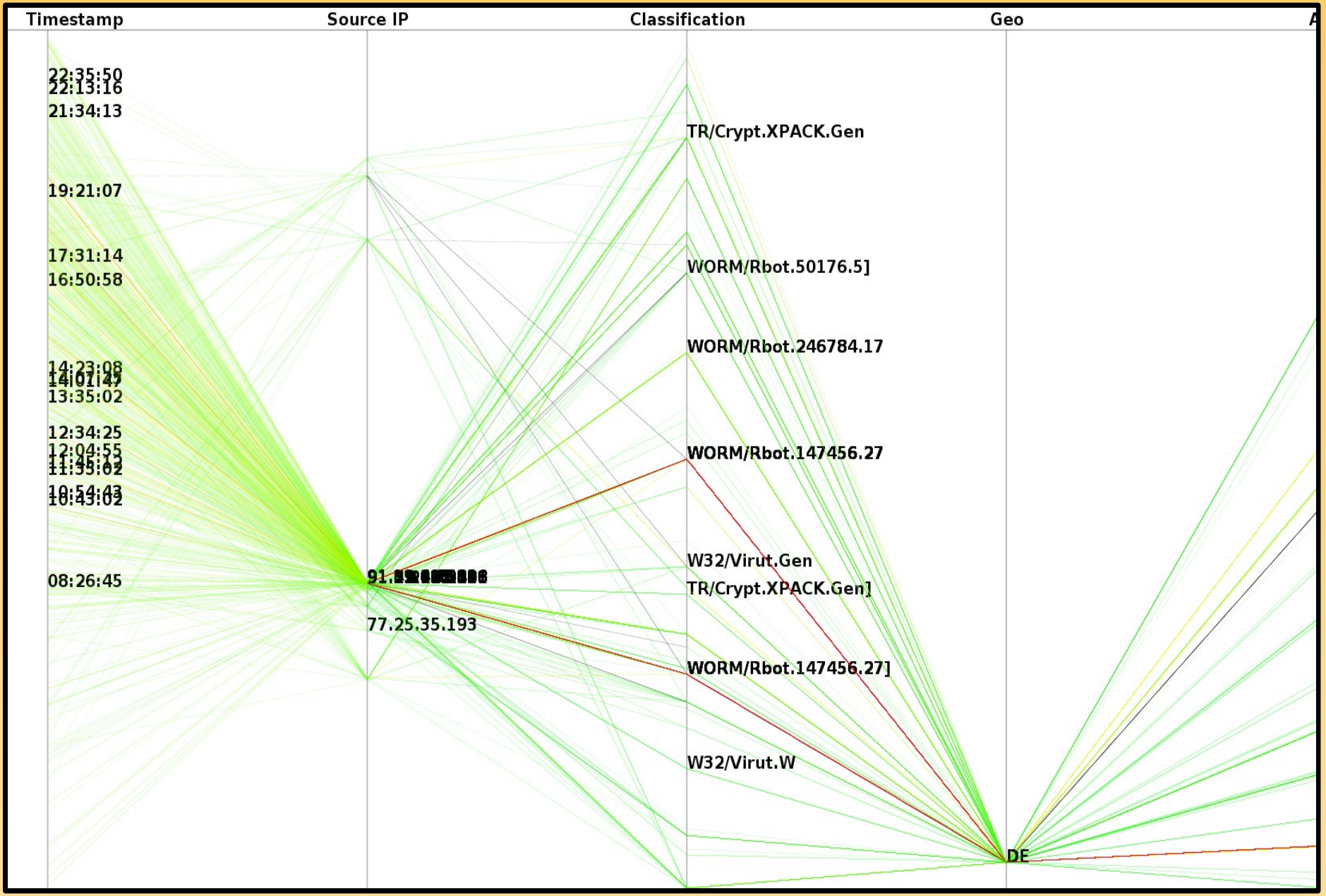
David Watson (david@honeynet.org.uk)



David Watson (david@honeynet.org.uk)



David Watson (david@honeynet.org.uk)


Timestamp
Source IP
Classification
Geo
22:35:50
22:13:16
21:34:13
19:21:07
17:31:14
16:50:58
14:23:08
14:01:47
13:35:02
12:34:25
12:04:55
11:35:02
10:54:43
10:43:02
08:26:45
91.
77.25.35.193
TR/Crypt.XPACK.Gen
WORM/Rbot.50176.5]
WORM/Rbot.246784.17
WORM/Rbot.147456.27
W32/Virut.Gen
TR/Crypt.XPACK.Gen]
WORM/Rbot.147456.27]
W32/Virut.W
DE

HonEeeBox v1 Goals

- Ship 100 sensors to members by April 2010
- Get budget to pay for hardware shipping
- Build prototype UI using ExtJS & backend
- Find more people to contribute to development
- Sensors in regions like China, Iran, Korea, etc to potentially interest funders
- 100+ nodes with zero day detection to demo a distributed sensor network and attract funding
- Decide if HonEeeBox and data will be an internal resource / community resource / open sourced / etc

HonEeeBox Successes

- Bought 145 sensors using $40k NIC funding July 2009
- $10k from Symantec to pay for hardware shipping
- Built Prototype UI using ExtJS & backend
- Ran operational blog and gradually added sensors
- Got a few people involved in UI development
- Current stats (past 24 hours):

Sensors:	39 (10)	(~90 Lance / Julia)
Total Attacks:	35230 (+74)	
Total Attacker IPs:	12545 (+25)	
Total Victim IPs:	212 (+15)	
Total MD5sums:	2326 (+22)	

HonEeeBox Failures

- Struggled with sensor shipping & logistics (50/145)
- Lack of active developers and sys-admins:
  - **David** = GSoC 2009/2010 Feb-Oct & travel/classes
  - **Lance** and **Arthur** = babies & new jobs
  - **Steve**, **Jamie, Sebastien** and **Rob** = New jobs
- Although sensors still operational, UI is a prototype
- Nepenthes rather than Dionaea, 'boring' samples
- Svn/Trac password protected, code not released
- Collected data only available to other participants
- External member perception of project was limited

Process for setting up new HonEeeBox participants and nodes

1. (**Lance**) Confirm participant has one or more unfiltered public static IP addresses on a netblock that we don't currently have a HonEeeBox sensor running on and is willing to participate in the HonEeeBox project, including sharing da
2. (**Lance**) Obtain shipping address from participant.
3. (**Lance**) Ship one or more sensors plus pre-written USB key and setup instructions to participat at requested shipping address, recording the shipping address, shipping date, shipment tracking ID and shipping cost in the Honeeebo
4. (**Lance**) Email participant with their shipment tracking ID. In this email include the welcome email which includes a link to the electronic version of the setup guides and tells the participant what data we need from them to complet
5. (**Lance**) Confirm when participant receives shipped sensor(s) and record the received date in the HoneeeboxSensorDepoyment.
6. (**Lance** or **David**) Participant replies to welcome email with sensor setup information once they have deployed it. Record all deployment details in HoneeeboxSensorDepoyment.
7. (**David**) Add sensor's static public IP address(es) to iptables rule on honeeebox.net:

```
sudo vi /etc/iptables.conf

# <NODE_ID> David Watson <DATE in format 01/01/10>
-A RH-Firewall-1-INPUT -s <SENSOR_IP> -m state --state NEW -m tcp -p tcp --dport 8443 -j ACCEPT

sudo iptables-restore < /etc/iptables.conf
```

Record sensor IP address and deployment date details in HoneeeboxSensorDepoyment.

8. (**David**) Create user's Apache account with a sane strong password:

```
sudo htpasswd /etc/apache2/htpasswd forename.surname
```

Record paricipant useranme in HoneeeboxSensorDepoyment.

9. (**David**) Test web access at https://honeeebox.net as participant's new user account:
1. (**David**) Add operational blog post for new participant, if necessary, setting blog post date to htpasswd change date and category to "Participation":

```
Subject: New Participant Added (Forename Surname)
Body: From the <ORG_NAME> (<EMAIL_ADDRESS>).
```

1. (**David**) Add operational blog post for sensor deployment, setting blog post date to iptables rule change date and category to "Sensor Deployment":

```
Subject: HonEeeBox Sensor Added (<NODE_ID>)
Body: Sensor <NODE_ID> hosted by Forename Surname in City, Country. DSL/CABLE/ETC connection with 1 public IP address.
```

1. (**David**) Update HonEeeBox blog list of participants and sensors (https://honeeebox.net/Blog/?page_id=8).
1. (**David**) Add the participant to the HonEeeBox mailing list (https://public.honeynet.org/mailman/listinfo/honeeebox).
1. (**David**) Email participant (using GPG to tell them their username/password, that their node is now live and remind them of the HonEeeBox UI URL (http://honeeebox.net) and operational blog (http://honeeebox.net/Blog).

In future we'll be confirming receipt of a signed data sharing agreement as step 0.

Do we need to create a blog account for each user too?

HonEeeBox Lessons Learned

- Shipping and **logistics** have to be streamlined
- Must be simple to **add sensors** to the backend
- Needs **core team** of **dev** and **ops** always available
- **David** can't be the bottleneck during GSoC 2011
- Most people happy to share low interaction data
- Need to balance data sharing and privacy concerns with wider access to membership & better member communication (all full members see data?)
- Lots of security community partners keen to host sensors for us, can definitely build large sensornet
- Presentations always gets in/external interest

HonEeeBox Lessons Learned

- Support **DHCP** (implications for sensor ID vs source IP, need for stronger auth not firewalling)
- Update packages from our own package repository
- Postgresql has native IP data sources, not MySQL
- Move from ExtJS + PHP to **Django/python**
- Event based, non-blocking wherever possible
- Members seemed ok with remote SSH admin
- Can't easily use VPN tunnel mode with Dionaea on ADSL (so still local sensors not SurfIDS model)
- GSoC student access to data is difficult:

  Give them anonymised sets of reference data?

The Honeynet PROJECT®

HonEeeBox v2:
Rapid Deployment of Many Distributed Low Interaction Malware Collectors (and this time suceeding!)

Nepenthes → Dionaea

- C with glib
- LibEv events
- Emdedded Python
- OpenSSL for TLS
- Udns (asynch)
- Curl and Libcfg
- SQL logging
- IPv6 support

- **SMB/CIFS protocol emulation for (unknown) RPC calls**
- **Generic shellcode detection via LibEmu**
- Actions on shellcode profile (windows shell, file download) via LibEmu execution

```
connection 610 smbd tcp accept 10.69.53.52:445 <- 10.65.34.231:2010
 dcerpc request: uuid '3919286a-b10c-11d0-9ba8-00c04fd92ef5' opnum 9
 p0f: genre:'Windows' detail:'XP SP1+, 2000 SP3' uptime:'-1' tos:'' dist:'11' nat:'0' fw
 profile: [{'return': '0x7c802367', 'args': ['', 'CreateProcessA'], 'call': 'GetProcAddr
          ...., {'return': '0', 'args': ['0'], 'call': 'ExitThread'}]
 service: bindshell://1957
 connection 611 remoteshell tcp listen 10.69.53.52:1957
   connection 612 remoteshell tcp accept 10.69.53.52:1957 <- 10.65.34.231:2135
     p0f: genre:'Windows' detail:'XP SP1+, 2000 SP3' uptime:'-1' tos:'' dist:'11' nat:'0
     offer: fxp://1:1@10.65.34.231:8218/ssms.exe
     download: 1d419d615dbe5a238bbaa569b3829a23 fxp://1:1@10.65.34.231:8218/ssms.exe
     connection 613 ftpctrl tcp connect 10.69.53.52:37065 -> 10.65.34.231/None:8218
       connection 614 ftpdata tcp listen 10.69.53.52:62087
         connection 615 ftpdata tcp accept 10.69.53.52:62087 <- 10.65.34.231:2308
           p0f: genre:'Windows' detail:'XP SP1+, 2000 SP3' uptime:'-1' tos:'' dist:'11' 
```

HonEeeBox v2 in 2011

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

HonEeeBox v2 in 2011

- Minimal **Debian-Live** system (Lenny 5.0)
- **Dionaea** .deb created from the current Dionaea release in git
- DHCP plus automatic live CD login
- Patch and upgrade on the fly via apt
- Permanent installation prompts for locale, network configuration, etc as normal
- HTTPS data submission to central server (**backwardly compatible** with HonEeeBox v1)

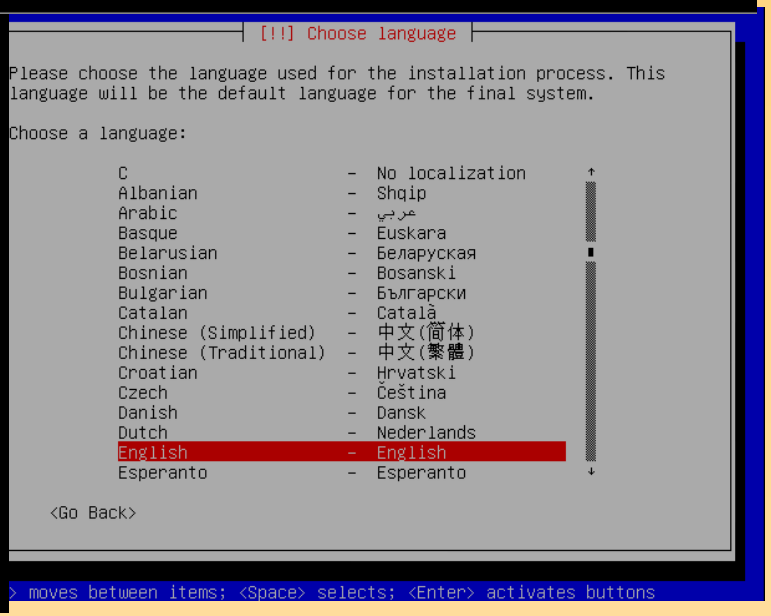

```
egin: Setting up locales ... Generating locales (this might take a while)...
  en_US.UTF-8... done
eneration complete.
one.
egin: Setting up automatic login ... done.
egin: Setting up console keyboard ... done.
egin: Configuring gnome-panel-data ... done.
egin: Configuring screensaver ... done.
egin: 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
    8.924259] input: Power Button (FF) as /class/input/input1
    8.956107] ACPI: Power Button (FF) [PWRF]
```

```
ress F1 for help, or ENTER to boot: _
```

```
config
  emulation
    limits
      files = "3"
      filesize = "524288"
      sockets = "3"
      sustain = "120"
      idle = "30"
      listen = "30"
      cpu = "120"
      steps = "1073741824"
    api
      connect
        host = "127.0.0.1"
        port = "4444"
allow
        # protocol   # type  accept
        # protocol  ftpctrl  # type  connect

deny
        # protocol  ftpdata ftpdatacon xmppclient  # type
```



```
root      2948     2  0 10:51 ?        00:00:00 [kstriped]
root      3089     1  0 10:51 ?        00:00:00 dhclient3 -pf /var/run/dhclient.
root      3227     1  0 10:51 ?        00:00:00 /usr/sbin/rsyslogd -c3
101       3247     1  0 10:51 ?        00:00:00 /usr/bin/dbus-daemon --system
root      3262     1  0 10:51 ?        00:00:00 /usr/sbin/sshd
root      3282     1  0 10:51 ?        00:00:00 /usr/sbin/cron
root      3299     1  0 10:51 tty1     00:00:00 /bin/login -f
root      3301     1  0 10:51 tty2     00:00:00 /bin/login -f
root      3303     1  0 10:51 tty3     00:00:00 /bin/login -f
admin     3305  3301  0 10:51 tty2     00:00:00 -bash
admin     3306  3299  0 10:51 tty1     00:00:00 -bash
root      3307     1  0 10:51 tty4     00:00:00 /bin/login -f
root      3309     1  0 10:51 tty5     00:00:00 /bin/login -f
admin     3313  3303  0 10:51 tty3     00:00:00 -bash
root      3318     1  0 10:51 tty6     00:00:00 /bin/login -f
root      3327     1  0 10:51 ?        00:00:00 runsvdir -P /etc/service log: ..
admin     3328  3307  0 10:51 tty4     00:00:00 -bash
admin     3330  3309  0 10:51 tty5     00:00:00 -bash
root      3331  3327  0 10:51 ?        00:00:00 runsv dionaea
nobody    3332  3331  2 10:51 ?        00:00:03 /opt/dionaea/bin/dionaea -l  -L
admin     3333  3318  0 10:51 tty6     00:00:00 -bash
root      3353     1  0 10:51 ?        00:00:00 /usr/sbin/p0f -i any -u root -Q
root      3364  3332  0 10:51 ?        00:00:00 /opt/dionaea/bin/dionaea -l  -L
admin     3376  3306  0 10:53 tty1     00:00:00 ps -ef
admin@debian:~$ _
```

HonEeeBox v2 in 2011

- **Updated disk image / ISOs** ready for testing
- Will **upgrade** existing sensor nodes **Q2 2011**
- Aim to deploy remaining ~90 sensors Q2-Q3
- **Core dev team**: David, Arthur, Mark, Rob, Sebastien, **You?** (need hands on python)
- **This week**:

  Plan *submit_http* → ***submit_XMPP / hpfeed***

  Plan new schema (consider Carniwwwhore)

  Plan and kickstart core development

  Brainstorm and plan UI plus visualizations

Project 2 - HonEeeBox Data Management Interface

Primary Mentor: David Watson (UK)

Backup mentor: Ben Reardon (AU), Arthur Clune (UK)

Type: New Development or Evolution of Existing Tool

Skill set required: Data driven web development skills, preferably Python/Django/Postgressql/Javascript/ExtJS but open to suitable alternative approaches

Project Goal: Implementation of a rich new web-based UI for exploration of malware data collected by a distributed network of international low interaction server honeypots

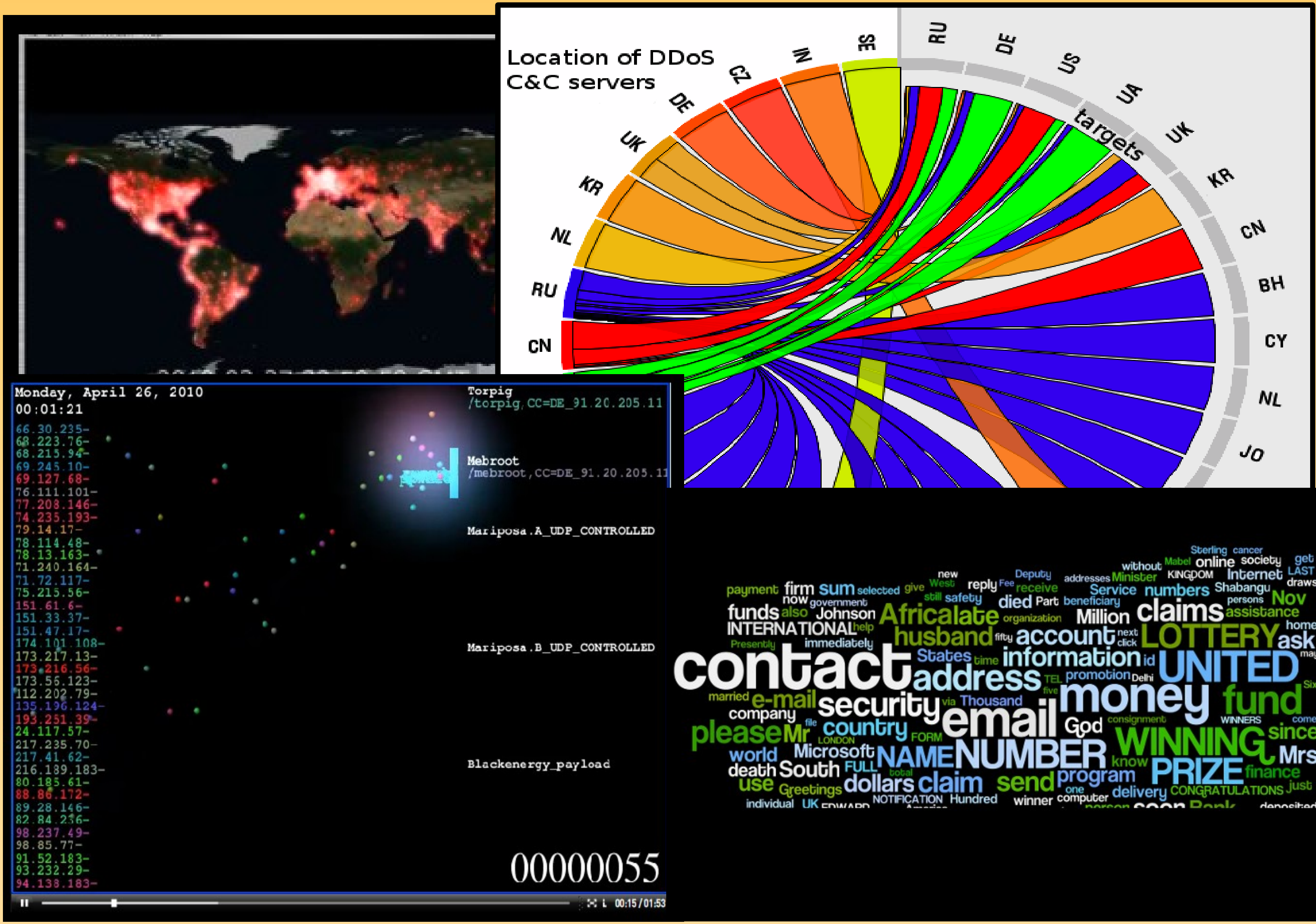
Project Description:

Honeynet Project members have developed a number of leading open source low interaction honeypot solutions that are used to automatically record data about network based malware attacks, such as Nepenthes, HoneyTrap and Dionaea (developed during GSoC 2009/2010). We have a number of active international sensor deployments to collect malware globally and are in the process of rolling out a larger low interaction sensor network called HonEeeBox, which was initially based on Nepenthes in 2009/20010 but is about to be upgraded to Dionaea in Q2 2011.

The goal of this project would be to implement a rich web based user interface and management reporting tool to allow analysts to easily explore large amounts of network attack and malware data. Typical tasks will be to view attack rates per sensor, search for high level trends (growth of a particular malware strain over time, attacks from a certain location on a particular day, etc) or drill down into the geographic detail of individual attacks. End users of the system will be the operators of malware collection sensors or interested analysts within the secuirty community or the Honeynet Project.

As input, the system will take reasonably simple CSV type data from low interaction malware sensors (such as timestamp, source IP, attack type, attacker IP address, MD5sum, etc in the form of an HTTP POST or via XMPP). This data is then automatically enriched by submitting the malware binary samples to multiplesandbox and antivirus engines for analysis (both public and private). The output from this post processing analysis is usally returned as XML or text after a short period, by HTTP or email. We also perform IP geo-location and ASN resolution against IP address to provide more information about sources, including latitude and longitutude for spatial mapping.

http://www.honeynet.org/gsoc/ideas


Location of DDoS C&C servers
targets
RU
DE
US
UA
UK
KR
CN
BH
CY
NL
JO
SE
IN
CZ
Monday, April 26, 2010
00:01:21
Torpig
/torpig,CC=DE_91.20.205.11
Mebroot
/mebroot,CC=DE_91.20.205.11
Mariposa.A_UDP_CONTROLLED
Mariposa.B_UDP_CONTROLLED
Blackenergy_payload
00000055
00:15 / 01:53
contact
address
security
email
money
fund
UNITED
LOTTERY
claims
Africalate
husband
account
information
NUMBER
NAME
WINNING
PRIZE
claim
dollars
send
program
please
country
Microsoft
South
death
world
Mrs
since
e-mail
company
INTERNATIONAL
funds
Johnson
Million
Internet
online
society
assistance
Nov

The Honeynet

PROJECT

HonEeeBox – Rapid Deployment of Many Distributed Low Interaction Malware Collectors

Any Questions?

David Watson david@honeynet.org.uk