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
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 Libcfg
- SQL logging
- IPv6 support
- SMB/CIFS protocol emulation for (unknown) RPC calls
- Generic shellcode detection via LibEmu
- Actions on shellcode profile (windows shell, file download) via LibEmu execution
Publish-subscribe generic data sharing

HP Generic Datafeeds

- Lukas
- Glastopf source
  - Publish Dorks/URLs
- Analysis machines
- Felix
- Binary sink
  - Subscribe binaries
  - Publish analysis
- Analysis source
- Mark
- Dionae source
  - Publish attacks/binaries
  - subscribe statistics
- Statistics sink
  - subscribe binaries
- David
- Attackinfo sink
  - subscribe attacks
- Binary sink
  - Honeebox Webinterface
Authkey bj3gn@hp1

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

The Authkey has access to the following channels:

<table>
<thead>
<tr>
<th>Channel</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>dionaea.dcerpcrequests</td>
<td>subscribe</td>
</tr>
<tr>
<td>dionaea.shellcodeprofies</td>
<td>subscribe</td>
</tr>
<tr>
<td>mwbinary.dionaea.sensorunique</td>
<td>subscribe</td>
</tr>
<tr>
<td>dionaea.capture</td>
<td>subscribe</td>
</tr>
</tbody>
</table>
pythonfeed.py --hosthpfreads.honeycloud.net -p 10000 -c
dionaeacapture -i your-sub-authkey-identifier -s your-pub-authkey-secret subscribe

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

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

pythonfeed.py --hosthpfreads.honeycloud.net -p 10000 -c
mwbinary.dionaea.sensorunique -i your-sub-authkey-identifier -s your-pub-authkey-secret subscribe
### Technical Details

<table>
<thead>
<tr>
<th>Analytic Number</th>
<th>Parent ID</th>
<th>Process ID</th>
<th>Filesize</th>
<th>MDS</th>
<th>Start Reason</th>
<th>Termination Reason</th>
<th>Start Time</th>
<th>Stop Time</th>
<th>Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1349</td>
<td>222720</td>
<td>fip:70.232.61.243</td>
<td>06/09/2011 00:00:00</td>
<td>NormalTermination</td>
<td>06/09/2011 00:04:15</td>
<td>06/09/2011 06:54:53</td>
<td>OK (CernAV)</td>
</tr>
</tbody>
</table>

### Scan Summary

- **Loaded DLLs**:
  - H:\Windows\system32\ntdll.dll
  - H:\Windows\system32\kernel32.dll
  - H:\Windows\system32\advapi32.dll
  - H:\Windows\system32\comctl32.dll
  - H:\Windows\system32\msvcrt.dll
  - H:\Windows\system32\kernel32.dll
  - H:\Windows\system32\ncrypt.dll
  - H:\Windows\system32\wsock32.dll
  - H:\Windows\system32\shlwapi.dll
  - H:\Windows\system32\user32.dll
  - H:\Windows\system32\advapi32.dll
  - H:\Windows\system32\OLEDDLL.dll
  - H:\Windows\system32\wsock32.dll
  - H:\Windows\system32\wininet.dll

- **New Files**:
  - H:\Windows\system32\ntdll.dll
  - H:\Windows\system32\kernel32.dll
  - H:\Windows\system32\advapi32.dll
  - H:\Windows\system32\comctl32.dll
  - H:\Windows\system32\msvcrt.dll
  - H:\Windows\system32\kernel32.dll
  - H:\Windows\system32\ncrypt.dll
  - H:\Windows\system32\wsock32.dll
  - H:\Windows\system32\shlwapi.dll
  - H:\Windows\system32\user32.dll
  - H:\Windows\system32\advapi32.dll
  - H:\Windows\system32\OLEDDLL.dll
  - H:\Windows\system32\wsock32.dll
  - H:\Windows\system32\wininet.dll

### DLL Handling

- PE32 executable for MS Windows (GUI) Intel 80386 32-bit

- **Attack Detail**:
  - ID: 15
  - Time: 1235891 109
  - Sensor: 64.236.114.1
  - MD5sum: 1a20e913086d0f9d0f0b650941c000

- **File Type**: PE32 executable for MS Windows (GUI) Intel 80386 32-bit

- **Attack IP**: 1189626331

- **Victim IP**: 1089373505

- **File Name**: 18745_up.exe

- **Country**: US

- **ISP**: AOL

- **ASN**: 1331
Activity Map

The Activity Map shows the count of IPs by geo.
David Watson (david@honeynet.org.uk)
HonEeeBox Future

- Splunk dashboard 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
Attacks Against Nepenthes Sensors

Hour: 6
Attacks: 12

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) ;-)

David Watson (david@honeynet.org.uk)
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 :-)

David Watson (david@honeynet.org.uk)
The Honeynet Project

HonEeeBox

http://www.honeynet.org

Any Questions?

David Watson  david@honeynet.org.uk