

The HoneyNet

P R O J E C T

HonEeeBox



Annual Workshop

Private Day

22/03/2012

David Watson

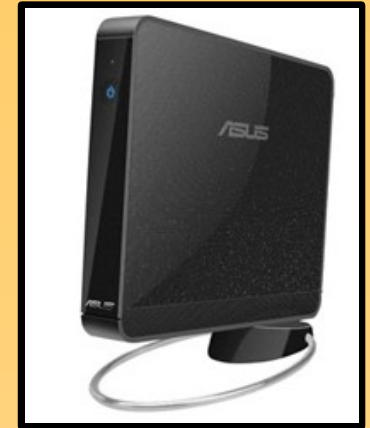
david@honeynet.org.uk



HonEeeBox Approach

- Build small, cheap, highly portable low interaction honeypots for distributed malware collection to a central location
- Deploy widely and internationally (100+)
- Centralised sample submission (anon opt)
- 'Outsource' malware binary analysis to Shadowserver, VirusTotal, etc
- Focus development on reporting and analysis UI, then data analysis
- Add p0f data, netflow, kippo, proxies, etc

Asus Eee PC Box (B202)



- Intel Atom x86 CPU
- 1.6 GHz HT
- 1GB RAM
- 160GB hard disk
- Standard PC I/O
- Hardware warranty
- Small, quiet, low power, easy to ship (Raspberry Pi?)
- Minimal Debian Squeeze installation
- Dionaea + HPFeeds
- Image or repos
- Live CD / USB / VM
- We ship it, you boot it and set locale

Deploying a HonEeeBox

HonEeeBox ISO URL

HonEeeBox Instructions URL

Burn ISO to USB and install in 5 minutes

Done this for you already on hardware here

The HoneyNet

P R O J E C T



shadowSERVER

Boot menu

Live

Live (failsafe)

Live 686

Live 686 (failsafe)

Text Install

Text Expert

Text Rescue

Text Auto

```
Checking file systems...fsck from util-linux-ng 2.17.2
done.
Mounting local filesystems...done.
Activating swapfile swap...done.
Cleaning up temporary files....
Setting kernel variables ...done.
Setting up resolvconf.../etc/resolvconf/update.d/libc: Warning: /etc/resolv.conf
is not a symbolic link to /etc/resolvconf/run/resolv.conf
done.
Setting up networking....
Configuring network interfaces...done.
Cleaning up temporary files....
Setting console screen modes.
Skipping font and keymap setup (handled by console-setup).
Setting up console font and keymap...done.
INIT: Entering runlevel: 2
Using makefile-style concurrent boot in runlevel 2.
Starting enhanced syslogd: rsyslogd.
Starting periodic command scheduler: cron.
Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd.

Debian GNU/Linux 6.0 debian tty1

debian login: _
```

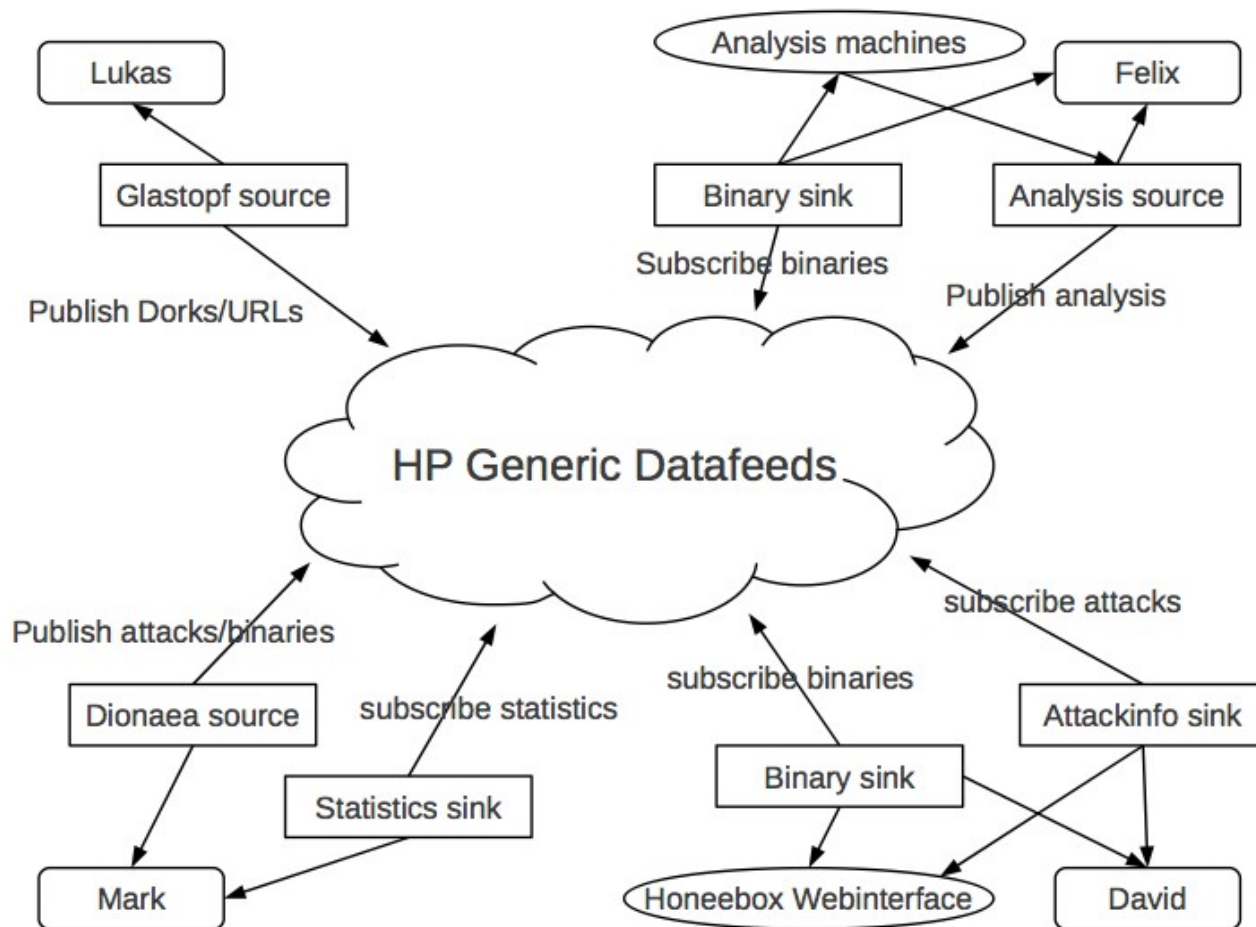


Nepenthes → Dionaea

- C with glib
- LibEv events
- Embedded Python
- OpenSSL for TLS
- Udns (asynch)
- Curl and Libcftp
- 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



Publish-subscribe generic data sharing



The screenshot shows a web browser window with the URL `hpfeeds.honeycloud.net/editak/bj3gn@hp1/`. The page has a blue header with the **hpfeeds** logo and the text **HONEYNET PROJECT GENERIC DATAFEEDS**. Below the header is a navigation bar with links: [Home](#), [Users](#), [Channels](#), [Authkeys](#), [Settings](#), and a status bar indicating **Logged in as « david »** with a [Logout](#) link.

The main content area displays the configuration for the authkey **Authkey bj3gn@hp1**, with an [EDIT](#) link on the right. The configuration details are:

- Identifier: bj3gn@hp1
- Secret: ykqztript3sn5hga
- Comment: My HonEeeBox Pub Key

Below this, it states: "The Authkey has access to the following channels:"

Channel	Access
dionaea.dcerpcrequests	<input type="checkbox"/> subscribe <input checked="" type="checkbox"/> publish
dionaea.shellcodeprofiles	<input type="checkbox"/> subscribe <input checked="" type="checkbox"/> publish
mwbinary.dionaea.sensorunique	<input type="checkbox"/> subscribe <input checked="" type="checkbox"/> publish
dionaea.capture	<input type="checkbox"/> subscribe <input checked="" type="checkbox"/> publish

At the bottom of the table is an [Update](#) button.

<https://hpfeeds.honeycloud.net>

David Watson (david@honeynet.org.uk)

```
pythonfeed.py --hosthpfeeds.honeycloud.net -p 10000 -c  
dionaea.capture -i your-sub-authkey-identifier -s your-pub-  
authkey-secret subscribe
```

```
pythonfeed.py --hosthpfeeds.honeycloud.net -p 10000 -c  
dionaea.shellcodeprofiles -i your-sub-authkey-identifier -s  
your-pub-authkey-secret subscribe
```

```
pythonfeed.py --hosthpfeeds.honeycloud.net -p 10000 -c  
dionaea.dcerpcrequests -i your-sub-authkey-identifier -s your-  
pub-authkey-secret subscribe
```

```
pythonfeed.py --hosthpfeeds.honeycloud.net -p 10000 -c  
mwbinary.dionaea.sensorunique -i your-sub-authkey-identifier -  
s your-pub-authkey-secret subscribe
```

Example HoneeBox Reporting Interface using Ext-JS - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://honeebox.net/demo_schema1/

Most Visited Getting Started Latest Headlines

Attack Summary Panel

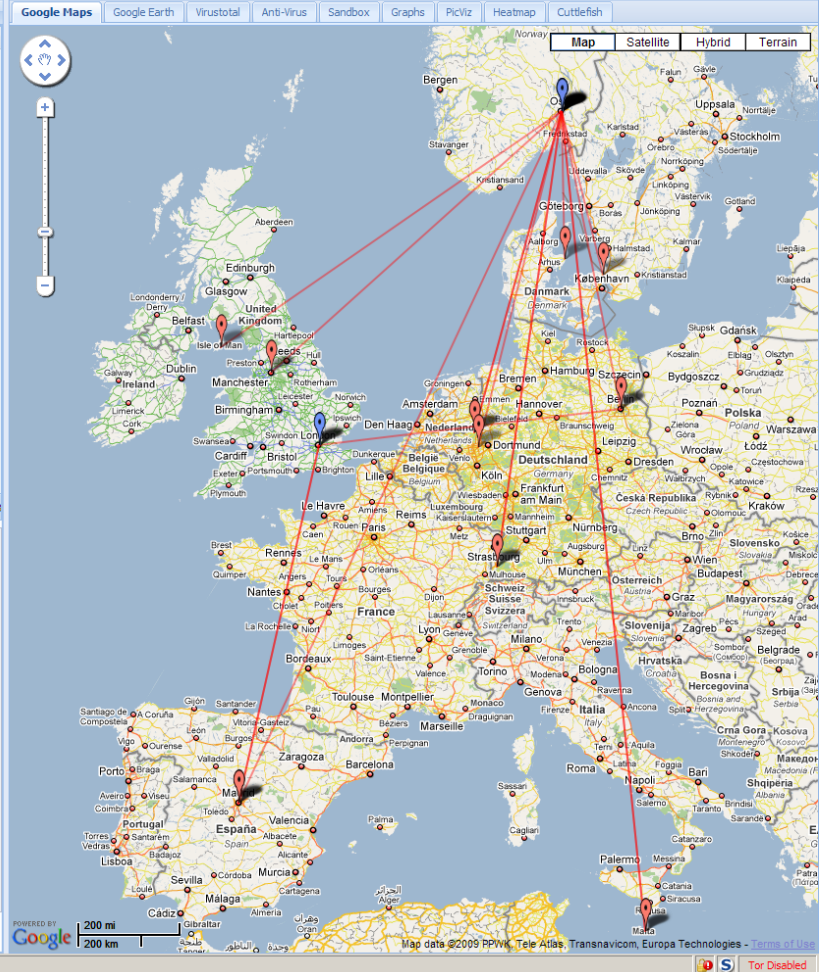
Total Attacks: 3409 (+36) Total Attacker IPs: 1202 (+28) Total Victim IPs: 167 (+17) Total MD5sums: 566 (+22) Sensors: 10 (4) AV Undetected: 4015 / 28579 (14.0%)

Attack Browser





































ID	Time	Attacker IP	Victim IP	MD5sum	Download
3381	03 Oct 2009 14:49:47	80.41.76.228	80.203	fd28c5e1c38caa35bf5e1987e6167f4c	tftp://80.41.76.228:69/sms.exe
3382	03 Oct 2009 15:19:32	88.8.235.161	88.96.	c636db42a58de90f6e2f62484bc935f9	ftp://1.1888.8.235.161:25832/runs.exe
3383	03 Oct 2009 17:13:57	71.1.81.9	192.168.1	2fa0e36b36382b74e6e6a437ad664a80	tftp://71.1.81.9:69/sms.exe
3384	03 Oct 2009 17:30:36	80.130.64.149	80.203	697f001bc330ab483d77a707cd40c8d9	tftp://80.130.64.149:69/sms.exe
3385	03 Oct 2009 18:11:58	80.62.34.192	80.203	98eb0fdadfa403c013a8b1882ec986d	tftp://80.62.34.192:69/sms.exe
3386	03 Oct 2009 18:32:11	80.144.39.99	80.203	14a09a48ad23fe0ea5a180bee8cb750a	tftp://80.144.39.99/sms.exe
3387	03 Oct 2009 18:59:00	80.131.240.234	80.203	3228f9bc721572422c268f244476dbb8	tftp://80.131.240.234:69/sms.exe
3388	03 Oct 2009 19:36:48	80.136.238.168	80.203	ea55dd10c429dc57041e455c834b7089	blink:///80.136.238.168:51617/cxIndg==
3389	03 Oct 2009 20:06:59	80.62.169.53	80.203	697f001bc330ab483d77a707cd40c8d9	tftp://80.62.169.53:69/sms.exe
3390	03 Oct 2009 20:19:04	80.85.106.120	80.203	f4a200f7818dfb166b9a3d238ac55a2d	tftp://80.85.106.120/sms.exe
3391	03 Oct 2009 20:55:55	80.36.127.228	80.203	3228f9bc721572422c268f244476dbb8	tftp://80.36.127.228/sms.exe
3392	03 Oct 2009 21:39:06	88.26.131.7	88.96.	c636db42a58de90f6e2f62484bc935f9	ftp://1.1888.26.131.7:9942/runs.exe
3393	03 Oct 2009 21:44:33	80.47.43.79	80.203	bf3e95a24e203f680465e165ba4a02b1	tftp://80.47.43.79/sms.exe
3394	03 Oct 2009 22:03:35	80.85.105.216	80.203	fcab6c9d17b2a3330f20ae2194c869fa	tftp://80.85.105.216/sms.exe
3395	04 Oct 2009 08:11:08	80.131.233.227	80.203	3228f9bc721572422c268f244476dbb8	tftp://80.131.233.227:69/sms.exe
3396	04 Oct 2009 08:09:08	202.67.19.238	202.67	a72b1cb332ea7bfddfe25c1f69468685	link://202.67.19.238:29150/vCHTfA==
3397	04 Oct 2009 08:10:37	71.51.110.90	192.168.1	df51e3310ef609e908a6b487a28a0c68	tftp://71.51.110.90:69/sms.exe
3398	04 Oct 2009 08:21:10	202.67.19.238	202.67	4f50e44f777bd8e16a0263f83b9815bb	link://202.67.19.238:35016/+Bkn/A==
3399	04 Oct 2009 08:43:52	80.130.95.115	80.203	e269d0462eb2b0b70d5e64dc7c676cd	tftp://80.130.95.115/sms.exe
3400	04 Oct 2009 08:55:33	88.134.29.250	88.96.	e23d9a57aef0986376776f5f685112f4	ftp://1.1888.134.29.250:17838/chostra.exe

Attack Detail Rows 3381 - 3400 of 3

ID: 3384
 Time: Sat Oct 03 2009 17:30:36 GMT+0100 (GMT Daylight Time)
 Sensor: 80.203.183.211
 Download: [tftp://80.130.64.149:69/sms.exe](#)
 Trigger: [tftp://0.0.0.0/sms.exe](#)
 MD5sum: 697f001bc330ab483d77a707cd40c8d9
 SHA512: bf53a6773dc2ca07c3855e6b9ee18b57781dcd9155632ab61e9a3074dd1ef5e
 File Type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
 Attacker IP: 1350713493
 Victim IP: 1355528147
 Filename: sms.exe
 Country: DE
 ISP: DEUTSCHE TELEKOM AG
 ASN: 3320



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	1a2c0e6130850f8fd9b5309413cd00	ftp://70.232.61.243	
2	20 Mar 2009 17:22:37	 64.236.114.1	 64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.204.18	
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	8f4e8e31fcd6f9635791ab009defelb5	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	11d31a4ebd7260193ffed8a9bb79156a	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	1a2c0e6130850f8fd9b5309413cd00	ftp://70.232.61.243	
9	20 Mar 2009 17:22:37	 64.236.114.1	 64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.204.18	
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	8f4e8e31fcd6f9635791ab009defelb5	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	11d31a4ebd7260193ffed8a9bb79156a	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	1a2c0e6130850f8fd9b5309413cd00	ftp://70.232.61.243	
16	20 Mar 2009 17:22:37	 64.236.114.1	 64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.204.18	
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	8f4e8e31fcd6f9635791ab009defelb5	creceive://211.200.	
19	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73	

</

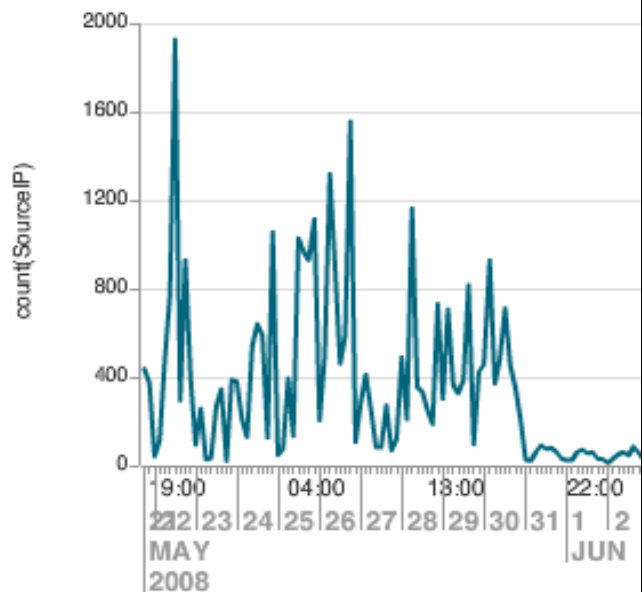
Attack Detail

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

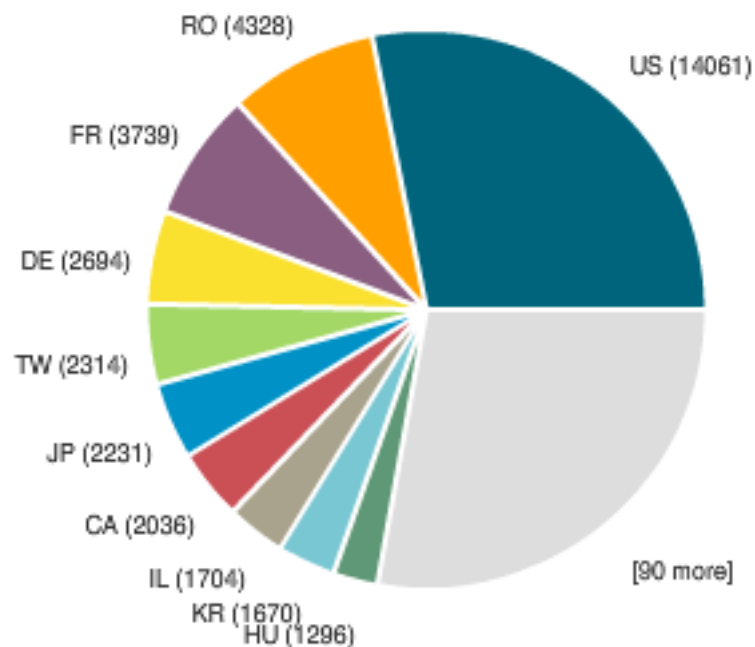
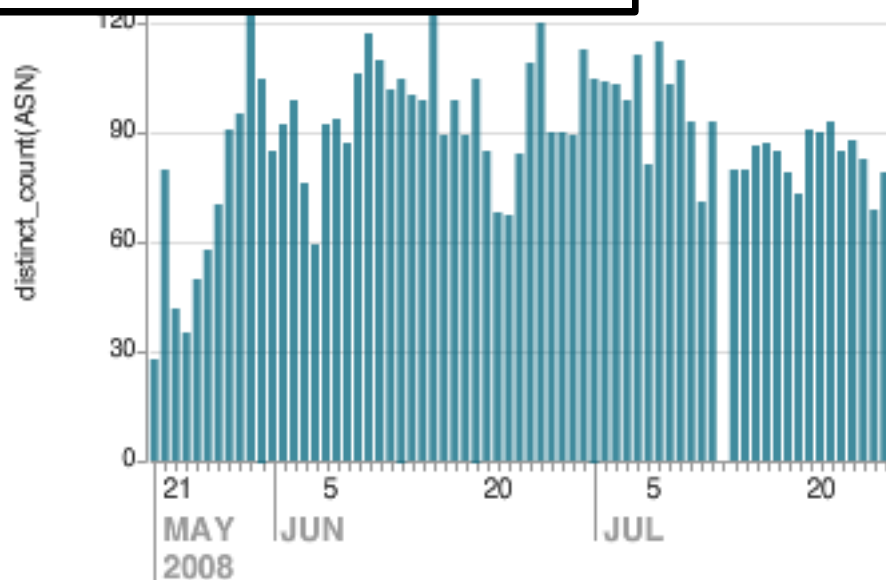
Google Map	Google Earth	Sandbox	Anti-Virus	Graphs	Pic/Viz	Heatmap	Cuttlefish
------------	--------------	---------	------------	--------	---------	---------	------------

Scan Summary	File Changes	Reg
--------------	--------------	-----

<div> <div></div> <div>Technical Details</div> </div>	
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-8...
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



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

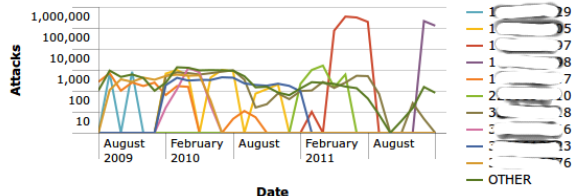


HonEeeBox

Print Schedule PDF delivery Edit: On Off

Attacks per sensor over time

18m ago



Total attacks per sensor

18m ago

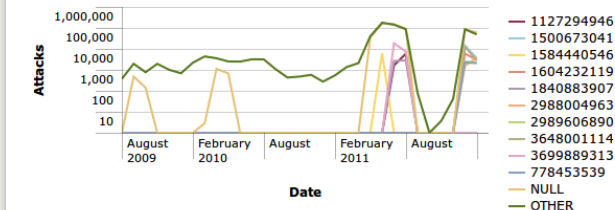
« prev 1 2 3 4 next »

sensor_ipn	count	percent
1 7	928869	70.941122
2 8	339983	25.965745
3 8	7509	0.573490
4 5	4832	0.369038
5 6	3702	0.282735
6 0	3538	0.270210
7 3	3518	0.268683
8 3	2152	0.164356
9 7	2136	0.163134
10 9	1524	0.116393

View results

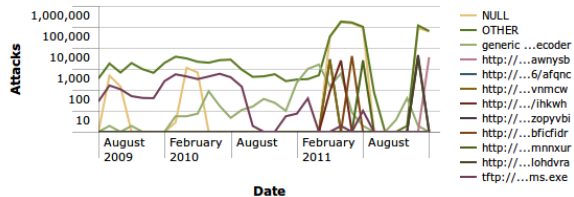
Top attacking IP addresses over time

18m ago



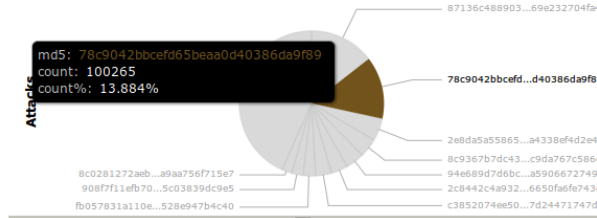
Top triggers over time

3m ago



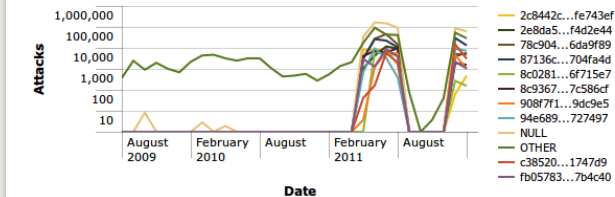
Top malware samples by MD5sum

18m ago



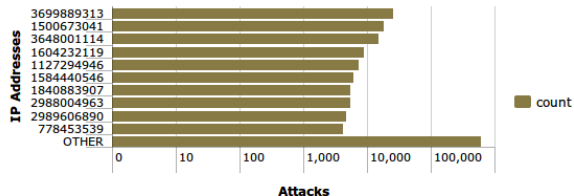
Top malware by MD5sum over time

18m ago



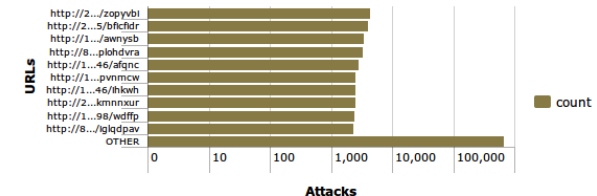
Top attacking IP addresses

18m ago



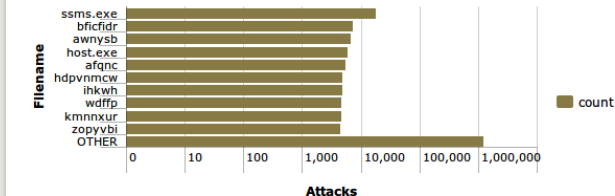
Top malicious URLs

18m ago



Top filenames

3m ago



THE HONEYNET PROJECT

splunk> Search

Administrator | App | Manager | Alerts | Jobs | Logout

Summary Search Status Dashboards & Views Searches & Reports

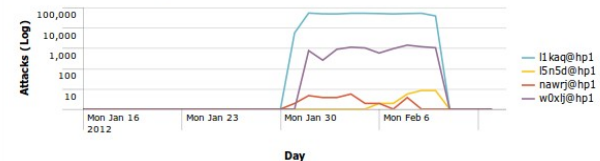
Help About

HonEeBox

Print Schedule PDF delivery Edit On Off

Attacks per sensor over last 30 days

6m ago



View results

Total attacks per sensor

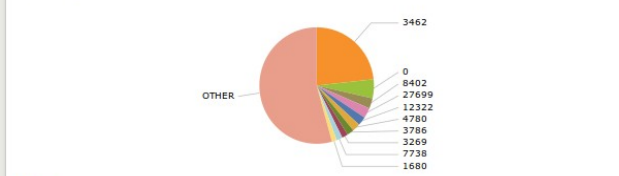
6m ago

identifier	sparkline	count
1 li kaq@hp1		497294
2 w0xj@hp1		9134
3 5n5d@hp1		23
4 nawj@hp1		21

View results

Top attacking ASNs

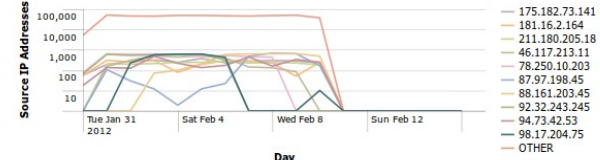
6m ago



View results

Top source IP addresses over time

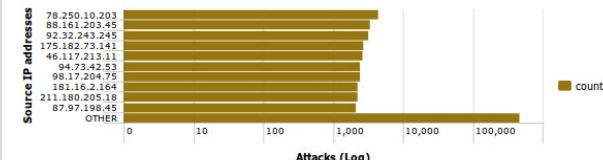
6m ago



View results

Top source IP addresses

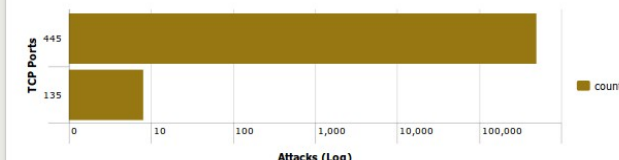
6m ago



View results

Target TCP ports

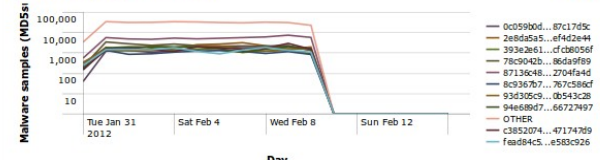
6m ago



View results

Top malware samples by MD5sum over time

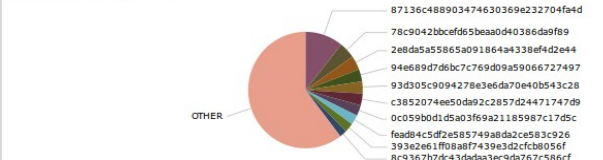
6m ago



View results

Top malware samples by MD5sum

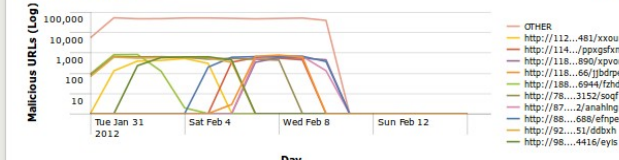
6m ago



View results

Top malicious URLs over time

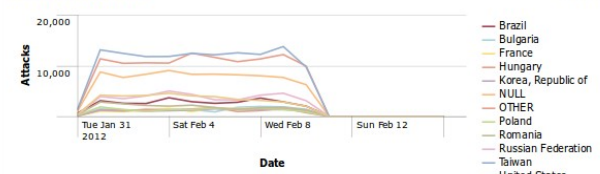
6m ago



View results

Attacks per country over time

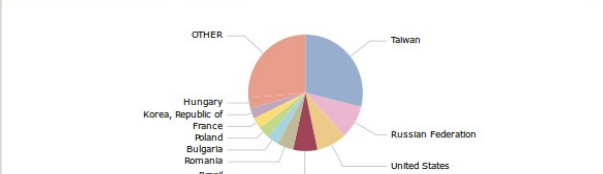
6m ago



View results

Top attacking country by IP Geolocated IP Address

6m ago



View results

Top attacking City by IP Geolocated IP Address

6m ago

client_city	count	percent
1 Taipei	101950	28.945635
2 Moscow	23437	6.654231
3 Bucharest	11388	3.233280
4 Seoul	10884	3.090184
5 Sofia	7358	2.089083
6 Annecy-le-veau	5420	1.538846
7 Budapest	5250	1.490580
8 Warsaw	3931	1.116089
9 Toul	3391	0.962772

David Watson (david@honeynet.org.uk)

THE HONEYNET PROJECT

splunk> Search

Administrator | App | Manager | Alerts | Jobs | Logout

Summary Search Status Dashboards & Views Searches & Reports

Help | About

Search

source="/Users//david/cli/honeeebox.csv"

All time

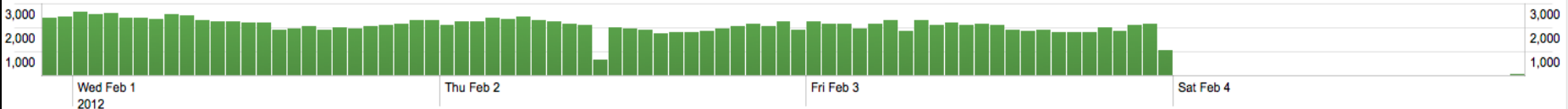
≥ 156,064 matching events | 156,064 scanned events

Save Create

Field extractor name=AutoHeader-1 is unusually slow (max single event time=1060ms, probes=1251 warning max=1000ms)

Hide Zoom out Zoom to selection Deselect

Linear scale 1 bar = 1 hour



Field discovery is: On

≥ 156,064 events over all time

Hide

Export Options

prev 1 2 3 4 5 6 7 8 9 10 next 10 per page

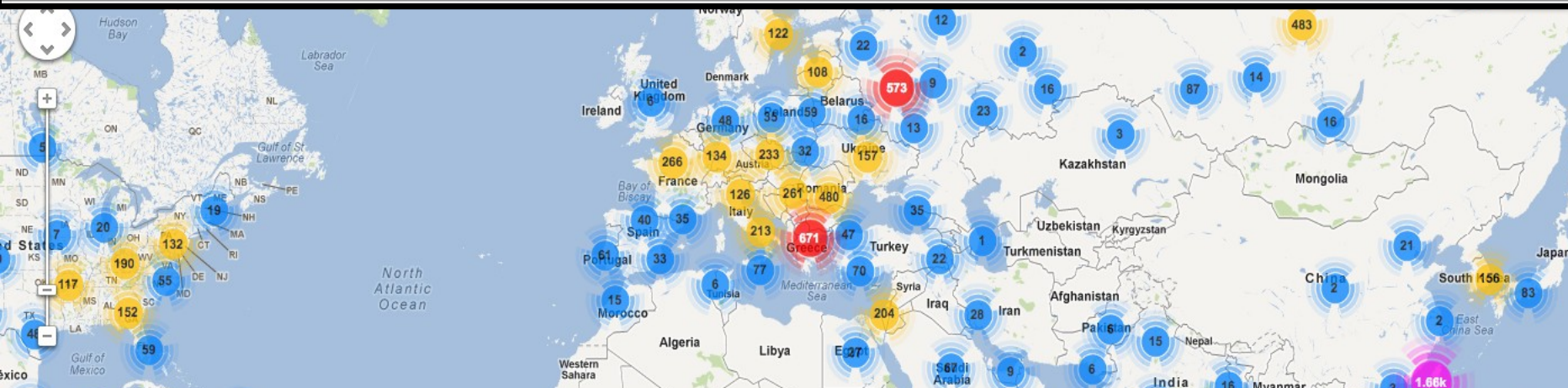
8 selected fields

Edit

a daddr (≥100)
a datetime (≥100)
dport (2)
a md5 (≥100)
a saddr (≥100)
a sha512 (≥100)
sport (≥100)
a url (≥100)

12 interesting fields

- 11 2/3/12 11:28:32.000 PM Fri Feb 3 23:28:32 2012, PUBLISH, dionaea.capture, l1kqa@hp1, http://95.68.120.170:1938/fpzctbb, 134.61.128.72, 95.68.120.170, 445, 4234, b0f52b3fb4cc5fa24dc27d82b14a47d88df4651f8ecb637bd75e93569c32f78a32840ba0874b01e4db6a2660fb33a6355030ef8dd62377f8510ded8046493ecc, acf4da36e762084070f8138a43144759
daddr=134.61.128.72 | datetime=Fri Feb 3 23:28:32 2012 | dport=445 | md5=acf4da36e762084070f8138a43144759 | saddr=95.68.120.170 | sha512=b0f52b3fb4cc5fa24dc27d82b14a47d88df4651f8ecb637bd75e93569c32f78a32840ba0874b01e4db6a2660fb33a6355030ef8dd62377f8510ded8046493ecc | sport=4234 | url=http://95.68.120.170:1938/fpzctbb
- 12 2/3/12 11:28:32.000 PM Fri Feb 3 23:28:32 2012, PUBLISH, dionaea.capture, l1kqa@hp1, http://189.38.181.121:1132/enkos, 134.61.128.75, 189.38.181.121, 445, 3552, 8f2c7b918fe88f15b2b750e746d8d787e4ce62e65c98ce7a0963601064b616a83aedc36900b576f8309556634105830da37ecc971f03000231668a8bd2c7ec9d, 7bb455ea4a77b24478fba4de145115eb
daddr=134.61.128.75 | datetime=Fri Feb 3 23:28:32 2012 | dport=445 | md5=7bb455ea4a77b24478fba4de145115eb | saddr=189.38.181.121 | sha512=8f2c7b918fe88f15b2b750e746d8d787e4ce62e65c98ce7a0963601064b616a83aedc36900b576f8309556634105830da37ecc971f03000231668a8bd2c7ec9d | sport=3552 | url=http://189.38.181.121:1132/enkos



splunk> Splunk for use with AMMAP

AMMap ▾

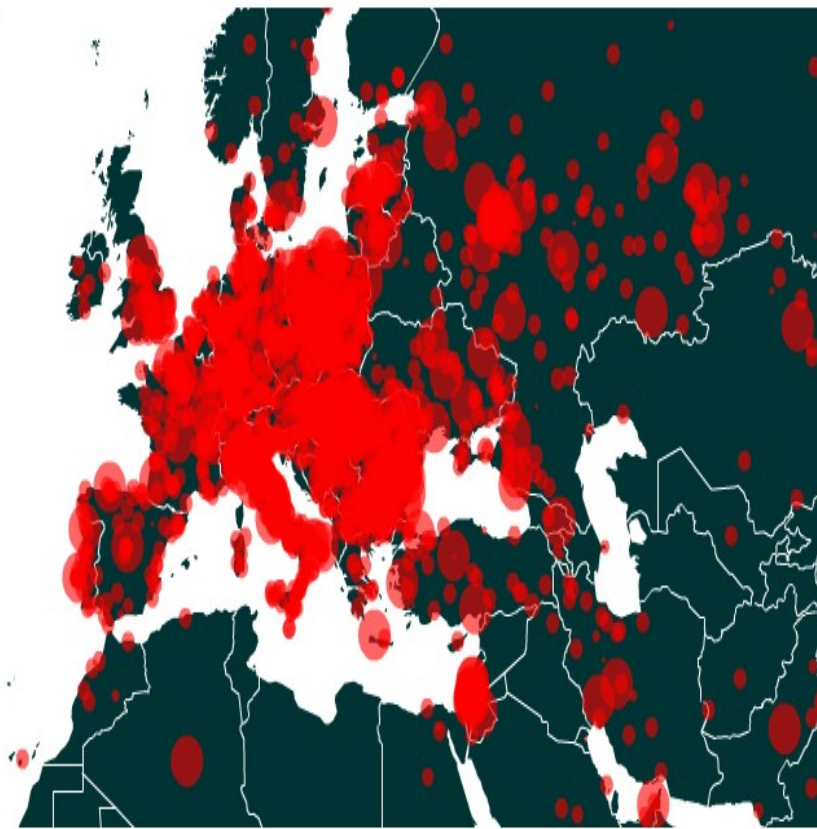
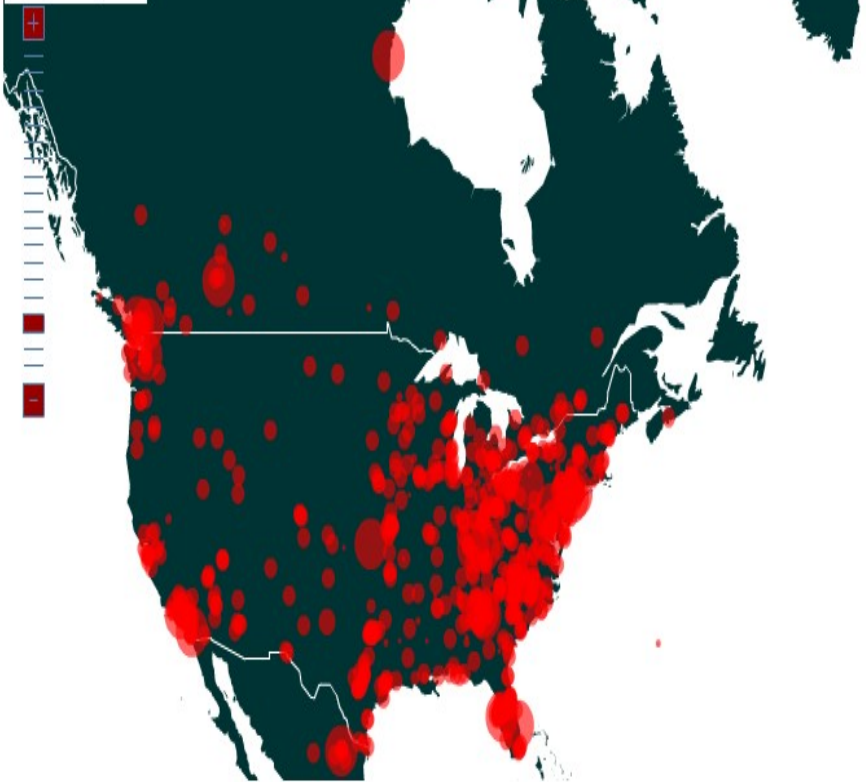
AMMAP View | Actions ▾

search

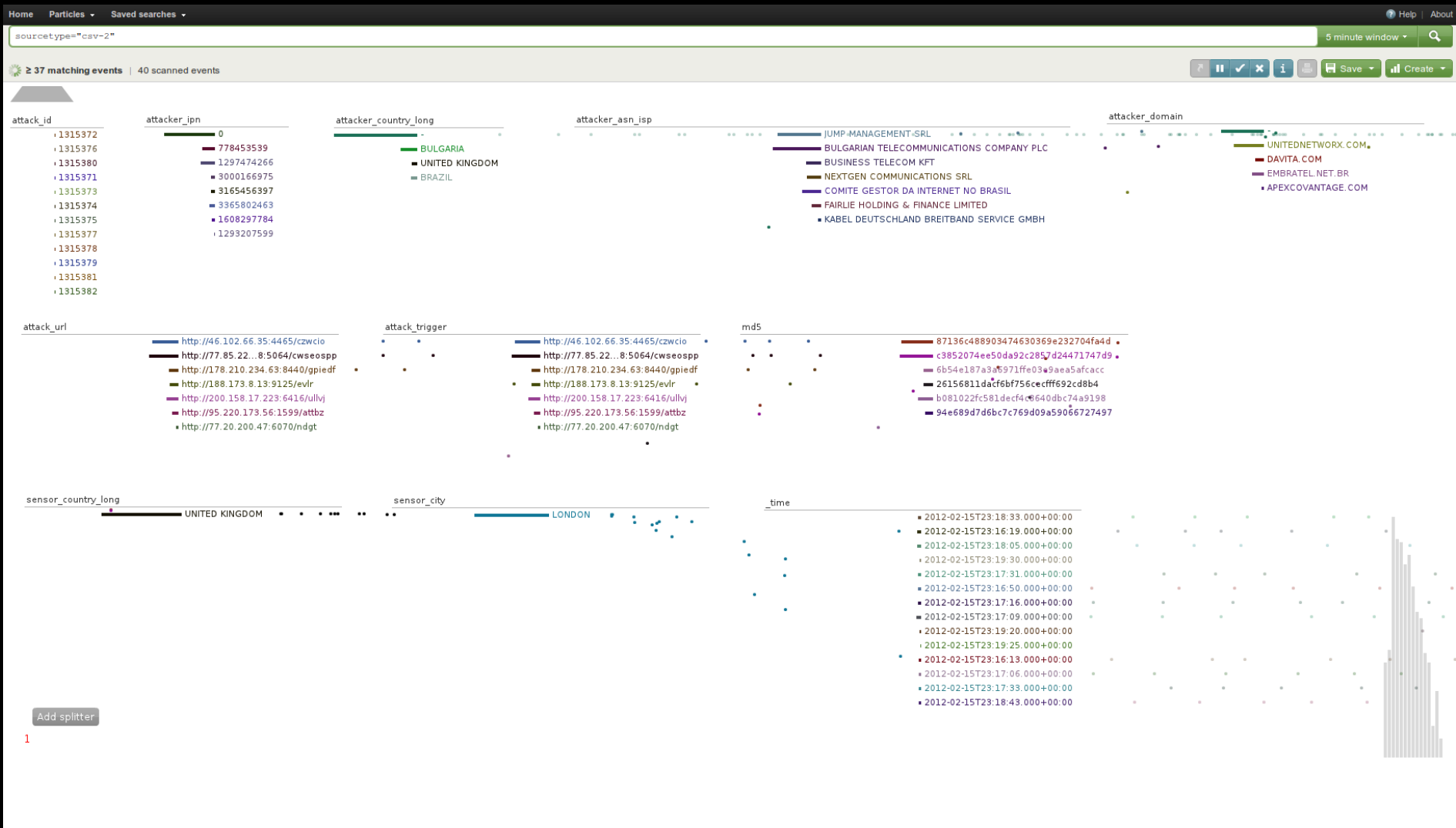
Activity Map

The Activity Map shows the count of IPs by geo

tool by ammap.com



THE HONEYNET PROJECT

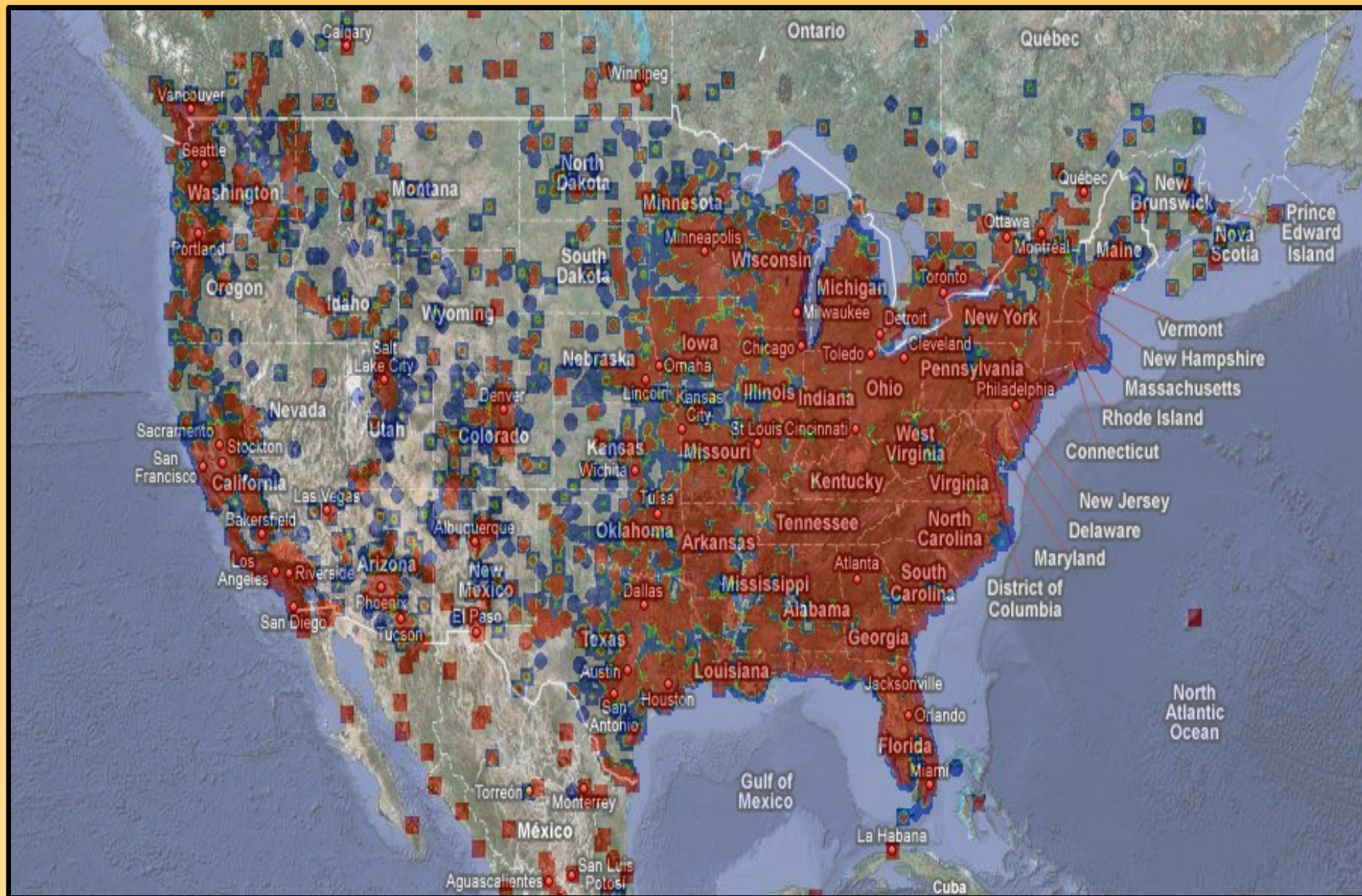


HonEeeBox Future

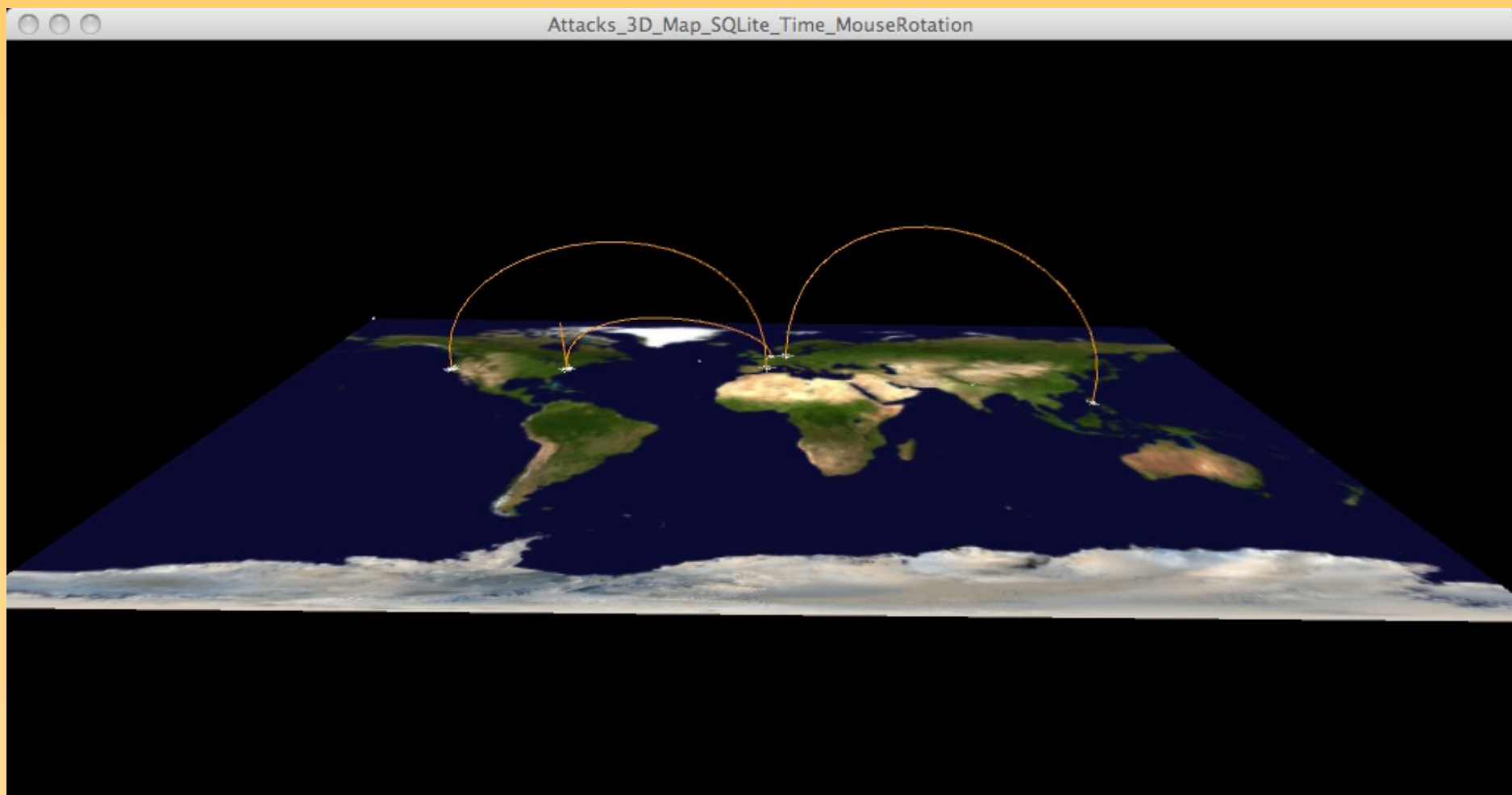
- Splunk dashboad enterprise license from Taiwan :-)
- Old prototype UI using ExtJS & MySQL backend
- Moving to Django/Python + HPFeeds from now
- Centralised repository of sensor data
- Improve collaborative development, data sharing and data analysis with the rest of the community
- Continuous data source for UI and data viz R&D
- Anonymized student data feeds for GSoC, etc

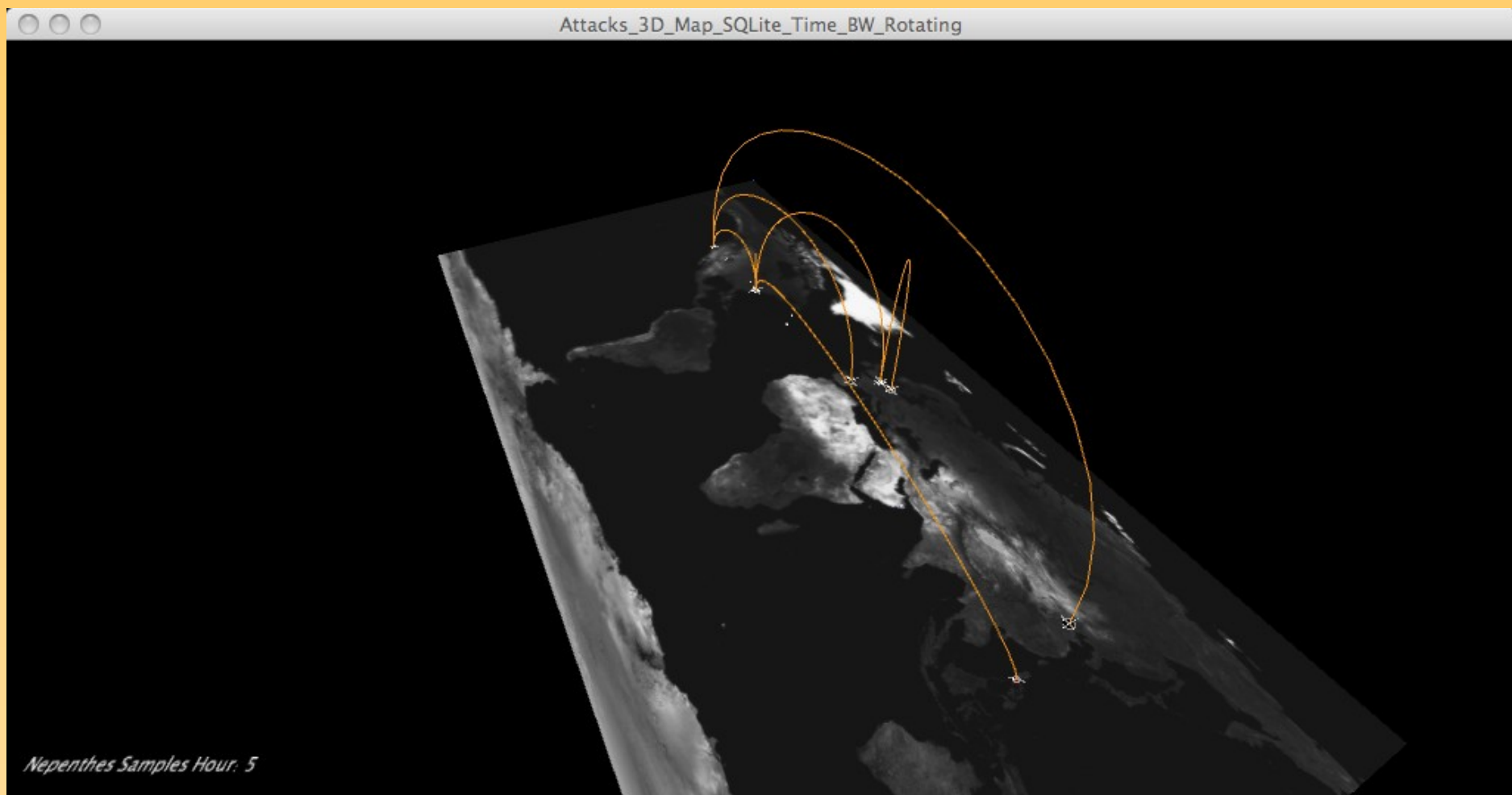
This map displays Europe and North Africa with purple cylindrical markers representing specific data points. The markers are labeled with numbers and dates, such as '193.137 - 734' and '194.8 - 1'. The map includes labels for countries like France, Germany, Italy, and Spain, as well as cities like Paris, Berlin, Rome, and Madrid. A scale bar at the bottom left shows 1034 km. The Google logo is in the bottom right corner.

THE HONEYNET PROJECT



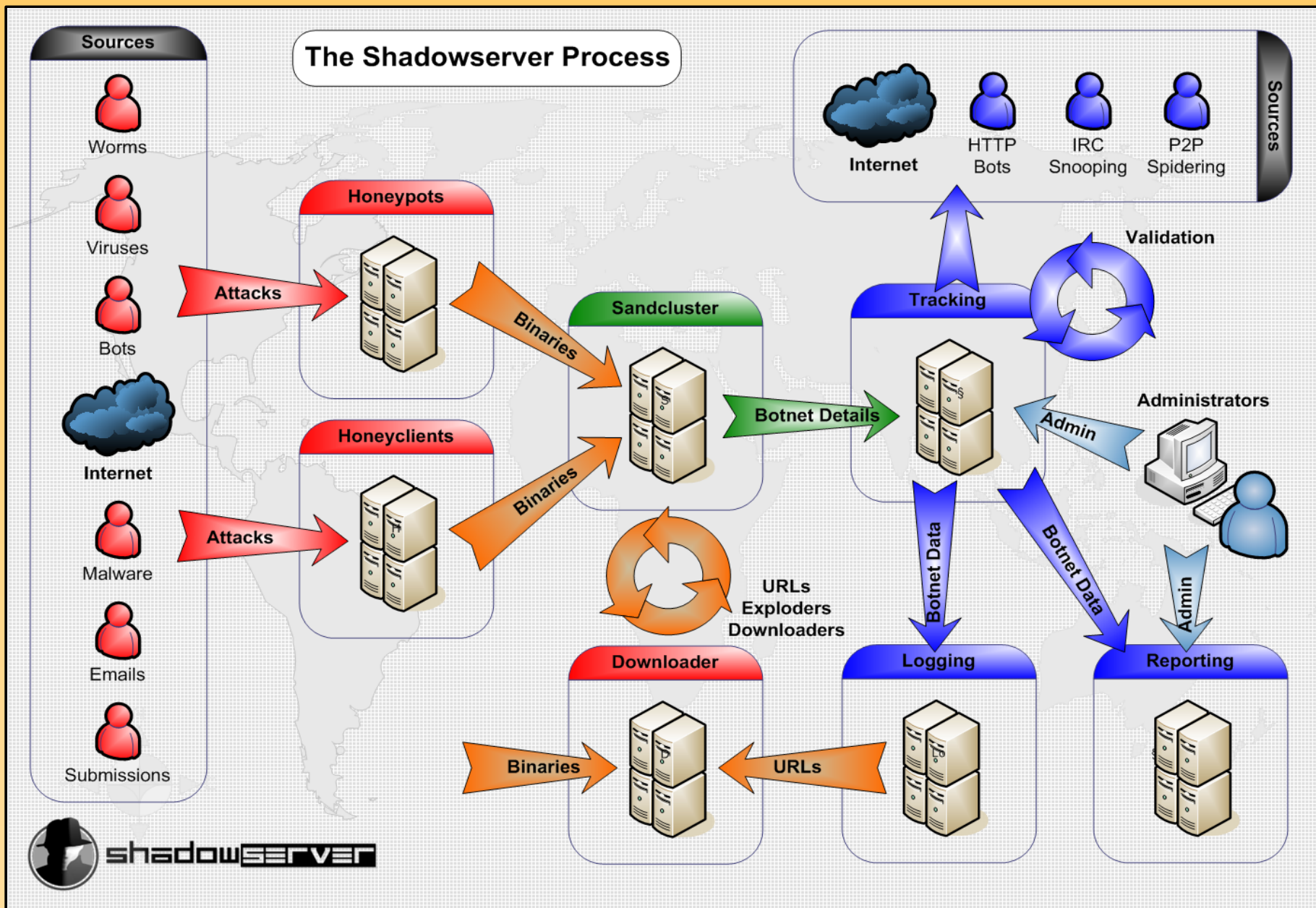
David Watson (david@honeynet.org.uk)





HonEeeBox Future

- 30-40 sensors today, want 100+ by end Q1 2012
- Cover low data regions like China, Iran, Korea
- Aim to demonstrate 100+ low interaction distributed sensor nodes with zero day detection operating 24/7
- Giving out hardware or arranging to ship final sensors to members today
- Have budget to pay for hardware shipping / tax
- Will have given 135 HonEeeBoxes to members
- Understand this isn't pushing the boundaries!
- HonEeeBox a baseline foundation service for the Project, like gas, electricity or water utilities



HonEeeBox Participation

- 1+ unfiltered 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)
- Be willing to share collected malware samples with all participants, Project members and partners / sponsors
- Accept submissions from existing Dionaea sensors
- Funding for additional sensor deployment
 - Regional, CERT, industry, academic, etc
- Always need sponsorship (buy more hardware, etc) ;-)

Will HonEeeBox Succeed?

- Designed and built entire system (Live ISO)
- Sourced \$40k hardware, paid for shipping/tax
- Developed next gen Dionaea honeypot
- Created HPFeeds data transport layer
- Signed packages for one command updates and rolling out new features like Kippo, proxy
- Trivial, free data access to all members
- Splunk dashboard next month, GUI after that
- Human/risk problem, not technical or logistics



EVERYONE:

We want each chapter to
deploy at least one
HonEeeBox sensor

Ideally one HonEeeBox
sensor per country

Takes 5 minutes

Minimum effort/risk

Hardware now

GET INVOLVED TODAY!



Getting Hardware Now

- We have 20 HonEeeBoxes here at Facebook
- We have another 14 in Taiwan to ship too
- Who wants one and will actually deploy it and contribute data immediately (in April)?
- Please **don't** take one if:
 - you have no public unfiltered IP addresses
 - you know you won't contribute data!
 - you already have one, unless there are spares
- Please do take one and help everyone else :-)

The Honeynet

P R O J E C T

HonEeeBox

<http://www.honeynet.org>

Any Questions?

David Watson

david@honeynet.org.uk