

OT Lab 4 (Malware Analysis) - AKOR JACOB TERUNGWA

⌚ Created	@May 10, 2025 11:30 PM
☑ Attendance Required	<input type="checkbox"/>

Task 1: Set up your environment.

1. Use any virtualization environment, better to use the latest version.
2. Prepare and secure malware analysis environment, e.g. FlareVM or Remnux, etc. Make sure that VM uses a **HOST ONLY** network adapter.
3. Or you can create a Virtual Machine and set it up as a malware analysis environment

Preparation:

(Setting Up Cuckoo Sandbox)

Setting up the host machine

My host machine is Ubuntu 18.04 with 16GB of RAM. Before installing Cuckoo on my host machine, it

is required to install some Python libraries and software packages.

I updated the package information and downloaded the available updates.

- **sudo apt-get update**
- **sudo apt-get upgrade**

Next, the following software packages from the apt repositories are required to get Cuckoo to install and run correctly:

1. Installed Dependencies

- sudo apt-get install python python-pip python-dev libffi-dev libssl-dev
- sudo apt-get install python-virtualenv python-setuptools

```

apt-get, or newly installed, or to remove one or more apt-get packages.
jakor@cuckoo:~/Downloads$ sudo apt-get install python python-pip python-dev libffi-dev libssl-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
libffi-dev is already the newest version (3.2.1-8).
python is already the newest version (2.7.15~rc1-1).
python-dev is already the newest version (2.7.15~rc1-1).
libssl-dev is already the newest version (1.1.1-1ubuntu2.1~18.04.23).
python-pip is already the newest version (9.0.1-2.3-ubuntu1.18.04.8).
The following packages were automatically installed and are no longer required:
  gir1.2-goa-1.0 gir1.2-snapd-1
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
jakor@cuckoo:~/Downloads$ sudo apt-get install python-virtualenv python-setuptools
Reading package lists... Done
Building dependency tree
Reading state information... Done
python-setuptools is already the newest version (39.0.1-2ubuntu0.1).
python-setuptools set to manually installed.
The following packages were automatically installed and are no longer required:
  gir1.2-goa-1.0 gir1.2-snapd-1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  python3-distutils python3-lib2to3 python3-virtualenv virtualenv
The following NEW packages will be installed:
  python-virtualenv python3-distutils python3-lib2to3 python3-virtualenv virtualenv
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 316 kB of archives.
After this operation, 3,459 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://gb.archive.ubuntu.com/ubuntu bionic/universe amd64 python-virtualenv all 15.1.0+ds-1.1 [46.8 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu bionic-updates/main amd64 python3-lib2to3 all 3.6.9-1~18.04 [77.4 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu bionic-updates/main amd64 python3-distutils all 3.6.9-1~18.04 [144 kB]
Get:4 http://gb.archive.ubuntu.com/ubuntu bionic/universe amd64 python3-virtualenv all 15.1.0+ds-1.1 [43.4 kB]
Get:5 http://gb.archive.ubuntu.com/ubuntu bionic/universe amd64 virtualenv all 15.1.0+ds-1.1 [4,476 B]
Fetched 316 kB in 2s (197 kB/s)
Selecting previously unselected package python-virtualenv.
(Reading database ... 172422 files and directories currently installed.)
Preparing to unpack .../python-virtualenv_15.1.0+ds-1.1_all.deb ...
Unpacking python-virtualenv (15.1.0+ds-1.1) ...
Selecting previously unselected package python3-lib2to3.
Preparing to unpack .../python3-lib2to3_3.6.9-1~18.04_all.deb ...
Unpacking python3-lib2to3 (3.6.9-1~18.04) ...
Selecting previously unselected package python3-distutils.
Preparing to unpack .../python3-distutils_3.6.9-1~18.04_all.deb ...
Unpacking python3-distutils (3.6.9-1~18.04) ...
Selecting previously unselected package python3-virtualenv.
Preparing to unpack .../python3-virtualenv_15.1.0+ds-1.1_all.deb ...
Unpacking python3-virtualenv (15.1.0+ds-1.1) ...
Selecting previously unselected package virtualenv.
Preparing to unpack .../virtualenv_15.1.0+ds-1.1_all.deb ...
Unpacking virtualenv (15.1.0+ds-1.1) ...
Setting up python-virtualenv (15.1.0+ds-1.1) ...
Setting up python3-lib2to3 (3.6.9-1~18.04) ...
Setting up python3-distutils (3.6.9-1~18.04) ...
Setting up python3-virtualenv (15.1.0+ds-1.1) ...
Setting up virtualenv (15.1.0+ds-1.1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...

```

- sudo apt-get install libjpeg-dev zlib1g-dev swig

```
[Processing triggers for man-db (2.8.3-2ubuntu0.1) ...]
jakor@cuckoo:~/Downloads$ sudo apt-get install libjpeg-dev zlib1g-dev swig
Reading package lists... Done
Building dependency tree
Reading state information... Done
swig is already the newest version (3.0.12-1).
The following packages were automatically installed and are no longer required:
  gir1.2-goa-1.0 gir1.2-snapd-1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libjpeg-turbo8-dev libjpeg8-dev
The following NEW packages will be installed:
  libjpeg-dev libjpeg-turbo8-dev libjpeg8-dev zlib1g-dev
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 404 kB of archives.
After this operation, 1,319 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://gb.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libjpeg-turbo8-dev amd64 1.5.2-0ubuntu5.18.04.6 [225 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu bionic/main amd64 libjpeg8-dev amd64 8c-2ubuntu8 [1,552 B]
Get:3 http://gb.archive.ubuntu.com/ubuntu bionic/main amd64 libjpeg-dev amd64 8c-2ubuntu8 [1,546 B]
Get:4 http://gb.archive.ubuntu.com/ubuntu bionic-updates/main amd64 zlib1g-dev amd64 1:1.2.11.dfsg-0ubuntu2.2 [176 kB]
Fetched 404 kB in 0s (368 kB/s)
Selecting previously unselected package libjpeg-turbo8-dev:amd64.
(Reading database ... 172850 files and directories currently installed.)
Preparing to unpack .../libjpeg-turbo8-dev_1.5.2-0ubuntu5.18.04.6_amd64.deb ...
Unpacking libjpeg-turbo8-dev:amd64 (1.5.2-0ubuntu5.18.04.6) ...
Selecting previously unselected package libjpeg8-dev:amd64.
Preparing to unpack .../libjpeg8-dev_8c-2ubuntu8_amd64.deb ...
Unpacking libjpeg8-dev:amd64 (8c-2ubuntu8) ...
Selecting previously unselected package libjpeg-dev:amd64.
Preparing to unpack .../libjpeg-dev_8c-2ubuntu8_amd64.deb ...
Unpacking libjpeg-dev:amd64 (8c-2ubuntu8) ...
Selecting previously unselected package zlib1g-dev:amd64.
Preparing to unpack .../zlib1g-dev_1%3a1.2.11.dfsg-0ubuntu2.2_amd64.deb ...
Unpacking zlib1g-dev:amd64 (1:1.2.11.dfsg-0ubuntu2.2) ...
Setting up libjpeg-turbo8-dev:amd64 (1.5.2-0ubuntu5.18.04.6) ...
Setting up libjpeg8-dev:amd64 (8c-2ubuntu8) ...
Setting up libjpeg-dev:amd64 (8c-2ubuntu8) ...
Setting up zlib1g-dev:amd64 (1:1.2.11.dfsg-0ubuntu2.2) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
jakor@cuckoo:~/Downloads$
```

To use the Django-based Web Interface, MongoDB is required:

- sudo apt-get install MongoDB

```

jakor@cuckoo:~/Downloads$ sudo apt-get install mongodb
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gir1.2-goa-1.0 gir1.2-snapd-1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libboost-program-options1.65.1 libgoogle-perfetto1s4 libpcrecpp0v5 libsnapy1v5 libtcmalloc-minimal4 libyaml-cpp0.5v5 mongo-tools mongodb-clients mongodb-server
The following NEW packages will be installed:
  libboost-program-options1.65.1 libgoogle-perfetto1s4 libpcrecpp0v5 libsnapy1v5 libtcmalloc-minimal4 libyaml-cpp0.5v5 mongo-tools mongodb-clients mongodb-server
0 upgraded, 11 newly installed, 0 to remove and 0 not upgraded.
Need to get 53.4 MB of archives.
After this operation, 217 MB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://gb.archive.ubuntu.com/ubuntu bionic/main amd64 libboost-program-options1.65.1 amd64 1.65.1+dfsg-0ubuntu5 [137 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu/bionic/main amd64 libtcmalloc-minimal4 amd64 2.5-2.2ubuntu3 [91.6 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu/bionic/main amd64 libgoogle-perfetto1s4 amd64 2.5-2.2ubuntu3 [198 kB]
Get:4 http://gb.archive.ubuntu.com/ubuntu/bionic-updates/main amd64 libpcrecpp0v5 amd64 2:8.39-9ubuntu0.1 [15.3 kB]
Get:5 http://gb.archive.ubuntu.com/ubuntu/bionic/universe amd64 libyaml-cpp0.5v5 amd64 0.5.2-4ubuntu1 [150 kB]
Get:6 http://gb.archive.ubuntu.com/ubuntu/bionic/universe amd64 mongo-tools amd64 3.6.3-0ubuntu1 [12.3 kB]
Get:7 http://gb.archive.ubuntu.com/ubuntu/bionic/main amd64 libsnappy1v5 amd64 1.1.7-1 [16.0 kB]
Get:8 http://gb.archive.ubuntu.com/ubuntu/bionic-updates/universe amd64 mongodb-clients amd64 1:3.6.3-0ubuntu1.4 [20.2 MB]
Get:9 http://gb.archive.ubuntu.com/ubuntu/bionic-updates/universe amd64 mongodb-server-core amd64 1:3.6.3-0ubuntu1.4 [20.3 MB]
Get:10 http://gb.archive.ubuntu.com/ubuntu/bionic-updates/universe amd64 mongodb-server all 1:3.6.3-0ubuntu1.4 [12.6 kB]
Get:11 http://gb.archive.ubuntu.com/ubuntu/bionic-updates/universe amd64 mongodb amd64 1:3.6.3-0ubuntu1.4 [10.2 kB]
Fetched 53.4 MB in 13s (4,238 kB/s)
Selecting previously unselected package libboost-program-options1.65.1:amd64.
(Reading database ... 172899 files and directories currently installed.)
Preparing to unpack .../00-libboost-program-options1.65.1.1-65.1+dfsg-0ubuntu5_amd64.deb ...
Unpacking libboost-program-options1.65.1:amd64 (1.65.1+dfsg-0ubuntu5) ...
Selecting previously unselected package libtcmalloc-minimal4.
Preparing to unpack .../01-libtcmalloc-minimal4_2.5-2.2ubuntu3_amd64.deb ...
Unpacking libtcmalloc-minimal4 (2.5-2.2ubuntu3) ...
Selecting previously unselected package libgoogle-perfetto1s4.
Preparing to unpack .../02-libgoogle-perfetto1s4_2.5-2.2ubuntu3_amd64.deb ...
Unpacking libgoogle-perfetto1s4 (2.5-2.2ubuntu3) ...
Selecting previously unselected package libpcrecpp0v5:amd64.
Preparing to unpack .../03-libpcrecpp0v5_2k3a8.39-9ubuntu0.1_amd64.deb ...
Unpacking libpcrecpp0v5:amd64 (2:8.39-9ubuntu0.1) ...
Selecting previously unselected package libyaml-cpp0.5v5:amd64.
Preparing to unpack .../04-libyaml-cpp0.5v5_0.5.2-4ubuntu1_amd64.deb ...
Unpacking libyaml-cpp0.5v5:amd64 (0.5.2-4ubuntu1) ...
Selecting previously unselected package mongo-tools.
Preparing to unpack .../05-mongo-tools_3.6.3-0ubuntu1_amd64.deb ...
Unpacking mongo-tools (3.6.3-0ubuntu1) ...
Selecting previously unselected package libsnappy1v5:amd64.
Preparing to unpack .../06-libsnappy1v5_1.1.7-1_amd64.deb ...
Unpacking libsnappy1v5:amd64 (1.1.7-1) ...
Selecting previously unselected package mongodb-clients.
Preparing to unpack .../07-mongodb-clients_1%3a3.6.3-0ubuntu1.4_amd64.deb ...
Unpacking mongodb-clients (1:3.6.3-0ubuntu1.4) ...
Selecting previously unselected package mongodb-server-core.
Preparing to unpack .../08-mongodb-server-core_1%3a3.6.3-0ubuntu1.4_amd64.deb ...
Unpacking mongodb-server-core (1:3.6.3-0ubuntu1.4) ...
Selecting previously unselected package mongodb-server.
Preparing to unpack .../09-mongodb-server_1%3a3.6.3-0ubuntu1.4_all.deb ...
Unpacking mongodb-server (1:3.6.3-0ubuntu1.4) ...
Selecting previously unselected package mongo.
Preparing to unpack .../10-mongo_1%3a3.6.3-0ubuntu1.4_amd64.deb ...
Unpacking mongo (1:3.6.3-0ubuntu1.4) ...
Setting up libtcmalloc-minimal4 (2.5-2.2ubuntu3) ...
Setting up libgoogle-perfetto1s4 (2.5-2.2ubuntu3) ...
Setting up libsnappy1v5:amd64 (1.1.7-1) ...
Setting up libpcrecpp0v5:amd64 (2:8.39-9ubuntu0.1) ...
Setting up libyaml-cpp0.5v5:amd64 (0.5.2-4ubuntu1) ...
Setting up libboost-program-options1.65.1:amd64 (1.65.1+dfsg-0ubuntu5) ...
Setting up mongo-tools (3.6.3-0ubuntu1) ...
Setting up mongodb-clients (1:3.6.3-0ubuntu1.4) ...

```

To use PostgreSQL as a database, PostgreSQL will have to be installed as well:

- sudo apt-get install postgresql libpq-dev

```

jakor@cuckoo:~/Downloads$ sudo apt-get install postgresql libpq-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  gir1.2-goa-1.0 gir1.2-snapd-1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libpq5 postgresql-10 postgresql-client-10 postgresql-client-common postgresql-common sysstat
Suggested packages:
  postgresql-doc-10 postgresql-doc locales-all libjson-perl isag
The following NEW packages will be installed:
  libpq-dev libpq5 postgresql postgresql-10 postgresql-client-10 postgresql-client-common postgresql-common sysstat
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 5,539 kB of archives.
After this operation, 22.0 MB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://gb.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libpq5 amd64 10.23-0ubuntu0.18.04.2 [107 kB]
Get:2 http://gb.archive.ubuntu.com/ubuntu bionic-updates/main amd64 libpq-dev amd64 10.23-0ubuntu0.18.04.2 [219 kB]
Get:3 http://gb.archive.ubuntu.com/ubuntu bionic-updates/main amd64 postgresql-client-common all 190ubuntu0.1 [29.6 kB]
Get:4 http://gb.archive.ubuntu.com/ubuntu bionic-updates/main amd64 postgresql-client-10 amd64 10.23-0ubuntu0.18.04.2 [943 kB]
Get:5 http://gb.archive.ubuntu.com/ubuntu bionic-updates/main amd64 postgresql-common all 190ubuntu0.1 [157 kB]
Get:6 http://gb.archive.ubuntu.com/ubuntu bionic-updates/main amd64 postgresql-10 amd64 10.23-0ubuntu0.18.04.2 [3,781 kB]
Get:7 http://gb.archive.ubuntu.com/ubuntu bionic-updates/main amd64 postgresql all 10+190ubuntu0.1 [5,884 B]
Get:8 http://gb.archive.ubuntu.com/ubuntu bionic-updates/main amd64 sysstat amd64 11.6.1-1ubuntu0.2 [295 kB]
Fetched 5,539 kB in 3s (1,631 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libpq5:amd64.
(Reading database ... 172993 files and directories currently installed.)
Preparing to unpack .../0-libpq5_10.23-0ubuntu0.18.04.2_amd64.deb ...
Unpacking libpq5:amd64 (10.23-0ubuntu0.18.04.2) ...
Selecting previously unselected package libpq-dev.
Preparing to unpack .../1-libpq-dev_10.23-0ubuntu0.18.04.2_amd64.deb ...
Unpacking libpq-dev (10.23-0ubuntu0.18.04.2) ...
Selecting previously unselected package postgresql-client-common.
Preparing to unpack .../2-postgresql-client-common_190ubuntu0.1_all.deb ...
Unpacking postgresql-client-common (190ubuntu0.1) ...
Selecting previously unselected package postgresql-client-10.
Preparing to unpack .../3-postgresql-client-10_10.23-0ubuntu0.18.04.2_amd64.deb ...
Unpacking postgresql-client-10 (10.23-0ubuntu0.18.04.2) ...
Selecting previously unselected package postgresql-common.
Preparing to unpack .../4-postgresql-common_190ubuntu0.1_all.deb ...
Adding 'division of /usr/bin/pg_config to /usr/bin/pg_config.libpq-dev by postgresql-common'
Unpacking postgresql-common (190ubuntu0.1) ...
Selecting previously unselected package postgresql-10.
Preparing to unpack .../5-postgresql-10_10.23-0ubuntu0.18.04.2_amd64.deb ...
Unpacking postgresql-10 (10.23-0ubuntu0.18.04.2) ...
Selecting previously unselected package postgresql.
Preparing to unpack .../6-postgresql_10+190ubuntu0.1_all.deb ...
Unpacking postgresql (10+190ubuntu0.1) ...
Selecting previously unselected package sysstat.
Preparing to unpack .../7-sysstat_11.6.1-1ubuntu0.2_amd64.deb ...
Unpacking sysstat (11.6.1-1ubuntu0.2) ...
Setting up sysstat (11.6.1-1ubuntu0.2) ...

Creating config file /etc/default/sysstat with new version
update-alternatives: using /usr/bin/sar.sysstat to provide /usr/bin/sar (sar) in auto mode
Created symlink /etc/systemd/system/multi-user.target.wants/sysstat.service → /lib/systemd/system/sysstat.service.
Setting up libpq5:amd64 (10.23-0ubuntu0.18.04.2) ...
Setting up postgresql-client-common (190ubuntu0.1) ...
Setting up postgresql-common (190ubuntu0.1) ...
Adding user postgres to group ssl-cert

Creating config file /etc/postgresql-common/createcluster.conf with new version
Building PostgreSQL dictionaries from installed myspell/hunspell packages...
  en_us
Removing obsolete dictionary files:
Created symlink /etc/systemd/system/multi-user.target.wants/postgresql.service → /lib/systemd/system/postgresql.service.
Setting up postgresql-client-10 (10.23-0ubuntu0.18.04.2) ...

```

```

Creating config file /etc/postgresql-common/createcluster.conf with new version
Building PostgreSQL dictionaries from installed myspell/hunspell packages...
    en_us
Removing obsolete dictionary files:
Created symlink /etc/systemd/system/multi-user.target.wants/postgresql.service → /lib/systemd/system/postgresql.service.
Setting up postgresql-client-10 (10.23-0ubuntu0.18.04.2) ...
update-alternatives: using /usr/share/postgresql/10/man/man1/psql.1.gz to provide /usr/share/man/man1/psql.1.gz (psql.1.gz) in auto mode
Setting up libpq-dev (10.23-0ubuntu0.18.04.2) ...
Setting up postgresql-10 (10.23-0ubuntu0.18.04.2) ...
Creating new PostgreSQL cluster 10/main ...
/usr/lib/postgresql/10/bin/initdb -D /var/lib/postgresql/10/main --auth-local peer --auth-host md5
The files belonging to this database system will be owned by user "postgres".
This user must also own the server process.

The database cluster will be initialized with locale "en_NG".
The default database encoding has accordingly been set to "UTF8".
The default text search configuration will be set to "english".

Data page checksums are disabled.

fixing permissions on existing directory /var/lib/postgresql/10/main ... ok
creating subdirectories ... ok
selecting default max_connections ... 100
selecting default shared_buffers ... 128MB
selecting default timezone ... Africa/Lagos
selecting dynamic shared memory implementation ... posix
creating configuration files ... ok
running bootstrap script ... ok
performing post-bootstrap initialization ... ok
syncing data to disk ... ok

Success. You can now start the database server using:

    /usr/lib/postgresql/10/bin/pg_ctl -D /var/lib/postgresql/10/main -l logfile start

Ver Cluster Port Status Owner   Data directory      Log file
10_main      5432 down  postgres /var/lib/postgresql/10/main /var/log/postgresql/postgresql-10-main.log
update-alternatives: using /usr/share/postgresql/10/man/man1/postmaster.1.gz to provide /usr/share/man/man1/postmaster.1.gz (postmaster.1.gz) in auto mode
Setting up postgresql (10:190@ubuntu0.1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Processing triggers for ureadahead (0.100.0-21) ...
Processing triggers for libc-bin (2.27-3ubuntu1.6) ...
Processing triggers for systemd (237-3ubuntu10.57) ...
jakor@cuckoo:~/Downloads$ █

```

Below is the command to install VirtualBox 6.0 on the Ubuntu LTS machine.

- sudo dpkg -i virtualbox-6.0_6.0.24-139119~Ubuntu~bionic_amd64.deb

```

virtualbox-6.0_6.0.24-139119-Ubuntu-bionic_amd64.deb
jakor@cuckoo:~/Downloads$ cd Downloads/^
jakor@cuckoo:~/Downloads$ sudo dpkg -i virtualbox-6.0_6.0.24-139119-Ubuntu-bionic_amd64.deb
Selecting previously unselected package virtualbox-6.0.
(Reading database ... 170369 files and directories currently installed.)
Preparing to unpack virtualbox-6.0_6.0.24-139119-Ubuntu-bionic_amd64.deb ...
Unpacking virtualbox-6.0 (6.0.24-139119-Ubuntu-bionic) ...
dpkg: dependency problems prevent configuration of virtualbox-6.0:
  virtualbox-6.0 depends on libcurl4 (>= 7.16.2); however:
    Package libcurl4 is not installed.
  virtualbox-6.0 depends on libqt5core5a (>= 5.9.0~beta); however:
    Package libqt5core5a is not installed.
  virtualbox-6.0 depends on libqt5gui5 (>= 5.4.0); however:
    Package libqt5gui5 is not installed.

VirtualBox - About
File Machine Help
Tools
ORACLE®
VM
VirtualBox 6.0
VirtualBox Graphical User Interface
Version 6.0.24 r139119 (Qt5.9.5)
Copyright © 2020 Oracle Corporation and/or its affiliates. All rights reserved.
Close
libcurl4 libdouble-conversion1 libqt5core5a libqt5dbus5 libqt5gui5
libqt5network5 libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5
libqt5x11extras5 libsdl1.2debian libxcb-xinerama0 qt5-gtk-platformtheme
qttranslations5-l10n
0 upgraded, 15 newly installed, 0 to remove and 0 not upgraded.
1 not fully installed or removed.
Need to get 7,772 kB/10.1 MB of archives.

```

Now I have a working instance of VirtualBox v6.0

Installing tcpdump

To dump the network activity performed by the malware during execution, you'll need a network Sniffer is adequately configured to capture the traffic and dump it into a file.

By default, Cuckoo adopts tcpdump, the prominent open-source solution.

- **sudo apt-get install tcpdump**

```
jakor@cuckoo:~/Downloads$ sudo apt-get install tcpdump
Reading package lists... Done
Building dependency tree
Reading state information... Done
tcpdump is already the newest version (4.9.3-0ubuntu0.18.04.3).
The following packages were automatically installed and are no longer required:
  gir1.2-goa-1.0 gir1.2-snapd-1
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

- sudo apt-get install swig
- sudo pip install m2crypto==0.27.0

```
jakor@cuckoo:~/Downloads$ sudo apt-get install swig
Reading package lists... Done
Building dependency tree
Reading state information... Done
swig is already the newest version (3.0.12-1).
The following packages were automatically installed and are no longer required:
  gir1.2-goa-1.0 gir1.2-snapd-1
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
jakor@cuckoo:~/Downloads$ sudo pip install m2crypto==0.27.0
The directory '/home/jakor/.cache/pip/http' or its parent directory is not owned by the current user and the cache has been disabled. Please check the permissions and try again.
The directory '/home/jakor/.cache/pip' or its parent directory is not owned by the current user and caching wheels has been disabled. Check the permissions and try again.
You may want to set the environment variable 'PIP_DISABLE_PIP_CACHE=1' to avoid this.
Collecting m2crypto==0.27.0
  Downloading https://files.pythonhosted.org/packages/01/bd/a41491718f9e2bebab015c42b5be7071c6695acfa301e3fc0480bfd6a15b/M2Crypto-0.27.0.tar.gz (1.1MB)
    100% |██████████| 1.1MB 1.0MB/s
  Collecting typing (from m2crypto==0.27.0)
    Downloading https://files.pythonhosted.org/packages/0b/cb/da856e81731833b94da70a08712f658416266a5fb2a9d9e426c8061becef/typing-3.10.0.0-py2-none-any.whl
  Installing collected packages: typing, m2crypto
    Running setup.py install for m2crypto ... done
Successfully installed m2crypto-0.27.0 typing-3.10.0.0
jakor@cuckoo:~/Downloads$
```

After installing these packages, I can now install Cuckoo on my system. To install, i run the following commands. Alternatively, I can simply download the zip file.

- sudo pip install -U pip setuptools

```
jakor@cuckoo:~/Downloads$ sudo pip install -U pip setuptools
The directory '/home/jakor/.cache/pip/http' or its parent directory is not owned by the current user and the cache has been disabled. Please check the permissions and try again.
The directory '/home/jakor/.cache/pip' or its parent directory is not owned by the current user and caching wheels has been disabled. Check the permissions and try again.
You may want to set the environment variable 'PIP_DISABLE_PIP_CACHE=1' to avoid this.
Collecting pip
  Downloading https://files.pythonhosted.org/packages/27/79/8a850fe3496446ff0d584327ae44e7500daf6764ca1a382d2d02789accf7/pip-20.3.4-py2.py3-none-any.whl (1.5MB)
    100% |██████████| 1.5MB 791kB/s
  Collecting setuptools
    Downloading https://files.pythonhosted.org/packages/e1/b7/182161210a13158cd3ccc41ee19aade54496b74f2817cc147006ec932b4/setuptools-44.1.1-py2.py3-none-any.whl
    100% |██████████| 583kB 1.3MB/s
  Installing collected packages: pip, setuptools
    Found existing installation: pip 9.0.1
      Not uninstalling pip at /usr/lib/python2.7/dist-packages, outside environment /usr
    Found existing installation: setuptools 39.0.1
      Not uninstalling setuptools at /usr/lib/python2.7/dist-packages, outside environment /usr
  Successfully installed pip-20.3.4 setuptools-44.1.1
jakor@cuckoo:~/Downloads$
```

- sudo pip install -U cuckoo

```

jakor@cuckoo:~/Downloads$ sudo pip install -U cuckoo
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
WARNING: The directory '/home/jakor/.cache/pip/' or its parent directory is not owned or is not writable by the current user. The cache has been disabled. Check the permissions and owner of that directory
If executing pip with sudo, you may want sudo's -H flag.
Collecting cuckoo
  Downloading cuckoo-2.0.7.tar.gz (0.6 MB)
    Collecting alembic==1.0.10
      Downloading alembic-1.0.10.tar.gz (1.0 MB)
        1.0 MB 4.5 MB/s
    Collecting androguard==3.0.1
      Downloading androguard-3.0.1.tar.gz (3.5 MB)
        3.5 MB 6.2 MB/s
    Collecting beautifulsoup4==4.5.3
      Downloading beautifulsoup4-4.5.3-py2-none-any.whl (85 kB)
        85 kB 5.8 MB/s
    Collecting chardet==2.3.0
      Downloading chardet-2.3.0-py2.py3-none-any.whl (180 kB)
        180 kB 7.1 MB/s
    Collecting click==6.6.1
      Downloading click-6.6.1-py2.py3-none-any.whl (71 kB)
        71 kB 5.9 MB/s
    Collecting django==1.8.4
      Downloading Django-1.8.4-py2.py3-none-any.whl (6.2 MB)
        6.2 MB 3.9 MB/s
    Collecting django_extensions==1.6.7
      Downloading django_extensions-1.6.7-py2.py3-none-any.whl (286 kB)
        286 kB 5.7 MB/s
    Collecting dptk==1.8.7
      Downloading dptk-1.8.7-py2-none-any.whl (112 kB)
        112 kB 4.4 MB/s
    Collecting eghatchr<0.3,>=0.2.3
      Downloading eghatchr-0.2.3.tar.gz (4.4 kB)
    Collecting elasticsearch==5.3.0
      Downloading elasticsearch-5.3.0-py2.py3-none-any.whl (66 kB)
        66 kB 11.2 MB/s
    Collecting flask==0.12.2
      Downloading Flask-0.12.2-py2.py3-none-any.whl (83 kB)
        83 kB 6.6 MB/s
    Collecting flask-sqlalchemy==2.4.0
      Downloading Flask_SQLAlchemy-2.4.0-py2.py3-none-any.whl (17 kB)
    Collecting httpreplay<0.3,>=0.2.4
      Downloading HTTPreplay-0.2.6.tar.gz (13 kB)
    Collecting ipaddress<2.1.1,>=1.1.0
      Downloading ipaddress-1.1.0-py2.py3-none-any.whl (18 kB)
    Collecting eventlet<3.3,>=1.2
      Downloading eventlet-1.2.2-cp27-cp27mu-manylinux1_x86_64.whl (1.6 MB)
        1.6 MB 5.5 MB/s
    Collecting Jinja2==2.9.6
      Downloading Jinja2-2.9.6-py2.py3-none-any.whl (340 kB)
        340 kB 5.3 MB/s
    Collecting Isbeautifier<1.6.2
      Downloading Isbeautifier-1.6.2.tar.gz (47 kB)
        47 kB 6.8 MB/s
    Collecting oletools==0.51
      Downloading oletools-0.51.tar.gz (1.5 MB)
        1.5 MB 6.2 MB/s
    Collecting peepdf<0.5,>=0.4.2
      Downloading peepdf-0.4.2.tar.gz (108 kB)
        108 kB 4.4 MB/s
    Collecting pefile<2.1.1
      Downloading pefile-2.1.1.tar.gz (5 kB)
        5 kB 9.8 MB/s
    Collecting pillow==3.2
      Downloading Pillow-3.2.0.tar.gz (10.3 kB)
        10.3 kB 3.7 MB/s

```

```

Building wheel for tlslite-ng (setup.py) ... done
Created wheel for tlslite-ng, filename=tlslite_ng-0.6.0-py2-none-any.whl size=155984 sha256=c086d63b72152e99fafe2a258cbeff6d1bbf02449807bf5d0995eba745e327
Stored in directory: /tmp/pip-ephem-wheel-cache-a56voZ/wheels/fd/ac/3c/bce943ae5d8808e740ddbd1603e7530abdeeb510dd3b647
Building wheel for future (setup.py) ... done
Created wheel for future, filename=future-1.0.0-py2-none-any.whl size=505077 sha256=b554b6966106bc0668545d21f8e7153a102873e0b7ca547b2969d508e4fe1614
Stored in directory: /tmp/pip-ephem-wheel-cache-a56voZ/wheels/3e/85/ab/b3b5e7e8a3dc5d9c7d0c01950f3ff54b13c783d59d1f6042
Building wheel for pyrsistent (setup.py) ... done
Created wheel for pyrsistent, filename=pyrsistent-0.16.1-py2-none-any.whl size=13732 sha256=444726950144da3737f765cd7b5ba002f86d881d452ef5fd39e7cff8851091
Stored in directory: /tmp/pip-ephem-wheel-cache-a56voZ/wheels/72/f7/f0/52088be2ac0f9e0390b674f105a1e2f015e17f4116d546f
Building wheel for functools32 (setup.py) ... done
Created wheel for functools32, filename=functools32-3.2.3-py2-none-any.whl size=10934 sha256=90113ab5ceea21dcf7ad516631860bfbd856a085c7488f61fc30df228b80
Stored in directory: /tmp/pip-ephem-wheel-cache-a56voZ/wheels/c2/e3/35af52f65f4d418a74df08d9cabb9e0b3755bd4dd0d3794
Building wheel for olefile (setup.py) ... done
Created wheel for olefile, filename=olefile-0.43-py2-none-any.whl size=116891 sha256=2002ad43d71e9462d7066099acc20735fc9a2183d695ace3cfcebe6a3548
Stored in directory: /tmp/pip-ephem-wheel-cache-a56voZ/wheels/4d/01/28/e4e969e4669b6e8ec3b1c2cd9dc2b1b7d7fdcc73a620c38
Building wheel for pyrsistent (setup.py) ... done
Created wheel for pyrsistent, filename=pyrsistent-0.16.1-cp27-cp27mu-linux_x86_64.whl size=92180 sha256=8fb105982b5c2628bc0c3a40bbebb79d03e02d31ed50c98a02ff07633f914664
Stored in directory: /tmp/pip-ephem-wheel-cache-a56voZ/wheels/04/bd/0e04aae10782b0c658b0e0f77046590a024f013b351
Building wheel for scandir (setup.py) ... done
Created wheel for scandir, filename=scandir-1.10.0-cp27-cp27mu-linux_x86_64.whl size=36332 sha256=051d2cc65a06f208aab0fc3a3979dc1db2a6021d470b557b5e8e9b50969ad9
Stored in directory: /tmp/pip-ephem-wheel-cache-a56voZ/wheels/58/2c/52406f7d1f9bcc7a70fb1d037a5f293492f5cf1d5c539ed8
Successfully built cuckoo alembic argparse httpreplay Isbeautifier oletools peepdf pefilez pillow pyyaml tools pyuacmole pymongo python-magic roach sqlalchemy wakeonlan yara-python scapy
Installing collected packages: sqlalchemy, MarkupSafe, Mako, python-editor, python-dateutil, alembic, androguard, beautifulsoup4, chardet, click, django, django-extensions, dptk, capstone, eghatch, urllib3, elasticsearch, Werkzeug, itsdangerous, Jinja2, flask, flask-sqlalchemy, edcsa, tlslite-ng, httpreplay, ipaddress, greenlet, Isbeautifier, oletools, colorama, future, pillow, pythonaes, peepdf, arch, olefile, flock, unicorn, wakeonlan, yara-python, scapy, cuckoo
Archiving untracked files...
  Found existing installation: ipaddress 1.0.17
    Uninstalling ipaddress-1.0.17...
      Successfully uninstalled ipaddress 1.0.17
  pip 20.1.1's legacy dependency resolver does not consider dependency conflicts when selecting packages. This behaviour is the source of the following dependency conflicts.
  successfully installed Mako-1.1.6 MarkupSafe-2.0.1 alembic-1.0.18 androguard-3.0.1 attr-21.4.0 beautifulsoup4-4.5.3 capstone-3.0.5rc2 chardet-2.3.0 click-6.6 colorama-0.3.7 configparser-4.2 contextlib2-0.6.0.post1 cuckoo-2.0.1 django-1.8.4 django-extensions-1.6.7 dptk-1.8.7 edcsa-0.19.1 eghatch-0.2.3 sqlalchemy-2.4.0 functions32-3.2.3.post2 future-0.6.0 gevent-1.2.2 greenlet-2.0.2.6 httpreplay-0.2.6 iproutil-metadatas-2.1.3 ipaddress-1.0.23 itsdangerous-1.1.0 jinjaz2-2.16.2 jsonschema-3.2.0 olefile-0.43 oletools-0.51 pathlib2-2.3.7.pst1 peepdf-0.4.2 pefile-0.2.11 pillow-3.2.0 pyopenssl-21.0.0 pyyaml-0.24 pyuacmole-0.6 pymysql-3.0.3 requests-0.16.1 python-dateutil-2.4.2 python-editor-1.0.4 python-magic-0.4.12 pythonaes-1.0 requests-2.23.0 roach-0.1.2 scandir-1.10.0 scapy-2.3.2 sflock-0.3.10 sqlalchemy-1.3.3 tlslite-ng-0.6.0 unicorn-1.0.1 urlib3-1.26.20 wakeonlan-0.2.2 yara-python-3.6.3 zipp-1.2.0

```

After installing Cuckoo, I correctly set up the VirtualBox and its networking.

I created "Host-Only Adapter" by running the following command:

vboxmanage hostonlyif create

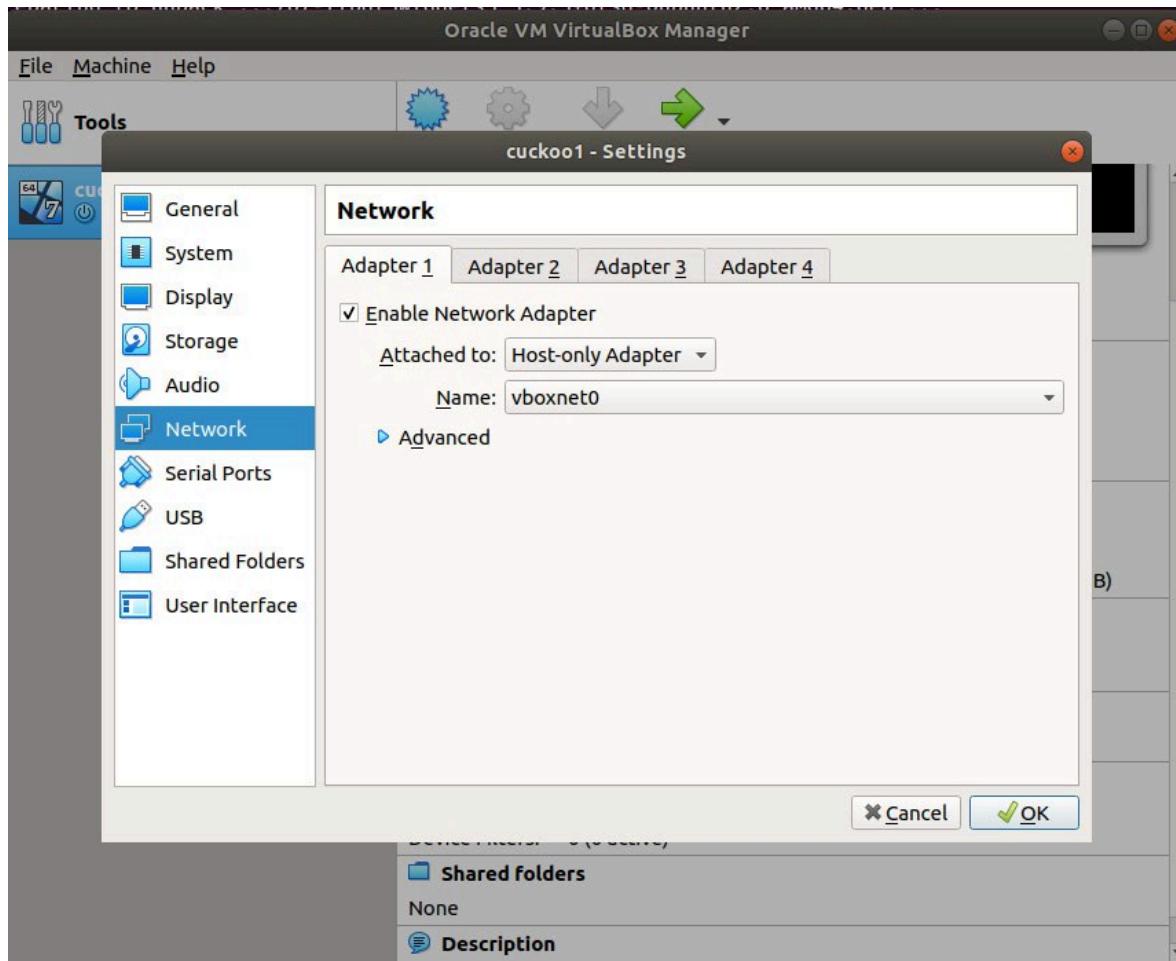
```

50.1
jakor@jakor-VirtualBox:~$ vboxmanage hostonlyif create
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Interface 'vboxnet1' was successfully created
jakor@jakor-VirtualBox:~$ 

```

I set the IP address for the vboxnet0 interface that I created before.
vboxmanage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1

Next, I created my virtual machine in VirtualBox and installed Windows 7 OS. After installing the OS, I configured the VM network adapter to "Host Only Adapter".





Configuration:

After that, I need to configure IP forwarding so that an internet connection gets routed from the host machine to the guest VM. Here, the interface assigned to my VM is enp0s3. The VM's IP address is 192.168.56.101, which is on the subnet of 192.168.56.0/24. The outgoing interface connected to the internet is eth0.

```
sudo iptables -t nat -A POSTROUTING -o eth0 -s 192.168.56.0/24 -j MASQUERADE  
sudo iptables -P FORWARD DROP  
sudo iptables -A FORWARD -m state --state RELATED, ESTABLISHED -j ACCEPT  
sudo iptables -A FORWARD -s 192.168.56.0/24 -j ACCEPT  
sudo iptables -A FORWARD -s 192.168.56.0/24 -d 192.168.56.0/24 -j ACCEPT  
sudo iptables -A FORWARD -j LOG
```

After executing the above commands i had to enable IP forwarding in the kernel. To do that, I executed the following commands:

- echo 1 | sudo tee -a /proc/sys/net/ipv4/ip_forward
- sudo sysctl -w net.ipv4.ip_forward=1

```
jakor@cuckoo:~/Downloads$ echo 1 | sudo tee -a /proc/sys/net/ipv4/ip_forward  
1  
jakor@cuckoo:~/Downloads$ sudo sysctl -w net.ipv4.ip_forward=1  
net.ipv4.ip_forward = 1  
jakor@cuckoo:~/Downloads$
```

I checked whether I had set up the rules correctly. I Run this command:

```
sudo iptables -L
```

```
jakor@cuckoo:~/Downloads$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT    all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT    all  --  192.168.56.0/24      anywhere
ACCEPT    all  --  192.168.56.0/24      192.168.56.0/24
LOG       all  --  anywhere             anywhere           LOG level warning
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
jakor@cuckoo:~/Downloads$
```

Setting up the Guest machine:

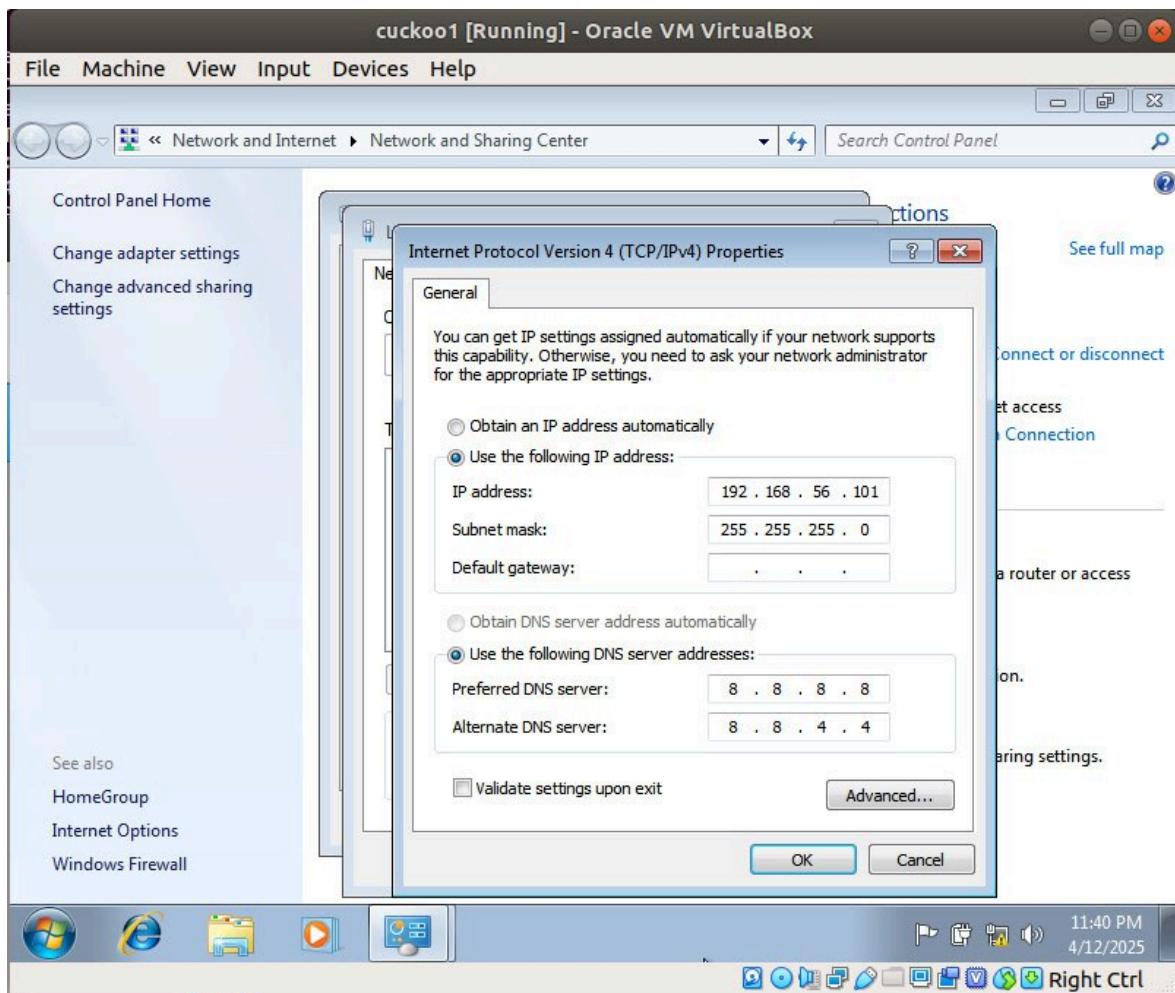
Now I started setting up the guest machine, which has Windows installed. First, I configured the Network Adapter settings are as follows,

IP Address — 192.168.56.101 (VM IP address)

Subnet Mask — 255.255.255.0

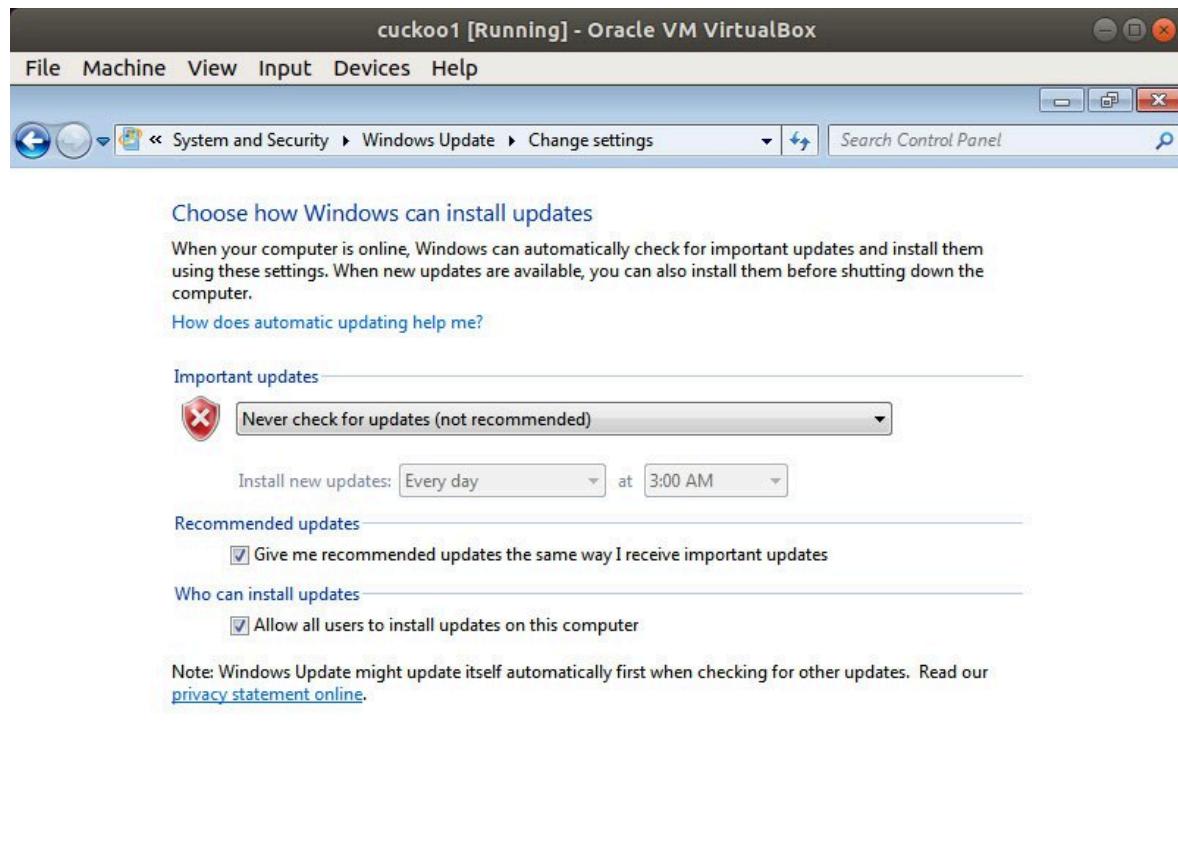
Default Gateway — 192.168.56.1 (Internet accessing interface)

DNS Servers — 8.8.8.8/8.8.4.4

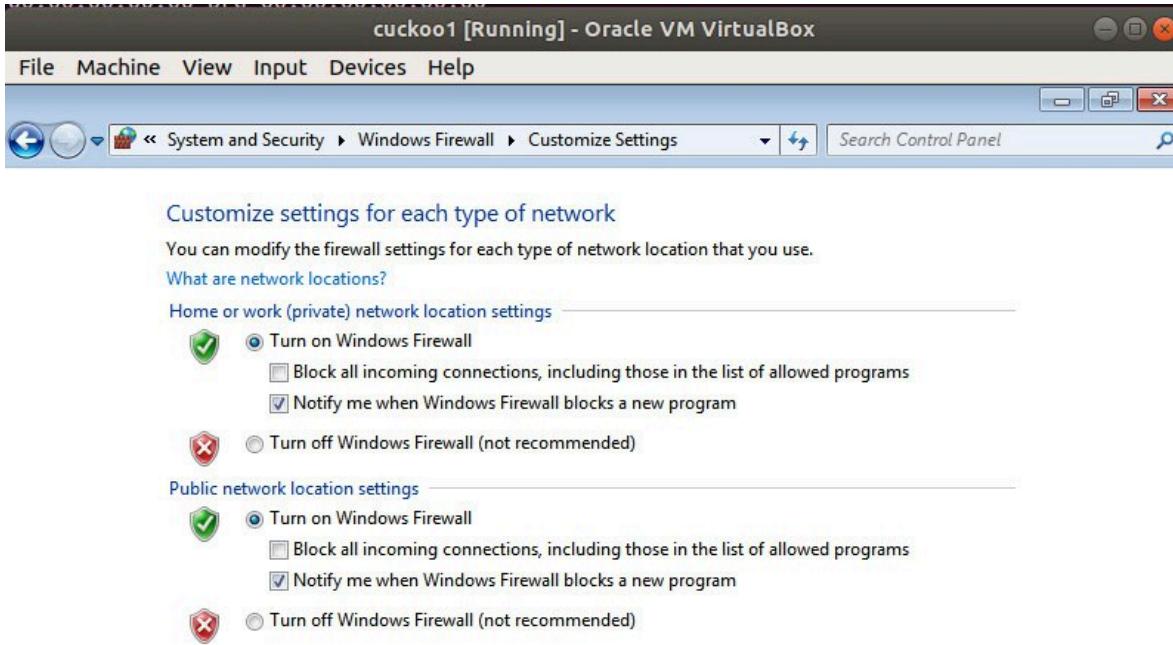


After changing the network configurations, i had to do the following customizations to the VM.

1. I disabled Windows Update and Windows Firewall.



2. Changed User Account Control Settings.



1. Installed Python 2.7 for Windows
2. Uploaded the `agent.py` file from your host machine, which can be found in the `~/cuckoo/agent` directory. Put it in the Windows startup folder located in `"C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup"`. After rebooting the VM, you will be able to see a terminal open in the VM. (You can enable drag and drop in VirtualBox settings. Enable only drag and drop from host to guest.

`pip install --upgrade "pyopenssl<20.0.0" "cryptography<3.0.0"`

```
Jakor@cuckoo:~/Downloads$ pip install --upgrade "pyopenssl<20.0.0" "cryptography<3.0.0"
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details about Python support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/#python-2-support pip 21.0 will remove support for this functionality.
Collecting pyopenssl<20.0.0
  Downloading pyOpenSSL-19.1.0-py2.py3-none-any.whl (53 kB)
Collecting cryptography<3.0.0
  Downloading cryptography-2.9.2-cp27-cp27m-manylinux2010_x86_64.whl (2.7 MB)
Requirement already satisfied, skipping upgrade: six<1.5.2 in /usr/lib/python2.7/dist-packages (from pyopenssl<20.0.0) (1.11.0)
Requirement already satisfied, skipping upgrade: ipaddress; python_version < "3" in /usr/local/lib/python2.7/dist-packages (from cryptography<3.0.0) (1.6.23)
Collecting cffi<1.11.3,>=1.8
  Downloading cffi-1.15.1-cp27-cp27mu-manylinux_x86_64.whl (390 kB)
Requirement already satisfied, skipping upgrade: enum34; python_version < "3" in /usr/lib/python2.7/dist-packages (from cryptography<3.0.0) (1.1.6)
Collecting pycparser
  Downloading pycparser-2.21-py2.py3-none-any.whl (118 kB)
Installing collected packages: pycparser, cffi, cryptography, pyopenssl
Successfully installed cffi-1.15.1 cryptography-2.9.2 pycparser-2.21 pyopenssl-19.1.0
Jakor@cuckoo:~/Downloads$
```

The cuckoo configuration files are located in the `~/cuckoo/conf` directory. I can open those files in gedit using this command:

- `sudo gedit cuckoo.conf`

After finishing configuring, I started Cuckoo.

Analyzing using Cuckoo:

I run the following commands to start Cuckoo and the Cuckoo web interface. I run those in two separate terminal windows.

Terminal #1: **cuckoo**

```
[jakor@cuckoo: ~/volatility$ cuckoo
.....[REDACTED].....
Cuckoo Sandbox 2.0.7
www.cuckoosandbox.org
Copyright (c) 2010-2018

2025-04-13 10:11:30,707 [cuckoo] ERROR: The maximum number of open files is low (4096). If you do not increase it, you may run into errors later on.
2025-04-13 10:11:30,707 [cuckoo] ERROR: See also: https://cuckoo.sh/docs/faqs/index.html#error-errno-24-too-many-open-files
Checking for updates...
[REDACTED] latest Cuckoo version: 4.0.7 Client Error: Forbidden for url: https://cuckoosandbox.org/updates.json?version=2.0.7!
2025-04-13 10:11:31,387 [cuckoo.core.scheduler] INFO: Using "virtualbox" as machine manager
2025-04-13 10:11:31,877 [cuckoo.core.scheduler] INFO: Loaded 1 machine/s
2025-04-13 10:11:31,894 [cuckoo.core.scheduler] INFO: Waiting for analysis tasks.
2025-04-13 10:11:31,894 [cuckoo.core.scheduler] INFO: Starting analysis of FILE "WannaCry.exe" (task #9, options "network-routing=None,procmemdump=yes,route=None")
2025-04-13 10:12:00,426 [cuckoo.core.scheduler] INFO: Task #9: acquired machine cuckoo1 (label=cuckoo1)
2025-04-13 10:12:00,459 [cuckoo.core.scheduler] INFO: Task #9: acquired machine cuckoo1 (label=cuckoo1)
2025-04-13 10:12:04,759 [cuckoo.core.guest] INFO: Started sniffer with PID 16288 (Interface=vboxnet0, host=192.168.56.101)
2025-04-13 10:12:08,831 [cuckoo.core.guest] INFO: Guest is running cuckoo Agent 0.10 (l=192.168.56.101)
2025-04-13 10:15:16,060 [cuckoo.core.guest] INFO: cuckoo1: end of analysis reached!
2025-04-13 10:15:13,922 [cuckoo.machinery.virtualbox] INFO: Successfully generated memory dump for virtual machine with label cuckoo1 to path /home/jakor/.cuckoo/storage/analyses/9/memory.dmp
[REDACTED] Gathering all referenced SSDTs from KeAddSystemServiceTable...
[REDACTED] Finding appropriate address space for tables...
2025-04-13 10:30:51,222 [cuckoo.core.scheduler] INFO: Task #9: reports generation completed
2025-04-13 10:30:51,228 [cuckoo.core.scheduler] INFO: Task #9: analysis procedure completed
```

Terminal #2: **cuckoo web runserver**

Then I can now access the web interface by going to this address in the web browser:

localhost:8000

The screenshot shows the Cuckoo Sandbox web interface running in a Firefox browser. The address bar indicates the URL is 127.0.0.1:8000. The main dashboard is divided into two main sections: 'Insights' on the left and 'Cuckoo' on the right.

Insights Section:

- Cuckoo Installation:** Version 2.0.7, You are up to date.
- Usage statistics:**

	reported	completed	total	running	pending
	0	1	1	0	0
- From the press:** No blogposts have been loaded (this indicates version_check has been disabled in cuckoo.conf). Click here for more.

Cuckoo Section:

- SUBMIT A FILE FOR ANALYSIS:** A file upload icon with the instruction "Drag your file into the left field or click the icon to select a file." and a "Submit" button.
- SUBMIT URLs/HASHES:** A text input field for submitting URLs or hashes.
- System info:** Three donut charts showing system resources.
 - FREE DISK SPACE:** 67.9 GB / 98.3 GB
 - CPU LOAD:** 31% / 3 cores
 - MEMORY USAGE:** 5.6 GB / 7.6 GB

Task 2 - Let's get some malware

I downloaded the following malware from the internet <https://github.com/Da2dalus/The-MALWARERepo>

1. WannaCry ransomware
2. CryptoLocker

Task 3 - Static Analysis

First, I installed Ghidra using snap

Then I launched Ghidra, created a new project, imported the malware, and started analysis

```

1 /* WARNING: Control flow encountered bad instruction data */
2
3 void entry(void)
4{
5
6{
7 byte bVar1;
8 byte *pbVar2;
9 undefined4 *unaff_EDI;
10
11 pbVar2 = (byte *)Ordinal_100("VB5!66");
12 pbVar2 = (byte *)pbVar2;
13 *pbVar2 = *pbVar2 + bVar1;
14 *pbVar2 = *pbVar2 + bVar1;
15 *pbVar2 = *pbVar2 + bVar1;
16 *pbVar2 = *pbVar2 ^ bVar1;
17 *pbVar2 = *pbVar2 + bVar1;
18 *pbVar2 = *pbVar2 + bVar1;
19 *pbVar2 = *pbVar2 + bVar1;
20 *pbVar2 = *pbVar2 + bVar1;
21 *unaff_EDI = pbVar2;
22 /* WARNING: Bad instruction - Truncating control flow here */
23 halt_baddata();
24}
25

```

Decompile: entry x Functions x

00401220 | entry | PUSH 0x401320

Attached below are the functions found

Name	L...	Function Signature	Function Size
DllFunctionCall	004010e0	thunk undefined DllFunctionCall()	6
Ordinal_305	004011d6	thunk undefined Ordinal_305()	6
Ordinal_311	004011dc	thunk undefined Ordinal_311()	6
Ordinal_313	004011e2	thunk undefined Ordinal_313()	6
Ordinal_301	004011e8	thunk undefined Ordinal_301()	6
Ordinal_307	004011ee	thunk undefined Ordinal_307()	6
Ordinal_300	004011f4	thunk undefined Ordinal_300()	6
Ordinal_306	004011f6	thunk undefined Ordinal_306()	6
Ordinal_303	00401206	thunk undefined Ordinal_303()	6
Ordinal_309	00401208	thunk undefined Ordinal_309()	6
ProcCallEngine	00401212	thunk undefined ProcCallEngine()	6
Ordinal_100	00401218	thunk undefined Ordinal_100()	6
entry	00401220	undefined entry(void)	44

Functions - 13 items

Filter:

Decompile: entry x Functions x

00401220 | entry | PUSH 0x401320

Then I checked defined strings, which contained a lot, but I found the name of a DLL

Location	String Value	String Representation	Data Type
00407aa8	qubk	u"qubk"	unicode
00407a70	zwb	u"zwb"	unicode
00407af0	ffffvv	u"ffffvv"	unicode
00407b58	hkbd	u"hkbd"	unicode
00407b80	oargr	u"oargr"	unicode
00407b90	yrxfI	u"yrxfI"	unicode
00407ba4	vhgtx	u"vhgtx"	unicode
00407bb4	taylk	u"taylk"	unicode
00407c5c	Class	"Class"	ds
00407c74	C:\Windows\system32\msvbm60.dll	[C:\Windows\system32\msvbm60.dll]	ds
00407c98	VBRUN	"VBRUN"	ds
00407cd8	C:\Windows\system32\dx7vb.dll	[C:\Windows\system32\dx7vb.dll]	ds
00407dc8	Initialize	"Initialize"	ds
00407dd4	Execute	"Execute"	ds
00407ddc	Terminate	"Terminate"	ds
00407de8	Update	"Update"	ds
00407df0	Interact	"Interact"	ds
00407dfc	Render	"Render"	ds
00407e04	Reset	"Reset"	ds
00407ea4	winmm.dll	"winmm.dll"	ds
00407eb4	timeGetTime	"timeGetTime"	ds
00407ef8	GetCursorPos	"GetCursorPos"	ds
00407f40	SetCursorPos	"SetCursorPos"	ds
00407f8c	ShowCursor	"ShowCursor"	ds
00407fd0	GetAsyncKeyState	"GetAsyncKeyState"	ds
0040801c	kernel32	"kernel32"	ds
0040802c	RtlMoveMemory	"RtlMoveMemory"	ds

Also, some commands could be found:

00407dc8	Initialize	"Initialize"	ds
00407dd4	Execute	"Execute"	ds
00407ddc	Terminate	"Terminate"	ds
00407de8	Update	"Update"	ds
00407df0	Interact	"Interact"	ds
00407dfc	Render	"Render"	ds
00407e04	Reset	"Reset"	ds
00407ea4	winmm.dll	"winmm.dll"	ds
00407eb4	timeGetTime	"timeGetTime"	ds
00407ef8	GetCursorPos	"GetCursorPos"	ds
00407f40	SetCursorPos	"SetCursorPos"	ds
00407f8c	ShowCursor	"ShowCursor"	ds
00407fd0	GetAsyncKeyState	"GetAsyncKeyState"	ds

And other strings that give an idea of some executables:

Location	String Value	String Representa...	Data Type
004082c8	ID_IDirect3DHALDevice	u"ID_IDirect3D...	unicode
004082fc	\gfx	u"\gfx"	unicode
00408318	\sndfmt.wav	u"\sndfmt.wav"	unicode
00408364	ViewportSize	"ViewportSize"	ds
004083c8	ChangeMap	"ChangeMap"	ds
004083d4	ChangeDaytime	"ChangeDaytime"	ds
00408504	ToggleSound	"ToggleSound"	ds
00408510	HitTest	"HitTest"	ds
00408597	AChangeRacer	"AChangeRacer"	ds
004085a4	Command	"Command"	ds
004085ec	welcome to ERACER ...	u"welcome to E..."	unicode
0040861c	demonstrating industrial quality 3D using visual basic ...	u"demonstrating..."	unicode
00408698	use arrow keys to steer, space to jump, ctrl to fire ...	u"use arrow key..."	unicode
00408720	use menu buttons to change environment and start combat ...	u"use menu butt..."	unicode
0040879c	new fighter arrived ...	u"new fighter arr..."	unicode
004087d4	Jaguar	u"Jaguar"	unicode
004087e8	WARTHOG	u"WARTHOG"	unicode
004087fc	daytime changed	u"daytime chan..."	unicode
00408820	new island selected ...	u"new island sel..."	unicode
00408858	incoming fighters detected, protect station ...	u"incoming fight..."	unicode
004088bc	\sndexplosmall.wav	u"\sndexplos..."	unicode
004088fc	sector clear, no enemy activity reported ...	u"sector clear, n..."	unicode
0040895c	jumps use up lots of fuel, watch the blue fuel bar ...	u"jumps use up..."	unicode
004089d0	\gfxcursor.bmp	u"\gfxcursor.bmp"	unicode
004089f4	\gfxinis.bmp	u"\gfxinis.bmp"	unicode
00408a14	\gfxlogo.bmp	u"\gfxlogo.bmp"	unicode
00408a68	Activate	"Activate"	ds

Then I opened the disassembler and discovered that the malware contains a lot of zeros at the head, which may be done to confuse a reader

The screenshot shows the IDA Pro interface with assembly code. The assembly window displays several zero-filled memory locations (00 00 b8 ...) and question mark filled locations (??). One specific entry point is highlighted with the address 00400220 and the instruction 4c 10 00. The assembly code also includes imports for IMAGE_BOUND_IMPORT_DESCRIPTOR_0_00400220 and MSVBVM60.DLL.

1. Compare the findings of both methods, and see if there are some artifacts that online solution did not manage to find, or vice versa. For example, a piece of code or information that helps you in your analysis

WannaCry Analysis

Aspect	Online Analysis (e.g., Hybrid Analysis)	Offline Manual Analysis (e.g., Cuckoo + IDA)
Static Signature	Detects it as WanaCryptor or WannaCry ; flags SMB exploitation	Confirms exploit via EternalBlue and includes specific SMB payload code
IOC Extraction	IPs, file hashes, mutex names	Deeper discovery of kill switch domain hardcoded in binary (www.iuqerfsodp9ifjaposdfjhgosurijfaewrwegwae.com)
Payload Behavior	Ransom note dropped and tor site contacted	Observes local encryption flow using AES + RSA and process injection (e.g., taskdl.exe)
Artifacts Missed by Online Tools	Limited system call tracing; some anti-VM behavior not triggered	Able to catch fake checks for disk space , VM artifacts , and obfuscation tricks

CryptoLocker Analysis

Aspect	Online Analysis	Offline Manual Analysis
--------	-----------------	-------------------------

Malware Family Identification	Identified as CryptoLocker variant via static signature	Confirms RSA-2048 key generation, registry persistence
Network Indicators	Detects communication with C2 servers over HTTPS	Observes domain generation algorithm (DGA) with time-based TLD changes
Ransom Behavior	Confirms ransom note file and encryption start	Tracks detailed registry keys used for persistence (HKCU\Software\CryptoLocker)
Artifacts Missed by Online Tools	Can't fully trace DGA logic or encryption functions	Able to extract embedded PE resources (e.g., ransom HTML templates) and decode communication headers

4. Try to describe which method is better (Sandboxing vs Static analysis) is better, and which one is more useful in which case.

Sandboxing vs Static Analysis – Comparison and Use Cases

Static Analysis (e.g., using Ghidra)

- **Advantages:**
 - Reveals the internal logic, algorithms, and hardcoded data (e.g., encryption keys, DGA routines).
 - Doesn't require executing the malware, so it's safer.
 - Useful for understanding obfuscation, code reuse, and stealth techniques.
- **Disadvantages:**
 - Time-consuming and requires reverse-engineering skills.
 - Can be defeated by strong packing or obfuscation.
- **Use Case:**
 - Deep understanding of malware logic.
 - Detecting **zero-day behavior**, obfuscated payloads, and **persistence mechanisms**.
 - Forensic-grade evidence collection.

Sandboxing (e.g., Cuckoo)

-
- **Advantages:**
 - Fast and automated — reveals high-level behavior, like dropped files, registry changes, and C2 traffic.
 - Good at identifying **Indicators of Compromise (IOCs)** quickly.
 - Useful for non-technical analysts and triage.
 - **Disadvantages:**

- Limited by anti-VM/anti-sandbox techniques.
 - May miss behaviors that are time-triggered or environment-dependent.
- **Use Case:**
 - Rapid behavioral assessment of malware.
 - IOC generation for SIEM or threat intel.
 - First-stage triage in incident response.

A Better One?

- To me, they are complementary, not competing.
 - Used sandboxing for quick insights and IOC extraction.
 - Used static analysis when sandbox output is inconclusive or when you need to understand the malware's true intent and structure.

Task 5 - Dynamic Analysis (Bonus)

Sandbox Analysis

Step 1: I submitted WannaCry Malware to Cuckoo



Analysis Summary of WannaCry Malware

The screenshot shows the Cuckoo Sandbox analysis interface. At the top, it displays the URL 127.0.0.1:8000/analysis/9/summary/. The main area is titled "Summary" and contains the following information:

- File WannaCry.exe**
- Score**: This file is very suspicious, with a score of 17.4 out of 10!
- Summary**:
 - Size: 224.0KB
 - Type: PE32 executable (GUI) Intel 80386, for MS Windows
 - MDS: 5c7fb0927db37372da25f270788183a2
 - SHA1: 120ed9279d85cbfa5e5b7779ffa7162074f7a29
 - SHA256: be22645c61949d6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844
 - SHA512: Show SHA512
 - CRC32: 02AC7126
 - ssdeep: None
 - Yara: None matched
- Information on Execution**:
 - Analysis: Category Started Completed Duration Routing Logs

The log from the analysis confirms the execution of WannaCry ransomware (or a variant) with clear behavioral patterns matching its known malicious activities. Below is a detailed breakdown:

Some important Observations

1. Initial Execution & Payload Dropping

Sample Executed: C:\Users\jakor\AppData\Local\Temp\WannaCry.exe (PID 1208)

Dropped Files:

Encryption components: c.wry, m.wry, r.wry, t.wry, u.wry

Batch script: 205981744552341.bat (likely for persistence or cleanup)

Ransom note: !Please Read Me!.txt

Encryption keys: 00000000.pky, 00000000.eky, 00000000.res

2. Document Encryption (Ransomware Behavior)

Appends .WCRYT extension to files (WannaCry's signature):

C:\Users\jakor\Documents\BZMcQrlAvBqslJ.ppt.WCRYT

C:\Users\jakor\Documents\IOFOjaEJOC.docx.WCRYT

C:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg.WCRYT

Targets multiple file types:

Office docs (.docx, .ppt, .docm)

Images (.jpg, .png, .bmp)

Media (.mp3, .wma, .wmv)

System files (thumbnails, databases, logs)

3. Persistence & Propagation

Creates a shortcut: !WannaDecryptor!.exe.lnk (likely for autorun)

Injects into explorer.exe (PID 1844) to maintain persistence.

Uses cmd.exe & cscript.exe to execute secondary scripts.

4. Anti-Recovery Measures

Executes vssadmin.exe (PID 2696) to delete shadow copies (prevents file recovery).

Uses WMIC.exe (PID 2648) for system interrogation (possibly checking for defenses).

5. Process Injection & Evasion

Injects into multiple processes:

cmd.exe (multiple instances)

!WannaDecryptor!.exe (malicious child processes)

explorer.exe (stealth)

Attempts to kill processes via taskkill.exe (likely disabling security tools).

6. Network Activity (Suspicious)

Queries

dns.msftncsi.com (Microsoft NCSI, checks for internet connectivity).

Connects to 8.8.8.8 (Google DNS)—possibly for C2 communication.

Sandbox Evasion Techniques Detected

The malware employs multiple anti-sandbox checks (as seen in earlier logs):

Debugger Detection (IsDebuggerPresent checks)

Foreground Window Monitoring (checks for human activity)

Memory & Disk Queries (detects low-resource VMs)

Delayed Execution (avoids automated analysis timeouts)

Analysis Summary of CryptoLocker:

The screenshot shows the Cuckoo Sandbox analysis interface. At the top, it displays the URL 127.0.0.1:8000/analysis/10/summary/. The main area is titled "Summary" and contains detailed information about the file "CryptoLocker.exe". Key details include:

- File**: CryptoLocker.exe
- Summary**:
 - Size: 338.0KB
 - Type: PE32 executable (GUI) Intel 80386, for MS Windows
 - MD5: 04fb36199787f2e3e2135611a38321eb
 - SHA1: 65559245709fe98052eb284577f1fd61c01ad20d
 - SHA256: d765e722e295969c0a5c2d90f549db8b89ab617980bf4698db41c7cdad993bb9
 - SHAS12: Show SHAS12
 - CRC32: 412C0FF3
 - ssdeep: None
 - Yara: None matched
- Score**: This file is very suspicious, with a score of 8.6 out of 10!
- Please notice**: The scoring system is currently still in development and should be considered an alpha feature.
- Feedback**: Expecting different results? Send us this analysis and we will inspect it. Click here.

Some important Observations

1. Malware Persistence & Evasion

Execution Path: C:\Users\jakor\AppData\Local\Temp\CryptoLocker.exe

Typical of ransomware using Temp folders to avoid detection.

Randomized Child Process Names: {34184A33-0407-212E-330B-0C020115E2C2}.exe

Avoids signature-based detection (UUID-style naming).

2. Process Injection & Encryption

Two child processes (PIDs 2908 and 2800) spawned and monitored.

These are likely responsible for file encryption (CryptoLocker uses multi-threaded encryption).

Memory dumps taken before termination (useful for forensic analysis).

3. Anti-Analysis Tactics

Short-lived parent process (CryptoLocker.exe exits after 11 seconds).

No screenshots (Pillow is not installed, but malware may also block screenshots).

No network activity logged (may use delayed C2 or encrypted channels).

Indicators of Compromise (IOCs)

Files

Main Payload:

C:\Users\jakor\AppData\Local\Temp\CryptoLocker.exe

Child Processes:

{34184A33-0407-212E-330B-0C020115E2C2}.exe (multiple instances)

Processes

Parent: CryptoLocker.exe (PID 2864)

Children: {34184A33...}.exe (PIDs 2908, 2800)

Behavioral Signatures

Ransomware-like process injection

Temp folder execution (common in CryptoLocker)

Randomized process names (evasion)

Rapid process termination (anti-debugging)
Comparison to Known CryptoLocker Variants
Feature This Sample Classic CryptoLocker
Execution Path %LocalAppData%\Temp %AppData% or %LocalAppData%
Process Names UUID-style ({...}.exe) Random names (e.g., uihf.exe)
Persistence Not yet observed Registry Run keys
Encryption Threads Multiple (PID 2908, 2800) Single-threaded in early versions
Conclusion: This is likely a newer variant with improved evasion tactics.

What kind of benefit does this method have?

- **Automated Dynamic Analysis**

Cuckoo runs malware in a controlled virtual environment, automatically capturing its behavior, such as file changes, network connections, and process activity.

- **Comprehensive Reports**

It generates detailed JSON/HTML reports with:

- API calls
- Dropped files
- Registry changes
- Memory dumps
- Screenshots

- **Network Traffic Capture**

Captures and analyzes full PCAPs, helping detect command-and-control (C2) communication, DNS requests, and data exfiltration attempts.

- **Customizable and Extensible**

You can add custom signatures, integrate YARA rules, or hook into other forensic tools (e.g., Volatility for memory analysis).

- **Supports Multiple Platforms**

Cuckoo can analyze Windows, Linux, macOS, and Android malware by configuring different virtual machines.

- **Safe Environment**

Malware is executed in isolated virtual machines, protecting the host system from infection.

- **Useful for Threat Intelligence and IOC Extraction**

It helps generate Indicators of Compromise (IOCs) that can be shared with SOC teams or used in SIEM systems like Wazuh.