The Honeynet PROJECT

HonEeeBox – Rapid Deployment of Many Distributed Low Interaction Malware Collectors

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
  - 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.

Agenda

- GDH and motivation for HonEeeBox
- Embedded Low Interaction (LI) Honeypots
- HonEeeBox sensors
- Next steps and how to get involved
- Prototype HonEeeBox UI plus basic LI data visualisation

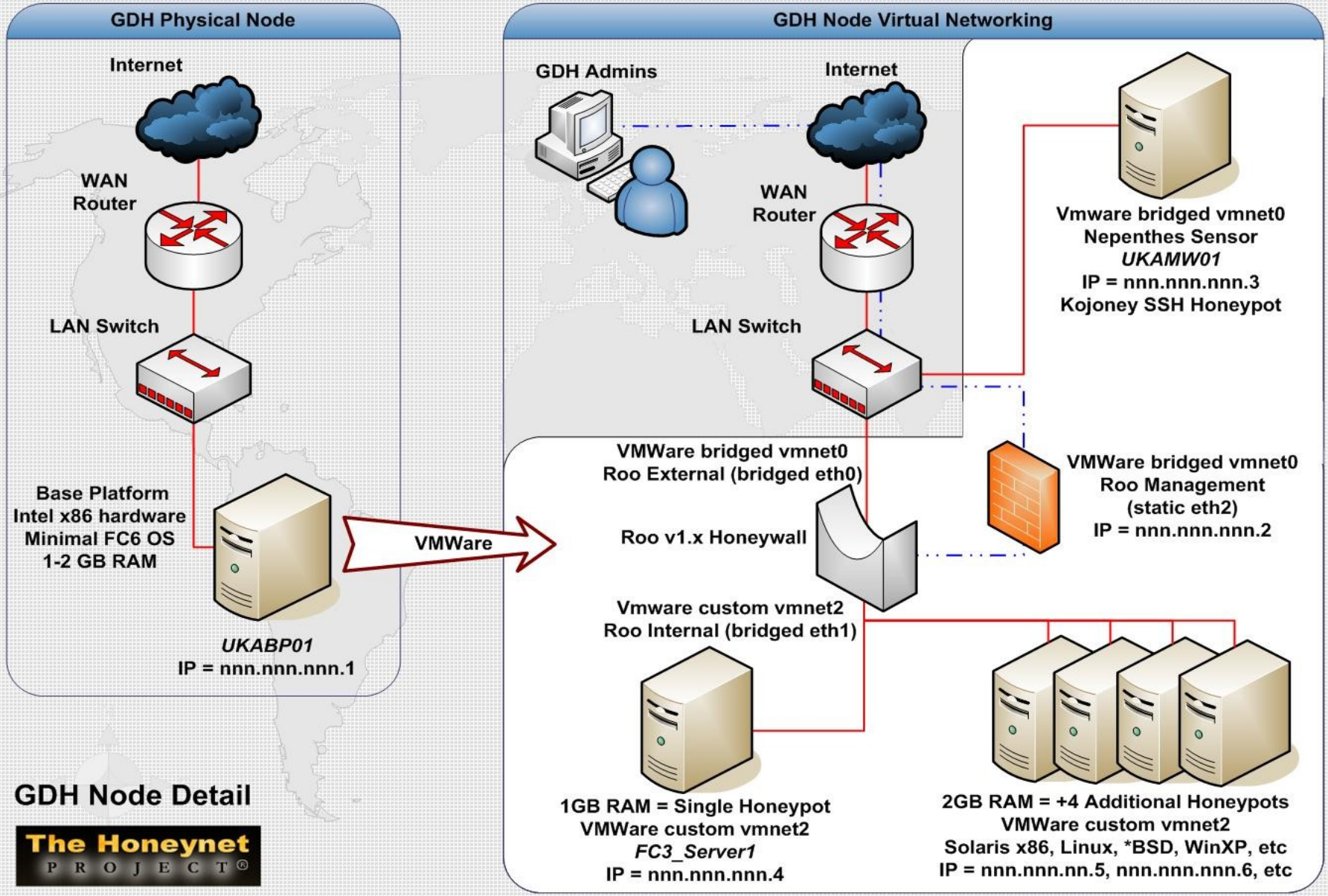
Global Distributed Honeynet (GDH) and Motivation for HonEeeBox

David Watson (david@honeynet.org.uk)

GDH Phases 1 and 2

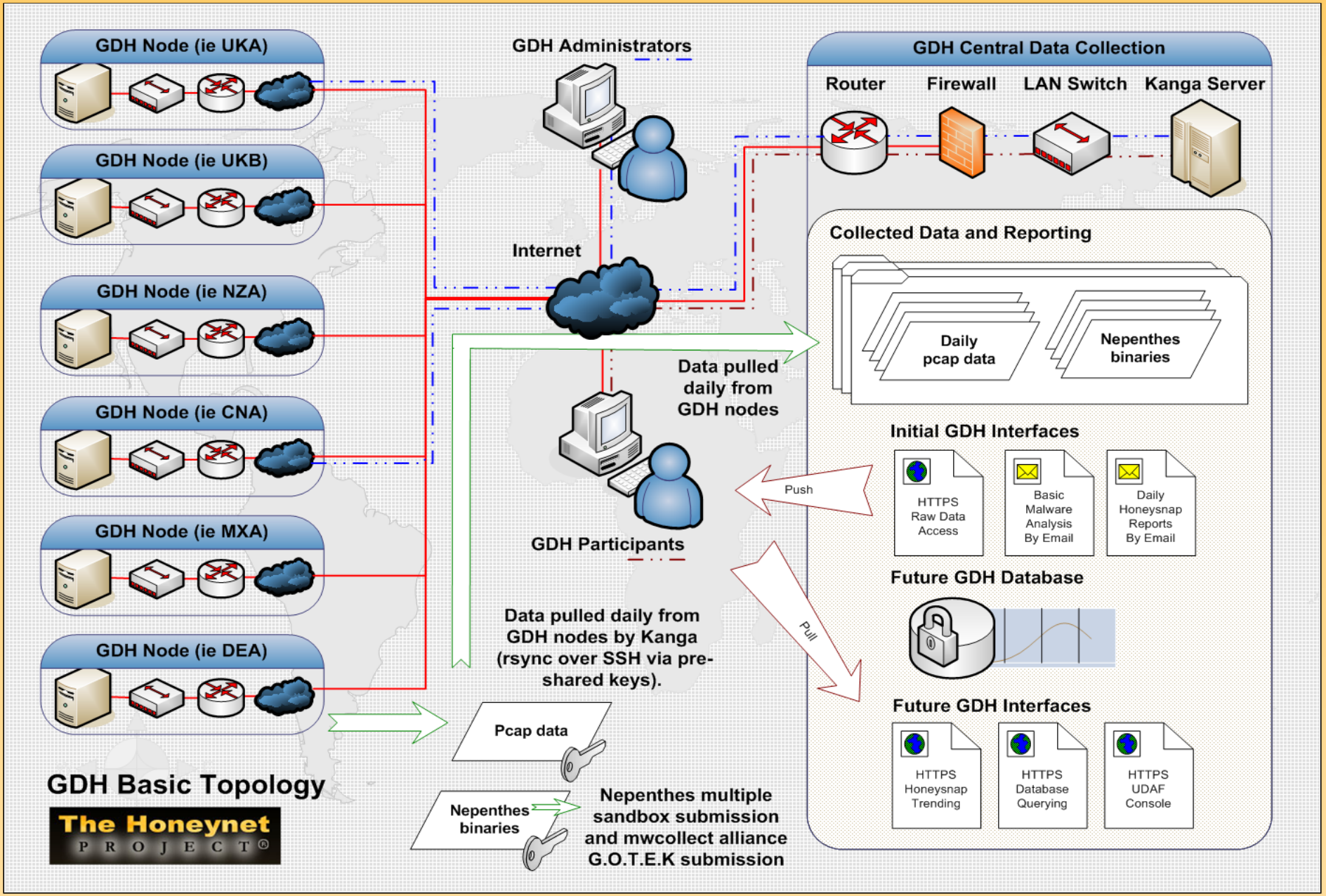
- Previous efforts to deploy and operate long running standardised low and high interaction virtual honeynets
- Multiple identical international nodes
- Centralised data collection and analysis (DA)
- Human analysts responding to incidents
- GDH1 voted best talk at PacSec 2007
- Ongoing R&D effort, continuing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

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



GDH 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 Participants
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
Future GDH Database
Pull
Future GDH Interfaces
HTTPS Honeysnap Trending
HTTPS Database Querying
HTTPS UDAF Console
Data pulled daily from GDH nodes by Kanga (rsync over SSH via pre-shared keys).
Pcap data
Nepenthes binaries
Nepenthes multiple sandbox submission and mwcollect alliance G.O.T.E.K submission
GDH Basic Topology
The Honeynet PROJECT®

Motivation

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

BUT

- Big, complex, development dependencies, manual, time consuming, resource intensive
- Significant funding to really be successful

Motivation

- Do something simple now, then more GDH2
- Reduce amount of new development required
- Minimise operational support and DA effort
- Keep up momentum from annual workshop
- Start project immediately (May 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

Obvious Questions

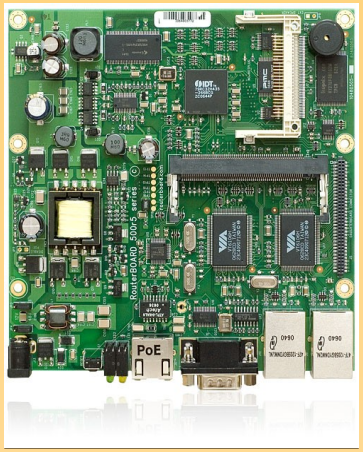
- Why do this now (or ever) - aren't we supposed to be getting GDH2 operational?
- Hasn't this all been done before?
- Isn't this just MWCollect.org, etc again?
- Where are the new tools. Not very novel?
- **Yes, to all of the above!** :-)
- But hopefully this initiative still has value
- Complete solution available to all members

Embedded Low Interaction Malware Collection Sensors

David Watson (david@honeynet.org.uk)

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

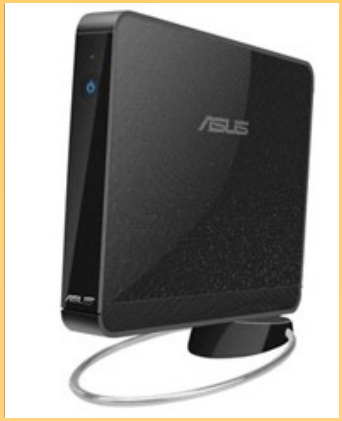
- ✔ Consumer hardware
- ✔ Cheap
- ✔ Small
- ✔ Quiet
- ✔ Low power
- ✔ Reliable
- ✔ Easy to ship
- ✔ Minimal footprint

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

HonEeeBox Low Interaction Malware Collection Sensors

David Watson (david@honeynet.org.uk)

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

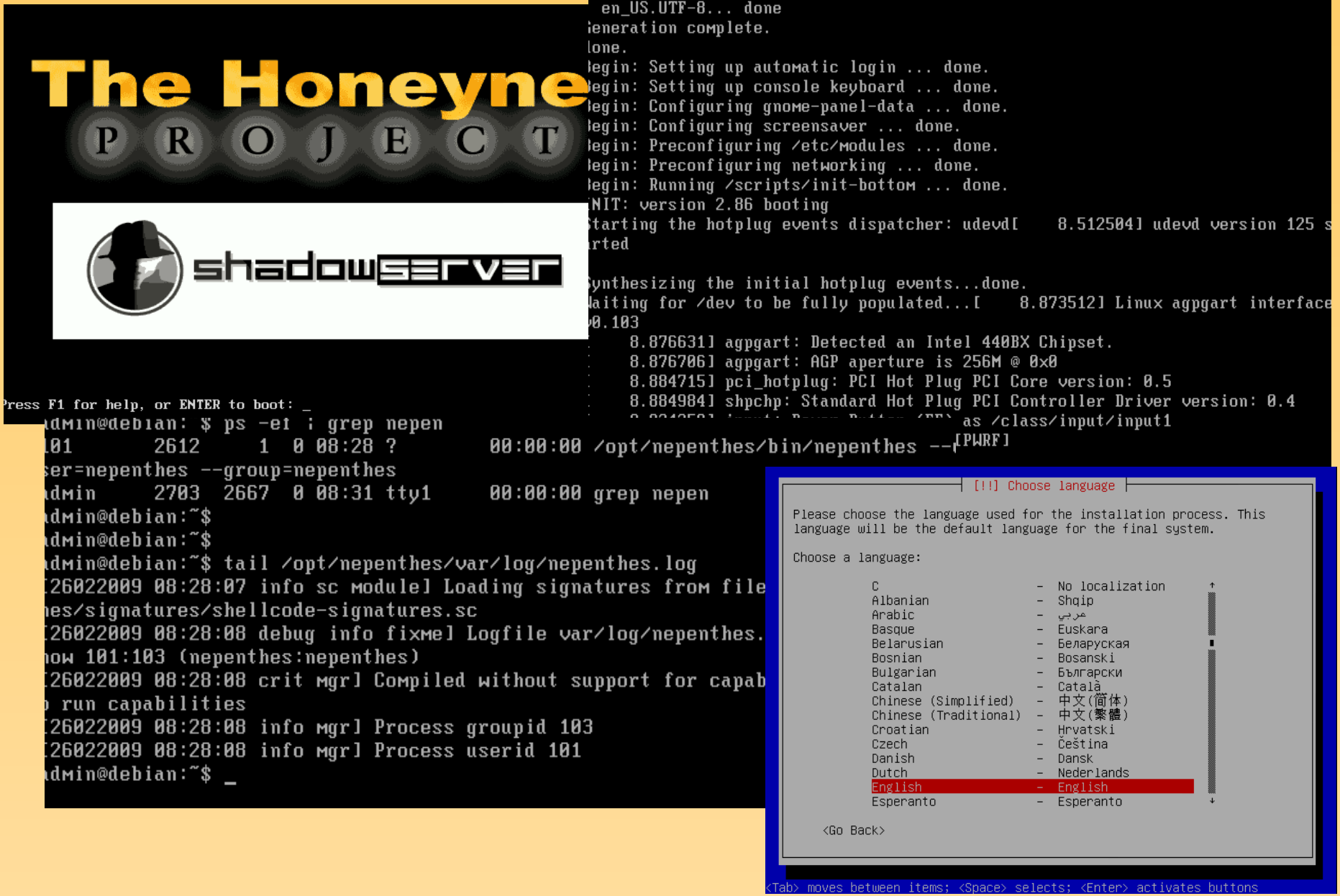
- Still small, quiet, low power, easy to ship
- Normal Linux distros
- Simple to reinstall
- Update from image
- Upgrade from repos

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


The Honeyne
PROJECT
shadowserver
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]
ress F1 for help, or ENTER to boot: _
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:~$ _
[!!] 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

Next Steps and How to Get Involved

Next Steps

- Move code base into svn/Trac, add silc
- Test sensor deployments
- Complete initial backend (RDBMS)
- **Roll out member nodes (ISO/USB/EeeBox)**
- Share data with all members (existing feeds)
- Begin developing web UI (or share/re-use)
- Discuss the best ways of improving reporting and analysis interfaces
- Get people actively involved in collaboration
- Additional functionality: VOIP and Proxies

What do you need?

- Interest in collaboration and sharing data
- Be willing to host a HonEeeBox sensor(s)
- Be willing to share collected malware samples with all members and project sponsors
- Be willing to share basic attack data

  (SRC IP, download URL, MD5, timestamp, etc)
- Ideally want to help carry out analysis and research on the shared data set we collect
- Even better, want to help improve the sensors, backend and reporting UI too

What do you need?

- Working Internet connection
- 1+ public IP addresses (many more is nice!)
- 1+ networked x86 PC/server(s) which can boot from an ISO image or USB key

  Or

  Space to host small, quiet HonEeeBox sensor hardware that we provide and ship to you

Also Very Helpful

- Contact at Asus in Taiwan / US (bulk orders)
- Contacts for people interested in distributed sensor networks
- Spare public IP space
- Submissions from existing Nepenthes sensors (can chose to hide IP address)
- Funding for additional sensor deployment
  - Regional, CERT, industry, academic, etc
- Sponsorship ;-)

The Honeynet PROJECT®

Prototype HonEeeBox UI and Basic Example Visualisations

David Watson (david@honeynet.org.uk)

Basic LI Attack Visualisation

- Dynamically updating GoogleMap
- Google Earth
- Hilbert Curves and heatmaps (animated?)
- CAIDA Cuttlefish animations
- Basic charting (Splunk)
- Parallel Coordinates (PicViz)
- Early days yet. Will get better faster if we share more of what we are individually working on and build a central set of tools

HonEeBox 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 | Googe Earth | Sandbox | Anti-Virus | Graphs | PicViz | Heatmap | Cuttlefish

HonEeBox Summary

Total Attacks: 84 Total Source IPs: 6 Total Target IPs: 1 Total MD5sums: 7

Attacks

ID	Time	Attacker IP	Victim IP	MD5sum	Download
1	20 Mar 2009 17:44:27	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
8	20 Mar 2009 17:44:27	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
15	20 Mar 2009 17:44:27	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
22	20 Mar 2009 17:44:27	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
29	20 Mar 2009 17:44:27	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
36	20 Mar 2009 17:44:27	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
43	20 Mar 2009 17:44:27	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
50	20 Mar 2009 17:44:27	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
57	20 Mar 2009 17:44:27	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
64	20 Mar 2009 17:44:27	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
71	20 Mar 2009 17:44:27	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
78	20 Mar 2009 17:44:27	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe

Page 1 of 5 | IP: 70.232.61.243 | MD5: 1a2c0e6130850f8fd9b9b53(| Rows 1 - 12 of 84

Attack Detail

ID:	1
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

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 | Googe Earth | Sandbox | **Anti-Virus** | Graphs | PicViz | Heatmap | Cuttlefish

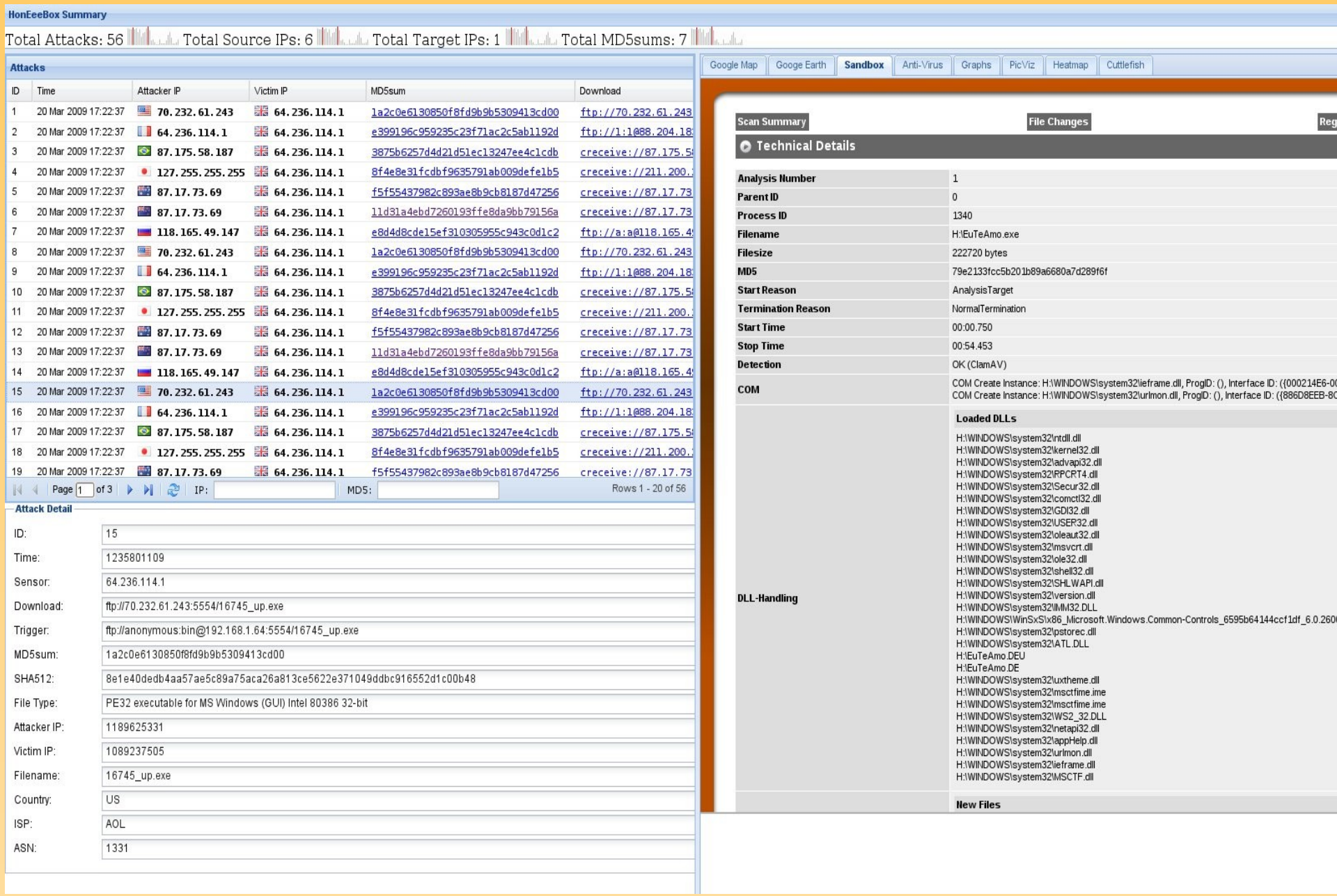
File **Sasser.B.exe.vir** received on **02.16.2009 14:12:41 (CET)**

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://l:l@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://l:l@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://l:l@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
Googe Earth
Sandbox
Anti-Virus
Graphs
PicViz
Heatmap
Cuttlefish
Scan Summary
File Changes
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
Loaded DLLs
DLL-Handling
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\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

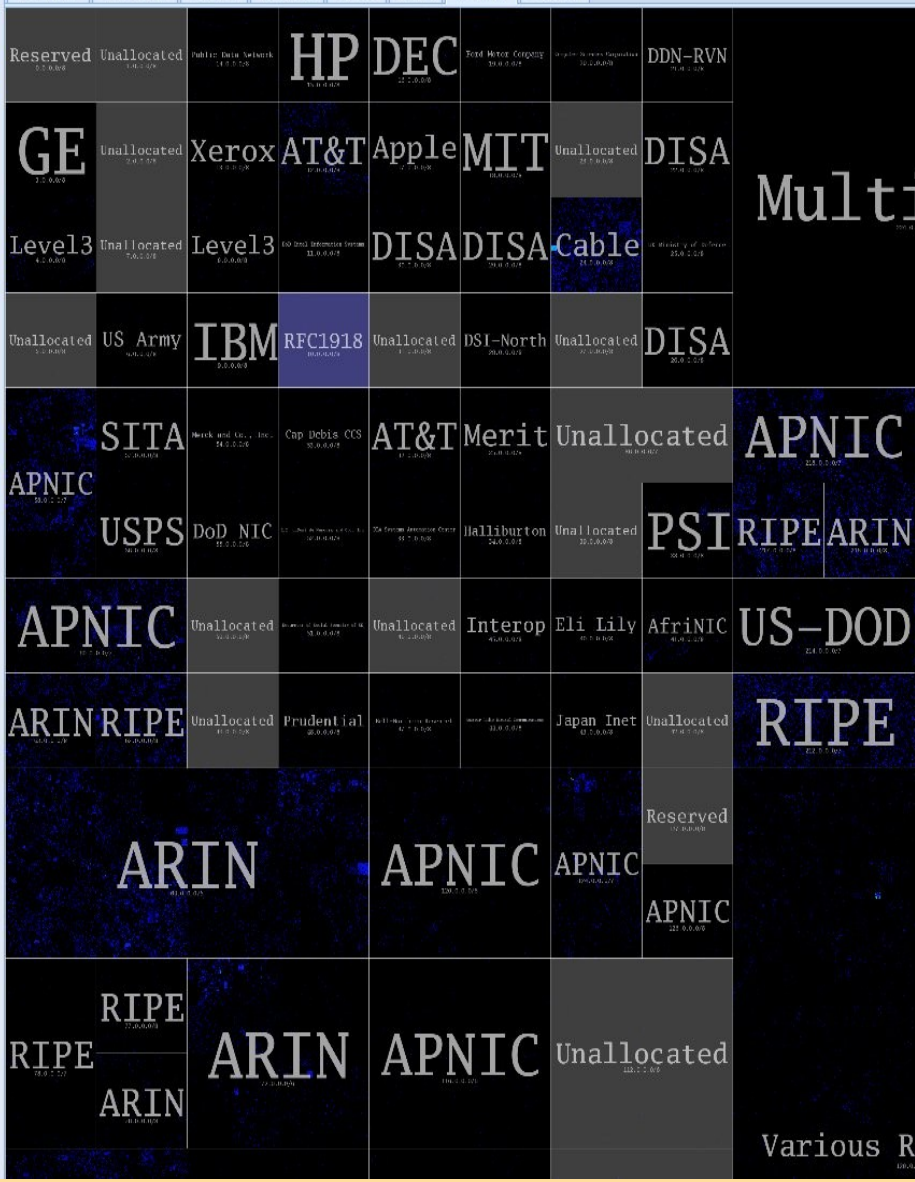
ID	Time	Attacker IP	Victim IP	MD5sum	Download
1	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_u
2	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.183.126:7293/ne
3	20 Mar 2009 17:22:37	87.175.58.187	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/iq
8	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_u
9	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.183.126:7293/ne
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/iq
15	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_u
16	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.183.126:7293/ne
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

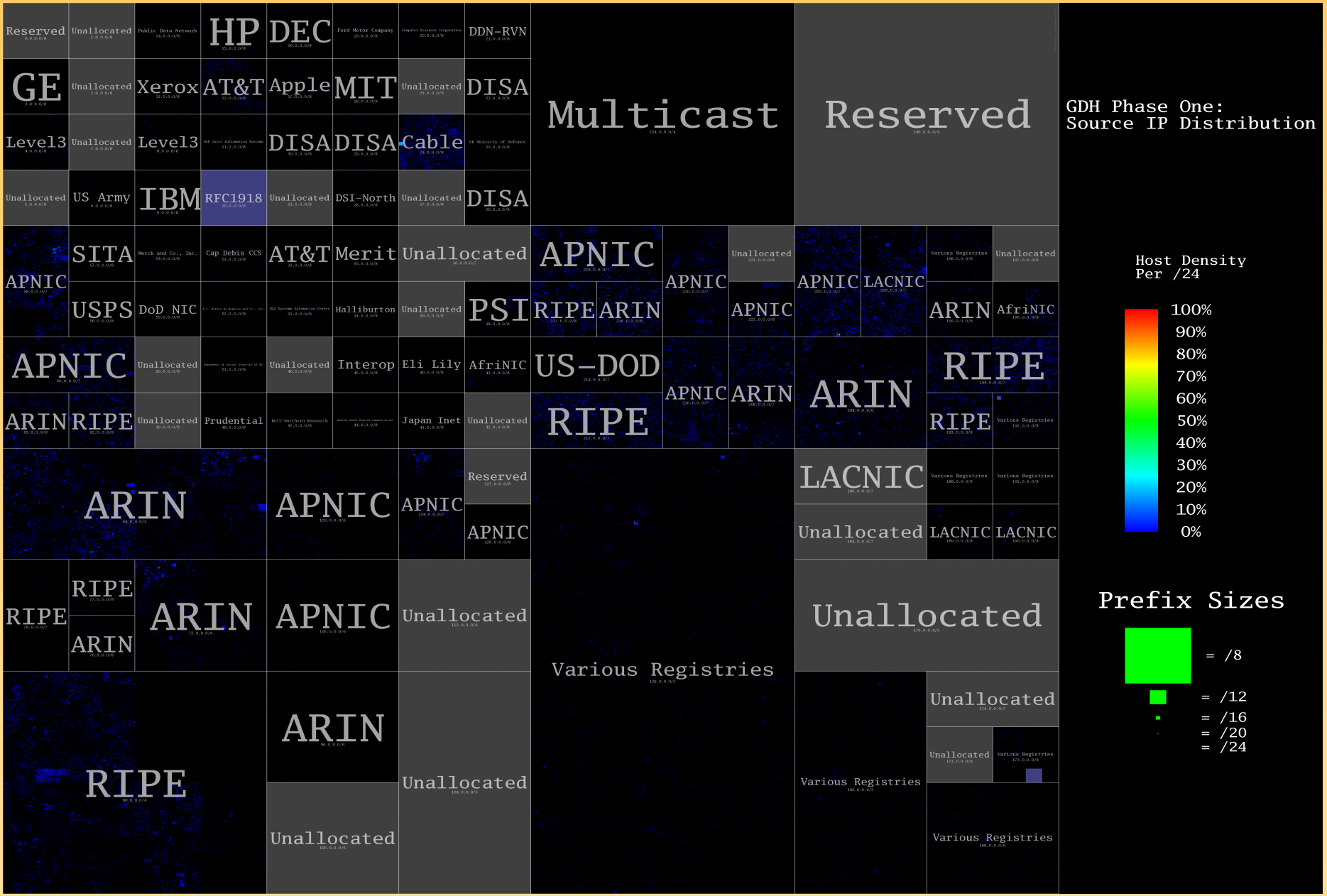
Page 1 of 3 IP: MD5: Rows 1 - 20 of 56

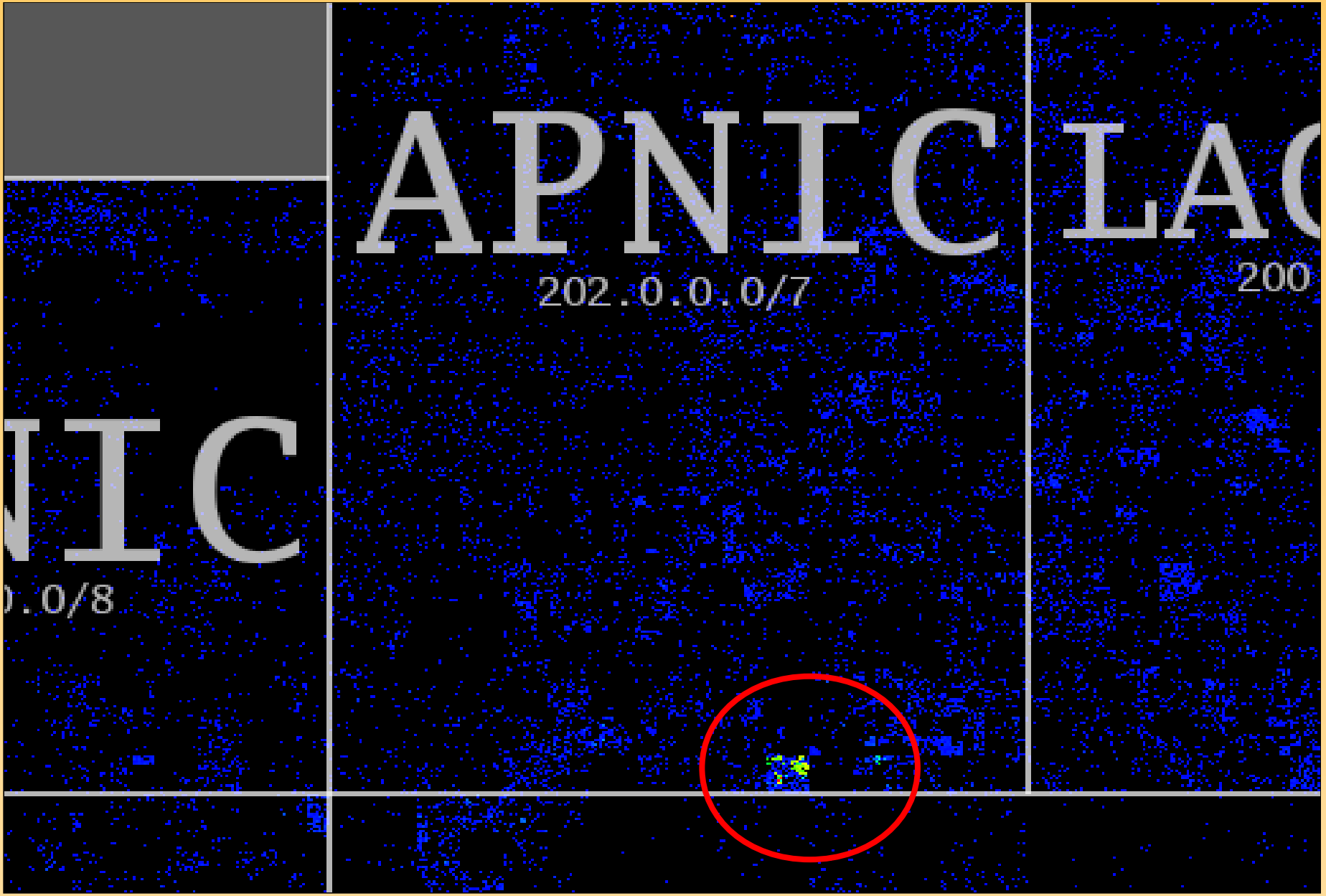
Attack Detail

ID:	6
Time:	1236037531
Sensor:	64.236.114.1
Download:	creceive://87.17.73.69:59800
Trigger:	creceive://87.17.73.69:59800
MD5sum:	11d31a4ebd7260193ffe8da9bb79156a
SHA512:	8096d0ce1fcd9b279d55037bd67af05873b57b4ca796f813a8449790a76e5c3a
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Attacker IP:	1460750661
Victim IP:	1089237505
Filename:	index.html
Country:	NZ
ISP:	Celestra NZ
ASN:	99421

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




Reserved
Unallocated
Public Data Network
HP
DEC
Ford Motor Company
Computer Sciences Corporation
DDN-RVN
GE
Unallocated
Xerox
AT&T
Apple
MIT
Unallocated
DISA
Level3
Unallocated
Level3
DISA
DISA
Cable
UK Ministry of Defence
Unallocated
US Army
IBM
RFC1918
Unallocated
DSI-North
Unallocated
DISA
Multicast
Reserved
GDH Phase One:
Source IP Distribution
APNIC
SITA
Merck and Co., Inc.
Cap Debis CCS
AT&T
Merit
Unallocated
APNIC
APNIC
Unallocated
APNIC
LACNIC
Various Registries
Unallocated
USPS
DoD NIC
Halliburton
Unallocated
PSI
RIPE
ARIN
APNIC
ARIN
AfriNIC
Host Density
Per /24
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
APNIC
Unallocated
Unallocated
Interop
Eli Lily
AfriNIC
US-DOD
APNIC
ARIN
ARIN
RIPE
ARIN
RIPE
Unallocated
Prudential
Japan Inet
Unallocated
RIPE
RIPE
Various Registries
ARIN
APNIC
APNIC
Reserved
APNIC
LACNIC
Various Registries
Various Registries
Unallocated
LACNIC
LACNIC
RIPE
RIPE
ARIN
ARIN
APNIC
Unallocated
Unallocated
Prefix Sizes
= /8
= /12
= /16
= /20
= /24
Various Registries
Unallocated
RIPE
ARIN
Unallocated
Unallocated
Unallocated
Various Registries
Various Registries



David Watson (david@honeynet.org.uk)

HonEeBox Summary

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

Attacks

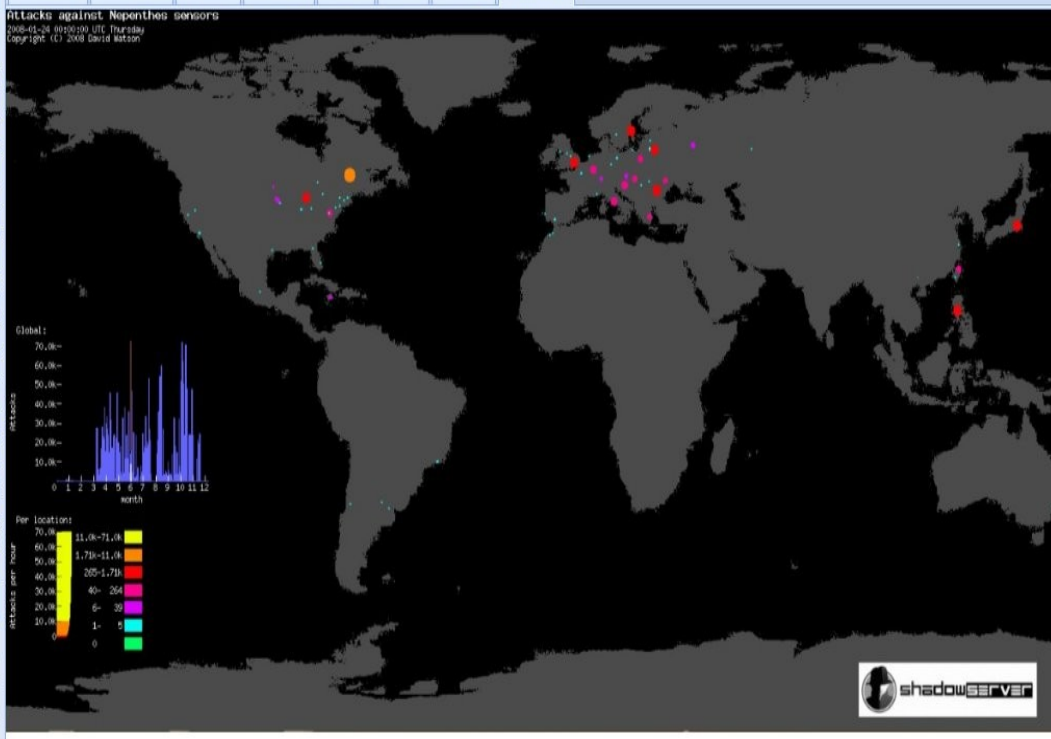
ID	Time	Attacker IP	Victim IP	MD5sum	Download
1	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243
2	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.18
3	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	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

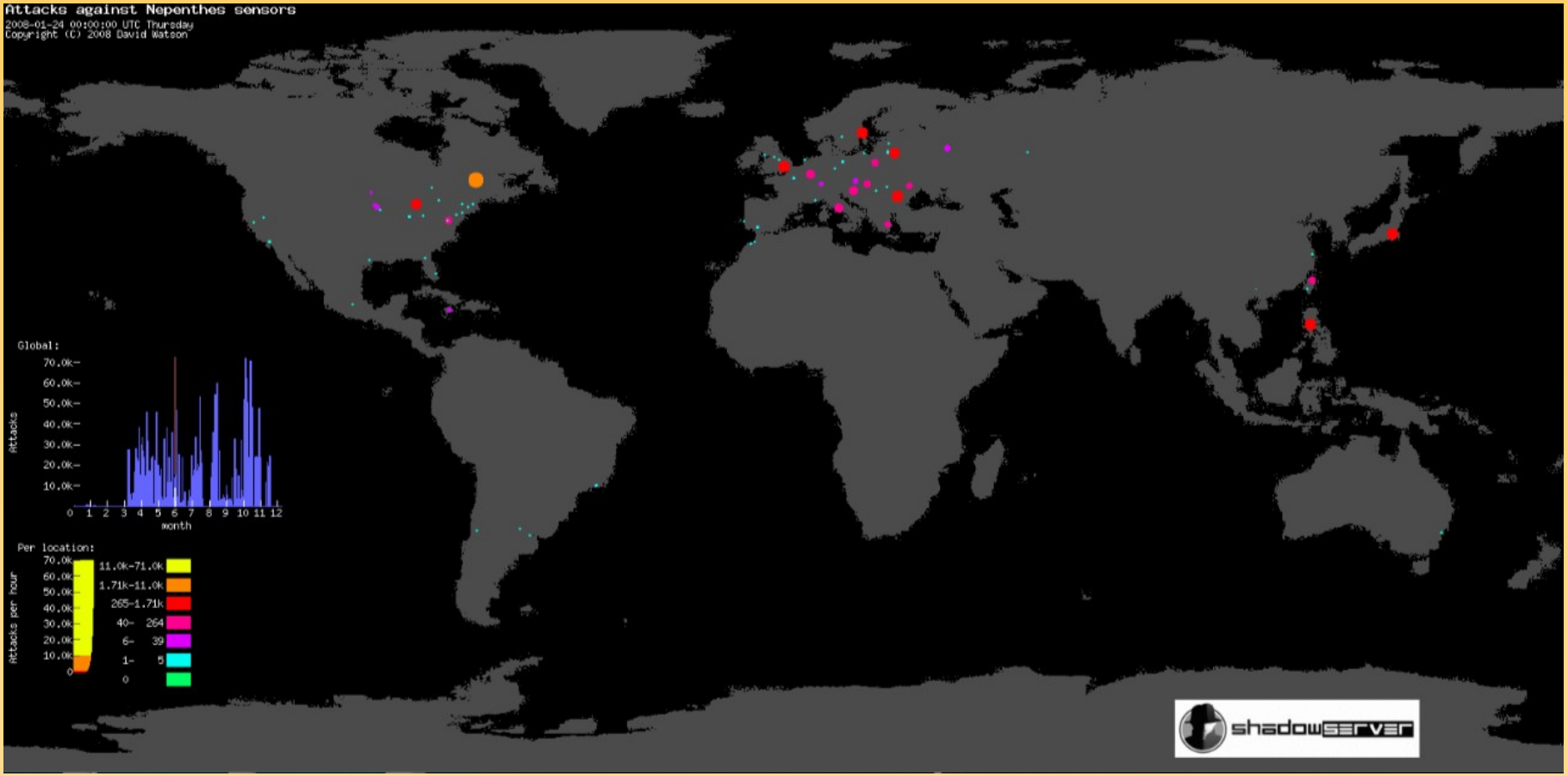
Page 1 of 3 IP: MD5: Rows 1 - 20 of 56

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 | Googe Earth | Sandbox | Anti-Virus | Graphs | PicViz | Heatmap | **Cuttlefish**





David Watson (david@honeynet.org.uk)

HonEeeBox Summary

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

Attacks

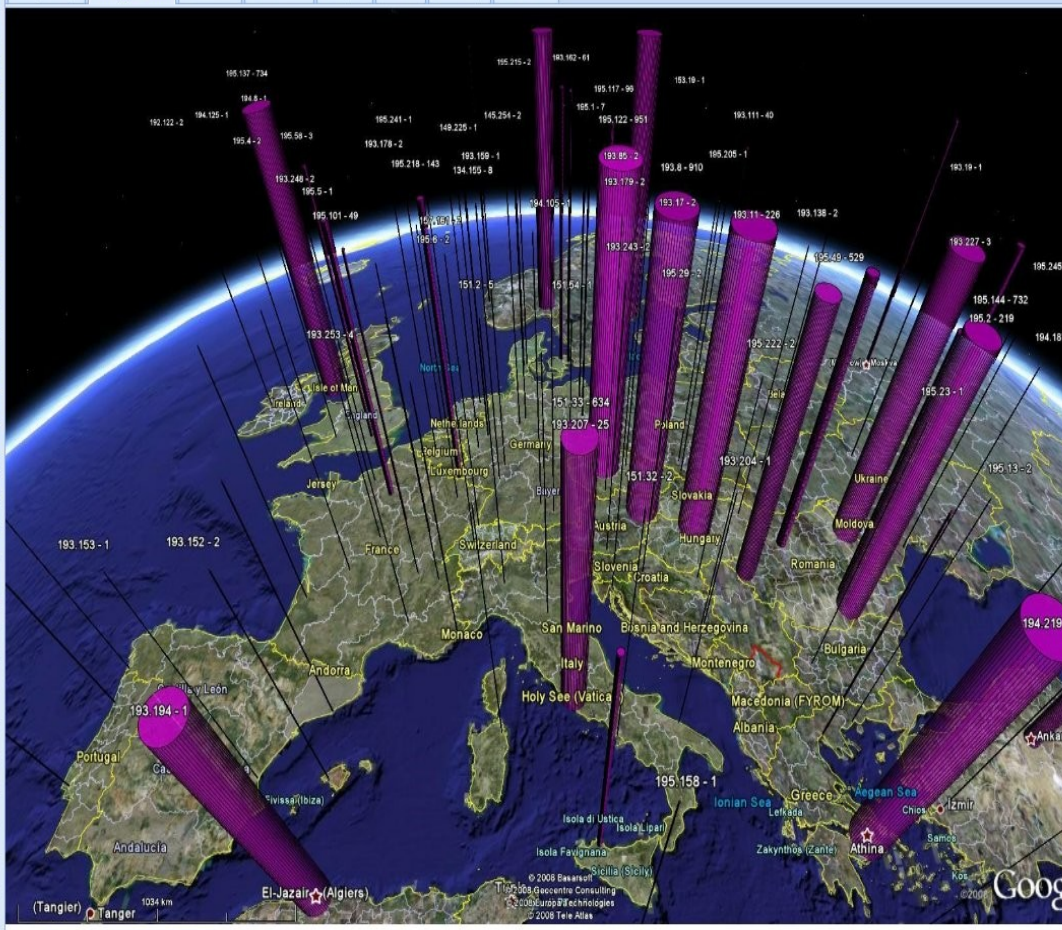
ID	Time	Attacker IP	Victim IP	MD5sum	Download
1	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243
2	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.18
3	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	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

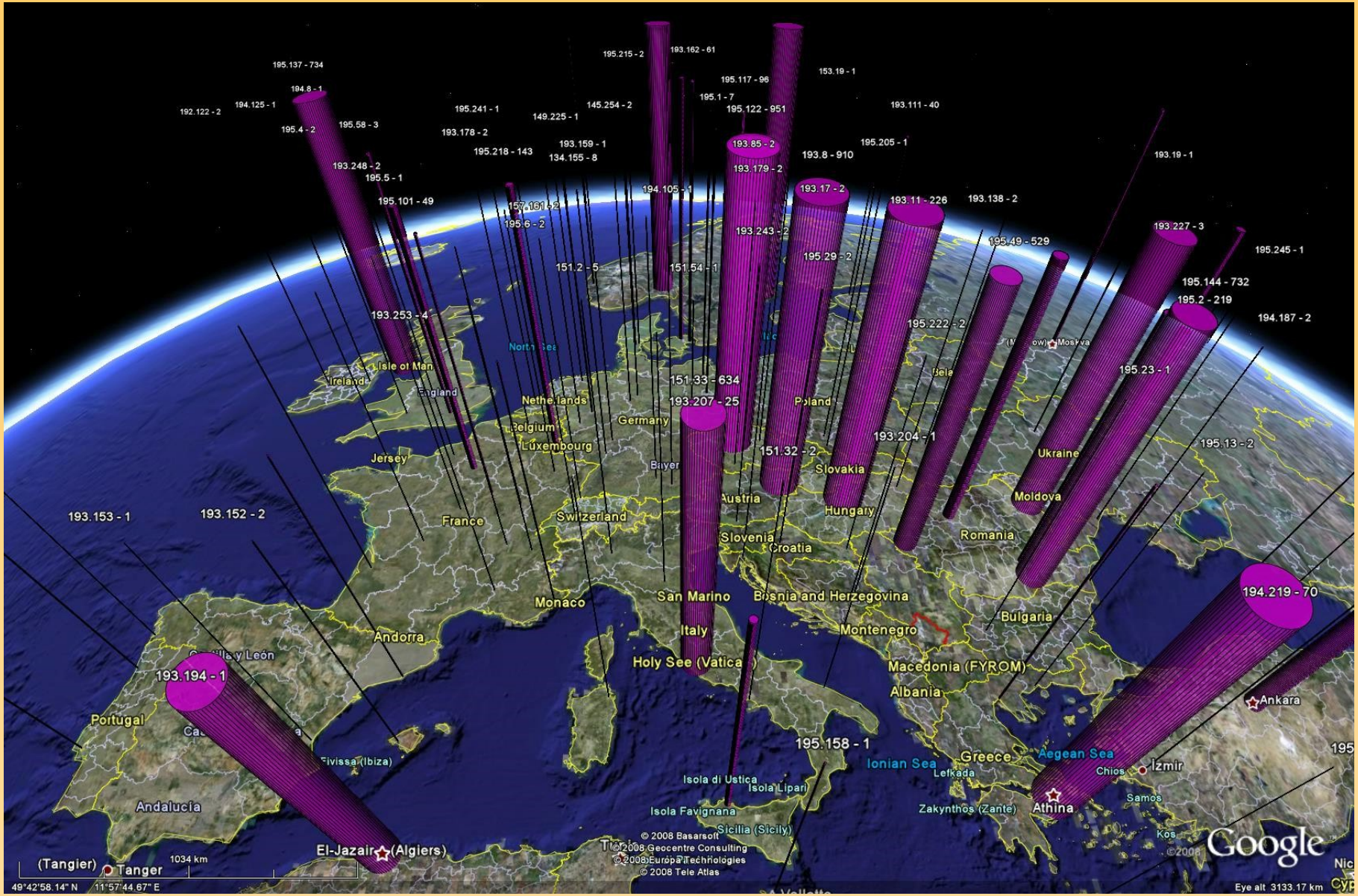
Page 1 of 3 IP: MD5: Rows 1 - 20 of 56

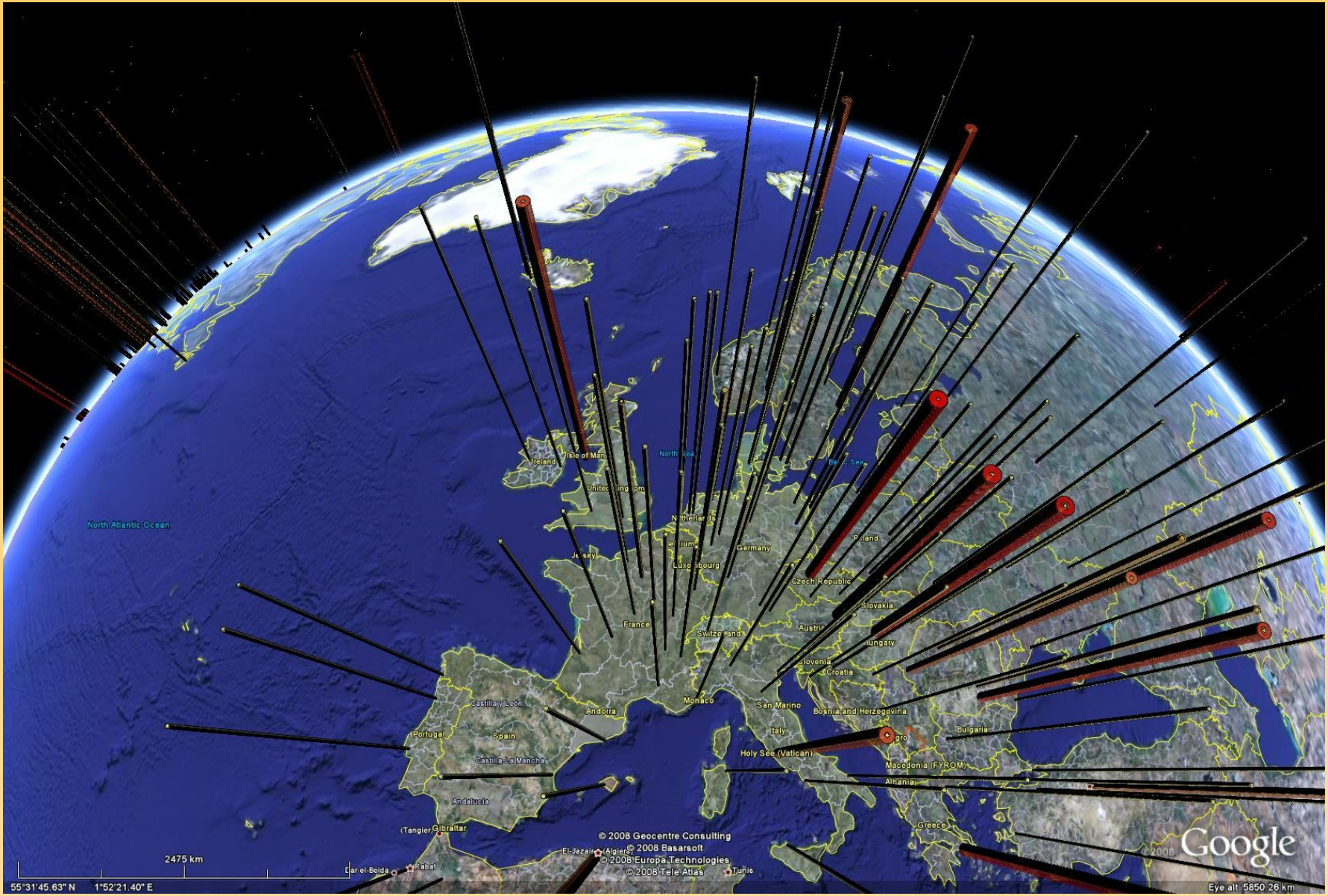
Attack Detail

ID:	1
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




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
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
157.161 - 2
195.6 - 2
193.243 - 2
193.227 - 3
195.49 - 529
195.245 - 1
151.2 - 5
151.54 - 1
195.29 - 2
195.144 - 732
195.2 - 219
193.253 - 4
195.222 - 2
194.187 - 2
195.23 - 1
151.33 - 634
193.207 - 25
193.204 - 1
195.13 - 2
151.32 - 2
193.153 - 1
193.152 - 2
193.194 - 1
195.158 - 1
194.219 - 70
Isle of Man
Ireland
England
Nethe.lands
Belgium
Luxembourg
Germany
Jersey
France
Switzerland
Austria
Slovakia
Hungary
Poland
Ukraine
Moldova
Romania
Slovenia
Croatia
San Marino
Bosnia and Herzegovina
Monaco
Andorra
Italy
Holy See (Vatica
Montenegro
Bulgaria
Macedonia (FYROM)
Albania
Greece
Aegean Sea
Ionian Sea
Ankara
Izmir
Chios
Lefkada
Zakynthos (Zante)
Athina
Samos
Kos
Portugal
Andalucía
Isola di Ustica
Isola Lipari
Isola Favignana
Sicilia (Sicily)
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


North Atlantic Ocean
Ireland
Isle of Man
United Kingdom
Netherlands
Belgium
Germany
Luxembourg
Jersey
Poland
Czech Republic
Slovakia
France
Switzerland
Austria
Hungary
Slovenia
Croatia
Monaco
San Marino
Bosnia and Herzegovina
Andorra
Italy
Bulgaria
Portugal
Spain
Holy See (Vatican)
Castilla-La Mancha
Macedonia (FYROM)
Albania
Andalucía
Gibraltar
(Tangier)
Greece
Algiers
Tunis
Rabat
2475 km
© 2008 Geocentre Consulting
© 2008 Basarsoft
© 2008 Europa Technologies
© 2008 Tele Atlas
Google
55°31'45.63" N 1°52'21.40" E
Eye alt 5850.26 km

HonEeeBox Summary

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

Attacks

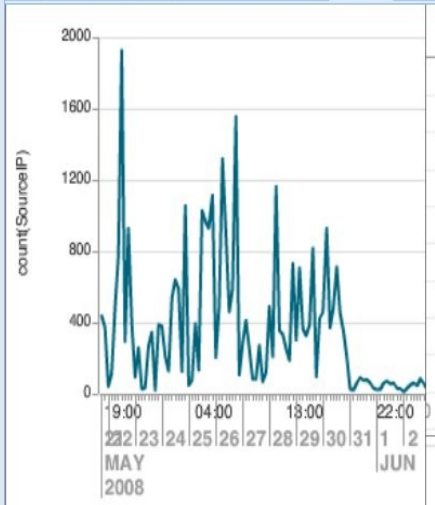
ID	Time	Attacker IP	Victim IP	MD5sum	Download
1	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe
2	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5abl192d	ftp://l:l@88.204.183.126:7293/netlibrary.exe
3	20 Mar 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	8f4e8e31fcdbf9635791ab009defelb5	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	lld31a4ebd7260193ffe8da9bb79156a	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	e399196c959235c23f71ac2c5abl192d	ftp://l:l@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	8f4e8e31fcdbf9635791ab009defelb5	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	lld31a4ebd7260193ffe8da9bb79156a	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	e399196c959235c23f71ac2c5abl192d	ftp://l:l@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	8f4e8e31fcdbf9635791ab009defelb5	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

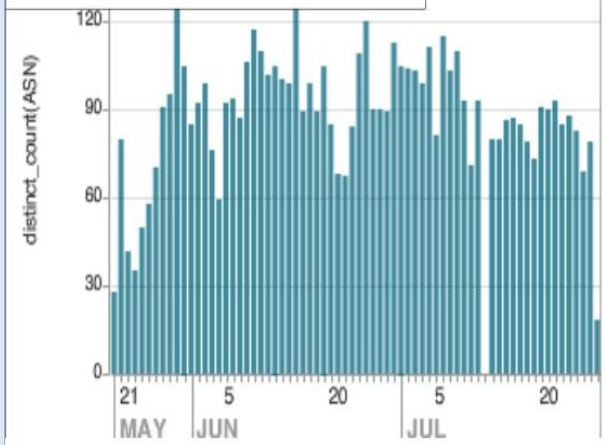
Attack Detail

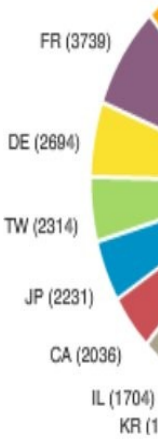
ID:	3
Time:	1236003748
Sensor:	64.236.114.1
Download:	creceive://87.175.58.187:4652
Trigger:	creceive://87.175.58.187:4652
MD5sum:	3875b6257d4d21d51ec13247ee4c1cdb
SHA512:	5e60dd302d73e64b2a4c7e3d7e22b684028a6d5a719c7869891783f5f86e2cf3
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit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

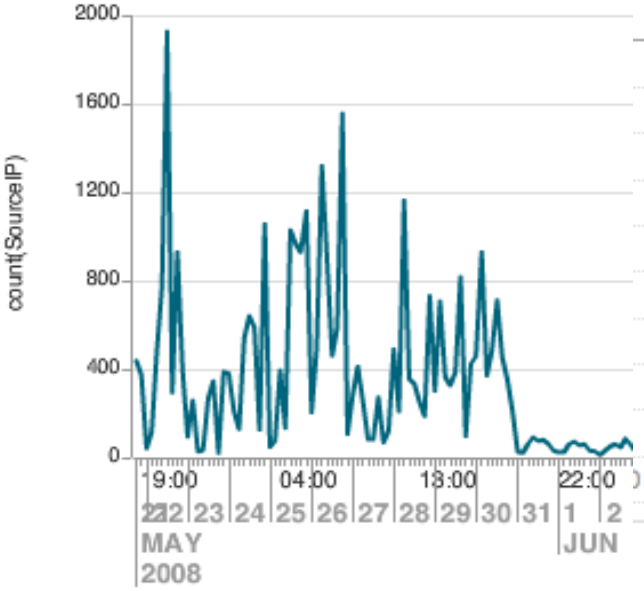
Google Map | Googe Earth | Sandbox | Anti-Virus | **Graphs** | PicViz | Heatmap | Cuttlefish



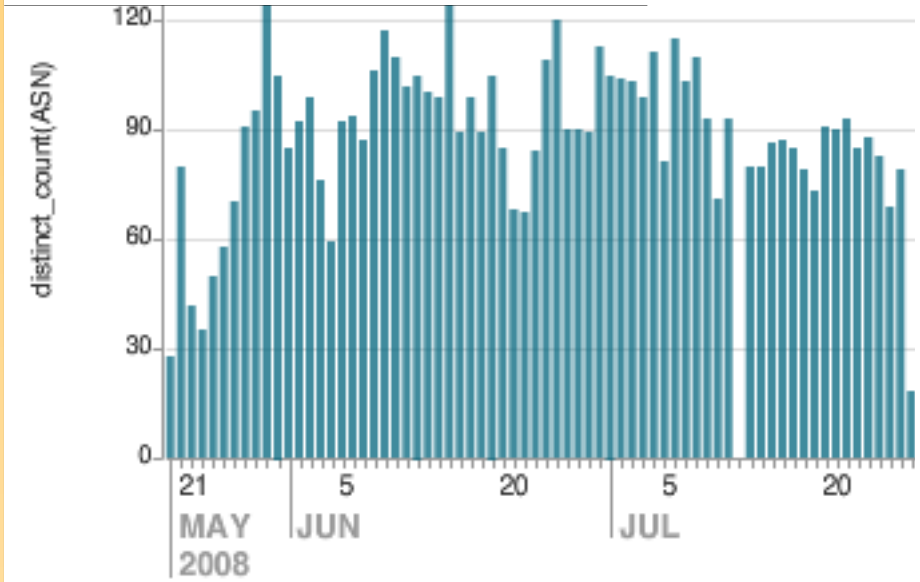
Classification	count
WORM/Allaple.Gen	14228
TR/Crypt.XPACK.Gen	9021
TR/Crypt.NSPM.Gen	5059
WORM/Allaple.Damaged.Gen	2700
W32/Virut.N.DR	2375
WORM/Rbot.147456.27	1830
WORM/Rbot.147456.27]	1774
W32/Virut.Gen	1550
WORM/Rbot.50176.5	975
W32/Virut.W	975

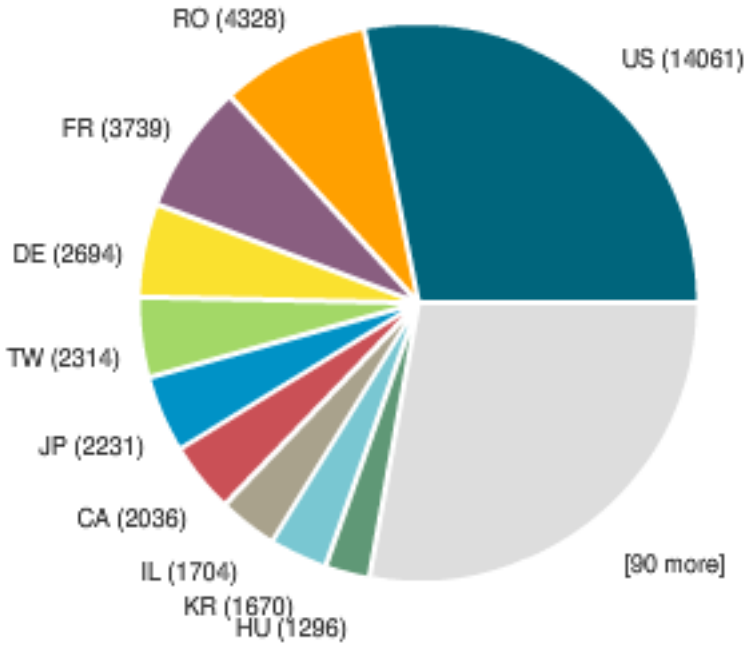






Classification	count	percent
WORM/Allaple.Gen	14228	28.951063
TR/Crypt.XPACK.Gen	9021	18.355886
TR/Crypt.NSPM.Gen	5059	10.294028
WORM/Allaple.Damaged.Gen	2700	5.493946
W32/Virut.N.DR	2375	4.832638
WORM/Rbot.147456.27	1830	3.723675
WORM/Rbot.147456.27]	1774	3.609726
W32/Virut.Gen	1550	3.153932
WORM/Rbot.50176.5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





David Watson (david@honeynet.org.uk)

HonEeeBox Summary

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

Attacks

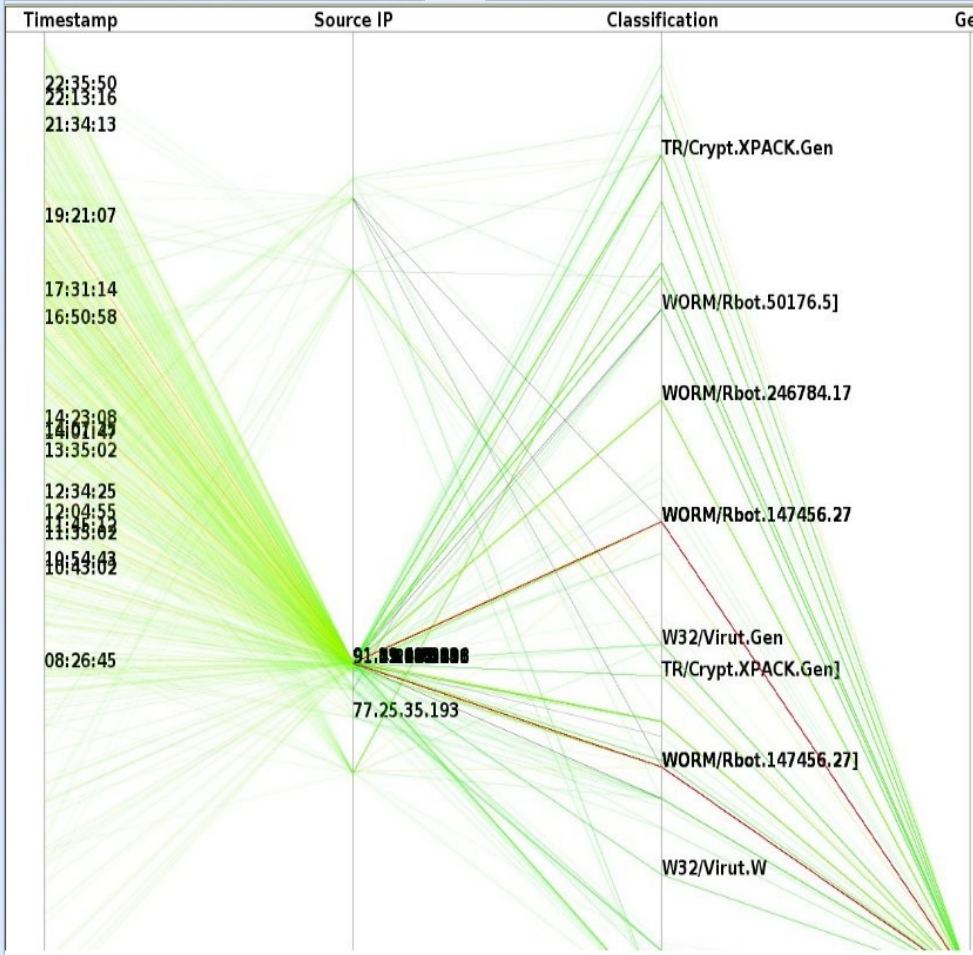
ID	Time	Attacker IP	Victim IP	MD5sum	Download
1	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.6
2	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.2
3	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.
4	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211
5	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.
6	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	creceive://87.
7	20 Mar 2009 17:22:37	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.
8	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.6
9	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.2
10	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.
11	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211
12	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.
13	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	creceive://87.
14	20 Mar 2009 17:22:37	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.
15	20 Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.6
16	20 Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.2
17	20 Mar 2009 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.
18	20 Mar 2009 17:22:37	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211
19	20 Mar 2009 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.

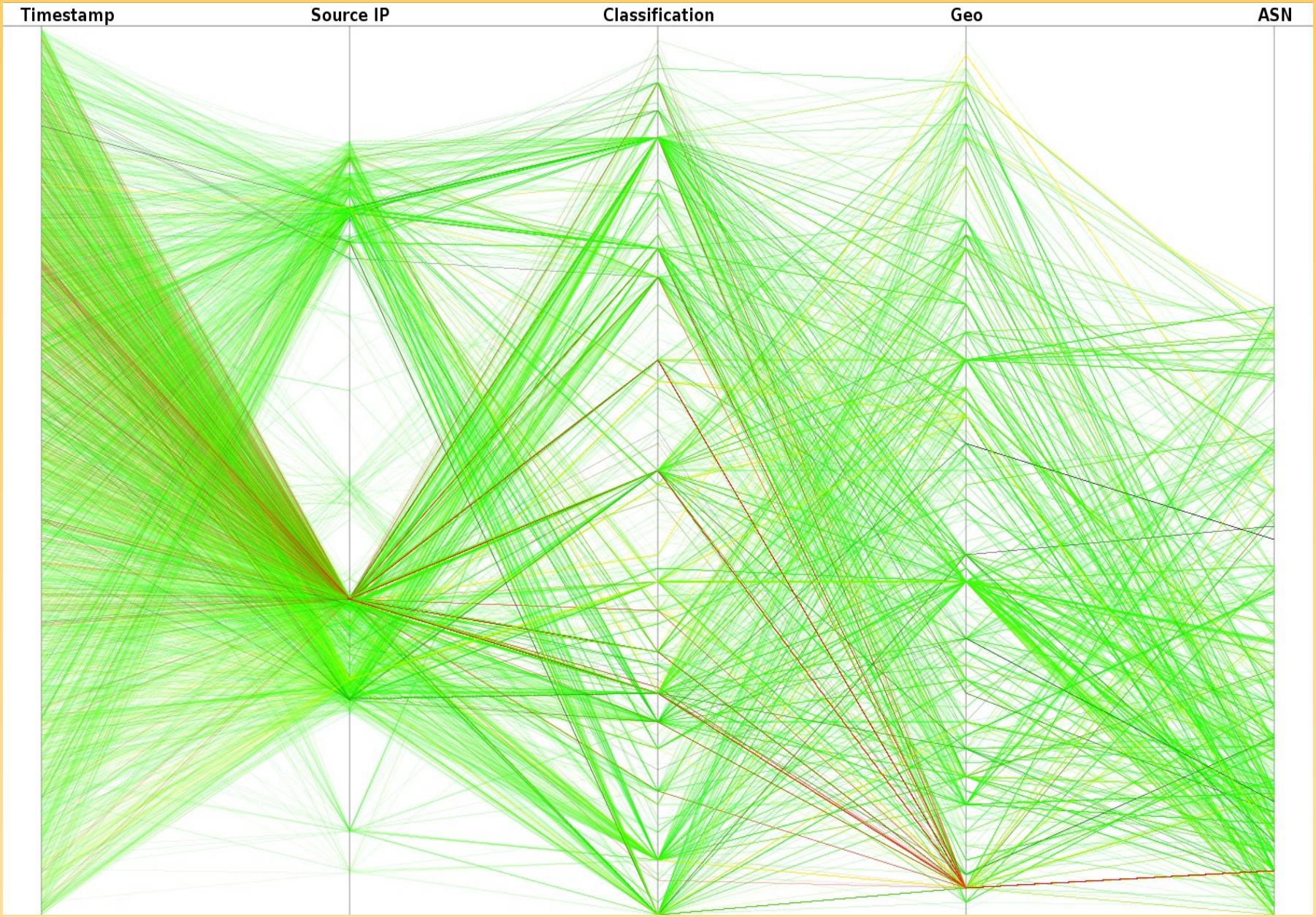
Page 1 of 3 IP: MD5: Rows 1 - 20 of 56

Attack Detail

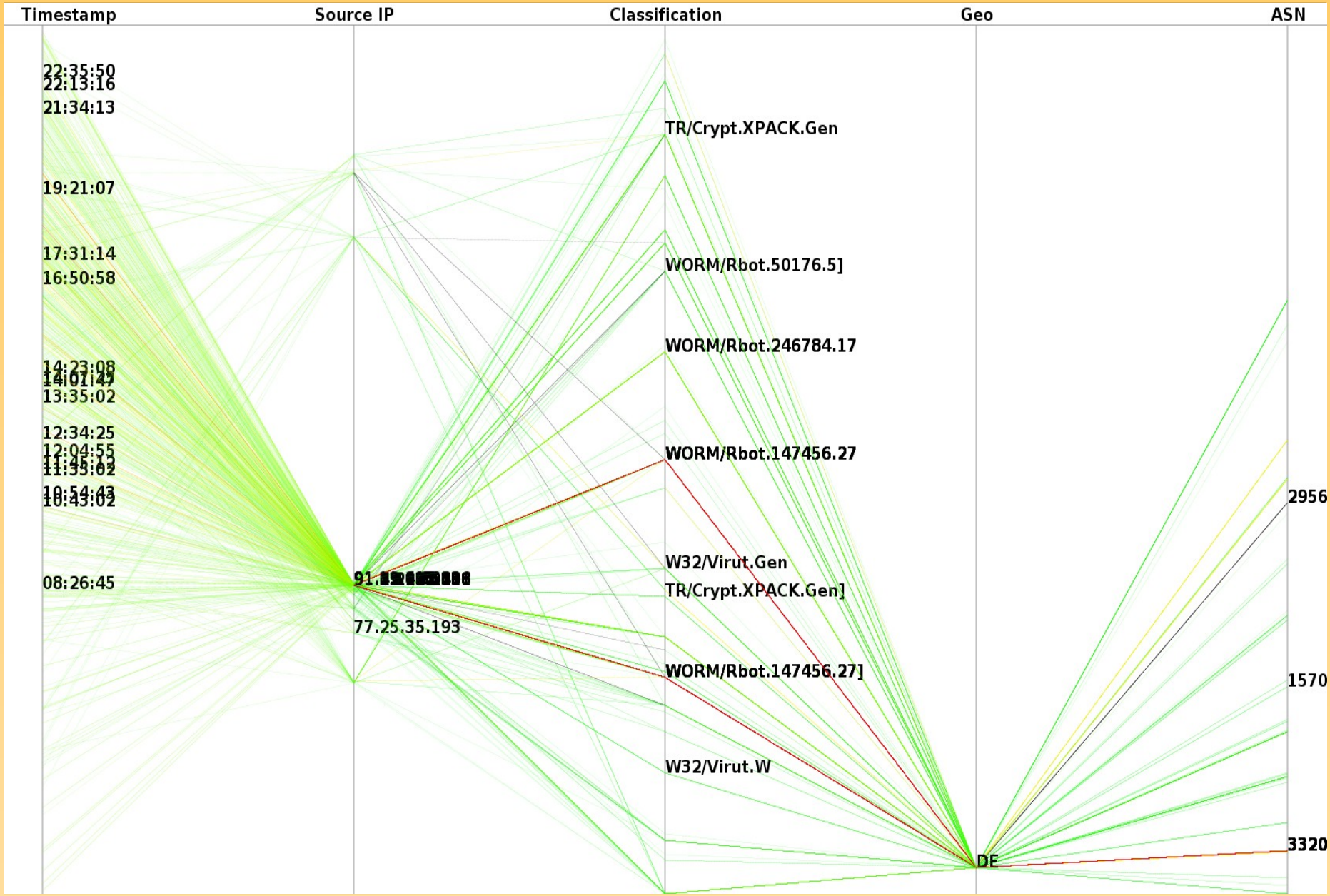
ID:	9
Time:	1235924337
Sensor:	64.236.114.1
Download:	ftp://1:1@88.204.183.126:7293/netlibrary.exe
Trigger:	ftp://1:1@88.204.183.126:7293/netlibrary.exe
MD5sum:	e399196c959235c23f71ac2c5ab1192d
SHA512:	d41821a576642131e32645afc3d531dca5f6d4a09a76ad0ce71a7d49021c6906
File Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Attacker IP:	1089237505
Victim IP:	1089237505
Filename:	netlibrary.exe
Country:	FR
ISP:	Vodafone FR
ASN:	5142

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

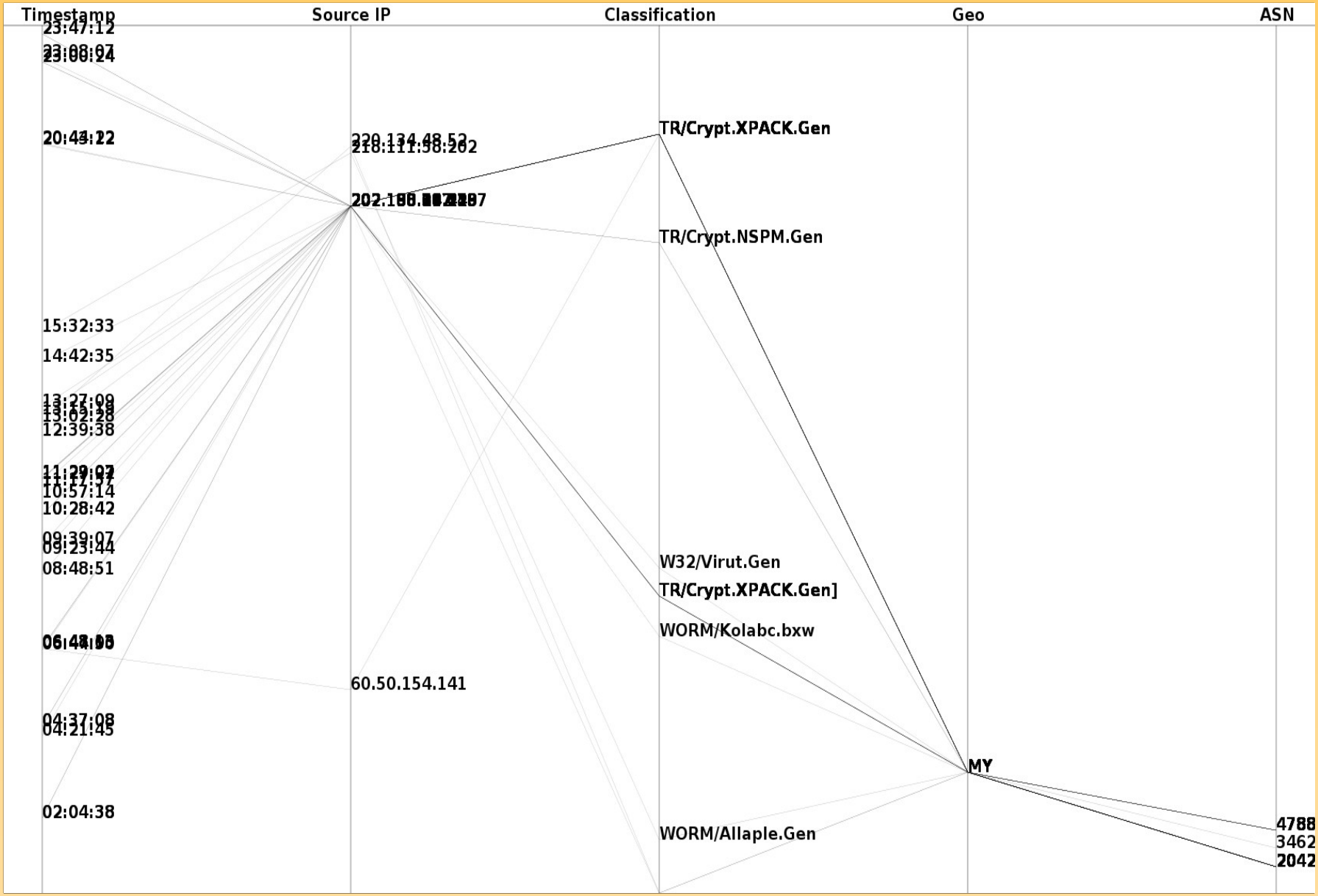




David Watson (david@honeynet.org.uk)



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

Any Questions?

David Watson david@honeynet.org.uk