The Honeyned P R O J E C T

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

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





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

Embedded Nepenthes

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



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

Embedded Sensors Pros/Cons

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

- Slow development
- Endian-ness
- Capacity
- * Performance
- × Poor console / UI
- Upgrade re-flash
- Making bricks!



HonEeeBox Low Interaction Malware Collection Sensors

Asus Eee PC Box (B202)

- Best of both worlds
- Intel Atom x86 CPU
- 1.6 GHz HT
- IGB 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

— ТНЕ НОМЕУМЕТ РКОЈЕСТ—

legin: Setting up loo	cales Generating locales (this might take a while)
en_US.UTF-8 done	<u>.</u>
ieneration complete.	
lone. Begin: Setting un aut	comatic login done
	isole kevboard done.
legin: Configuring gr	юме-panel-data done.
D D D D D D D D D D D D D D D D D D D	creensaver done.
P K O J E C I legin: Preconfiguring	/etc/modules done.
legin: Preconfiguring	networking done.
NIT: upreion 2.86 h	ots/Init-Dottom done.
tarting the hotplug	events disnatcher: udevd[8.512504] udevd version 125 s
irted	r
() SNADOWSERVER Synthesizing the init	ial hotplug eventsdone.
laiting for /dev to 1	be fully populated[8.873512] Linux agpgart interface
0.103	
8.876631J agpgat	t: Detected an Intel 440BX Chipset.
8.8847151 nci h	t, Har apertare is 2504 @ 000 htmlug: PCI Hot Plug PCI Core version: 0.5
ess F1 for help, or ENTER to boot: 8.884984] shpch	: Standard Hot Plug PCI Controller Driver version: 0.4
dMin@debian: \$ ps -et ; grep nepen	new netter (nn) as /class/input/input1
101 2612 1 0 08:28 ? 00:00:00 /opt/nepenthes/b	in∕nepenthes[^[PWRF]
ser=nepenthesgroup=nepenthes	
ıdmin 2703 2667 0 08:31 tty1 00:00:00 grep nepen	[!!] Choose language
ıdmin@debian:~\$	Please choose the language used for the installation process. This
ıdmin@debian∶~\$	language will be the default language for the final system.
dMin@debian:~\$ tail ∕opt/nepenthes/var/log/nepenthes.log	Choose a language:
[26022009 08:28:07 info sc module] Loading signatures from file	C – No localization 🔸
hes/signatures/shellcode-signatures.sc	Albanian – Shqip Arabic
[26022009 08:28:08 debug info fixme] Logfile var/log/nepenthes.	Basque – Euskara
now 101:103 (neventhes:neventhes)	Belarusian – Беларуская Вosnian – Bosanski
[26022009 08:28:08 crit mgr] Compiled without support for capab	Bulgarian – Български
n run canahilities	Chinese (Simplified) - 中文(简体)
[26022009 08:28:08 info mor] Process arounid 103	Chinese (Traditional) - 中文(繁體) Croatian - Hrwatski
[26022009 08:28:08 info mor] Process userid 101	Czech – Čeština
ldmin@debian:~\$	Danish – Dansk Dutch – Nederlands
	English – English
	Esperanto
	<go back=""></go>

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 ;-)



Prototype HonEeeBox UI and Basic Example Visualisations

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

HE HONEYNET PROJECT-

HonEeeBox Summary

Т

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

Attacks					Google Map	Googe Earth	Sandbox	Anti-Virus	Graphs P	ic∨iz Heatmap	Cuttlefish
ID Time	Attacker IP	Victim IP	MD5sum	Download	1			1 insu	1		
1 20 Mar 200	9 17:22:37 70. 232. 61. 243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243	← ₩→				1		r - 195,000
2 20 Mar 200	9 17:22:37 🚺 64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	<u>ftp://l:1088.204.18</u>	\checkmark		136		<u>Ri</u>	New Y	
3 20 Mar 200	9 17:22:37 🔯 87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	<u>creceive://87.175.5</u>	+		ST E.		1	7 7	
4 20 Mar 200	9 17:22:37 🏾 🍨 127. 255. 255. 255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	<u>creceive://211.200.</u>	1						
5 20 Mar 200	9 17:22:37 📓 87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	<u>creceive://87.17.73</u>		Cont VE	R	Greenla	and 🖄		1
6 20 Mar 200	9 17:22:37 📓 87.17.73.69	64.236.114.1	<u>11d31a4ebd7260193ffe8da9bb79156a</u>	<u>creceive://87.17.73</u>			1.	8	E.	1	
7 20 Mar 200	9 17:22:37 📕 118. 165. 49. 147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	<u>ftp://a:a@118.165.4</u>		2001	5 • <u>3</u> %,	÷.,	Aunt	Su	omi and
8 20 Mar 200	9 17:22:37 70. 232. 61. 243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243			N 53 8		lceland	Sverige	1.0
9 20 Mar 200	917:22:37 64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.204.18	E.	- C	A TAK			Norge Norway	40 3
10 20 Mar 200	9 17:22:37 87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	<u>creceive://87.175.5</u>	I.	Canada				United Kingdom OPolska	him
11 20 Mar 200	917:22:37 • 127.255.255.255	64.236.114.1	8+4e8e31+cdb+9635791ab009de+e1b5	creceive://211.200.1		N	A STATE	2		Deutschland	Vinalitia
12 20 Mar 200	917:22:37 87.17.73.69	64.236.114.1	15155437982c893ae8b9cb8187d47256	creceive://87.17.73	र य	Sterry 1	1 - A			France	Ulvaine
13 20 Mar 200	917:22:37 87.17.73.69	ata 64.236.114.1	11d31a4ebd/260193ffe8da9bb/9156a	creceive://8/.1/./3		United				España Italy P	Türkiye
14 20 Mar 200	917.22.37 118.165.49.147	64.236.114.1	250406C021521510505955C945C001C2	ftp://70.222.61.242		outcoy	1	Atlanti	C	J. C.	Jurkey Jan
16 20 Mar 200	917:22:37 64 236 114 1	64 236 114 1	e399196c959235c23f71ac2c5ab1192d	ftp://1.1088_204_18						Algeria Libya	Egypt Saudi
17 20 Mar 200	917:22:37 🛐 87, 175, 58, 187	64. 236. 114. 1	3875b6257d4d21d51ec13247ee4c1cdb	creceive: //87,175,5		Mexico			Maurit	ania Mali Niger	Arabia
18 20 Mar 200	9 17:22:37 • 127, 255, 255, 255	64, 236, 114, 1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.1			1 diam			Chad	Sudan
19 20 Mar 200	9 17:22:37 🔡 87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73			Colombia	13		Q Same	
🛛 🖣 🔤 Page 🕻	of 3 🕨 🕅 🥲 IP:	MD	5:	Rows 1 - 20 of 56			27			Cong	o Kenya Tanzania
Attack Detail							Perú	Brazil		Angola	St.
ID:	2						Bolly	the start		Namibia	Madagascar
Time:	1235924337				South Pacific	th tic	0				
Sensor:	64.236.114.1				Ocean		2	9	Uce	an South Africa	
Download:	ftp://1:1@88.204.183.126:7293	B/netlibrary.exe					Arger	iuna			
Trigger:	ftp://1:1@88.204.183.126:7293	B/netlibrary.exe									
MD5sum:	e399196c959235c23f71ac2c5	ab1192d			Google		10				
SHA512:	d41821a576642131e32645af	c3d531dca5f6d4a09a76a	d0ce71a7d49021c6906								
File Type:	PE32 executable for MS Windo	ows (GUI) Intel 80386 32-b	it								
Attacker IP:	1089237505										
Victim IP:	1089237505										
Filename:	netlibrary.exe										
Country:	FR										
ISP:	Vodafone FR										
ASN:	5142										

HONEYNET PROJECT

God

HonEeeBox Summary

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

HE

Т

Attacks					ooogie map	oboge Earth Dana	
ID Time	Attacker IP	Victim IP	MD5sum	Download	<u>↑</u>		
1 20 Mar 2009 1	7:44:27 370.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe	< ↔ →	N. Y.	5 G.S.
8 20 Mar 2009 1	7:44:27 70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	<pre>ftp://70.232.61.243:5554/16745_up.exe</pre>	\mathbf{A}	1 3 1 1 C	
15 20 Mar 2009 1	7:44:27 70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe	🛨 🏑	1. 1. 10 CO	E.
22 20 Mar 2009 1	7:44:27 70.232.61.243	64.236.114.1	<u>1a2c0e6130850f8fd9b9b5309413cd00</u>	ftp://70.232.61.243:5554/16745_up.exe			
29 20 Mar 2009 1	7:44:27 70.232.61.243	64.236.114.1	<u>1a2c0e6130850f8fd9b9b5309413cd00</u>	<pre>ftp://70.232.61.243:5554/16745_up.exe</pre>		CON VE COR	Greenlan
36 20 Mar 2009 1	7:44:27 70.232.61.243	64.236.114.1	<u>1a2c0e6130850f8fd9b9b5309413cd00</u>	<pre>ftp://70.232.61.243:5554/16745_up.exe</pre>		E Shink	S 8
43 20 Mar 2009 1	7:44:27 70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe			288 8 🖉
50 20 Mar 2009 1	7:44:27 70.232.61.243	64.236.114.1	1a2c0e6130850†8†d9b9b5309413cd00	<u>ttp://70.232.61.243:5554/16745_up.exe</u>			
57 20 Mar 2009 1	7:44:27 70.232.61.243	ata 64.236.114.1	1a2c0e6130850†8†d9b9b5309413cd00	ttp://70.232.61.243:5554/16745_up.exe	l l	1-1-1	
54 20 Mar 2009 1	7:44:27 70.232.61.243	GIG 64.236.114.1	1-2-0-61 2050 61 500 500 41 3-400	<u>ttp:///0.232.61.243:5554/16745_up.exe</u>	45	Canada	- alla
71 20 Mar 2009 1	7:44:27 70.232.01.243		1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe			al.
76 20 Mai 2009 1	7.44.27 70.232.61.243	1212 64.236.114.1	182000130030181030303413000	<u>110,///0.232.01.243.3334/10/45_00.exe</u>		United The	for the second s
						States	North Atlantic
						the second	Ocean
						México	
						Store 1	
						Color	Venezuela Ibla
A Page 1	of 5 🕨 🔰 🎅 IP: 70.23	2.61.243 M	D5: 1a2c0e6130850f8fd9b9b530	Rows 1 - 12 of 84		Q.	Y The Part
Attack Detail						Per	u Brasil
ID:	1						Bolivia
Time:	1235801109				South Pacific		Chile .
Sensor:	64.236.114.1				Ocean		1.9
Download:	ftp://70.232.61.243:5554/1674	15_up.exe					Argenuna
Trigger:	ftp://anonymous:bin@192.168	3.1.64:5554/16745_up.exe	9		POWERED BY		
MD5sum:	1a2c0e6130850f8fd9b9b530	9413cd00			Google		Abr
SHA512:	8e1e40dedb4aa57ae5c89a7	5aca26a813ce5622e371	049ddbc916552d1c00b48				
File Type:	PE32 executable for MS Wind	ows (GUI) Intel 80386 32-	bit				
Attacker IP:	1189625331						
Victim IP:	1089237505						
Filename:	16745_up.exe						
Country:	US						
ISP:	AOL						
ASN:	1331						

Centrica Internet

3310

ISP:

ASN:

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

Н

п

Т

Atta	cks							
ID	Time	Attacker IP	Victim IP	MD5sum	Download			
1	20 Mar 2009 17:22:3	87 📑 70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe	1		
2	20 Mar 2009 17:22:3	87 🚺 64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.204.183.126:7293/netlibrary.exe			
3	20 Mar 2009 17:22:3	87 🔯 87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.58.187:4652			
4	20 Mar 2009 17:22:3	87 🔎 127. 255. 255. 255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	<pre>creceive://211.200.220.64:3647</pre>			
5	20 Mar 2009 17:22:3	87 🔠 87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73.69:43074			
6	20 Mar 2009 17:22:3	87 🔤 87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	creceive://87.17.73.69:59800			
7	20 Mar 2009 17:22:3	87 📕 118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.165.49.147:2866/igxdfdfds.com			
8	20 Mar 2009 17:22:3	37 🦉 70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe			
9	20 Mar 2009 17:22:3	87 🚺 64.236.114.1	64.236.114.1	<u>e399196c959235c23f71ac2c5ab1192d</u>	ftp://1:1@88.204.183.126:7293/netlibrary.exe	11		
10	20 Mar 2009 17:22:3	87 🔯 87.175.58.187	64.236.114.1	<u>3875b6257d4d21d51ec13247ee4c1cdb</u>	<pre>creceive://87.175.58.187:4652</pre>			
11	20 Mar 2009 17:22:3	³⁷ • 127. 255. 255. 255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	<pre>creceive://211.200.220.64:3647</pre>			
12	20 Mar 2009 17:22:3	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	<u>creceive://87.17.73.69:43074</u>			
13	3 20 Mar 2009 17:22:37 📰 87.17.73.69		64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	<pre>creceive://87.17.73.69:59800</pre>			
14	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.c			
15	20 Mar 2009 17:22:3	37 🦉 70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.exe			
16	20 Mar 2009 17:22:3	87 1 64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.204.183.126:7293/netlibrary.exe			
17	20 Mar 2009 17:22:3	87 🔯 87.175.58.187	64.236.114.1	<u>3875b6257d4d21d51ec13247ee4c1cdb</u>	creceive://87.175.58.187:4652	_		
18	20 Mar 2009 17:22:3	³⁷ 127. 255. 255. 255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.220.64:3647			
19	20 Mar 2009 17:22:3	87.17.73.69	64.236.114.1	t5t55437982c893ae8b9cb8187d47256	creceive://87.17.73.69:43074	56		
-Att	ack Detail	V VI IC IF:	MD	J:	10001-2001	00		
10.						7		
ID:	3					_		
Tim	ie: 12	36003748						
Ser	nsor: 64	.236.114.1						
Do	vnload: cre	eceive://87.175.58.187:4652				1		
Trig	ger: cre	eceive://87.175.58.187:4652				1		
MD	5sum: 38	75b6257d4d21d51ec132476	ee4c1cdb			Ĩ		
SH	A512: 5e	60dd302d73e64b2a4c7e3d3	re22b684028a6d5a719c	7869891783f5f86e2cf3		i.		
File	Type: PE	32 executable for MS Windov	vs (GUI) Intel 80386 32-bi	it		i		
Atta	cker IP: 14	71101627				2		
Vict	im IP: 10	89237505				1		
File	name: ind	lex.html				1		
Co	untry: BR	200000000000000000000000000000000000000				1		

Compact			esult: <mark>38/39 (97</mark>	.44%)	
					Print results 🔒
Antivirus		Version	Last Update	Result	
a-squared		85	38	Net-Worm.Win32.Sasser	IIK
AhnLab-V3			-	Win32/Sasser.worm.158	72.B
Anti∨ir		15	70	Worm/Sasser.B	
Authentium			-	W32/IRCBotX.BRM	
Avast		15	70	Win32:Sasser-N	
AVG			-	Obfustat.KwY	
BitDefende	r	15	70	Win32.Worm.Sasser.B	
CAT-QuickH	eal		50	W32.Sasser.B	
ClamAV		15	3 0	Worm.Sasser.B	
Comodo			50	Worm.Win32.Sasser.B	
DrWeb		11	30	Win32.HLLW.Jobaka	
eSafe		17	50	-	
e⊤rust-∨et		15	30	Win32/Sasser.B	
F-Prot		17	-	W32/IRCBotX.BRM	
F-Secure		11	3 0	Net-Worm:W32/Sasser.A	
Fortinet		17	31	W32/Sasser.B	
GData		117	9 0	Win32.Worm.Sasser.B	
Ikarus		17	3	Net-Worm.Win32.Sasser	
K7AntiViru	s	Nē	70	Net-Worm.Win32.Sasser	.a
Kaspersky		17	1 0	Net-Worm.Win32.Sasser	.a
McAfee		Ne	30	W32/Sasser.worm.b	
McAfee+Art	emis	17	50	W32/Sasser.worm.b	
Microsoft		No.	30	Worm:Win32/Sasser.dam	
N0D32			-	Win32/Sasser.B	
Norman		Ne	-	Sasser.B	
nProtect		17	-	Win32.Worm.Sasser.B	

THE HONEYNET PROJECT-

IonEeel	Box Summary	1						
otal	Attacks:	56 Total Sou	ırce IPs: 6	. Total Target IPs: 1	'otal MD5sums: 7 🛛	hill manadhar		
Attacks						Google Map Googe Earth Sandbox Ar	nti-Virus Graphs PicViz Heatmap Cuttlefish	
ID Tii	ne	Attacker IP	Victim IP	MD5sum	Download	1		
1 20) Mar 2009 17:2	22:37 50.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243			
2 20) Mar 2009 17:2	22:37 64. 236. 114. 1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.204.18	Scan Summary	File Changes	Reg
3 20) Mar 2009 17:2	22:37 🔯 87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.5	Technical Details		
4 20) Mar 2009 17:2	22:37 🚺 127. 255. 255. 255	64.236.114.1	8f4e8e3lfcdbf963579lab009defelb5	creceive://211.200.:	Analysis Number	1	
5 20) Mar 2009 17:2	22:37 🔛 87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	<u>creceive://87.17.73</u>	Parent ID	0	
6 20) Mar 2009 17:2	22:37 📓 87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	<u>creceive://87.17.73</u>	Process ID	1340	
7 20) Mar 2009 17:2	22:37 📕 118. 165. 49. 147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	<u>ftp://a:a@118.165.4</u>	Filename	H:\EuTeAmo.exe	
8 20) Mar 2009 17:2	22:37 70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243	Filesize	222720 bytes	
9 20) Mar 2009 17:2	22:37 🚺 64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://l:1088.204.18	MD5	79e2133fcc5b201b89a6680a7d289f6f	
10 20) Mar 2009 17:2	22:37 87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	<u>creceive://87.175.5</u>	Start Reason	AnalysisTarget	
11 20) Mar 2009 17:2	22:37 127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	<u>creceive://211.200.</u>	Termination Reason	Normal Termination	
12 20) Mar 2009 17:2	22:37 📓 87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	<u>creceive://87.17.73</u>	Start Time	00:54 453	
13 20) Mar 2009 17:2	22:37 📓 87.17.73.69	64.236.114.1	<u>11d31a4ebd7260193ffe8da9bb79156a</u>	<u>creceive://87.17.73</u>	Detection	OK (ClamAV)	
14 20) Mar 2009 17:2	22:37 📕 118. 165. 49. 147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	<u>ftp://a:a@118.165.4</u>		COM Create Instance: H:\WINDOWS\system32\ieframe.dll.	ProgID: (), Interface ID: ({000214E6-0
15 20) Mar 2009 17:2	22:37 50.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243	СОМ	COM Create Instance: H:\WINDOWS\system32\urimon.dll, P	rogID: (), Interface ID: ({886D8EEB-80
16 20) Mar 2009 17:2	22:37 64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	<u>ftp://1:1088.204.18</u>		Loaded DLLs	
17 20) Mar 2009 17:2	22:37 87.175.58.187	64.236.114.1	3875b6257d4d2ld5lec13247ee4clcdb	creceive://87.175.5		H:\WINDOWS\system32\ntdll.dll	
18 20) Mar 2009 17:2	22:37 127.255.255.255	64.236.114.1	8+4e8e31+cdb+9635791ab009de+e1b5	creceive://211.200.1		H:\WINDOWS\system32\kernel32.dll H:\WINDOWS\system32\advapi32.dll	
19 20 14 4	Page 1 of	22.37 DE 87.17.73.69	ata 64.236.114.1	t5t5543/982c893ae8b9cb818/d4/256	creceive://8/.1/./3 Rows 1 - 20 of 56		H:\WINDOWS\system32\RPCRT4.dll H:\WINDOWS\system32\Secur32.dll	
Attack	Detail			5.			H:\WINDOWS\system32\comcti32.dll H:\WINDOWS\system32\GDI32.dll	
10.		15					H:\WINDOWS\system32\USER32.dll	
ID.	L	15					H:\WINDOWS\system32\oleaut32.dll H:\WINDOWS\system32\msvcrt.dll	
Time:		1235801109					H:\WINDOWS\system32\ole32.dll H:\WINDOWS\system32\shell32.dll	
Senso	r:	64.236.114.1					H:\WINDOWS\system32\SHLWAPI.dll	
Downlo	oad:	ftp://70.232.61.243:5554/16745	5_up.exe			DLL-Handling	H:WINDOWSISystem32/Version.all H:\WINDOWS\system32\IMM32.DLL	
Trigger		ftp://anonymous:bin@192.168.	1.64:5554/16745_up.exe				H:\WINDOWS\WinSxSlx86_Microsoft.Windows.Common- H:\WINDOWS\system32\pstorec.dll	Controls_6595b64144ccf1df_6.0.260
MD5su	im:	1a2c0e6130850f8fd9b9b53094	413cd00				H:\WINDOWS\system32\ATL.DLL H:\EuTeAmo.DEU	
SHA51	2:	8e1e40dedb4aa57ae5c89a75	aca26a813ce5622e3710	49ddbc916552d1c00b48			H:IEuTeAmo.DE H:IWINDOWSIsystem32\uxtheme.dll	
File Ty	pe:	PE32 executable for MS Windo	ws (GUI) Intel 80386 32-b	it			H:\WINDOWS\system32\msctfime.ime H:\WINDOWS\system32\msctfime.ime	
Attacke	r IP:	1189625331					H:\WINDOWS\system32\WS2_32.DLL H:\WINDOWS\system32\netapi32.dll	
Victim	IP:	1089237505					H:\WINDOWS\system32\appHelp.dll H:\WINDOWS\system32\urimon.dll	
Filenar	ne:	16745_up.exe					H:\WINDOWS\system32\ieframe.dll H:\WINDOWS\system32\MSCTF.dll	
Countr	y:	US					New Files	
ISP:	Ī	AOL						
ASN:	Ī	1331						

THE HONEYNET PROJECT-

HonEeeBox Summary

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

Attacks					Google Map	Googe Earth	Sandbox Am	ti-Virus Graph	s PicViz H	leatmap Cut	tlefish		
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	Reserved	Unallocated	Public Data Network 14.0.0.028	HP	DEC	Ford Motor Company 19.0.0.07	troples Scenes Capabian 30.0.0.00	DDN-RVN	
2 20 Mar 2009	17:22:37 🚺 64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.204.183.126:7293/net				15.10.01.024	12 2.0.0/0			331335) 	
3 20 Mar 2009	17:22:37 🔯 87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	<u>creceive://87.175.58.187:4652</u>				3.37					
4 20 Mar 2009	17:22:37 🏾 🖲 127. 255. 255. 255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	<pre>creceive://211.200.220.64:3647</pre>		Unallocated	Xerox	AT&T	Apple	MTT	Unallocated	DTSA	
5 20 Mar 2009	17:22:37 📓 87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	<pre>creceive://87.17.73.69:43074</pre>			TO BOX	TALX L	T FILLER		28 5 8 Iv3		N 7 7 1
6 20 Mar 2009	17:22:37 📓 87.17.73.69	64.236.114.1	<u>11d31a4ebd7260193ffe8da9bb79156a</u>	<u>creceive://87.17.73.69:59800</u>									MUIT
7 20 Mar 2009	17:22:37 📕 118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.165.49.147:2866/ig	Torrol 2		Torrol 2	feb back between a farmer		DTCA	Cabla		
8 20 Mar 2009	17:22:37 📕 70.232.61.243	64.236.114.1	<u>1a2c0e6130850f8fd9b9b5309413cd00</u>	ftp://70.232.61.243:5554/16745_u	Tever2		Tevero	11.0.0.0/5	DTOU	DTOA	Cable	25.0 0.0/6	
9 20 Mar 2009	17:22:37 🚺 64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.204.183.126:7293/ne				r — 4			BOGNIG		
10 20 Mar 2009	17:22:37 🔯 87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	<u>creceive://87.175.58.187:4652</u>			TD1						
11 20 Mar 2009	17:22:37 . 127. 255. 255. 255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	<u>creceive://211.200.220.64:3647</u>	Unallocated	US Army	TRW	RFC1918	Unallocated	DSI-North	Unallocated	DISA	
12 20 Mar 2009	17:22:37 🔛 87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	<u>creceive://87.17.73.69:43074</u>			9.0.0.018					47.9 St. 2 P	
13 20 Mar 2009	17:22:37 🔤 87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	<pre>creceive://87.17.73.69:59800</pre>	1.47								
14 20 Mar 2009	17:22:37 📫 118. 165. 49. 147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	<u>ftp://a:a@118.165.49.147:2866/ig</u>		SITA	Merck and Co., Inc. 54.0.0.0/0	Cap Debis CCS	AT&T	Merit	Unallo	ocated	APNT('
15 20 Mar 2009	17:22:37 70.232.61.243	64.236.114.1	<u>1a2c0e6130850f8fd9b9b5309413cd00</u>	ftp://70.232.61.243:5554/16745_u	ADUTO	10/10/01/01			U 1.0.098		40 B -	4.422	
16 20 Mar 2009	17:22:37 64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.204.183.126:7293/net	APNIC								
17 20 Mar 2009	17:22:37 🔯 87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.58.187:4652	N. M. delay	τιςρς	DOD NTC			Halliburton	Unallocated	DQT	RTDE ARTN
18 20 Mar 2009	17:22:37 • 127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	<u>creceive://211.200.220.64:3647</u>	in the		55.0.0.0.0				39.0.0.0/0	ТОТ	
19 20 Mar 2009	17:22:37 87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73.69:43074	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1								
Attack Detail		M	55:	100051-200130	ΛΟΝ	ITC	Unallocated	decamper of Social January of SK	Unallocated	Interop	Eli Lilv	AfriNIC	
D.	6					TC		SL0.0.07		45.0.0.078	en n a iya	41.4.2.2.9	
Time	1236037531				19 14 10	Pol par							
0	64 336 44 44				ARTN	RTPF	Unallocated	Prudential		same take in of termsecon	Japan Inet	Unallocated	DTDE
Sensor.	04.230.114.1				TAINE IN	L L L		az.0.0.0/8			43.0.0.0/8	17 H T 5/K	
Download:	creceive://87.17.73.69:59800				North.		W. C. C. C.	S. W. S. M.			1.500		
Trigger:	creceive://87.17.73.69:59800											Reserved	
MD5sum:	11d31a4ebd7260193ffe8da9b	b79156a								170	Survey and	DV ISBARA	
SHA512:	8096d0ce1fcd9b279d55037bc	d67af05873b57b4ca796f	813a8449790a76e5c3a			AR	IN		APN		APNIC		
File Type:	PE32 executable for MS Windo	ows (GUI) Intel 80386 32-	bit				0.075		120.7	0. Bre	1040404.171	ADNITC	
Attacker IP:	1460750661				A State							AL NL C	
Victim IP:	1089237505					- 19 - 19 - 19 - 19 - 19 - 19 - 19 - 19	1999						
Filename:	index.html					RTPE	20 - C						
Country:	NZ				DTDT	L \ <u>H</u> <u>H</u> <u>H</u>		TNT		ITC	rr		
ISP:	Celestra NZ				KT BF		AR		AP	NTC	unallo	cated	
ASN:	99421					ARIN							
19792236	1999-92 (197												Various I
					and the second for								various n

— THE HONEYNET PROJECT—



- THE HONEYNET PROJECT[.]



н Ν Ξ J н Ν Y Т • R п С Т п 0 0

HonEeeBox Summary

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

Atta	icks				
ID	Time	Attacker IP	Victim IP	MD5sum	Download
1	20 Mar 2009 17:22:37	50.232.61.243	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://1:1088.204.18
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	8f4e8e3lfcdbf963579lab009defelb5	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://1:1088.204.18
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	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	10.232.61.243	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://1:1088.204.18
17	20 Mar 2009 17:22:37	🔯 87.175.58.187	H 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
14	4 Page 1 of 3	N 2 IP:	м	D5·	Rows 1 - 20 of 56



44 -	-1-	D - 4 - 11	
ma	CK.	Herall -	
uuu	un.	Dottan	

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



THE HONEYNET PROJECT-

onEeeBox Sun	nmary										
otal Attac	ks: 56	Total Sou	irce IPs: 6	Total Target IPs: 1	'otal MD5sums: 7	li da _{terra} lia					
Attacks						Google Map Googe Earth	Sandbox Anti-Virus G	raphs PicViz Heatmap	Cuttlefish		
D Time		Attacker IP	Victim IP	MD5sum	Download						
1 20 Mar 200	09 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243				165 215		
2 20 Mar 200	9 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.204.18		165,137 - 734		195,117 - 99	153.19 - 1	
3 20 Mar 200	9 17:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.5		194.8-1	195 241 - 1	195.1-7	193.111 - 40	
4 20 Mar 200	09 17:22:37	• 127. 255. 255. 255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.:	192122	-2 195.4-2 195.58-3	149.225 - 1 193.178 - 2			
5 20 Mar 200	09 17:22:37	🗱 87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73		107 248 - 2	195.218 - 143 134.155 -	a 193.85 2 a 19	195.205 - 1 3.8 - 910	
20 Mar 200	09 17:22:37	📓 87.17.73.69	64.236.114.1	<u>11d31a4ebd7260193ffe8da9bb79156a</u>	<u>creceive://87.17.73</u>		195.5 - 1		193.179-2	17-2	
20 Mar 200	09 17:22:37	📕 118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.165.4	2	195.1	01-49		193.11 - 226 193.138 - 2	
20 Mar 200	09 17:22:37	🦉 70.232.61.243	64.236.114.1	<u>1a2c0e6130850f8fd9b9b5309413cd00</u>	ftp://70.232.61.243			19916 - 2	193.243 - 2	195.49-5	29
20 Mar 200	09 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.204.18	<u>-</u>		151.2	5 151 54 - 1	529-2	R FA
0 20 Mar 200	09 17:22:37	87.175.58.187	64.236.114.1	<u>3875b6257d4d21d51ec13247ee4c1cdb</u>	<u>creceive://87.175.5</u>	<u>.</u>					
1 20 Mar 200	09 17:22:37	• 127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	<u>creceive://211.200.</u>	1	193.25	53.4		195.222-2	
2 20 Mar 200	09 17:22:37	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.17.73		1 TH	North Jea			MI Master
3 20 Mar 200	09 17:22:37	87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	creceive://87.17.73		relands	at Main	151 33-634		195.23
4 20 Mar 200	09 17:22:37	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.165.4		Filt	Publianc Nethe lands	193.207 - 25 Pal		
5 20 Mar 200	19 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243			- tetelgium I	Germatry	193 204 - 1	
6 20 Mar 200	19 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23†71ac2c5ab1192d	<u>ttp://1:1088.204.18</u>		Jersey	V-ALL Luxembourg	Biver 151.32 -		Ukraine
7 20 Mar 200	1917:22:37	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.5		The Real	- ALAKADAN	TTLL	Dovakia	11 1/23
8 20 Mar 200	19 17:22:37	• 127.255.255.255	ata 64.236.114.1	65455427002-002-002-00-0004070105	creceive://211.200.	193.153 - 1 18	93.152 - 2	France	erland	Hungary	And And
A Page	of 3	• • • P:	MC 04.230.114.1	15155457962C6958E609CD6167047256	Rows 1 - 20 of 56	Xara	N A VI	V THE	Slovenia	Romania	LA D
Attack Detail			/			X X may -		Short int	STOP VARS	10 Paralant	
D.	1							Monaco	San Marino Busniatar	d Herzegovina	Stal.
Cimo:	1225	5901100					And	ATTA CARACTER STORE	Italy	Montenegro	
Ronsor:	64.25	126 114 1					Way León		Holy See (Vatica)	Macedonia (FYROM)	15th
Download:	fm-1/2	70 222 61 242-6664/46746	UD OVO			193.194		ALL ALL	A H H H	Albania	-45
ownioad.	rtp:///	10.232.01.243.0004/10/40				Portugal				N Chron	
rigger:	πp://a	anonymous:bin@192.168.1	1.64:5554/16/45_up.exe	<i>i</i>			Sivissaî/thiza)		19	158 - 1 Greece	Aegean Sea
ID5sum:	1a2c	c0e6130850f8fd9b9b53094	413cd00			- Barris	THEODILINE A		Isola di Ustica Isola Lipari	Lefkada	Chies
SHA512:	8e1e	e40dedb4aa57ae5c89a75a	aca26a813ce5622e3710	49ddbc916552d1c00b48		Andalucia	A State	-	Isola Favignana	Zakynthös (Zante)	Athina Same
File Type:	PE32	2 executable for MS Windov	ws (GUI) Intel 80386 32-1	pit		The spin	El-lazaiz A (A	Injere)	© 2006 Basarsoff Sicilia (Sicily)	And And	S : 84
Attacker IP:	1189	9625331				(Tangler) Tanger		Augusta Augusta	2008)Európ #Jechnológies	470	1
/ictim IP:	1089	9237505									
ilename:	1674	45_up.exe				-					
Country:	US										
SP:	AOL										
ASN:	1331	1									

THE HONEYNET PROJECT-





HonEeeBox Summary

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

Attacks							Google	e Map	Googe Earth	Sandbox A	nti-Virus Graph	s PicViz	Heatmap Cuttlefish			
ID Time	Atta	acker IP	Victim IP	MD5sum	Download			2000 -					Classification -		count -	
1 20 Mar 20	09 17:22:37 📃	70.232.61.243	64.236.114.1	<u>1a2c0e6130850f8fd9b9b5309413cd00</u>	ftp://70.232.61.243:5554/16745_up.e	xe ^			1						count +	-
2 20 Mar 20	09 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.204.183.126:7293/netli	brary.exe							WORM/Allaple.Gen		14228	
3 20 Mar 20	09 17:22:37 🛛 🔯	87.175.58.187	64.236.114.1	<u>3875b6257d4d21d51ec13247ee4c1cdb</u>	<u>creceive://87.175.58.187:4652</u>			1600-		1			TR/Crypt.XPACK.Ger	٦	9021	
4 20 Mar 20	09 17:22:37 🔹	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.220.64:3647		â		1				TR/Crypt.NSPM.Gen		5059	
5 20 Mar 20	0917.22.37	87.17.73.69	GG 64.236.114.1	11 d21 = 4ebd72601 02ffe8d=0bb70156=	creceive://87.17.73.69:430/4		loe	1200-			1		WORM/Allaple.Dama	ged.Gen	2700	
7 20 Mar 20	09 17:22:37	118 165 49 147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a0118.165.49.147:2866/igrdf	dfds.com	Sou		1				W32/Virut N DR		2375	-
8 20 Mar 20	09 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745 up.e.	xe	funt	800-					WODWPhat 147456	27	1020	
9 20 Mar 20	09 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.183.126:7293/netli	brary.exe _	8						WORW/RDOL 14/430	.21	1030	-
10 20 Mar 20	09 17:22:37 🛛 🔯	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.58.187:4652			400			I MAN		WORM/Rbot.147456	.27]	1774	
11 20 Mar 20	09 17:22:37 🛛 🖲	127.255.255.255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	creceive://211.200.220.64:3647			400-	AV.	N N.	VIV I		W32/Virut.Gen		1550	
12 20 Mar 20	09 17:22:37 🛛 🎆	87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	<u>creceive://87.17.73.69:43074</u>				A MAA	M IM		~ ~	WORM/Rbot.50176.5	;	975	
13 20 Mar 20	09 17:22:37 🛛 🎆	87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	<pre>creceive://87.17.73.69:59800</pre>			0_1	19.00	04.00	18:00	00.55	W32/Virut W		975	
14 20 Mar 20	09 17:22:37 🛛 💼	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.165.49.147:2866/igxdf	dfds.com			272 23 24	25 26 27	28 29 30 31	1 2	TTOLTINGET		510	
15 20 Mar 20	09 17:22:37 📑	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.61.243:5554/16745_up.e	xe			MAY			JUN			R	0 (4)
16 20 Mar 20	09 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1@88.204.183.126:7293/netli	brary.exe			2008							
17 20 Mar 20	09 17:22:37 🔯	87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.175.58.187:4652			120			—					
18 20 Mar 20	0917:22:37	127.255.255.255	64.236.114.1	814e8e311cdb19635/91ab009de1e1b5	creceive://211.200.220.64:364/					I.		it al			FR (3739)	
19 20 Mar 20	1 of 3	1 87.17.73.69	MC 64.236.114.1	1515543/982C893ae809C0818/04/256	Creceive://8/.1/./3.69:430/4	ows 1 - 20 of 56	2 S			i. Illi	6 I II	In. I				
Attack Detail		• • •	1				ť(AS	90	1				II . II.			
ID:	3						LINO						Մ և սՈհ ՍՈհ է	DE (2694)	
Time:	12360037	748					0 t		1.11					,		
Sensor:	64,236,11	4.1					stino	60								
Download:	creceive://	/87.175.58.187:4652					ġ							TW (2314)	
Trigger:	creceive://	/87.175.58.187:4652						30								
MD5sum:	3875b625	57d4d21d51ec13247e	e4c1cdb											JF	° (2231)	
SHA512:	5e60dd30)2d73e64b2a4c7e3d7	e22b684028a6d5a719d	c7869891783f5f86e2cf3											CA (2036)	
File Type:	PE32 exec	cutable for MS Window	vs (GUI) Intel 80386 32-k	oit				0	21	5	20	5	20		11.74	704)
Attacker IP:	14711016	527							MAY	JUN	20	JUL	20		IL (1	(R (1
Victim IP:	10892375	505					1									
Filename:	index.html	1														
Country:	BR															
ISP:	Centrica Ir	nternet														
ASN:	3310															

н н п Ν п J п п 0 Ν Y Г Ξ R 0 С



HonEeeBox Summary

THE HONEYNET PROJECT-

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

Attacks						Google Map Googe Earth Sandbox Anti-Virus Graphs PicViz Heatmap Cuttlefish		
ID Tir	me	Attacker IP	Victim IP	MD5sum	Download	Timestamp	Source IP	Classification G
1 20) Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.6	N.		
2 20) Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	<u>ftp://l:1088.2</u>	22:35:50		
3 20) Mar 2009 17:22:37	🔯 87.175.58.187	64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	<pre>creceive://87.</pre>	22:13:10		
4 20) Mar 2009 17:22:37	• 127. 255. 255. 255	64.236.114.1	8f4e8e31fcdbf9635791ab009defe1b5	<pre>creceive://211</pre>	21,34,13		TR/Crypt.XPACK.Gen
5 20) Mar 2009 17:22:37	🎬 87.17.73.69	64.236.114.1	f5f55437982c893ae8b9cb8187d47256	creceive://87.			A A A
6 20) Mar 2009 17:22:37	📓 87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	<pre>creceive://87.</pre>	10.01.07		
7 20) Mar 2009 17:22:37	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	<u>ftp://a:a@118.</u>	19:21:07		
8 20) Mar 2009 17:22:37	50.232.61.243	64.236.114.1	<u>1a2c0e6130850f8fd9b9b5309413cd00</u>	ftp://70.232.6		74 M	
9 20) Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23f71ac2c5ab1192d	ftp://1:1088.2	17:31:14		WORM/Rhot 50176 51
10 20) Mar 2009 17:22:37	🔯 87.175.58.187	64.236.114.1	<u>3875b6257d4d21d51ec13247ee4c1cdb</u>	creceive://87.	16:50:58		WORM[RD0L30170.5]
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.			WODW/01-4 246784 17
13 20) Mar 2009 17:22:37	87.17.73.69	64.236.114.1	11d31a4ebd7260193ffe8da9bb79156a	creceive://87.	14:23:08		WORM/RDot.246784.17
14 20) Mar 2009 17:22:37	118.165.49.147	64.236.114.1	e8d4d8cde15ef310305955c943c0d1c2	ftp://a:a@118.	14107149		
15 20) Mar 2009 17:22:37	70.232.61.243	64.236.114.1	1a2c0e6130850f8fd9b9b5309413cd00	ftp://70.232.6	13:33:02		
16 20) Mar 2009 17:22:37	64.236.114.1	64.236.114.1	e399196c959235c23t71ac2c5ab1192d	<u>ttp://1:1088.2</u>	12:34:25		
17 20) Mar 2009 17:22:37	87.175.58.187	ata 64.236.114.1	3875b6257d4d21d51ec13247ee4c1cdb	creceive://87.			WORM/Rbot.147456.27
18 20	Mar 2009 17:22:37	127, 255, 255, 255	ata 64.236.114.1	8T4e8e31TC0DT9635/918D009deTe1D5	creceive://211	18:54:43		
19 20	Page 1 of 3	▶ ► 27.17.73.69	MD5	5:	Rows 1 - 20 of 56	10:45:02		
-Attack Detail								
ID:	9					08:26:45	91.12 800 896	W32/Virut.Gen
Time	123	5924337				TR/Crypt.XPACK.Gen]		
Sonsor	r 64.2	36.11/1				CH -	77.25.35.193	
Downle	n. 04.2	1.4 @00 004 102 106:7002	/notlibran: ovo			10 A		WORM/Rhot 147456 271
Downie	np.//	1.1@88.204.183.120.7293	/netlibrary.exe					MONINDULT414201211
ingger	т. п.р. <i>н</i>	1.1@88.204.183.126.7293	/netilprary.exe					
MD5su	im: e39	J19609592350231/1ac205	ab1192d			67/1/		
SHA51	2: d41	321a576642131e32645afc	:3d531dca5f6d4a09a76ac	10ce71a7d49021c6906				W32/Virut.W
File Typ	pe: PE3	2 executable for MS Windov	ws (GUI) Intel 80386 32-bi	t				
Attacke	er IP: 108	9237505				1111		
Victim I	IP: 108	9237505						
Filenar	me: netli	netlibrary.exe						
Country	y: FR							
ISP:	Vod	Vodafone FR						
ASN:	514	2						







PROJECT

HonEeeBox – Rapid Deployment of Many Distributed Low Interaction Malware Collectors

Any Questions?