

Experimental Evaluation of Malware in Sandboxing Environments

Radhika Pai, Vignesh Rajan, Nishant Rodrigues

Project Report

December 14, 2016

Introduction

The most widespread way of discovering malware attacks is sandboxing. This involves isolation of the unknown suspected files in a virtual environment which emulates an actual host system. The suspected files are then monitored in the virtual environment, to check if they do in fact possess viral strains. If they do, they are labelled as malicious and the information acquired through monitoring is used to prevent further attacks from the new malware. By acting upon the virtual environment, the malware exposes its true self.

However, the art of sandboxing has not seen a lot of new features in the recent year, and that has resulted in attackers trying to detect if their programs are running in virtual environments. While not all the malware includes this additional layer of self-protection, they are beginning to appear more frequently.

Our project involves creation and analysis of how such environment sensing malware evade sandboxes and invade systems.

We use a sandbox called Cuckoo Sandbox to do our malware analysis. We intended to use one more sandbox as per our project proposal, but we decided against using it since a free version of the software was not available. However, cuckoo sandbox is sufficient for the scope of this project and we provide further details about installing, using and analyzing malware using it.

Installation

The installation for Cuckoo requires installing three main components:

- Host Virtual Machine**

We needed a host system to run the cuckoo application on. We chose to use Ubuntu 15.10 since Linux is freeware and provides nice features for simulating server like behavior. Linux also provides good support for virtualization.

We use VMWare Fusion (license obtained through UMD) for running Ubuntu 15.10. For setting up the VM, download .iso file for the VM from <https://www.ubuntu.com/download/desktop>, and install inside VMWare. For our VM we use a configuration with 8Gb of memory and 40 Gb of storage.

- **Cuckoo and Dependencies**

The Cuckoo Sandbox is available for download at <https://cuckoosandbox.org/>. The developers of the project also maintain a development release on Github. Cuckoo is open source and free to use. Cuckoo doesn't run out of the box, but rather needs a lot of configuration and customized tuning depending on what you intend to use it for. We wanted to use it for malware analysis primarily, so we outline the steps required to install cuckoo:

1. Obtain cuckoo:

```
$ git clone https://github.com/cuckoosandbox/cuckoo.git
```

2. Install dependencies:

```
$ sudo apt-get install python python-pip python-dev libffi-dev libssl-dev  
$ sudo apt-get install mongodb  
$ sudo pip install -r cuckoo/requirements.txt
```

3. TcpDump

```
$ sudo apt-get install tcpdump  
$ sudo setcap cap_net_raw,cap_net=ep /usr/sbin/tcpdump
```

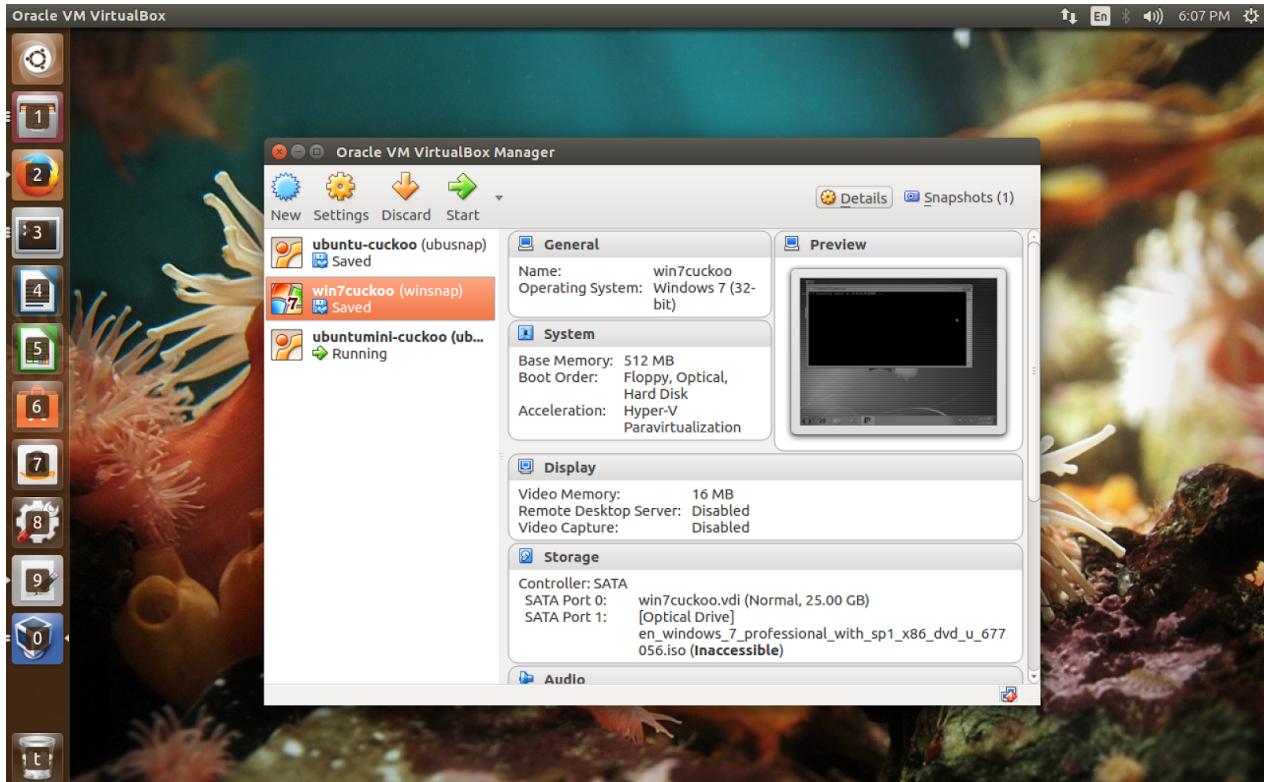
4. Installing cuckoo:

```
$ sudo adduser cuckoo  
$ sudo usermod -a -G vboxusers cuckoo
```

5. Postgresql (database)

```
$ sudo apt-get install postgresql postgresql-server
```

- **Test VMs (for sandboxing)**



We use three virtual machines inside our host virtual machine. All three VMs are run inside VirtualBox which is free to use. We describe the three VMs (also shown in screenshot above):

1. **Ubuntu 14.04 (minimal):** This is a minimal installation of Ubuntu. It does not contain any packages except for the linux kernel itself and few essential packages like gcc and other core utilities.
2. **Windows 7:** This is a full installation of Windows 7 Professional. It does not have any extra installed applications other than the ones that come with the installation. We did install Python 2.7 to be able to run a script used by Cuckoo to communicate with the VM.
3. **Ubuntu 14.04:** This is a full installation of Ubuntu 14.04. We use this to see if there is a difference in the behavior of malware when it runs on the minimal VM versus this VM.

Getting Started with Cuckoo

To get started with cuckoo on your virtual machine (in our case: Ubuntu), navigate to the Cuckoo folder and run the `cuckoo.py` file.

```
Terminal File Edit View Search Terminal Help
nishant@nishant-ubuntu:~$ cd cuckoo
nishant@nishant-ubuntu:~/cuckoo$ cuckoo.py
cuckoo.py: command not found
nishant@nishant-ubuntu:~/cuckoo$ ./cuckoo.py

[1] Cuckoo Sandbox? OH NOES!
[2]
[3] Cuckoo Sandbox 2.0-dev
www.cuckoosandbox.org
Copyright (c) 2010-2015
[4]
[5] Checking for updates...
You are running a development version! Current stable is 2.0-rc1.
2016-12-13 00:41:22,692 [root] CRITICAL: CuckooCriticalError: Unable to bind ResultServer on 192.168.56.1:2042 [Errno 99] Cannot assign requested address. This usually happens when you start Cuckoo without bringing up the virtual interface associated with the Result Server IP address. Please refer to http://docs.cuckoosandbox.org/en/latest/faq/#troubles-problem for more information.
nishant@nishant-ubuntu:~/cuckoo$ python cuckoo.py

[6] CUCKOO
[7]
[8] Cuckoo Sandbox 2.0-dev
www.cuckoosandbox.org
Copyright (c) 2010-2015
[9]
[10] Checking for updates...
You are running a development version! Current stable is 2.0-rc1.
2016-12-13 00:42:23,445 [root] CRITICAL: CuckooCriticalError: Unable to bind ResultServer on 192.168.56.1:2042 [Errno 99] Cannot assign requested address. This usually happens when you start Cuckoo without bringing up the virtual interface associated with the Result Server IP address. Please refer to http://docs.cuckoosandbox.org/en/latest/faq/#troubles-problem for more information.
nishant@nishant-ubuntu:~/cuckoo$ VBoxManage hostonlyif create
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Interface 'vboxnet2' was successfully created
nishant@nishant-ubuntu:~/cuckoo$ VBoxManage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1 --netmask 255.255.255.0
nishant@nishant-ubuntu:~/cuckoo$ python cuckoo.py
```

At times, an error occurs which can be resolved by running the below commands as shown in the above screen shot:

```
$VBoxManage hostonlyif create  
$VBoxManage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1 --netmask 255.255.255.0
```

```

nishant@nishant-ubuntu: ~/cuckoo
[1] 11923 pts/0 00:46:42 nishant
$ ./cuckooctl start
[...]
Cuckoo Sandbox 2.0-dev
www.cuckoosandbox.org
Copyright (c) 2010-2015

[!] Checking for updates...
[!] You are running a development version! Current stable is 2.0-rc1.
2016-12-13 00:45:59,954 [lib.cuckoo.core.scheduler] INFO: Using "virtualbox" as machine manager
2016-12-13 00:46:02,852 [lib.cuckoo.core.scheduler] INFO: Loaded 2 machine/s
2016-12-13 00:46:02,863 [lib.cuckoo.core.scheduler] INFO: Waiting for analysis tasks.
2016-12-13 23:39:26,135 [lib.cuckoo.core.scheduler] INFO: Starting analysis of FILE "malware1.file" (task #5, options "")
2016-12-13 23:39:29,402 [lib.cuckoo.core.scheduler] INFO: Task #5: acquired machine win7cuckoo (label=win7cuckoo)
2016-12-13 23:39:29,438 [modules.auxiliary.sniffer] INFO: Started sniffer with PID 10460 (interface=vboxnet0, host=192.168.56.101, pc ap=/home/nishant/cuckoo/storage/analyses/5/dump.pcap)
2016-12-13 23:39:42,869 [lib.cuckoo.core.scheduler] ERROR: Machinery error: VboxManage failed starting the machine in HEADLESS mode: VBoxManage: error: cpum#1: "CPU model" mismatch: host=0x3d saved=0x2a [ver=17 pass=final] (VERR_SSM_LOAD_CPUID_MISMATCH)
VBoxManage: error: Details: code NS_ERROR_FAILURE (0x80004005), component ConsoleWrap, interface IConsole

2016-12-13 23:39:42,939 [lib.cuckoo.core.scheduler] CRITICAL: A critical error has occurred trying to use the machine with name win7cuckoo during an analysis due to which it is no longer in a working state, please report this issue and all of the related environment details to the developers so we can improve this situation. (Note that before we would simply remove this VM from doing any more analyses, but as all the VMs will eventually be depleted that way, hopefully we'll find a better solution now).
2016-12-13 23:39:45,201 [modules.processing.behavior] WARNING: Analysis results folder does not exist at path '/home/nishant/cuckoo/storage/analyses/5/logs'.
2016-12-13 23:39:48,158 [modules.processing.static] CRITICAL: You do not have the m2crypto library installed preventing certificate extraction: pip install m2crypto
2016-12-13 23:39:48,502 [lib.cuckoo.common.objects] WARNING: Unable to import yara (please compile from sources)
2016-12-13 23:39:48,540 [modules.processing.network] ERROR: Unable to open /home/nishant/cuckoo/storage/analyses/5/dump_sorted.pcap
2016-12-13 23:39:52,475 [lib.cuckoo.core.scheduler] INFO: Task #5: reports generation completed (path=/home/nishant/cuckoo/storage/analyses/5)
2016-12-13 23:39:52,519 [lib.cuckoo.core.scheduler] INFO: Task #5: analysis procedure completed
2016-12-14 00:24:30,455 [lib.cuckoo.core.scheduler] INFO: Starting analysis of FILE "Malware2.file" (task #6, options "")
2016-12-14 00:24:30,493 [lib.cuckoo.core.scheduler] INFO: Task #6: acquired machine ubuntu-cuckoo (label=ubuntu-cuckoo)
2016-12-14 00:24:34,431 [modules.auxiliary.sniffer] INFO: Started sniffer with PID 11923 (interface=vboxnet0, host=192.168.56.101, pc ap=/home/nishant/cuckoo/storage/analyses/6/dump.pcap)
2016-12-14 00:24:37,326 [lib.cuckoo.core.scheduler] ERROR: Machinery error: VboxManage failed starting the machine in HEADLESS mode: VBoxManage: error: cpum#1: "CPU model" mismatch: host=0x3d saved=0x2a [ver=17 pass=final] (VERR_SSM_LOAD_CPUID_MISMATCH)

```

Next open another terminal, navigate to the web folder within cuckoo and run the manage.py file to run the server.

```

nishant@nishant-ubuntu: ~/cuckoo/web
nishant@nishant-ubuntu:~/cuckoo$ cd web
nishant@nishant-ubuntu:~/cuckoo/web$ ./manage.py runserver
Performing system checks...

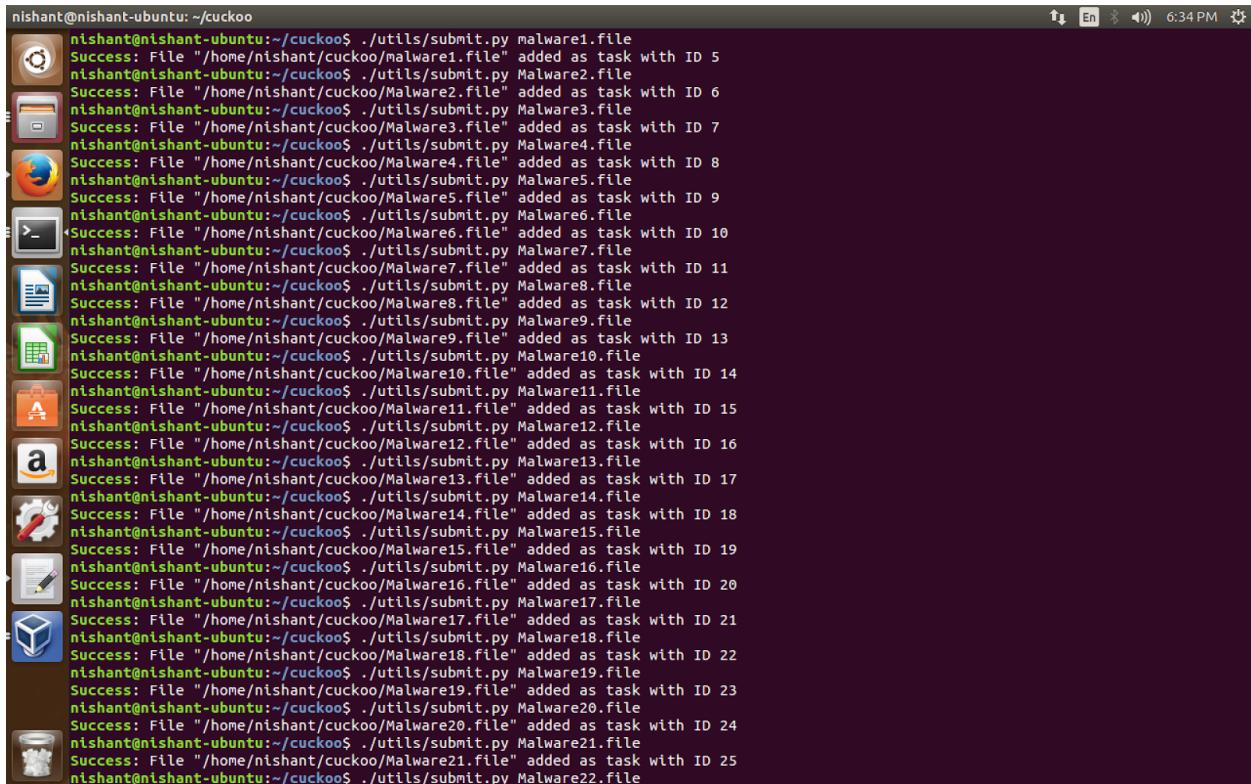
System check identified no issues (0 silenced).
December 13, 2016 - 01:05:20
Django version 1.8.4, using settings 'web.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CONTROL-C.
[13/Dec/2016 01:06:54] "GET / HTTP/1.1" 200 4476
[13/Dec/2016 01:06:54] "GET /static/css/bootstrap.min.css HTTP/1.1" 304 0
[13/Dec/2016 01:06:54] "GET /static/css/style.css HTTP/1.1" 304 0
[13/Dec/2016 01:06:54] "GET /static/css/lightbox.css HTTP/1.1" 304 0
[13/Dec/2016 01:06:54] "GET /static/js/jquery.js HTTP/1.1" 304 0
[13/Dec/2016 01:06:54] "GET /static/js/bootstrap-fileupload.js HTTP/1.1" 304 0
[13/Dec/2016 01:06:54] "GET /static/js/bootstrap.min.js HTTP/1.1" 304 0
[13/Dec/2016 01:06:54] "GET /static/js/lightbox.js HTTP/1.1" 304 0
[13/Dec/2016 01:06:54] "GET /static/js/app.js HTTP/1.1" 304 0
[13/Dec/2016 01:06:54] "GET /static/graphic/cuckoo_inverse.png HTTP/1.1" 304 0
[13/Dec/2016 01:06:54] "GET /static/img/close.png HTTP/1.1" 304 0
[13/Dec/2016 01:06:54] "GET /static/img/loading.gif HTTP/1.1" 304 0
[13/Dec/2016 01:06:54] "GET /static/img/prev.png HTTP/1.1" 304 0
[13/Dec/2016 01:06:54] "GET /static/img/next.png HTTP/1.1" 304 0
[13/Dec/2016 01:06:54] "GET /favicon.ico HTTP/1.1" 404 2667
[13/Dec/2016 23:41:02] "GET / HTTP/1.1" 200 4473
[13/Dec/2016 23:41:02] "GET /static/css/bootstrap.min.css HTTP/1.1" 304 0
[13/Dec/2016 23:41:02] "GET /static/css/style.css HTTP/1.1" 304 0
[13/Dec/2016 23:41:02] "GET /static/css/lightbox.css HTTP/1.1" 304 0
[13/Dec/2016 23:41:02] "GET /static/js/jquery.js HTTP/1.1" 304 0
[13/Dec/2016 23:41:02] "GET /static/js/bootstrap-fileupload.js HTTP/1.1" 304 0
[13/Dec/2016 23:41:02] "GET /static/js/lightbox.js HTTP/1.1" 304 0
[13/Dec/2016 23:41:02] "GET /static/js/bootstrap.min.js HTTP/1.1" 304 0
[13/Dec/2016 23:41:02] "GET /static/js/app.js HTTP/1.1" 304 0
[13/Dec/2016 23:41:02] "GET /static/img/close.png HTTP/1.1" 304 0
[13/Dec/2016 23:41:02] "GET /static/img/loading.gif HTTP/1.1" 304 0
[13/Dec/2016 23:41:02] "GET /static/img/prev.png HTTP/1.1" 304 0
[13/Dec/2016 23:41:03] "GET /static/graphic/cuckoo_inverse.png HTTP/1.1" 304 0
[13/Dec/2016 23:41:03] "GET /static/img/next.png HTTP/1.1" 304 0
[13/Dec/2016 23:43:38] "GET /static/fonts/glyphicons-halflings-regular.woff2 HTTP/1.1" 304 0
[13/Dec/2016 23:46:52] "GET /analysis/ HTTP/1.1" 200 8401
[13/Dec/2016 23:47:07] "GET /dashboard/ HTTP/1.1" 200 4473
[14/Dec/2016 01:21:30] "GET /dashboard/ HTTP/1.1" 200 4477
[14/Dec/2016 01:21:30] "GET /static/css/bootstrap.min.css HTTP/1.1" 304 0

```

To upload the malware sample for testing on the virtual machine via cuckoo, navigate to cuckoo folder and use the below command.

```
$ ./utils/submit.py [malware file path]  
$ ./utils/submit.py Malware21.file
```

Malware sample named “Malware21” is located in Cuckoo folder.



```
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py malware1.file  
Success: File "/home/nishant/cuckoo/malware1.file" added as task with ID 5  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware2.file  
Success: File "/home/nishant/cuckoo/Malware2.file" added as task with ID 6  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware3.file  
Success: File "/home/nishant/cuckoo/Malware3.file" added as task with ID 7  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware4.file  
Success: File "/home/nishant/cuckoo/Malware4.file" added as task with ID 8  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware5.file  
Success: File "/home/nishant/cuckoo/Malware5.file" added as task with ID 9  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware6.file  
Success: File "/home/nishant/cuckoo/Malware6.file" added as task with ID 10  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware7.file  
Success: File "/home/nishant/cuckoo/Malware7.file" added as task with ID 11  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware8.file  
Success: File "/home/nishant/cuckoo/Malware8.file" added as task with ID 12  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware9.file  
Success: File "/home/nishant/cuckoo/Malware9.file" added as task with ID 13  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware10.file  
Success: File "/home/nishant/cuckoo/Malware10.file" added as task with ID 14  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware11.file  
Success: File "/home/nishant/cuckoo/Malware11.file" added as task with ID 15  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware12.file  
Success: File "/home/nishant/cuckoo/Malware12.file" added as task with ID 16  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware13.file  
Success: File "/home/nishant/cuckoo/Malware13.file" added as task with ID 17  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware14.file  
Success: File "/home/nishant/cuckoo/Malware14.file" added as task with ID 18  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware15.file  
Success: File "/home/nishant/cuckoo/Malware15.file" added as task with ID 19  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware16.file  
Success: File "/home/nishant/cuckoo/Malware16.file" added as task with ID 20  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware17.file  
Success: File "/home/nishant/cuckoo/Malware17.file" added as task with ID 21  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware18.file  
Success: File "/home/nishant/cuckoo/Malware18.file" added as task with ID 22  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware19.file  
Success: File "/home/nishant/cuckoo/Malware19.file" added as task with ID 23  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware20.file  
Success: File "/home/nishant/cuckoo/Malware20.file" added as task with ID 24  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware21.file  
Success: File "/home/nishant/cuckoo/Malware21.file" added as task with ID 25  
nishant@nishant-ubuntu:~/cuckoo$ ./utils/submit.py Malware22.file
```

Next, open Firefox and go to localhost:8000 which is the web application for cuckoo.

The screenshot shows the Cuckoo Sandbox web interface in Mozilla Firefox. The title bar says "Cuckoo Sandbox - Mozilla Firefox". The address bar shows "localhost:8000/analysis/". The main content area displays a table titled "Recent Files" with columns: "Timestamp", "Filename", "MD5", and "Status". The table lists 14 entries, all of which are marked as "reported". The last entry is "Malware190" with MD5 "d32f89ee3eef00501a92978269c28aa7". The interface has a sidebar on the left with various icons for file operations like upload, download, and analysis.

Timestamp	Filename	MD5	Status
Dec. 14, 2016, 3:21 p.m.	Malware200	d32f89ee3eef00501a92978269c28aa7	reported
Dec. 14, 2016, 3:21 p.m.	Malware199	ccfa99f13f9e9dd52915c64f5fabae0f	reported
Dec. 14, 2016, 3:21 p.m.	Malware198	c28df132438de065ff8c5a69c97aeb11	reported
Dec. 14, 2016, 3:21 p.m.	Malware197	c3f3ceedcd77792b25f3af64c0fa08cf	reported
Dec. 14, 2016, 3:21 p.m.	Malware196	b78b366d18b5198075cd958e9ac95502	reported
Dec. 14, 2016, 3:21 p.m.	Malware195	a6233fe45e816f0a7f3025731537fe10	reported
Dec. 14, 2016, 3:21 p.m.	Malware194	77307d8e7c4d70868a5d09c31b3781d9	reported
Dec. 14, 2016, 3:21 p.m.	Malware193	2943d8da60adae18fb33f32b66891673	reported
Dec. 14, 2016, 3:21 p.m.	Malware192	691a7baad70a03407835086aebf37010	reported
Dec. 14, 2016, 3:21 p.m.	Malware191	86df1dc95ce11748d57b72d2d0ff5e4	reported
Dec. 14, 2016, 3:21 p.m.	Malware190	34db7f97e0856941ed9c35716700d266	reported
Dec. 14, 2016, 3:21 p.m.	Malware189	27cf39d205567505d840391e4761a7a0	reported
Dec. 14, 2016, 3:21 p.m.	Malware188	10a90073eef40fa09a01f7a7a	reported
Dec. 14, 2016, 3:21 p.m.	Malware190	10a90073eef40fa09a01f7a7a	reported

This application provides information regarding the number of malware samples that have been submitted in Cuckoo. It lets us know if any of the submitted malwares have failed, are pending, in progress, reported, etc.

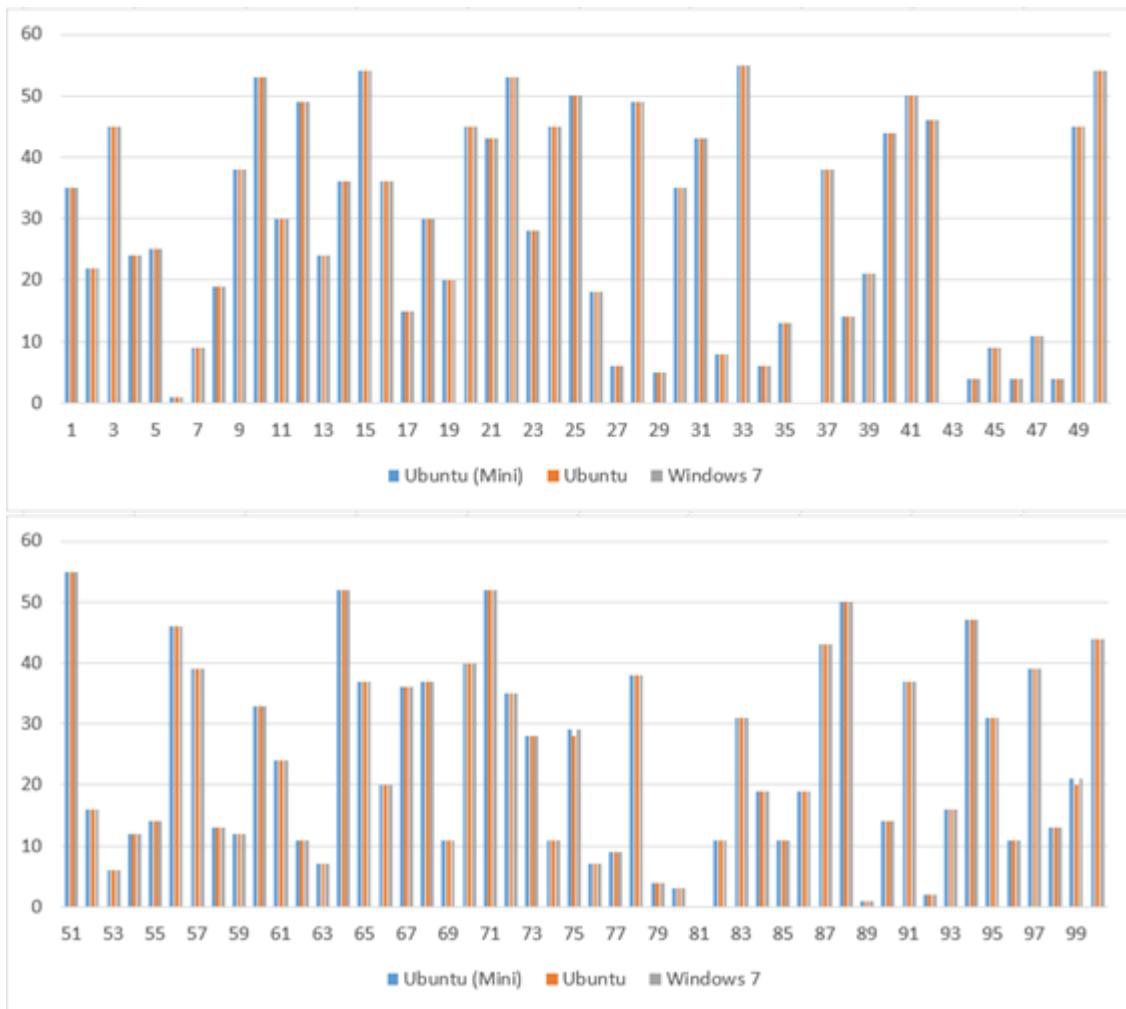
The terminal in below screen shot confirms that the last malware sample run has been successfully completed.

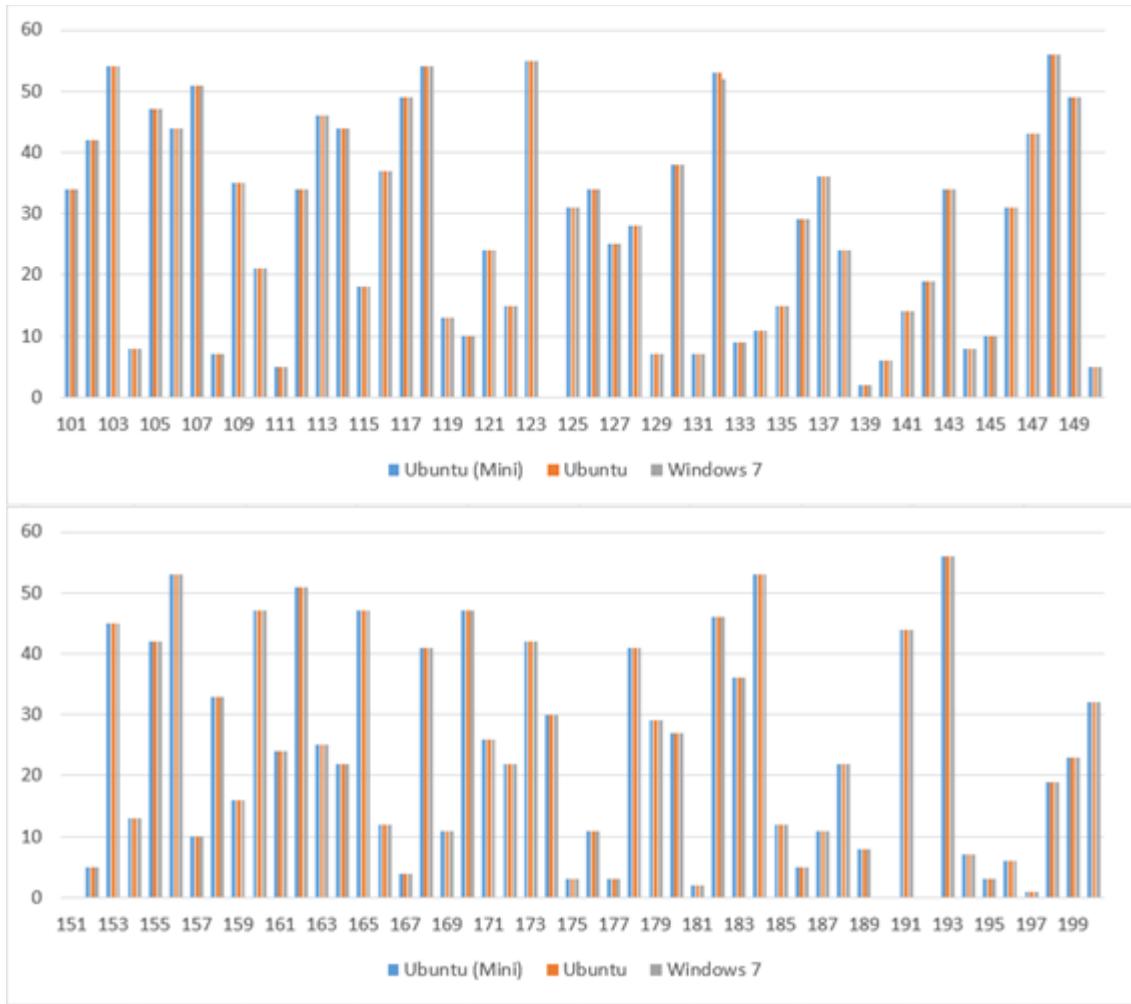
The screenshot shows a terminal window on an Ubuntu system. The command "nishant@nishant-ubuntu: ~/cuckoo\$" is at the prompt. The terminal output shows the log of a Cuckoo analysis task. It starts with task #203 and ends with task #204. The log includes messages from the scheduler, auxiliary modules, processing modules, and the core module. Key messages include "INFO: Task #203: acquired machine win7cuckoo (label=win7cuckoo)", "INFO: Started sniffer with PID 60028 (interface=vboxnet0, host=192.168.56.101, pcap=/home/nishant/cuckoo/storage/analyses/203/dump.pcap)", and "INFO: Task #204: reports generation completed (path=/home/nishant/cuckoo/storage/analyses/204)". The log concludes with "INFO: Task #204: analysis procedure completed".

```
nishant@nishant-ubuntu: ~/cuckoo$ 2016-12-14 15:21:47,170 [lib.cuckoo.core.scheduler] INFO: Task #203: acquired machine win7cuckoo (label=win7cuckoo) 2016-12-14 15:21:47,220 [modules.auxiliary.sniffer] INFO: Started sniffer with PID 60028 (interface=vboxnet0, host=192.168.56.101, pcap=/home/nishant/cuckoo/storage/analyses/203/dump.pcap) 2016-12-14 15:21:47,452 [modules.processing.behavior] WARNING: Analysis results folder does not exist at path '/home/nishant/cuckoo/storage/analyses/203/logs'. 2016-12-14 15:21:47,942 [modules.processing.network] ERROR: Unable to open /home/nishant/cuckoo/storage/analyses/202/dump_sorted.pcap 2016-12-14 15:21:48,071 [lib.cuckoo.core.scheduler] ERROR: Machinery error: VBoxManage failed starting the machine in HEADLESS mode: VBoxManage: error: cpun#1: "CPU model" mismatch: host=0x3d saved=0x2a [ver=17 pass=final] (VERR_SSM_LOAD_CPUID_MISMATCH) VBoxManage: error: Details: code NS_ERROR_FAILURE (0x800040005), component ConsoleWrap, interface IConsole 2016-12-14 15:21:48,075 [lib.cuckoo.core.scheduler] CRITICAL: A critical error has occurred trying to use the machine with name win7cuckoo during an analysis due to which it is no longer in a working state, please report this issue and all of the related environment details to the developers so we can improve this situation. (Note that before we would simply remove this VM from doing any more analyses, but as all the VMs will eventually be depleted that way, hopefully we'll find a better solution now). 2016-12-14 15:21:48,295 [lib.cuckoo.core.scheduler] INFO: Task #202: reports generation completed (path=/home/nishant/cuckoo/storage/analyses/202) 2016-12-14 15:21:48,316 [lib.cuckoo.core.scheduler] INFO: Task #202: analysis procedure completed 2016-12-14 15:21:49,363 [lib.cuckoo.core.scheduler] WARNING: ResultServer did not have 192.168.56.101 in its task info. 2016-12-14 15:21:49,425 [modules.processing.behavior] WARNING: Analysis results folder does not exist at path '/home/nishant/cuckoo/storage/analyses/203/logs'. 2016-12-14 15:21:49,781 [modules.processing.network] ERROR: Unable to open /home/nishant/cuckoo/storage/analyses/203/dump_sorted.pcap 2016-12-14 15:21:50,114 [lib.cuckoo.core.scheduler] INFO: Task #203: reports generation completed (path=/home/nishant/cuckoo/storage/analyses/203) 2016-12-14 15:21:50,139 [lib.cuckoo.core.scheduler] INFO: Task #203: analysis procedure completed 2016-12-14 15:21:50,291 [lib.cuckoo.core.scheduler] INFO: Starting analysis of FILE "Malware200" (task #204, options "") 2016-12-14 15:21:50,332 [lib.cuckoo.core.scheduler] INFO: Task #204: acquired machine ubuntu-cuckoo (label=ubuntu-cuckoo) 2016-12-14 15:21:50,365 [modules.auxiliary.sniffer] INFO: Started sniffer with PID 60186 (interface=vboxnet0, host=192.168.56.101, pcap=/home/nishant/cuckoo/storage/analyses/204/dump.pcap) 2016-12-14 15:21:51,030 [lib.cuckoo.core.scheduler] ERROR: Machinery error: VBoxManage failed starting the machine in HEADLESS mode: VBoxManage: error: cpun#1: "CPU model" mismatch: host=0x3d saved=0x2a [ver=17 pass=final] (VERR_SSM_LOAD_CPUID_MISMATCH) VBoxManage: error: Details: code NS_ERROR_FAILURE (0x800040005), component ConsoleWrap, interface IConsole 2016-12-14 15:21:51,033 [lib.cuckoo.core.scheduler] CRITICAL: A critical error has occurred trying to use the machine with name ubuntu-cuckoo during an analysis due to which it is no longer in a working state, please report this issue and all of the related environment details to the developers so we can improve this situation. (Note that before we would simply remove this VM from doing any more analyses, but as all the VMs will eventually be depleted that way, hopefully we'll find a better solution now). 2016-12-14 15:21:52,395 [modules.processing.behavior] WARNING: Analysis results folder does not exist at path '/home/nishant/cuckoo/storage/analyses/204/logs'. 2016-12-14 15:21:52,716 [modules.processing.network] ERROR: Unable to open /home/nishant/cuckoo/storage/analyses/204/dump_sorted.pcap 2016-12-14 15:21:53,168 [lib.cuckoo.core.scheduler] INFO: Task #204: reports generation completed (path=/home/nishant/cuckoo/storage/analyses/204) 2016-12-14 15:21:53,189 [lib.cuckoo.core.scheduler] INFO: Task #204: analysis procedure completed
```

Analysis of Malwares using Cuckoo in Ubuntu (Mini), Ubuntu and Windows 7

200 malware samples were uploaded onto the Virtual environment and their outputs were analyzed. Cuckoo generates JSON reports for each malware uploaded. This report contains information as to whether an antivirus running on that OS would detect the malware file or not. 56 such antiviruses were considered and the information from the JSON reports of the malwares submitted via Cuckoo were parsed to plot a graph, to determine if the same number of antiviruses were detected by the malware on multiple OSes.





After plotting the graph, it was evident that malware 75, 99, 132 were environment sensitive. They were detected with different values in different VMs. This suggested that they were checking the VMs for various parameters and if they were satisfied, they would lay dormant and lie undetected. We labelled these malware as Environment Sensing Malware.

By not providing generic values for such parameters in the sandboxing environments, we could greatly improve the detection rate of malware.

Future Work

We think it is a good idea to port the cuckoo sandbox we currently run on our personal laptops to a server dedicated to running cuckoo. As such, it will provide a platform to continuously check and monitor new threats, and provide real time analysis of unknown samples that need to be labeled. The dedicated server needs to have sufficient amount of memory to be able to spawn multiple VMs for malware analysis and have a good amount of storage to store the analysis logs

to do further statistical analysis on them. These logs can also be used for academic as well as industry purposes. The server can also be used as part of an Intrusion Prevention System.

Another scope for future work is contributing to the open source project itself. Cuckoo sandbox is hosted on Github and it would be nice to add some features to it or increase code coverage for the code by writing test cases for it. This helps to be involved in the community and contribute towards making computing accessible and secure for people and the community as a whole.

Contributions

- Nishant Rodrigues - Installation of cuckoo sandbox, creation of virtual environment for malware analysis.
- Radhika Pai - Testing first 100 samples of malware on the virtual environment and documenting the test results.
- Vignesh Rajan - Testing next 100 samples of malware on the virtual environment and documenting the test results.

All three team members equally contributed in the analysis of the malware samples and in documenting the test results.

References

1. Rieck, Konrad, et al. "Automatic analysis of malware behavior using machine learning." *Journal of Computer Security* 19.4 (2011): 639-668.
2. Balzarotti, Davide, et al. "Efficient Detection of Split Personalities in Malware." *NDSS*. 2010.
3. Lindorfer, Martina, Clemens Kolbitsch, and Paolo Milani Comparetti. "Detecting environment-sensitive malware." International Workshop on Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2011.
4. Inoue, Daisuke, et al. "Automated malware analysis system and its sandbox for revealing malware's internal and external activities." *IEICE transactions on information and systems* 92.5 (2009): 945-954.
5. Jacob, Grégoire, Hervé Debar, and Eric Filiol. "Behavioral detection of malware: from a survey towards an established taxonomy." *Journal in computer Virology* 4.3 (2008): 251-266.

Appendix

Deliverables:

Our VM is hosted on Google Drive and can be found here:

<https://drive.google.com/drive/folders/0B36t7HEJk5sdchFhOU5JMUZxOUU?usp=sharing>

The username for Ubuntu 15.10 is ‘nishant’ and password is ‘abcd123’

The password for the virtual machines inside the host VM is also set to ‘abcd123’.

Our malware samples were obtained from and can be found at:

<http://dasmalwerk.eu/>

<http://malwaredb.malekal.com/>