

The Honeyned P R O J E C T

HonEeeBox – Lessons Learned and Plan For 2011

Annual Workshop Private Day 22/03/11

The Honeynet project®

Speaker



David Watson (UK)

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





Global Distributed Honeynets (GDH1) (2006-2008)



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



http://www.honeynet.org/speaking/PacSec07_David_Watson_Global_Distributed_Honeynet.pdf David Watson (david@honeynet.org.uk)

н ο М П

тне HONEYNET PROJECT

GDH: Top Level Statistics

- 3 month steady state data collection period March – May 2007:
- > 122 GBytes pcap data collected
- > 730 million packets captured
- > 73 million Argus network flows
- > 301,200 unique source IP addresses
- > 672,800 brute force SSH attacks
- > 1680 unique malware samples
- 300 page GDH Phase One status report

David Watson (david@honeynet.org.uk)

EC ÷ П н 0 R 0 J

GDH: Sample Data Summaries 2



GDH: Nepenthes Malware Analysis



http://www.honeynet.org/speaking/PacSec07_David_Watson_Global_Distributed_Honeynet.pdf David Watson (david@honeynet.org.uk)



http://www.honeynet.org/speaking/PacSec07 David Watson Global Distributed Honeynet.pdf David Watson (david@honeynet.org.uk)





Global Distributed Honeynets (GDH2) (2008-2009)

Motivation

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

BUT

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





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

Motivation

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

Proposed Approach

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

Embedded Nepenthes

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



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!

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

HonEeeBox v1

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

— THE HONEYNET PROJECT—

| 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 |
| | Esperanto |
| | <go back=""></go> |

. Tab> moves between items; <Space> selects; <Enter> activates buttons



HonEeeBox Participation

- 1+ public static IP addresses (more is better)
- 1+ networked x86 PC/server(s) to boot ISO or USB key or space to host HonEeeBox sensor hardware
- Be willing to submit basic attack data (SRC IP, download URL, MD5, timestamp, binary, etc)
- Be willing to share collected malware samples with all participants and project sponsors
- Submissions from existing Nepenthes sensors
- Tried to find sponsorship (NIC \$40k, Symantec \$10k)
- Potential funding for additional sensor deployment
 - Regional, CERT, industry, academic, etc

Honeeebox --

About Honeeebox

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

Using Honeeebox

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

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

Subscribing to Honeeebox

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

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

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

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

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

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

HonEeeBox Operational Blog

Discussion about HonEeeBox operational events and data analysis

HonEeeBox Sensor Added (HK002)

HonEeeBox Sensor Added (NO002) +

Good day for sensor deployments and attack data

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

Attacks 1409 and 1410 = HK001.

Attacks 1436 to 1438 = FR001

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

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

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

| т | H | E | Н | 0 | Ν | E | Y | Ν | E | Т | ŀ | 8 C |) . |) E | E C | Τ - | | | |
|-----------|---|---|---|---|---|---|---|---|---|---|---|-----|------|-----|-------|---------|---|----------|--------|
| 🜟 isotoma | | | | | | | | | | | | | | | | | | | la |
| | | | | | | | | | | | | W | /iki | Tim | eline | Roadmar | ρ | Browse 5 | Source |

Honeeebox Sensors

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

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

- · A live CD sensor
- A live CD sensor with persistence (via an additional USB or HDD)
- A live USB sensor
- A live USB sensor with persistence (to the USB device)
- A pre-built virtual appliance
- A means to install the same disk image to a local hard disk and make it permanently bootable
- A means to install the same disk image to a local media device (such as an SHDC card) and make it permanently, for solid state operation and people not

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

Testing Pre-built Sensor Images

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

HoneeeboxSensorTesting

Building A Sensor Image

Honeeebox-dev --

About Honeeebox-dev

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

Using Honeeebox-dev

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

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

Subscribing to Honeeebox-dev

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

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

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

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

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

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



Prototype HonEeeBox v1 UI and Basic Example Visualisations

ТНЕ НО**ЛЕУЛЕТ Р**КОЈЕСТ-

| 🙆 HonEeeBox Temporary Home Page - Windows Internet Explorer | | | |
|--|------------------------|---|------------|
| COO V //honeeebox.net/ | Certificate Error | 🗟 😽 🗙 🔀 Google | P - |
| <u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp | | | |
| 🖕 Favorites 🛛 👍 🙋 Free Hotmail 🖉 Web Slice Gallery 🔻 🏀 Suggested Sites 👻 | | | |
| HonEeeBox Temporary Home Page | | 🏠 🔹 🔂 👻 🖃 🖶 👻 Page 🔹 Safety 🕶 Too | ls • 🕡 • 👋 |
| HonEeeBox Temporary Home Pa | ge | | × |
| Welcome to what will soon be the front end web UI for the HonEeeBox syst | em. For now, be dazzle | ed by it's temporary visual splendor! ;-) | |

Getting started:

Done

- Operational Blog. Operational events and data analysis discussions will happen here, and you can follow it as an secure RSS feed.
- Basic Data Grid. A simple demo Extjs based data grid that presents live sensor submission data in a pagable, searchable grid.
- Demo UI #1. An example of what one possible HonEeeBox demo UI might look like, with some elements of functionality still only mocked up.
- Basic Data Grid #2. A refactored clone of the monolithic Basic Data Grid #1 with some more features wired up (and perhaps a few new bugs too!).
- Demo UI #2. A refactored clone of the monolithic Demo UI #1 with some more features wired up (and perhaps a few new bugs too!).
- <u>Participant mailing list</u>, for discussing all things HonEeeBox and data analysis related.
- <u>HonEeeBox-Deployment-QuickStart.pdf</u>. Quick start instructions for setting up your HonEeeBox sensor.
- <u>HonEeeBox-Instructions.pdf</u>. Detailed instructions for setting up your HonEeeBox sensor.

If you require any further information of assistance, please contact mailto:honeeebox@honeynet.org

David Watson (david@honeynet.org.uk)

🖓 🗸 🔍 100

의 Internet

| | HUNE | I N | | РК | UJE | <u>с</u> Г- | |
|--|------------------------------|--------------------|---------------|-----------------|---------------|------------------|-------------------|
| 😻 Simple HonEeeBox Schema1 Data | Grid - Mozilla Firefox | | | | | | |
| <u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmark | s <u>T</u> ools <u>H</u> elp | | | | | | 11 |
| C × 6 | https://honeeebox.net/demo_s | schema 1/grid.html | | | ☆ · | G - Google | P |
| 🔎 Most Visited 🌸 Getting Started 🔊 | Latest Headlines | | | | | | |
| Simple HonEeeBox Schema1 Data G | rid | | | | | | |
| Sensor Lastseen Sensor Counts | seen Attacker IP | Attacker CCS A | Attacker CCL | Attacker Region | Attacker City | Attacker ISP | Attacker Latitude |
| 15 Sep 2009 23:51:14 708 | 82.233.140.134 | FR F | RANCE | PROVENCE-ALPE | MARTIGUES | PROXAD / FREE 5 | 43.4000015259 |
| 15 Sep 2009 23:51:14 708 | 82.233.179.228 | FR F | RANCE | ILE-DE-FRANCE | PARIS | PROXAD / FREE S | 48.8541984558 |
| 15 Sep 2009 23:51:14 708 | 82.236.249.239 | FR F | RANCE | PROVENCE-ALPE | NICE | PROXAD / FREE S | 43.7000007629 |
| 15 Sep 2009 23:51:14 708 | 82.236.249.239 | FR F | RANCE | PROVENCE-ALPE | NICE | PROXAD / FREE S | 43.7000007629 |
| 15 Sep 2009 23:51:14 708 | 82.255.241.198 | FR F | RANCE | PROVENCE-ALPE | NICE | PROXAD / FREE \$ | 43.7000007629 |
| 15 Sep 2009 23:51:14 708 | 200.231.59.9 | BR B | RAZIL | - | - | COMITE GESTOR | -22.8999996185 |
| 15 Sep 2009 23:51:14 708 | 82.226.133.77 | FR F | RANCE | PROVENCE-ALPE | NICE | PROXAD / FREE S | 43.7000007629 |
| 15 Sep 2009 23:51:14 708 | 82.240.11.44 | FR F | RANCE | PROVENCE-ALPE | NICE | PROXAD / FREE 5 | 43.7000007629 |
| 15 Sep 2009 23:51:14 708 | 209.149.4.189 | us u | INITED STATES | GEORGIA | RANGER | BELLSOUTH.NET | 34.5363006592 |
| 15 Sep 2009 23:51:14 708 | 67.159.61.68 | US U | INITED STATES | ILLINOIS | CHICAGO | FDC SERVERS.NI | 41.8650016785 |
| 15 Sep 2009 23:51:14 708 | 82.239.75.103 | FR F | RANCE | PROVENCE-ALPE | NICE | PROXAD / FREE 5 | 43.7000007629 |
| 15 Sep 2009 23:51:14 708 | 69.162.79.197 | US U | INITED STATES | CALIFORNIA | RIALTO | ADELPHIA | 34.1341018677 |
| 15 Sep 2009 23:51:14 708 | 82.212.46.114 | DE G | GERMANY | BADEN-WURTTEI | REUTLINGEN | KABEL BADEN-W | 48.483001709 |
| 15 Sep 2009 23:51:14 708 | 82.239.127.108 | FR F | RANCE | PROVENCE-ALPE | NICE | PROXAD / FREE 5 | 43.7000007629 |
| 15 Sep 2009 23:51:14 708 | 82.232.241.183 | FR F | RANCE | PROVENCE-ALPE | NICE | PROXAD / FREE 5 | 43.7000007629 |
| 15 Sep 2009 23:51:14 708 | 82.238.247.185 | FR F | RANCE | PROVENCE-ALPE | NICE | PROXAD / FREE 5 | 43.7000007629 |
| 15 Sep 2009 23:51:14 708 | 82.66.123.243 | FR F | RANCE | ILE-DE-FRANCE | PARIS | PROXAD / FREE 5 | 48.8541984558 |
| 15 Sep 2009 23:51:14 708 | 82.171.37.99 | NL N | IETHERLANDS | NOORD-HOLLAN | AMSTERDAM | WOL | 52.3499984741 |
| 15 Sep 2009 23:51:14 708 | 1 82.128.255.141 | FI FI | INLAND | OULUN LAANI | OULU | OULU TELEPHON | 65.016998291 |
| 15 Sep 2009 23:51:14 708 | 82.239.81.250 | FR F | RANCE | ALSACE | STRASBOURG | PROXAD / FREE 5 | 48.5830001831 |
| | | | | | | | |
| | Sensor CCS | ▼ . | = FR | | | | |
| | | | | | | | ▼ ▶ |
| Done | | | | | hone | eebox.net 🔒 S | Tor Disabled |

THE HONEYNET PROJECT

Example HonEeeBox Reporting Interface using Ext-J5 - Mozilla Firefox

<u>Eile Edit View Higtory Bookmarks Tools Help</u>

- C 🗙 🏠 📄 https://honeeebox.net/demo_schema1/

ዾ Most Visited 🏾 🗫 Getting Started 🔊 Latest Headlines

Attack Summary Panel

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

| D Mindate P Votin P Udsam Devided 135 156 160 151 152 150 | Attack Browser | | | | | « | Google Maps | Google Earth Virustotal | Anti-Virus San | dbox Graphs | PicViz Heatmap | Cuttlefish | |
|---|----------------------|--|--------------------------|----------------------------------|--|-----------------------|--------------|-------------------------|---------------------|-----------------------|------------------------------|----------------|--|
| 1381 00 02009 149-47 iiii 00, 1.7, 7, 2.28 iiiii 00, 1.7, 7, 2.28 iiiiii 00, 1.7, 7, 2.28 iiiiiii 00, 1.7, 7, 2.28 iiiiii 00, 1.7, 7, 2.28 iiiiii 00, 1.7, 7, 2.28 iiiiiii 00, 1.7, 7, 2.28 iiiiiii 00, 1.7, 7, 2.28 iiiiii 00, 1.7, 7, 2.28 iiiiii 00, 1.7, 7, 2.28 iiiiii 00, 1.7, 7, 2.28 iiiii 00, 1.7, 7, 2.28 iiiiii 00, 1.8, 1.8, 2.7, 7, 2.8, 2.8, 2.8 iiiiii 00, 1.8, 1.8, 2.7, 2.8, 2.8 iiiiiiii 10, 1.7, 7, 2.28 iiiiii 10, 1.7, 7, 2.28 iiiiii 10, 1.8, 2.7, 2.8, 2.8 iiiiiiiiii 10, 1.8, 2.7, 2.8, 2.8, 2.8 iiiiii 10, 1.8, 2.7, 2.8, 2.8 iiiiii 10, 1.8, 2.7, 2.8, 2.8 iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii | ID Time | Attacker IP | Victim IP | MD5sum | Download | | | | | | Non | Map | Satellite Hybrid Terrain |
| 1382 00 002000 15102 0 0 15102 0 150 | 3381 03 Oct 2009 14 | 49:47 80.41.76.228 | 80.2 | fd28c5e1c38caa35bf5e1987e6167f4c | tftp://80.41.76.228:69/ssms.exe | | < 🕫 >) | | | | to the | NY R | |
| 1338 00 00 2009 1713 57 121.18.1 152.168 22.268 27.2001bc330204656437_40265429 1750//7.1.51.10.56//mm.ess 1338 00 00 2009 1730 56 10.13.0.6.4.4.192 120.264 150.0.6.4.4.192 120.264 150.0.6.4.4.192 120.264 150.0.6.4.4.192 120.264 150.0.6.4.4.192 120.264 150.0.6.4.1.92 150.0.6.4.1.92 150.0.6.4.1.92 150.0.6.4.1.92 150.0.6.4.1.92 150.0.6.4.1.92 150.0.6.4.1.92 150.0.6.1.0.1.0.6.4.1.92 150.0.6.1.0.1.0.6.4.1.92 150.0.6.1.0.1.0.6.4.1.92 150.0.6.1.0.1.0.6.1.0.1.0.6.4.1.92 150.0.6.1.0.1.0.6.4.1.92 150.0.6.1.0.1.0.6.1.0.1.0.6.4.1.92 120.264 150.0.1.1.2.0.0.2.4.1.92 150.0.1.1.2.0.0.2.4.1.92 150.0.1.1.2.0.2.1.6.9.1.0.6.1.0.1.0.6.1.0.1.0.6.1.0.1.0.6.1.0.1.0 | 3382 03 Oct 2009 15 | 19:32 🏧 88.8.235.161 | 88.9 | c636db42a58de90f6e2f62484bc935f9 | ftp://1:1000.0.235.161:25032/runs.exe | | \checkmark | | | Berg | ien State | 1011 | Tu Tu |
| 338 60 00 d2009 173036 ■ 00.130.64.149 ■ 00.2 <u>Principalizability according to the principality accordity accordity accordity according to the princity acco</u> | 3383 03 Oct 2009 17 | 13:57 📕 71.1.81.9 | 192.168 | 2fa0e36b36382b74e6e6a437ad664a80 | tftp://71.1.81.9:69/ssms.exe | | (+) | | | | | 0 | Uppsala Norrtälle |
| 3356 00 od 2000 1011115 20.02 Phaboffaddfe4030011abb1982e9584 1ftp://20.144.33.99/ass.exe 3386 00 od 2000 103211 80.144.39.99 80.12 1d09448ad2360bas8b97584 1ftp://20.144.33.99/ass.exe 3386 00 od 2008 103211 80.144.39.99 80.127.022 2227fbbc711724222642440764bs 1ftp://20.136.123.023/159/asss.exe 3386 00 od 2008 10324.40 80.127.022 80.02 4556450/c2385 1ftp://20.136.123.023/asst.exe 3386 00 od 2008 10324.40 80.127.228 80.02 6556450/c2385 1ftp://20.148.127.2283/asst.exe 3396 00 od 2008 20 859 80.62.148.13 90.147.328 97.2001bc338ad48ad37a 070re404bb2 1ftp://20.136.127.2283/asst.exe 3396 00 od 2008 20 859 80.62.148.13 90.147.328 90.22 1ftp://20.148.127.2283/asst.exe 3396 00 od 2008 20 859 80.62.148.13 90.147.3283 90.22 1ftp://20.148.127.2283/asst.exe 3396 00 od 2008 2136 66 88.16.132.7 1ftp://20.148.127.2283/asst.exe 1ftp://20.148.127.2283/asst.exe 3396 00 od 2008 2136 66 88.16.108.214 80.127.228 80.166.108.214 80.127.228 1ftp://20.148.127.2283/asst.exe 3396 00 od 2008 20135 80.56.106.214 80.22 1ftp://20.147.33.238.227.57/asst.exe | 3384 03 Oct 2009 17 | 30:36 🔳 80.130.64.149 | 80.2 | 697f001bc330ab483d77a707cd40c8d9 | tftp://80.130.64.149:69/ssms.exe | | Ţ | | | 2 | AT NO | Englandad of | Caristad Vasteras |
| 1326 03 Oct 2009 18.2:11 0.144.38.99 0.0.2 1409845842154094581180bes8cb750a 1ftp://80.114.38.95/sms.exe 3387 03 Oct 2009 18.5:40 0.0.2 222878bc7115742202652444764bes 1ftp://80.114.40.244.159.159/sms.exe 3387 03 Oct 2009 18.5:40 0.0.2 establic 456c9340778 707c440c842 1ftp://80.151.128.15617/rxtindgrm 3388 03 Oct 2009 20.859 0.0.2.165.53 0.0.2 ftab027285704760be84 1ftp://80.85.105.120/sms.exe 3390 03 Oct 2009 20.859 0.0.6.127 222878bc721572422026724477dbe8 1ftp://80.85.105.120/sms.exe 3391 03 Oct 2009 20.859 0.0.6.127.228 0.0.55.126 0.0.2 fts://20.26.127.228/sms.exe 3391 03 Oct 2009 20.1594 0.0.55.126 0.0.2 fts://20.26.127.228/sms.exe fts://20.26.127.228/sms.exe 3393 03 Oct 2009 21.169 0.0.2 fts://20.26.127.228/sms.exe fts://20.26.127.228/sms.exe 0.0.6.127.228/sms.exe 3393 03 Oct 2009 21.169 0.0.2 fts://20.26.12.17.292/sms.exe 0.0.6.127.228/sms.exe 0.0.6.127.228/sms.exe 3393 03 Oct 2009 21.169 0.0.2 fts://20.26.71.15.28.127.228/sms.exe 0.0.6.127.228/sms.exe 0.0.6.127.228/sms.exe 3393 04 Oct 2009 21.169 0.0.2 fts:0.64107738204202570404554156954594776240004553127776242020657244 | 3385 03 Oct 2009 18 | 11:58 🔚 80.62.34.192 | 80.2 | 98eb0fdadf8a403c013a8b1882ec986d | tftp://80.62.34.192:69/ssms.exe | | - | | e li | Star | anger 1 | ALL AL | Orebro Sodertalje |
| 337 03 Oct 2009 138.60 0 0 0.131.240.24 0 0.2 1 <u>3228288-071357241226262744764888</u> <u>trtp://80.131.240.234 (27147846888)</u> <u>trtp://80.151/rztladgem</u> 3386 03 Oct 2009 128.66 0 0.2 1.65 3 0 0.2 (351.65 3 0 0.2 (357781.465628407032 bitm://80.166.120/sms.exe 3390 03 Oct 2009 20.65 0 0 0.6 2.1.65 3 0 0.2 (351.65 1.2712415742226262744764888) trtp://80.55 1.06 1.20/sms.exe 3390 03 Oct 2009 20.95 0 0 0.6 2.1.65 3 0 0.2 (351.65 1.2712474876888) trtp://80.55 1.06 1.20/sms.exe 3390 03 Oct 2009 20.95 0 0 0.6 2.1.65 3 0 0.2 (351.65 1.271241574422264264474676888) trtp://80.55 1.06 1.20/sms.exe 3391 03 Oct 2009 20.95 0 0 0.6 2.1.65 3 0 0.2 (351.65 1.27124744768888) trtp://80.55 1.06 1.20/sms.exe 3390 03 Oct 2009 20.95 0 0 0.5 1.05 1.0 0 2.227781874472628624484893552 trtp://80.47.43.739 80.2 (55805438265926 trtp://11888.26.131.7:9947/tutus.exe 3396 03 Oct 2009 20.95 0 0 0.5 1.05 1.0 0 2.22778187447262862444766888 trtp://10.55 1.05 1.16/sms.exe 3396 03 Oct 2009 20.95 0 0 0.5 1.05 1.0 0 2.227781874472689555 trtp://10.131.233.227769/sms.exe 3396 03 Oct 2009 08.098 0 0 0.22 c.7.15 .338 0 2.20 c.7.15 .338 0.216659565 trtp://10.131.233.227769/sms.exe 3397 04 Oct 2009 08.098 0 0 0.22 c.7.15 .338 0 2.20 c.7.15 .338 0.21665958 trtp://10.131.233.227769/sms.exe 3397 04 Oct 2009 08.098 0 0 0.22 c.7.15 .338 0 2.20 c.7.15 .338 0.21665958 trtp://10.110.90.59/sms.exe 3396 04 Oct 2009 08.098 0 0 0 0.22 c.7.15 .338 0 2.20 c.7.15 .338 0.21665958 trtp://10.111.233.2277 69/sms.exe 3397 04 Oct 2009 08.098 0 0 0 0.22 c.7.15 .338 0 2.20 c.7.15 .338 0.21665958 trtp://10.111.09.59/sms.exe 3398 04 Oct 2009 08.098 0 0 0 0.22 c.7.15 .338 0 2.20 c.7.15 .338 0.21665958 trtp://10.111.09.059/sms.exe 3398 04 Oct 2009 08.0130 0 0 0.20 c.7.15 .338 0 0 | 3386 03 Oct 2009 18 | 32:11 📕 80.144.39.99 | 80.2 | 14a09a48ad23fe0ea5a180bee8cb750a | tftp://80.144.39.99/ssms.exe | | | A 2000 | Ĩ | | Value and | Uddevalla | Skövde |
| 338 03 Oct 2009 193.44 B0.142.382.168 B0.2 ##55/d10/c23965/7314/c10/c2365/7314/c10/c2365/7414/c10/c2365/7776556551111/c1/c2365/777655655111261/c10/c2365/777655655111261/c | 3387 03 Oct 2009 18 | 59:00 📕 80.131.240.234 | 80.2 | 3228f8bc721572422c268f244476dbb8 | tftp://80.131.240.234:69/ssms.exe | | | | | / | • | N | Vastervik Cotland |
| 338 03 Oct 2009 20 06 59 0.0.2 597 00 01 b83 04 77 70 7c 44 00 B49 5 f 5 p 1// 0.62.169.53 169 / sams.exe 338 03 Oct 2009 20 1944 0.0.8.1.06.1.20 0.0.2 597 00 01 b83 04 77 70 7c 44 00 B49 5 f 5 p 1// 10.62.169.53 169 / sams.exe 339 03 Oct 2009 20 1930 0 80.2.2 5228 5 bb 71 5 7 242 22 6 5 85.106.120 / sams.exe 5 f 5 p 1// 11.198.50.127.228 / sams.exe 5 f 5 p 1// 11.198.50.127.228 / sams.exe 339 03 Oct 2009 21 340 0 80.2.2 5228 5 ba 105.216 (sams.exe) 5 f 5 p 1// 11.198.50.216 / sams.exe 5 f 5 p 1// 11.198.50.216 / sams.exe 339 03 Oct 2009 21 344.3 80.0.47.43.79 80.2 5 f 5 p 1// 11.198.50.216 / sams.exe 5 f 5 p 1// 11.198.50.216 / sams.exe 339 03 Oct 2009 21 340 0 80.5105.216 80.2 5 p 1/ 11.198.50.216 / sams.exe 5 p 1/ 11.198.30.277 (sp / sams.exe 339 03 Oct 2009 20 313 0 80.85.105.216 80.2 5 p 1/ 10.532.82 f 15 p 2// 80.85.105.216 / sams.exe 5 p 1/ 11.198.30.277 (sp / sams.exe 5 p 1/ 11.198.133.227 (sp / sams.exe 5 p 1/ 11.198.133.227 (sp / sams.exe 5 p 1/ 10.50 / sp / sams.exe 5 | 3388 03 Oct 2009 19 | 36:48 🔳 80.136.238.168 | 80.2 | ea55dd10c429dc57041e465c834b7089 | blink://80.136.238.168:51617/rxLndg== | | | N. C | Aberdeen | | | Göteborg O Bo | /as Jönköping |
| 3380 03 Od 2008 201904 8 0.85.106.120 90.2 f4200f78184fb166b9332238ac5522 tfp://80.85.106.120/smms.axe 3381 03 Od 2008 201904 8 0.25.106.120 32228bc72157242248f24447dbb8 tfp://80.35.137.228 xmm.axe 3392 03 Od 2008 21430 8 0.26.131.7 8 8.26.131. | 3389 03 Oct 2009 20 | 06:59 80.62.169.53 | 80.2 | 697f001bc330ab483d77a707cd40c8d9 | tftp://80.62.169.53:69/ssms.exe | | | THE STATE | ^ | | | alborg Varberg | Kalmar |
| 3391 03 Od 2000 2015355 80 04 2000 2015355 80 .36 .127 .228 90 .2 822856b4228584005625624244476dbbs 157b 1/111882.26 .131 .7 138 88.9 82385 03 Od 2000 213986 88 .26 .131 .7 138 88.9 82385 03 Od 2000 213986 88 .26 .131 .7 138 88.9 82385 04 0242085204568165ba4802D1 157b 1/111882.26 .131 .7 13942/runs .exe 15385 04 0200 220335 80 .25 .152 .216 30.2 1528552 .2202569244176dbbs 157b 1/2422 202667244476dbbs 157b 1/242 202667244476dbbs 157b 1/242 202667244476dbbs 157b 1/242 202667244476dbbs 157b 1/242 202676724476dbbs 15b 1/242 202676724476dbbs 15b 1/242 202676724476dbbs 15b 1/242 202676724476dbbs 15b 1/10 .90 659 98ms .exe 100 04 0d 2009 08:10.03 2022 .6 1.15 .238 2022 .4 7250449777048e1660026936938e195 29 100 /yCHTfAwe 11b 1/2/202 .67 .15 .238 1202 .4 750449777048e1660026936938e195 29 100 /yCHTfAwe 13389 04 0d 22009 08:10.33 80 .131 .233 .227 .28 .01 .20 .25 .115 /s man .exe 100 04 0d 2009 08:10.33 80 .131 .233 .25 .115 /s man .exe 100 04 0d 2009 08:10.37 11, 11 .10 .90 659 /smm .exe 11b 1/2/20 .26 .71 .15 .238 .20 .26 .71 .5 .238 .20 .26 .71 .5 .238 .20 .26 .71 .5 .238 .20 .26 .71 .5 .238 .20 .26 .71 .5 .238 .20 .26 .71 .5 .238 .20 .20 .4 .45 .20 .46 .47 .47 .40 .47 .40 .47 .40 .47 .40 .47 .40 .47 .40 .47 .40 .47 .40 .47 .40 .47 .40 .47 .40 | 3390 03 Oct 2009 20 | 19:04 📕 80.85.106.120 | 80.2 | f4a200f7818dfb166b9a3d238ac55a2d | tftp://80.85.106.120/ssms.exe | | - | | hurah | / / | | vinus | Haimstadi, Liepäja |
| 332 03 04 2009 21:40:0 88.2.6.1:1.7 88.9.9 <u>ed364428269264264264568595 fp://1:1982.26.1:17; 1992.2rung.sxe</u> <u>bf3855246203E630465165ba4602b1</u> ±ftp://80.47.43.79.2942.rung.sxe <u>bf3855246203E630465165ba4602b1</u> ±ftp://80.47.43.79.2942.rung.sxe <u>bf3855246203E630465165ba4602b1</u> ±ftp://80.47.43.79.2942.rung.sxe <u>bf3855246203E630465165ba4602b1</u> ±ftp://80.47.43.79.2942.rung.sxe <u>bf3855246203E630466155a</u> ±ftp://80.131.233.227 <u>bf3855246203E630466554</u> ±ftp://80.131.233.227 <u>bf3855246203E630465554</u> ±ftp://80.131.233.227 <u>bf3855246203E630465554</u> ±ftp://80.131.233.227 <u>bf3855246203E630465554</u> ±ftp://80.131.233.227 <u>bf3855246203E630467625621457444764b55554</u> ±ftp://80.131.233.227 <u>bf385524620256314476425611654586555</u> ±ftp://70.15.110.90.197 <u>bf38552462025636497a2562655115654586555</u> ±ftp://71.52.381:20160/yCHTfAw= <u>bf38552462025057046614677764566561447267664</u> ±ftp://71.53.110.90.95(<i>bf38mm.sxe</i> <u>bf38552462025057046614677764566561447267664</u> ±ftp://71.53.110.90.55.115 = 80.2 <u>af584447267664 ±ftp://71.53.110.90.55.115 sman.sxe</u> <u>bf38552462025704664476767664</u> ±ftp://71.133.95.115 sman.sxe <u>bf385564472625651776756565511254</u> ±ftp://71.133.95.115 sman.sxe <u>bf3855644726767665656351254</u> ±ftp://71.133.95.115 sman.sxe <u>bf38556474746476777655656511254</u> ±ftp://11.1988.134.29.250.177838/chosts.exe <u>bf38556474766777655656511254</u> ±ftp://11.1988.134.29.250.177838/chosts.exe <u>bf38556474766777655656511254</u> ±ftp://11.1988.134.29.250.177838/chosts.exe <u>bf385647476476777655656511254</u> ±ftp://11.1 | 3391 03 Oct 2009 20 | 53:55 💶 80.36.127.228 | 80.2 | 3228f8bc721572422c268f244476dbb8 | tftp://80.36.127.228/ssms.exe | | - | | N | | | Københ | avn Kristianstad Klapeda |
| 3333 03 Od 2000 214433 iii 80.47.43.79 | 3392 03 Oct 2009 21 | 39:06 🚾 88.26.131.7 | 88.9 | c636db42a58de90f6e2f62484bc935f9 | ftp://1:1088.26.131.7:9942/runs.exe | | | Londonderry / Glasgow | United | | | enmark | 🎅 🔪 - La Al |
| 334 03 Oct 2008 22:03.5 8 0.85.105.216 9 0.2 fcab6c917b2a3302020e2194c865fa tftp://80.85.105.216/sams.exe 338 04 Oct 2008 06:10.8 = 0.131.283.227 = 0.2 322287bc721572422c268244476dbb8 tftp://80.131.383.227:65/sams.exe Dubin Petero 5 'bin | 3393 03 Oct 2009 21 | 44:33 80.47.43.79 | 80.2 | bf3e95a24e203f680465e165ba4a02b1 | tftp://80.47.43.79/ssms.exe | | | Belfast 🚺 K | ingdom o | | | | Słupsk Gdańsk |
| 3385 04 Oct 2000 06:110.0 B0.131.233.227 B0.2 32225bcr211572422582244756bb8 tftp://20.131.233.227;69/smms.exe 3385 04 Oct 2009 06:09:00 2.02. a72bicb332ea7bfddfe25c1f69459655 11nk://202.67.19.238 23105/VCHT7Ame 3387 04 Oct 2009 06:09:00 2.02. a72bicb332ea7bfddfe25c1f69459655 11nk://202.67.19.238 23105/VCHT7Ame 3387 04 Oct 2009 08:01:0.37 T.15.1.10.90 592.165 tttk://202.67.19.238 tttk://202.67.19.238 Tttp:///0.51.10.90:69/smms.exe 3389 04 Oct 2009 08:10.37 T.15.1.10.90 592.165 tttk://202.67.19.238 tttk://202.67.19.238 Tttp:///1.10.90:69/smms.exe 3389 04 Oct 2009 08:10.37 T.15.1.10.90:69/smms.exe tttp:///1.10.90:69/smms.exe ttttr://10.0000/smms/me Dubin Pretion 0 Amsterdam Pretain Vision Vis | 3394 03 Oct 2009 22 | 03:35 📕 80.85.105.216 | 80.2 | fcab6c9d17b2a3330f20ee2194c869fa | tftp://80.85.105.216/ssms.exe | | | Isle offan | eeds-u.a | | | Restock | Kastalin Exam Olether |
| 3386 04 0d 2009 08:00 05 202. c7.15.288 202. ar22bib332ea7bfadfe2561f6345865 1ink://202. c7.15.282 20160/yCHTfAme 3387 04 0d 2009 08:00 05 202. c7.15.288 202. c7.15.288 202. c7.15.288 1ink://202. c7.15.288 | 3395 04 Oct 2009 06 | 11:08 🔳 80.131.233.227 | 80.2 | 3228f8bc721572422c268f244476dbb8 | tftp://80.131.233.227:69/ssms.exe | | | Galway Dublin Prest | ton O O | / | | Hamburg ST | rzacin G Budassaan Grudziadz |
| 3387 04 Oct 2009 08:10.37 12.168 df51e5310ef609e908a6b487a28ac068 ttp://1.51.110.90:69/smms.exe 3387 04 Oct 2009 08:10.37 12.168 df51e5310ef609e908a6b487a28ac068 ttp://1.51.110.90:69/smms.exe 3388 04 Oct 2009 08:10.37 202. 67.19.288 202. 4f50ef4f777bde16a0263f3b981bb 11hk://202. 67.19.288:39016/+8kn/A= 3389 04 Oct 2009 08:35:2 8.0.130.95.115 8.0.2 2269d462eb2bDb70d5e64dcd7e67ecd ttp://0.130.95.115/smms.exe 3400 04 Oct 2009 08:55:3 8.8.134.29.250 18.8.9 e23d9a57aef09863767765f6665112f4 tp://1.1188.134.29.250:17838/chosts.exe 14 Image: Comparing | 3396 04 Oct 2009 08 | 09:08 🔍 202.67.19.238 | 202. | a72b1cb332ea7bfddfe25c1f69458685 | link://202.67.19.238:29150/yCHTfA== | | | Pireland Manche | ester Rotherham | Gron | ngeno | 2 | • • Torun |
| 3388 04 Oct 2009 08:21:10 2.02. 67.19.238 2.02. 67.19.238:35016/+8km/Aw= 3389 04 Oct 2009 08:21:10 2.02. 67.19.238 2.01.30.95.115 8.0.2 26530462262b2b270d5e64dd7c676cd ftp://80.130.95.115/sams.exe 3399 04 Oct 2009 08:55:33 8.134.29.250 8.8.134.29.250 18.8.9 223d957aef098637677655665112f4 ftp://111888.134.29.250:17838/chosts.exe Durksmark eve Durksmark eve Durksmark eve Durksmark eve Ofference Durksmark eve Durksmark eve Durksmark eve Durksmark eve Ceskon | 3397 04 Oct 2009 08: | 10:37 📕 71.51.110.90 | 192.168 | df51e3310ef609e908a6b487a28ac068 | tftp://71.51.110.90:69/ssms.exe | | | Limerick Birmin | gham o o | Amsterd | am Orimen Han | nover | Poznaň O Polska |
| 3399 04 Od 2000 08:4552 B0.130.95.115 B0.2 e265d0462eb2b0b70d5e64dad7e576cd tftp://80.130.95.115/sams.exe tdtp://80.130.95.115/sams.exe 3400 04 Od 2009 08:4553 B8.134.29.250 B8.8.134.29.250 B8.8.134.29.250 B8.8.134.29.250 Duttstant Duttstant Duttstant Ocesade | 3398 04 Oct 2009 08 | 21:10 . 202.67.19.238 | 202. | 4f50e44f777bd8e16a0263f83b9815bb | link://202.67.19.238:35016/+Bkn/A== | | | Cork | Swindon Lonyon | Den Haag ONed | erland | Braunschweig | a Zielona Poland Warszawa |
| 3400 04 Oct 2009 08:55:3 8 88.134.29.250 8 88.5 e23d9a57aef099637677655665112f4 ftp://1:1988.134.29.250:17838/chosts.exe | 3399 04 Oct 2009 08 | 43:52 📕 80.130.95.115 | 80.2 | e269d0462eb2b0b70d5e64dcd7c676cd | tftp://80.130.95.115/ssms.exe | | | Cardiff | Bristol | Dunkerque Belgie | Venio De | utschland | Wrocław Łódź L |
| Vessele do ann Main Cesta Republita . Nor to Cesta Republica . Nor to Cesta Republita . Nor to Cesta Republica . Nor to C | 3400 04 Oct 2009 08 | 55:33 📕 88.134.29.250 | 88.9 | e23d9a57aef0986376776f5f685112f4 | ftp://1:1088.134.29.250:17838/chosts.exe | | | Exeter | Portsmouth O Bright | Lille Belgium | Köln | Germany Cher | nnitz Waibrzych Katowice |
| | I 4 4 | —————————————————————————————————————— | A-0 | CC: V-IP: V- | CC: MD5: | Rows 3381 - 3400 of 3 | | Plymouth 🖓 | Le Havre | Amiens | Wiesbaden O am | Main | Česká Republika Rybniko Kraków |
| Attack Detail | Attack Detail- | | | | | | | | Ro | en Paris | serslauterno OMann Stuttg | art Nürnber | 9 Por Zilo Kolea |
| ID: 3384 | TD: | 3384 | | | | | | Brest | Rennes | ALT | Strachaur | Augsburg | Slovensko e Slovensko e Slovensko e Slovensko e |
| Time: Sat Oct 03 2009 17:30:36 GMT+0100 (GMT Daylight Time) | Time: | Sat Oct 03 2009 17:30:36 GM | 1T+0100 (GMT Daylight Ti | me) | | | | Quimper | Angers Tour | © Orléans | Mulhouse | München | Osterreich Budapest Debrece |
| Sensor: | Sensor: | | | | | | | | Cholet Potters | France Dijon | Suisse Svizzera | Imsbruck | Austria O Graz Magyarország O Grad |
| Download: tftp://80.130.64.149:69/ssms.exe | Download: | tftp://80.130.64.149:69/ssms | .exe | | | | | | La Rochele 9 Nion | Lyon | Genève Switzenand | Trento | Slovenija Zagreb Szeged |
| Trigger: tftp://0.0.0./ssms.exe Borteaux Same de Construction of the Construction of t | Trigger: | tftp://0.0.0.0/ssms.exe | | | | | | | Bordeaux | oges Saint-Etienne | Grenoble | Verona | Hrvatska (Cowfop) Belgrade (Beorpag) |
| MD5sum: 697f01bc330ab483d77a707cd40c8d9 | MD5sum: | 697f001bc330ab483d77a7070 | cd40c8d9 | | | | | | | Valence | Torino | enova Ra | erna Croatia Bosna i Zaj Hercegovina Srbija (3a) |
| SHA512: bf53a6773dc2cca07c3855e6b9ee18b57781dcd9155632ab61e9a3074dd1ef5e central and centr | SHA512: | bf53a6773dc2cca07c3855e6b | 9ee18b57781dcd915563 | 2ab61e9a3074dd1ef5e | | | Sar | ntiago de oA Coruña | Ser Pau | Nontpeller | Monaco Draguignan | Firenze Italia | Ancona Spita Herzegovina |
| File Type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit View of Autom Company | File Type: | PE32 executable for MS Wind | ows (GUI) Intel 80386 32 | -bit | | | | Vigo Qurense Burgo | A | ndorra Perpignan | aille | Terr | Crna Gora Kosova Montenegro Kosovo |
| Attacker IP: 1350713493 Shubble Attacker IP: 1350713493 Barcelona | Attacker IP: | 1350713493 | | | | | | Valadolid | Zaragoza | Barcelona | 1 👬 | Roma | Latra Foggia Shkodër Makedor |
| Victm IP: Construction of the second se | Victim IP: | | | | | | | Salamanca | LAN ST | 0 | Sassari | Konna G | Napoli Bari Macedonia (r Shqipëria |
| Filename: SSTS-EXE Communication | Filename: | ssms.exe | | | | | | Coimbrao | Valancia | Palma | 1 M | <u> </u> | Salemo Taranto Brindisi Sarande Qu |
| Country: DE España de Cajam Casaro | Country: | DE | | | | | To | orres O Santarém Espai | ña Albacete | - | Caglia | n | Catanzaro |
| ISP: DEUTSCHE TELEKOM AG Palema Maga | ISP: | DEUTSCHE TELEKOM AG | | | | | ve | Lisboa Badajoz | Alicante | | | Pe | alermo Messina |
| ASN: 3320 Several @Control MURGING | ASN: | 3320 | | | | | | Loule Sevilla Cordob | Cartagena | الجزائر | | | Catania Patra |
| Cádze Ameria diga Ameria diga Ager | | | | | | | | Cádiz | Almeria وهران | Alger | Y AN | 25 | Rusa Sracusa |
| | | | | | | | Google 20 | 00 km | Oran | Map data | @2009 PPWK Tek | Atlas, Transna | Maka vicom, Europa Technologies - Terms of Use |
| Done | Done | | | | | | | Tannari | | | | 28.49 | S Tor Disabled |

David Watson (david@honeynet.org.uk)

_ 8 ×

P

ि • Google

н Ν ΕY Ν Т Ρ R 0 J п 0 0 Т -

😻 Example HonEeeBox Reporting Interface using Ext-JS - Mozilla Firefox

<u>File Edit View History Bookmarks Tools Help</u>

🔊 🗸 🔁 🗋 https://honeeebox.net/demo_schema1/

🔎 Most Visited p Getting Started 🔝 Latest Headlines

Attack Summary Panel

Total Attacks: 3409 (+36) June Total Attacker IPs: 1202 (+28) Total Victim IPs: 167 (+17) Internal June 7 Total MD5sums: 566 (+22) Sensors: 10 (4) enumeration AV Undetected: 4015 / 28579 (14.0%)

| Attack Browser | | | | | « | Google Maps Google Earth Virustotal Anti-Virus Sandbox Graphs PicViz Heatmap Cuttlefish |
|----------------------|------------------------------|-------------------------|----------------------------------|-----------------------------------|----------------------|--|
| ID Time | Attacker IP | Victim IP | MD5sum | Download | | Map Satellite Hybrid Terrain |
| 2436 21 Sep 2009 00 | 00:53 📕 71.96.244.111 | 192.168.1.6 | 14a09a48ad23fe0ea5a180bee8cb750a | tftp://71.96.244.111:69/ssms.exe | | くの >) Hudson Bay |
| 2437 21 Sep 2009 00: | 13:20 🧮 71.124.134.21 | 192.168.1.6 | df51e3310ef609e908a6b487a28ac068 | tftp://71.124.134.21/ssms.exe | | |
| 2438 21 Sep 2009 00: | 25:13 🧮 71.105.122.131 | 192.168.1.6 | 2fa0e36b36382b74e6e6a437ad664a80 | tftp://71.105.122.131/ssms.exe | | Canada |
| 2439 21 Sep 2009 03: | 25:42 📕 71.105.122.131 | 192.168.1.6 | 2fa0e36b36382b74e6e6a437ad664a80 | tftp://71.105.122.131/ssms.exe | | Alberta |
| 2455 21 Sep 2009 17 | 14:48 🧮 71.188.64.55 | 192.168.1.6 | 14a09a48ad23fe0ea5a180bee8cb750a | tftp://71.188.64.55/ssms.exe | | |
| 2459 21 Sep 2009 18 | 54:47 📕 71.41.238.102 | 192.168.1.6 | 66bf4bbb8c4131f682812e654df47282 | tftp://71.41.238.102/ssms.exe | | British Columbia Saskatchewan |
| 2465 22 Sep 2009 00: | 58:42 📕 71.96.226.162 | 192.168.1.6 | 14a09a48ad23fe0ea5a180bee8cb750a | tftp://71.96.226.162:69/ssms.exe | | Edmonton |
| 2468 22 Sep 2009 01 | 47:35 📕 71.105.183.46 | 192.168.1.6 | 6ded5c92a3983af55fef5d5815919de9 | tftp://71.105.183.46/ssms.exe | | |
| 2470 22 Sep 2009 02 | 17:29 📕 71.109.73.228 | 192.168.1.6 | b8076e37aef1105d045fc39f780da5a2 | tftp://71.109.73.228/ssms.exe | | Guebec Quebec |
| 2473 22 Sep 2009 04 | 35:31 🔜 71.116.1.87 | 192.168.1.6 | df51e3310ef609e908a6b487a28ac068 | tftp://71.116.1.87:69/ssms.exe | | |
| 2475 22 Sep 2009 05: | 49:06 📕 71.110.235.36 | 192.168.1.6 | df51e3310ef609e908a6b487a28ac068 | tftp://71.110.235.36:69/ssms.exe | | |
| 2481 22 Sep 2009 09 | 47:54 📕 71.105.114.21 | 192.168.1.6 | 2fa0e36b36382b74e6e6a437ad664a80 | tftp://71.105.114.21:69/ssms.exe | | Attacker IP: 171.110.235.36 |
| 2488 22 Sep 2009 14 | 19:35 📕 71.97.206.3 | 192.168.1.6 | bb39f29fad85db12d9cf7195da0e1bfe | tftp://71.97.206.3:69/ssms.exe | | Country: UNITED STATES (US) |
| 2491 22 Sep 2009 15: | 35:08 📕 71.41.99.199 | 192.168.1.6 | 3228f8bc721572422c268f244476dbb8 | tftp://71.41.99.199/ssms.exe | | ASN: 19262 Wisconsin Ottawa Maine's Scotia |
| 2499 22 Sep 2009 19 | 22:42 📕 71.41.99.199 | 192.168.1.6 | 3228f8bc721572422c268f244476dbb8 | tftp://71.41.99.199:69/ssms.exe | | ISP. VERIZON INTERNET SERVICES INC |
| 2500 22 Sep 2009 19 | 30:30 📕 71.41.99.23 | 192.168.1.6 | 14a09a48ad23fe0ea5a180bee8cb750a | tftp://71.41.99.23/ssms.exe | | Latitude: 34.0359992981 Iska Oowa o Touteo Pennsykania New Hampshir |
| 2502 22 Sep 2009 20 | 20:46 📕 71.121.172.28 | 192.168.1.6 | b8076e37aef1105d045fc39f780da5a2 | tftp://71.121.172.28/ssms.exe | | Longitude: -117.010998291 Massachusetts City |
| 2505 22 Sep 2009 21 | 57:12 🧮 71.31.67.198 | 192.168.1.6 | bb39f29fad85db12d9cf7195da0e1bfe | tftp://71.31.67.198/ssms.exe | | Colorado Kansas ^{or St} Louis Concinatio Vest Sall o Starking Connecticut |
| 2508 23 Sep 2009 01 | 46:53 📕 71.116.1.87 | 192.168.1.6 | df51e3310ef609e908a6b487a28ac068 | tftp://71.116.1.87/ssms.exe | | Francisco California Wichiao Kentucia Virginia New Jersey |
| 2509 23 Sep 2009 01 | 49:09 📕 71.172.112.166 | 192.168.1.6 | 833cda5b5bef5989deb6bf57c557ce30 | tftp://71.172.112.166:69/ssms.exe | | Bakers As Vegas Abuserna Oklaj ma Arkansas Dentessee North Delaware |
| 14 4 🕕 🔤 | 💴 🕨 🕅 🛛 😂 🗍 A-IP: | A | -CC: V-IP: 192.168.1.6 V- | CC: MD5: | Rows 61 - 80 of 3409 | Angeles Mexicali Phoenix Mexico Da Mississippi Carolina District of Columbia |
| Attack Detail | | | | | | Ensenada Tucson Texas Georgia |
| ID: | 3363 | | | | | Hermosillo Chihuahua Nuevo San Houston Atlantic |
| Time: | Fri Oct 02 2009 22:16:19 GMT | +0100 (GMT Daylight T | ïme) | | | Ciudad Laredo Antonio Florida Ocean Obregón Hantorio Reynosa |
| Sensor: | | | | | | Cultacan Rosales Satullo Heroica Matamoros |
| Download: | tftp://71.31.67.198/ssms.exe | | | | | Mazetlano Mazetlano Centra de Contra |
| Trigger: | tftp://71.31.67.198/ssms.exe | | | | | Agusscaliertes@ Los Aldama Merida Cancun Cuba Gradialeare Morela |
| MD5sum: | bb39f29fad85db12d9cf7195da | a0e1bfe | | | | Cudadisais Concerniz Compete Commenter Comment |
| SHA512: | 55d2096e39e4cf2fc19afce3c2 | e1becbf31da602e7c2a6 | 57af0a8ad23803bc2cb | | | Acapulco Turtia Guatemala |
| File Type: | PE32 executable for MS Windo | ows (GUI) Intel 80386 3 | 2-bit | | | North Pacific Ocean Gustemale |
| Attacker IP: | | | | | | Nicaragua Managua Managua |
| Victim IP: | 3232235782 | | | | | Costa Barranquila O Valencia |
| Filename: | ssms.exe | | | | | Panama Medelin Venezuela |
| Country: | US | | | | | Tulus Bagota |
| ISP: | ALLTEL - ST. MARYS | | | | | Cai Colombia |
| ASN: | 7029 | | | | | Curto - Friday Rora |
| | | | | | | Ecuador Ecuador |
| | | | | | | Coordo Iquitos |
| | | | | | | Map data ©2009 LeadDog Consulting, Tak Abos Mt GI, Europa Technologies - Terms of Use |

David Watson (david@honeynet.org.uk)

<u>_8×</u>

P

☆ • G• Google

Example HonEeeBox Reporting Interface using Ext-JS - Mozilla Firefox

Eile Edit View Higtory Bookmarks Tools Help

🕑 🗸 🔂 🗋 https://honeeebox.net/demo_schema1/

н

-

п

🖻 Most Visited 🎓 Getting Started 脑 Latest Headlines

Attack Summary Panel

<

Total Attacks: 3409 (+36) Sensors: 10 (4) utantati AV Undetected: 4015 / 28579 (14.0%)

Ν

ΕY

Ν

Т

Ρ

R

0 J

П

С

☆ · Google

Т

.

0

| D Tme Attacker P Vicim P MD5sim Download 138 V2 Oct 2009 22:06:17 3 4.10.9.190.125 358 8.3 62268d2ae57ab777627d9603d75aa6 crecei.ver//44.109.190.125:25628 crecei.ver//44.109.190.125:25764 tretei.ver//44.109.190.125:25628 crecei.ver//44.109.190.125:25628 | 193.111 - 40 5.205 - 1 193.11-226 193.138 - 2 |
|--|--|
| 3361 02 Oct 2009 22:06:17 3 8 4.109.190.125 38 8 2. c22233d2e657ab777e57d56032f75as6 creceive://84.109.190.125:37501 18 9.1 < | 193.111 - 40 5.205 - 1 193.11-226 193.138 - 2 |
| 3382 02 0d: 2009 22:06:01 Image: second | 193.111-40 5.205-1 193.11-226 193.138-2 |
| 3383 02 Oct 2009 22:16:19 71.31.67.198 192.16: bb39529fad95db12d9cf7195da0elbfe tftp://1.31.67.198/ssms.exe 145.7 | 193.111 - 40 5.205 - 1 193.111 - 226 193.135 - 2 |
| 3364 02 Oct 2009 23/06/7 8 0.165.178.241 80.1 14209488d23fe0ea5a180bee8cb750a tftp://0.165.178.241/ssms.exe 1924.9 | 5.205 - 1 193:11-226 193.138 - 2 |
| 3385 03 Oct 2009 08:38:03 | 193.11-226 193.138-2 |
| 3386 03 Oct 2009 09:54:46 12:11:1:11:13 192:16(a259d9452eb2bb70d5e64dcd7c676cd tfp://71.115.111.43:69/ssms.exe 3387 03 Oct 2009 10:03:45 8:134:29:250 IB:8: a239b57aef0986376776f5f685112f4 ftp://11088.134:29:250:11515/chosts.exe | 193:11-226 193.138-2 |
| 3387 03 Oct 2009 10:03:45 = 88.134.29.250 = 88.134.29.250 = 88.134.29.250 = 88.134.29.250 = 12:05 = 9 | 193.11-226 193.130-2 |
| | Maria |
| 3388 03 Oct 2009 10:13:53 80.171.109.19 80. d35eed1695a610bbd580d5f7d96167b3 ttp://80.171.109.19/ssms.exe | 192.00 |
| 3389 03 Oct 2009 10:2025 8 88.134.29.250 8 88. <u>e23d9a57aef0986376776f5f685112f4</u> ftp://11088.134.29.250:11515/chosts.exe | |
| 3370 03 Oct 2009 10:33:16 = 80.171.109.19 = 80. d35eed1695aed10bbd580d5f7d96167b3 vtpp://80.171.109.19/ssms.exe | |
| 3371 03 Oct 2009 1126:35 🖬 80.5.30.87 🐂 80. <u>a759a39900655a280de28d5ae5684e9</u> <u>tftp://80.5.30.87:69/ssms.exe</u> | 195.222 - 2 |
| 3372 03 Oct 2009 11:27:53 = 80.1 6597£001bc330ab483d77a707cd40c8d9 tftp://80.161.55.235/ssms.exe | SH J |
| 3373 03 Oct 2009 11:58:04 202.183.52.12 2 2 99eb0fdadf8a403c013a8b1882ec986d tftp://202.183.52.12:69/ssms.exe | Per - C |
| 3374 03 0d 2009 120 220 = 88.70.201.129 da 88. 055a235Tcf5f28b239d24cd91866fcce fp://88.70.201.129:80578/mobile.exe | NT - ~ |
| 3375 03 04 2009 12:5022 8 81.34.29.250 til 88. e23d9s57acf298637677cf5f685112f4 fcp://1.1088.134.29.250:11515/chosts.exe | 193:204 -1 |
| 3376 03 04 2008 133201 8 81. at 88. a7e25d717ac8c626e4db044eb4dca5dd fpp://11888.134.144.39 title 8. ar 825d717ac8c626e4db044eb4dca5dd fpp://11888.134.144.39 title 8. ar 8. a | |
| 33/1 03 0d 200# 133:5:3 = 80.71.226.226 tais 80. 2dsf2046f3e2315b255dd6be1f1ac244 ftp://11888.71.226.22624890/lhost.exe | |
| 3/8 U3 Ud 2009 1350/01 = 85.71.226.226 am 85. 2ddf20463a231b255dd6ba1f1ac744 fpp://11885.71.226.22624830/lhost.exe 193 152 - 2 Fando Alternative Control of the control of | |
| 33/9 03 04 2009 135524 8 0, 165, 202, 131 8 0. 14402413424843356068540750a 11407045, 202, 131, 2 | Romania |
| 3360 03 001/2009 1420.33 6 cs./0.201.129 6 as cs. 00592436316551266239644639165512662396446391655126623964463916616468 | Sales and |
| I 4 | Bul |
| Attack Detail | enegro |
| ID: 3363 | Macedonia (FYROM |
| Tme: Fri Oct 02 2009 22:16:19 GMT+0100 (GMT Davidht Time) | Albania |
| Sensor: | |
| Download: tftp://1.31.67.198/ssms.exe | onian Sea Lefkada |
| Trigger: tftp://1.31.67.198/ssms.exe | Zakynthös (Zante) |
| MD5sum: bb39/29fad85db12d9cf7195da0e1bfe | |
| SHA512: 55d2096e39e4cf2fc19afce3c2e1bechf31da602e7c2a67af0a8ad23803bc2cb (Tangler) Panger (| 5-2 |
| File Type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit | |
| Attacker IP: 1193231302 | |
| Victim IP: | |
| Filename: ssms.exe | |
| Country: US | |
| ISP: ALLTEL - ST. MARYS | |
| ASN: 7029 | |
| | |
| | |
| Done S | S Tor Disabled |

David Watson (david@honeynet.org.uk)

_ 8 ×

P

THE HONEYNET PROJECT-



HE HONEYNET PROJECT-

Т

| taoks | | | | | Google Map Despait an | * SPECK | Anti-time 1 | Rapin Pella mathaga Cultiefan |
|--------------|------------------------------|-------------------------|--|--|-----------------------|---------------|-----------------|--|
| Tran | Adactiv: P | Vielin P | MDC 92.71 | De A viteral | | | | |
| 20 May 2009 | 17:22.37 📕 70.232.61.243 | 10 \$4.236.114.1 | 122X955190855787496595909418cd00 | f101//71.232 61.243 5554/16745_00_685 | File Sast | ser.B.exe.vir | received on 02 | 18.2009 14:12:41 (CET) |
| 32 May 2009 | 1202.07 1 64.298.114.1 | ID \$4.258.114.1 | 4399/30-959235-33H7/4c3c5ab1193k | Hp://1.1600.204.100.120:7290/netliginary.ece | | G. | ment status fin | nished |
| 20 Mar 2003 | 17.22.8/ 🕮 07.135.50.103 | HR \$4,2%,114.1 | 30776 (2776/02145) er 13247ee4clock | znecet xec//07-175.50-107:2072 | | Ek | sut: 36/39 (97 | A1% |
| Z. Mar 2009 | 1222.87 • 127. 255. 255. 255 | HR \$4.236.114.1 | 8f4c8c11fcch/0005/01ab000ccfell6 | 17024140: (/2.1.200.227.64:384/ | Hill Contract | | | File e.s. is i |
| 30 May 2009 | 12:22 37 37.13.73.60 | G 84.238.114.1 | Poil564570822.535ac863c36187147256 | pressive://87.17.73.80:49074 | CL MALANCE | | | |
| 20 May 2009 | 17.22.37 📓 37.13.73.69 | 6 \$4.256, 114.1 | 11c%.a4ebc72521931*eE4e6tt75196e | <pre></pre> | Antivirus | Version | Last Update | Result |
| X Mar 2003 | 17:22:37 118, 165, 49, 147 | 18 64.236, 114.1 | e8c4(Ecde15e*EL0806855c948c1dLc2 | ftp://bi.ak038_195.49_147(2866/kove*dfds.cen | 5-2319.60 | | | Net-Worn Win82 Basser 14 |
| 20 100 2003 | 17:22.8 1 70.292.61.248 | 10 64.236.114.1 | 1a2r0#113007273Hz985313094135600 | Hp://71.202.01.203.5554(16745_up.aca | 4hrLab-45 | - | | W1/82/Easser //ore.15872.8 |
| 2. 46 2.0.3 | 1622.8 1 64.216.114.1 | HE 64.216.114.1 | active and an and a set of the set of the | Hp://111600.204.100.12017290/net1107ary.ede | Art171* | | | worm/Sasser.E |
| 20 Mile 2003 | 17.22.9 | The res 114.1 | Stream for him and compared of a | 17441421/16/ 1/3/00 15/14004 | Automatica | | | WSZ/GROBOTX.BRT |
| Vide 1973 | 12/227 2 12 12 12 12 15 | T 14.156.114.1 | 45455437500×000×000×000×000×000 | Trace as //07 13 75 62 4007/ | Avast | | | winst is as series |
| X Ver 200 | 12/2.87 37.17.73.69 | 18 54.236.114.1 | 11c8 adab/726219214484y81175159 | never ##1 / /87 17, 73 53 99800 | ANT | - 22 | | constat. www. |
| X Ver 2009 | 12/2 27 = 118 165.49 142 | 18 64.236.114.1 | atte 4d0 de 15e ⁴ 010305605c940c1d1c2 | ftp://s:s9135 155.49 147:2000/issefdfds.com | Eltopfersur | | | vintz worm.sessor.8 |
| 25 14/ 2003 | 17.22.97 1 70.232.61.241 | 18 \$4.236.114.1 | 1x2x2x1x113005260fc965x130941.5x400 | Hp://71.232 61.243 5554/16745 up.ece | ceguickeaal | | | W32.58588f.B |
| 25 Mir 2003 | 17:22.37 1 64. 216. 114. 1 | H \$4.2%, 114.1 | e9990.85/95/055/2817(ar2x5a61192x | ftp://lilass 214,188 125:7255/het/Larany.ess | Classo | | | Vorm.Saasar.d |
| 31 Mar 2009 | 17:22 2 37.105.58.187 | E 64.236.114.1 | 387565257(4c)1d51cc18247cc4c1cdb | Crock145: 7787 175,58 187:4681 | Cenado | | | Vormul 112.Sabaar.D |
| 32 Mar 2009 | 17:22 1 127, 255, 266, 255 | T 64.298.114.1 | Office Petitics and State Petitissis and Operate Physics | trecet #e://211.200.220.64:3647 | trivia | | | Wind2-HTML2cbake |
| 25 Ver 2003 | 17.22.37 🐻 87.17.73.69 | HR \$4.236.114.1 | 15155437902x153xx0x52x0007x47256 | zhecet #et //07 17, 73 65: 43074 | #5#/# | 1 | | |
| Page 1 | N3 3 9 15 15 | 4 | | *ses 1 - 22 of 58 | eTrust-vec | | | W1/182/Sesser.8 |
| thack Detail | 0 | | | | F-Prot | | | V02/DECEDIX.EET |
| | 3 | | | | F-Secure | 2.1 | | tet-Worn:WS2/Ensser.4 |
| TC: | 1230033748 | | | | Fortiget | | | WE2-NERSER R |
| 21506 | 64.230.1141 | | | | (1273 | | | wind: yora sessor a |
| tecnos | croce ve #87,176,58,187,4652 | | | | stores. | | | ant were wired, samer |
| igget: | croco vo 887,176,58,187,4652 | | | | stantistics. | | 1. | ast west winst same a |
| C5sur: | 387515257641214516130475 | 244° 168 | | | are special | 1975 - C | | sat was winn same a |
| 45611 | Sect #1000/03/03/07/07/07/07 | 220165432826252710 | ZORKEN ZORRENG THE | | Acadas . | | 1 | NAMES OF A DESCRIPTION OF A DESCRIPTIONO |
| | 0163 con kits for both | | | | PLA BE | | | ALCONDER AND A |
| 4 124 | POLI SACEBER OF PS WEEP | 60(0.0) 18 803151515151 | | | FLC BRAY ALLS | | | #12/585881.HETT. 0 |
| atter P | 14 (1, 1185) | | | | F10138011 | | | WOTHER, STREET, ORT |
| shr P | 1013237508 | | | | 1(1)? | - (C) | | MUCC/Second |
| | intectini. | | | | 1cr 1st | 1 C | | Sacer 3 |
| CLT.71 | 84 | | | | rfratect | 1 | n. | W1/432.Worm.Samer.B |
| P: | Cert calmanet | | | | | | | |
| | and a | | | | | | | |

. O J н п 0 Ν П Υ Ν Ξ Т Ρ R П С Т

🛦 Total Target IPs: 1 👫 🖉 🛦 Total MD5sums: 7 🖬 🕼 🗤 🤅

| | | Geogle Hest Geogle Entit Sandbox | And-Virus Draphs Pickle Heatnap Cutdelish | | | | |
|--|--|----------------------------------|--|--|--|--|--|
| UC South | Download | | | | | | |
| 142:00015025015105004150 | <u>100 (15:777) 252, 5., 245</u> | Span Summary | Print Chargeners | Boonston Champes. | | | |
| e399196c959235c23f71ac2c5as115 | 924 <u>#11:771:1999.294.18</u> | | 115.0000 | collina il come fore | | | |
| 3875b625714d21151ec18247ee4c1/ | odb creceive //87.175.5 | O Technical Details | | | | | |
| Of 4e Bell fach fS 535/7SL ab 008 de fe3 | 165 creceive //211_200. | Analysis Humber | 1 | | | | |
| £5655437902c053840b5c50073472 | 256 creceive //07.17.73 | Percette | | | | | |
| 11351a4cm/2e0105[feeaabb./bit | an arrive 1/8/. 17.72 | Process D | 1941 | | | | |
| 48534c8cds15c7510505055c545c9c7 | 1c2 ft:://acapul8.185.4 | filename | rt/bullsAmplexe | | | | |
| 1a2c0e6189850181c9b6a5809418c/ | 000 <u>ft.11//70 232.51.243</u> | Filesios | 2.227 20 by see | | | | |
| e856196c558295c28171ac2c5as115 | 924 ft:://1/1998.294.18 | MDG | 79ed 1331 cc5 c201 c68 e668 he7 c208 69* | | | | |
| 00758625754d21d51ec10247ee4c1v | ob creceive //07.175.5 | Start Reason | Analysis larger | | | | |
| Of the DeCIL Factor's D35751 ab 005 dense? | 165 creceive //211_200. | Termination Reason | Mamel Terraination | | | | |
| fofssantessantesabarbaratian | 200 graning //87.17.73 | Stort Time | 50 00 760 | | | | |
| 11351a4aaa7200185ffa8ca5bb700 | 21a graceive //87.17.73 | SupTime | 00 54,460 | | | | |
| e814c8cds15cf819805955c948c9c | 1c2 fts://ara@18.165.4 | Detection | OK (CRMAV) | | | | |
| 142000015050151600015004150 | dog <u>(15-1775-282, 51-248</u> | сан | COM Create Instance: H2WH00W3 system32 ic instanced, Progli COM Create Instance: H2WH00W5 system32 utrian dil, Progli | C. (), Interface ID: ((00023455-0000-0000-0000-000000045)) 210, Interface ID: ((000500171-001244445-0002-0206-00052538)) | | | |
| +199096c959235c20t7Lac2c5ab115 | 924 Ho://1:1900.204.18 | | Loaded DLLs | | | | |
| 3875k6257x4d21d51ec18247ee4c1/ | odb creceive //87.175.5 | | H WINDOW Stovers with not at | | | | |
| 0f4eBe31fccbf3055731e5003defe3 | 165 <u>sressive //211_200.</u> | | H Welk/COWS/system/32 Assimility of H January COWS/Sectors and Courses 20, 40 | | | | |
| 457524079024090ee0534472 405: | 250 creceive //07.17.73 Rows 1-20 of 55 | | H. Weinz GYM Staty memol: JPFUETH all H. Weinz GYM Staty memol: JPFUETH all H. Weinz GYM Staty memol: JC accord 52: 51 H. Weinz GYM Staty memol: JC accord 52: 51 H. Weinz GYM Staty memol: JC JC 22: 51 H. Weinz GYM Staty memol: JC JC 22: 51 H. Weinz GYM Staty memol: JC JC 22: 51 H. Weinz GYM Staty memol: JC JC 22: 52 H. Weinz GYM Staty memol: JC JC 20: 52 | | | | |
| 50 10 | | 111-Handling | H Weinz GW Stagetten Solar SVC Coll H Weinz GW Stagetten S2 as http://dl H Weinz GW Stagetten S2 as http://dl H Weinz GW Stagetten S2 as http://dl H Weinz GW Stagetten G2 Advice M L H Weinz GW Stagetten G2 Advice M L H Weinz GW Stagetten S2 aptorect of H Weinz GW | ds_5555-54144-colle1_6.0.2600-2062_x-www_ae256c0# | | | |
| 10495cbc918552c1c00b48 | | | H WINDOWSkystemS2 are here at | | | | |
| Ala | | | H Welt/COVVStoymen/Clansscrittine has H Welt/COVVStoymen/Clansscrittine has H Welt/COVVStoymen/Clansscrittine has H Welt/COVVStoymen/Clansscrittine/Clanscrittine/Cl | H Well-XCYVSAvy tecnic/Carsorfine have H Well-XCYVSAvy tecnic/Carsorfine have H Well-XCYVSAvy tecnicS and tec: H Well-XCYVSAvy tecnicS and tepics.cl H Well-XCYVSAvy tecnicS and tepics.cl H Well-XCYVSAvy tecnicS and text cl H We | | | |
| | | | New Files | | | | |

— ТНЕ НОМЕУМЕТ РКОЈЕСТ—

F

| urce IPs: 6 114. | - Total Target IPs: 1 📶 👍 1 | Fotal MD3sums: 7 1 1 Colo | | | | | | | | | |
|---|-----------------------------------|-----------------------------------|--------------|--------------|----------------------|--|--|--|-----------|-----------------------|------|
| | | | Coople Page | Corge Earl | Sancisce Aru- | Vius Chiefe | Bella Heatmap | Culk In 1 | | | |
| Velin P | VCSsur | Dewrekad | | | | | | | | | |
| 35 64.235.114.1 | 1.0.041305078701016500413.000 | ft.p://70.282.61.248:5554/16745_1 | Reserved | Unallegated | Part : Data Table 4. | HP | DEC | The second se | DN-RVN | | |
| 64.235.114.1 | 4221126-220726-29171-c2x5-b11928 | ftp://111668.204.183.126.7295/re | Tests. | | | 10000 | 22.244 | | | | |
| 1 64.235.114.1 | 357555257d4d2ld5lec13247ee4clocb | creceive://87.175.58.187:4652 | | | | | | | | | |
| 5 🖶 64.236.114.1 | 814686811fcdb19688791ab009dc1c1L5 | creceive://211.299.229.64:8647 | CF | Unullocated | Xerox. | AT&T | Apple MT | T test. start T | AZTO | | |
| 64.235.114.1 | f5f25437502c053ae0b9cb0107647256 | creceive://87.17.73.69:43074 | UL | | inci on i | TOLT | T.F. TAT | T **** T | TOU | M | |
| 35 \$4.235.114.1 | 11431a4sbd7260193ffe8da6bb79056a | creceive1//87.17.73.69:59699 | | | | | | TO BE OWNER | | MUIT | C |
| \$ \$4.715.114.1 | e044dbcde15ef310305955c943c0d1c2 | ftp://x:xe110.165.49.147:2005/1g | Taxa 12 | | Larra 12 | | DTCADTC | A Cabla | | THULL OF | |
| 30 64.235.114.1 | 1x2+0+0100000060648585309403e400 | ftp://70.232.61.2/3:555//167/5_k | revers | Charlingater | revera. | 11112 | DISUDIS | ALabre | Paties | | |
| 35 64.235.114.1 | 2521126-250275-29f71ac2c5-b11926 | ftp://111688.294.183.128.7295/rs | | | | | _ | Constant of the | | | |
| 31 64.235.114.1 | 3875b1257d4d21d51ec13247ee-4c1cdb | creasive://87.175.58.187:4852 | | | TTN | | | | | | |
| 5 33 64.235.114.1 | 314c8c81fcdb19695791ab009dc1c1L5 | creceive://211.299.229.64:8647 | Unallocated | US Army | TRW | RFC1918 | RaalLocated RSI-No | erh សរដ្ឋភ្លេងៅ 📗 | DISA | | |
| 64.236.114.1 | 15155457052.8753.8163.18187447256 | creceive://87.17.78.60.48974 | | | 1914 | and the second s | and a second second | | 24.0 | | |
| 64.235.114.1 | 11d31a4ebd7260193ffe8da6bb79056a | creceive1//87.17.73.69:59609 | | | | | | | | Same Street and | |
| 34.716.114.1 | e844d8cde15ef310305955c943c0c1c2 | ftp://aia#118.165.49.147/2866/18 | - E | STTA | and set of the set | 00 [25:1-03 | AT&T Mer | it linalloc | ated | APNIC | |
| a 64.236.114.1 | 1a2c0e5L30350f0fd5b5b5309/03cd00 | ftp://70.232.61.243:5554/16745_k | | 0 ± ± · · · | | 10-0-1 | TILCEL COL | | | ULUTC | |
| 35 64.235.114.1 | a355155-555235-23971ac3c5ab1193c | ftp://1:1400.204.103.125:7290/re | APNIC | | | | | | | State Land | APN |
| · 64.295.114.1 | 357561257d4d21d51ec13247ee-4c1cdb | creative://87.175.58.187:4852 | AS | TICDC | Den with a | | and the second sec | | DCT | DTDEADTH | |
| 5 12 64.235.114.1 | 0f4ete11fodbf9035791ab003defe1b5 | creceive://211.200.220.64:3647 | 1.1 | 0552 | non arc. | 54125 | and the second second | T and a second s | COT. | RIFEARIN | |
| 32 64.235.114.1 | fefeste/uszcarsusLochers/d4/256 | creceive://87.17.78.69:48874 | | | | | | | | All the second second | |
| PD PD | 5: | Powrs:1 - 20 of 58 | 1 733 | TTO | | | | | | NO DOD | |
| | | | AP | IIC | Omillocated - | 10.10 ² | Initiated Inter | op Ili Lily A | friNIC | US-DOD | |
| | | | | - | | | | ÷ | | 14117 | ATEN |
| | | | - | 1000 | | | | 10 | | Star Barry St. | APN |
| | | | ARTN | RTPE | Unallocated | sudent al | at an interest and the set | Japan Inet U | allecated | RTPF | |
| | | | CHINTLY I | UTT D | 11.44 | 40-641 | | 10.04 | 14.0 | IVIT T | |
| | | | J. S. Martin | | | | | 1000 | | | |
| | | | 2.00 | | | | | - | | | |
| tt75156z | | | 1 | | C | | | _ | eservea | | |
| ct/atter/2te/t4ca/491 | 100000701075e5:50 | | | AR | TN | | APNT | APNIC | | | |
| car (0 Ib what states of a | | | 1000 | AIN | TIA | | LUT INT A | - | | | |
| CAN (BUILT FINITE STORE | 1 | | 1. | | | | | A | PNIC | | |
| | | | AND CA | | | | | | | | |
| | | | | | | | | Ar | | | |
| | | | | RTPE | | | | | | | |
| | | | | Land L | 4.00 | TNT | ADATE | - | | | |
| | | | RTLE | | AK | IN | APNL | Unallog | ated | | |
| | | | 211.6 | ADTA | | | B. 10. | | | | |
| | | | () | | | | 1.2 | | | | |

THE HONEYNET PROJECT





THE HONEYNET PROJECT-











shadowser

5/1086

The Honeynet PROJECT®





— THE HONEYNET PROJECT——





HonEeeBox v1 Goals

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

HonEeeBox Successes



- Bought 145 sensors using \$40k NIC funding July 2009
- \$10k from Symantec to pay for hardware shipping
- Built Prototype UI using ExtJS & backend
- Ran operational blog and gradually added sensors
- Got a few people involved in UI development
- Current stats (past 24 hours):
 Sensors: 39 (10) (~90 Lance / Julia)
 Total Attacks: 35230 (+74)
 Total Attacker IPs: 12545 (+25)
 Total Victim IPs: 212 (+15)
 Total MD5sums: 2326 (+22)

HonEeeBox Failures



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

THE HONEYNET PROJECT

Process for setting up new HonEeeBox participants and nodes

1. (Lance) Confirm participant has one or more unfiltered public static IP addresses on a netblock that we don't currently have a HonEeeBox sensor running on and is willing to participate in the HonEeeBox project, including sharing da

- 2. (Lance) Obtain shipping address from participant.
- 3. (Lance) Ship one or more sensors plus pre-written USB key and setup instructions to participat at requested shipping address, recording the shipping address, shipping date, shipping date, shipping cost in the Honeeebox
- 4. (Lance) Email participant with their shipment tracking ID. In this email include the welcome email which includes a link to the electronic version of the setup guides and tells the participant what data we need from them to complete
- 5. (Lance) Confirm when participant receives shipped sensor(s) and record the received date in the HoneeeboxSensorDepoyment.
- 6. (Lance or David) Participant replies to welcome email with sensor setup information once they have deployed it. Record all deployment details in HoneeeboxSensorDepoyment.
- 7. (David) Add sensor's static public IP address(es) to iptables rule on honeeebox.net:

audo vi /etc/iptables.conf

KNODE ID> David Wataon KDATE in format 01/01/1D> -A RH-Firewall-1-INPUT -s KEENEOR IP> -m state --state NEW -m top -p top --dport 8443 -j ACCEPT

sudo iptables-restore < /etc/iptables.conf

Record sensor IP address and deployment date details in HoneeeboxSensorDepoyment.

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

sudo htpasswd /etc/spache2/htpasswd forename.surname

Record paricipant useranme in HoneeeboxSensorDepoyment.

9. (David) Test web access at ~ https://honeeebox.net as participant's new user account:

1. (David) Add operational blog post for new participant, if necessary, setting blog post date to htpasswd change date and category to "Participation":

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

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

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

1. (David) Update HonEeeBox blog list of participants and sensors (~ https://honeeebox.net/Blog/7page_id=8).

1. (David) Add the participant to the HonEeeBox mailing list (** https://public.honeynet.org/mailman/listinfo/honeeebox).

1. (David) Email participant (using GPG to tell them their usemame/password, that their node is now live and remind them of the HonEeeBox UI URL (~ http://honeeebox.net) and operational blog (~ http://honeeebox.net/Blog).

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

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

HonEeeBox Lessons Learned



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

HonEeeBox Lessons Learned



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





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



Nepenthes \rightarrow **Dionaea**

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

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

connection 610 smbd tcp accept 10.69.53.52:445 <- 10.65.34.231:2010 dcerpc request: uuid '3919286a-b10c-11d0-9ba8-00c04fd92ef5' opnum 9 pOf: genre: 'Windows' detail: 'XP SP1+, 2000 SP3' uptime: '-1' tos: '' dist: '11' nat: '0' fw: profile: [{'return': '0x7c802367', 'args': ['', 'CreateProcessA'], 'call': 'GetProcAddre, {'return': '0', 'args': ['0'], 'call': 'ExitThread'}] service: bindshell://1957 connection 611 remoteshell tcp listen 10.69.53.52:1957 connection 612 remoteshell tcp accept 10.69.53.52:1957 <- 10.65.34.231:2135 pOf: genre:'Windows' detail:'XP SP1+, 2000 SP3' uptime:'-1' tos:'' dist:'11' nat:'0 offer: fxp://1:1010.65.34.231:8218/ssms.exe download: 1d419d615dbe5a238bbaa569b3829a23 fxp://1:1010.65.34.231:8218/ssms.exe connection 613 ftpctrl tcp connect 10.69.53.52:37065 -> 10.65.34.231/None:8218 connection 614 ftpdata tcp listen 10.69.53.52:62087 connection 615 ftpdata tcp accept 10.69.53.52:62087 <- 10.65.34.231:2308 pOf: genre: 'Windows' detail: 'XP SP1+, 2000 SP3' uptime: '-1' tos: '' dist: '11' :

HonEeeBox v2 in 2011

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

HonEeeBox v2 in 2011

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

— ТНЕ НОМЕУМЕТ РКОЈЕСТ—

| | legin: Setting up locales Generating locales (this might take a while) |
|---|--|
| | en_US.UTF-8 done |
| | lone |
| | legin: Setting un automatic login done |
| The Honevne | tegin: Setting up console keyhoard dome. |
| | legin: Configuring gnome-panel-data done. |
| | legin: Configuring screensaver done. |
| | legin: Preconfiguring /etc/modules done. |
| | legin: Preconfiguring networking done. |
| | legin: Running /scripts/init-bottom done. |
| | NIT: version 2.86 booting |
| | itarting the notplug events alspatcher; uaeval 8.5125041 uaeva version 125 s |
| | rteu |
| () X) SREDDU <u>SEL V</u> EL | Sunthesizing the initial bothlug eventsdome. |
| | laiting for /dev to be fully populated[8.873512] Linux appgart 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 |
| ress F1 for help, or ENTER to boot: _ | 8.884984J shpchp: Standard Hot Plug PUI Controller Driver version: 0.4 |
| # μιστούοι εμωσημεί πιζωτιτοία | 8.9242591 Input: Power Button (FF) as /Class/Input/Input1 |
| | |
| conrig overlation | |
| | [!!] CHOUSE Tanguage |
| files = "3" | Please choose the language used for the installation process. This |
| filesize = "524288" | tanguage will be the default language for the final system. |
| sockets = "3" | Choose a language: |
| sustain = "120" | C – No localization 👲 |
| idle = "30" | Albanian - Shqip Arabic - Shqip |
| listen = "30" | Basque – Euskara |
| cpu = "120" | Belarusian – Беларуская I Bosnian – Bosanski |
| steps = "1073741824" | Bulgarian – Български |
| api | Catalan - Català Chinese (Simplified) - 中文(简体) |
| connect | Chinese (Traditional) - 中文(繁體) |
| host = "127.0.0.1" | Croatian – Hrvatski Czech – Čeština |
| port = "4444" | Danish – Dansk |
| allow # www.toccl # tune pecent | Dutch – Nederlands English – English |
| # protocol # type accept # protocol ftpetri # tupo connect | Esperanto – Esperanto 🐺 |
| * prococor repetir * type connect | <go back=""></go> |
| lenu | |
| # protocol ftndata ftndatacon xmnncl | lient # type |
| - protocol repaired repaired in Anppor | > moves hatwaan items: /Space/ selects: /Enter/ activates huttons |

н H Ν Υ Ν п Т Ρ OJECT Т п 0 п R

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

HonEeeBox v2 in 2011

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

Plan submit_http → submit_XMPP / hpfeed
Plan new schema (consider Carniwwwhore)
Plan and kickstart core development
Brainstorm and plan UI plus visualizations

Project 2 - HonEeeBox Data Management Interface Primary Mentor: David Watson (UK) Backup mentor: Ben Reardon (AU), Arthur Clune (UK) Type: New Development or Evolution of Existing Tool Skill set required: Data driven web development skills, preferably Python/Django/Postgressql/Javascript/ExtJS but open to suitable alternative approaches Project Goal: Implementation of a rich new web-based UI for exploration of malware data collected by a distributed network of international low interaction server honeypots

Project Description:

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

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

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

http://www.honeynet.org/gsoc/ideas David Watson (david@honeynet.org.uk)

– ТНЕ НОМЕУМЕТ РКОЈЕСТ–



PROJECT

HonEeeBox – Rapid Deployment of Many Distributed Low Interaction Malware Collectors

Any Questions?