HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
MÃ ĐỘC

BÀI THỰC HÀNH SỐ 09

Hệ thống tự động phân tích mã độc

Người thực hiện bài thực hành:

TS. Đặng Xuân Bảo

Hà Nội, 2020

MỤC LỤC

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Hệ thống tự động phân tích mã độc

Học phần: Mã độc

Số lượng sinh viên cùng thực hiện:

Địa điểm thực hành: Phòng máy

Yêu cầu:

- Yêu cầu phần cứng:
  - Máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 4GB, HDD 500GB
- Yêu cầu phần mềm trên máy:
  - Hệ điều hành Windows 10
  - VMware Worstation 15.0
  - Máy ảo VMware: Ubuntu 18.04
  - Bộ cài windows 7(*.ISO), python 2.7, pypi pillow 5.1.0
- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

Hệ thống tự động phân tích mã độc

1.1. Mô tả

Bài thực hành giới thiệu và hướng dẫn sinh viên sử dụng hệ thống tự động phân tích mã độc Cuckoo Sandbox.

Cuckoo là một hệ thống mã nguồn mở cho phép phân tích phần mềm độc hại một cách tự động. là một tập các mã kịch bản viết bằng ngôn ngữ Python.

Cuckoo được sử dụng để tự động chạy phân tích các tệp và thu thập các kết quả phân tích toàn diện để phác thảo những gì phần mềm độc hại làm trong khi chạy bên trong một hệ điều hành bị cô lập.

Cuckoo có thể thu thập được dữ liệu như sau:

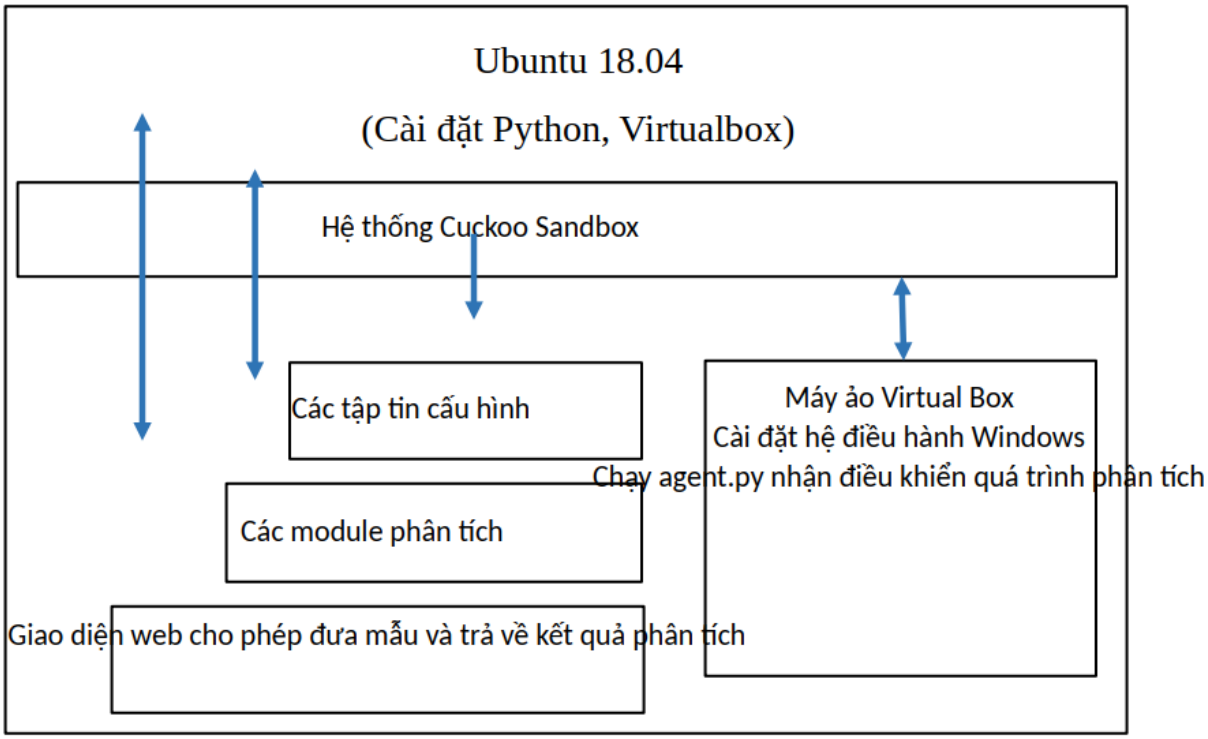
- Dấu vết của các hàm API được gọi bởi tất cả các tiến trình malware sinh ra.
- Các tệp tin được tạo, xóa, sửa và tải xuống bởi phần mềm độc hại trong suốt quá trình thực thi của chúng.
- Trích xuất toàn bộ bộ nhớ của một tiến trình.
- Theo dõi lưu lượng mạng ở định dạng PCAP.
- Ảnh chụp màn hình trong quá trình thực thi phần mềm độc hại.
- Trích xuất bộ nhớ đầy đủ của hệ thống.

Cuckoo được thiết kế để được sử dụng như một ứng dụng độc lập cũng như được tích hợp trong các framework lớn, nhờ được thiết kế bởi mô-đun đặc biệt. Cuckoo có thể được sử dụng để phân tích:

- Các tệp thực thi của Windows
- Các tệp DLL
- Các tài liệu PDF
- Các tài liệu Microsoft Office
- Các tệp URLs và HTML
- PHP scripts

- Các tệp CPL
- Visual Basic (VB) scripts
- Các tệp ZIP
- Java JAR
- Các tệp Python
- Và các tệp tin khác…

1.2. Triển khai hệ thống tự động phân tích mã độc



Mô hình hệ thống phân tích mã độc Cuckoo sandbox

Cài đặt các gói phần mềm cần thiết

- Để tiện việc cài đặt nên tạo và đăng nhập user có tên: cuckoo

- Các gói phần mềm được cài đặt từ kho apt trên HĐH Ubuntu 18.04

- Cài đặt git:

```
$ sudo apt-get update

$ sudo apt-get install git
```

- Các thành phần máy chủ Cuckoo được viết hoàn toàn bằng Python, do đó bắt buộc phải cài đặt phiên bản Python thích hợp. Tại thời điểm bài thực hành được xây dưng, Cuckoo sandbox chỉ hỗ trợ đầy đủ Python 2.7.

```
$ sudo apt-get install python python-pip python-dev libffi-dev libssl-dev -y

$ sudo apt-get install python-virtualenv python-setuptools -y

$ sudo apt-get install libjpeg-dev zlib1g-dev swig -y
```

- Để sử dụng Giao diện web dựa trên Django, ta cài đặt MongoDB:

```
$ sudo apt-get install mongodb -y
```

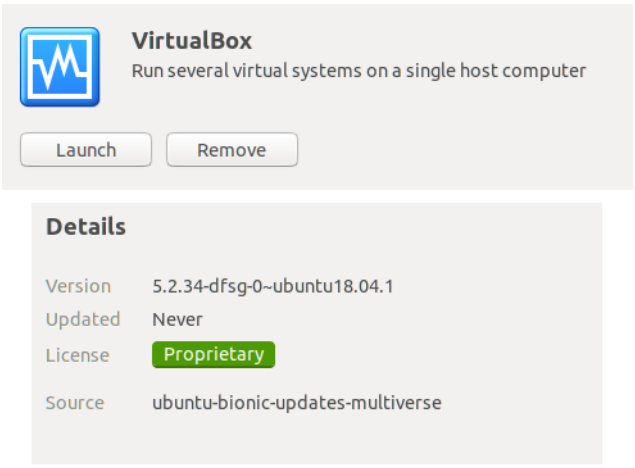
- Dùng PostgreSQL làm cơ sở dữ liệu:

```
$ sudo apt-get install postgresql libpq-dev -y
```

- Cài đặt phần mềm ảo hóa Virtualbox 5.2:

```
$ echo deb http://download.virtualbox.org/virtualbox/debian xenial contrib | sudo tee -a /etc/apt/sources.list.d/virtualbox.list

$ wget -q https://www.virtualbox.org/download/oracle_vbox_2016.asc -O- | sudo apt-key add -

$ sudo apt-get update

$ sudo apt-get install virtualbox-5.2
```

Nếu quá trình cài đặt xảy ra lỗi ta có thể cài đặt qua Ubuntu software:



- Cài đặt tcpdump:

  $ sudo apt-get install tcpdump apparmor-utils

  $ sudo aa-disable /usr/sbin/tcpdump

- Cài đặt Volatility:

  $ sudo git clone https://github.com/volatilityfoundation/volatility

  $ cd volatility

  $ sudo python ./setup.py install

- Cài đặt M2Crypto:

  $ sudo apt-get install swig

  $ sudo pip install m2crypto

- Sau khi cài lần lượt các phần mềm trên, ta tiến hành cài đặt Cuckoo sandbox

Cài đặt Cuckoo sandbox

Trên máy Ubuntu 18.04

Bước 1: cài đặt Cuckoo sandbox

$ sudo pip install -U pip setuptools

$ sudo pip install -U cuckoo

$ sudo pip install distorm3

- Nếu xuất hiện lỗi như sau hình dưới, ta cài đặt cryptography 2.8

$ sudo pip install cryptography==2.8

```
ERROR: pyopenssl 19.1.0 has requirement cryptography>=2.8, but you'll have cryptography 2.1.4 which is incompatible.
```

Bước 2: Cấu hình đường dẫn CWD:

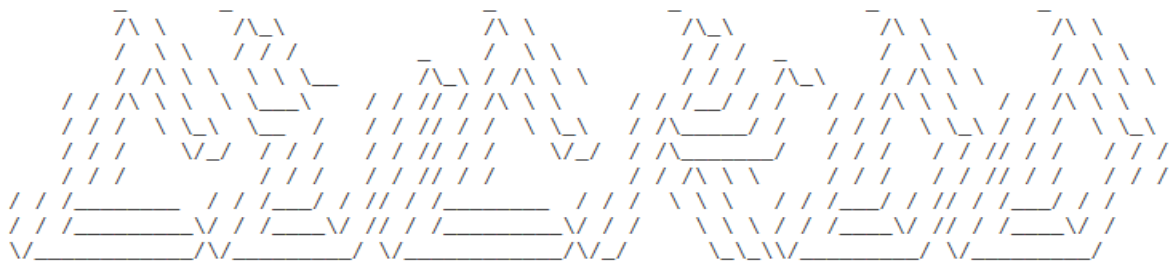
$ sudo mkdir /opt/cuckoo

$ sudo chown cuckoo:cuckoo /opt/cuckoo

$ cuckoo --cwd /opt/cuckoo

- Kết quả khi cài đặt thành công:

```
$ cuckoo -d
```



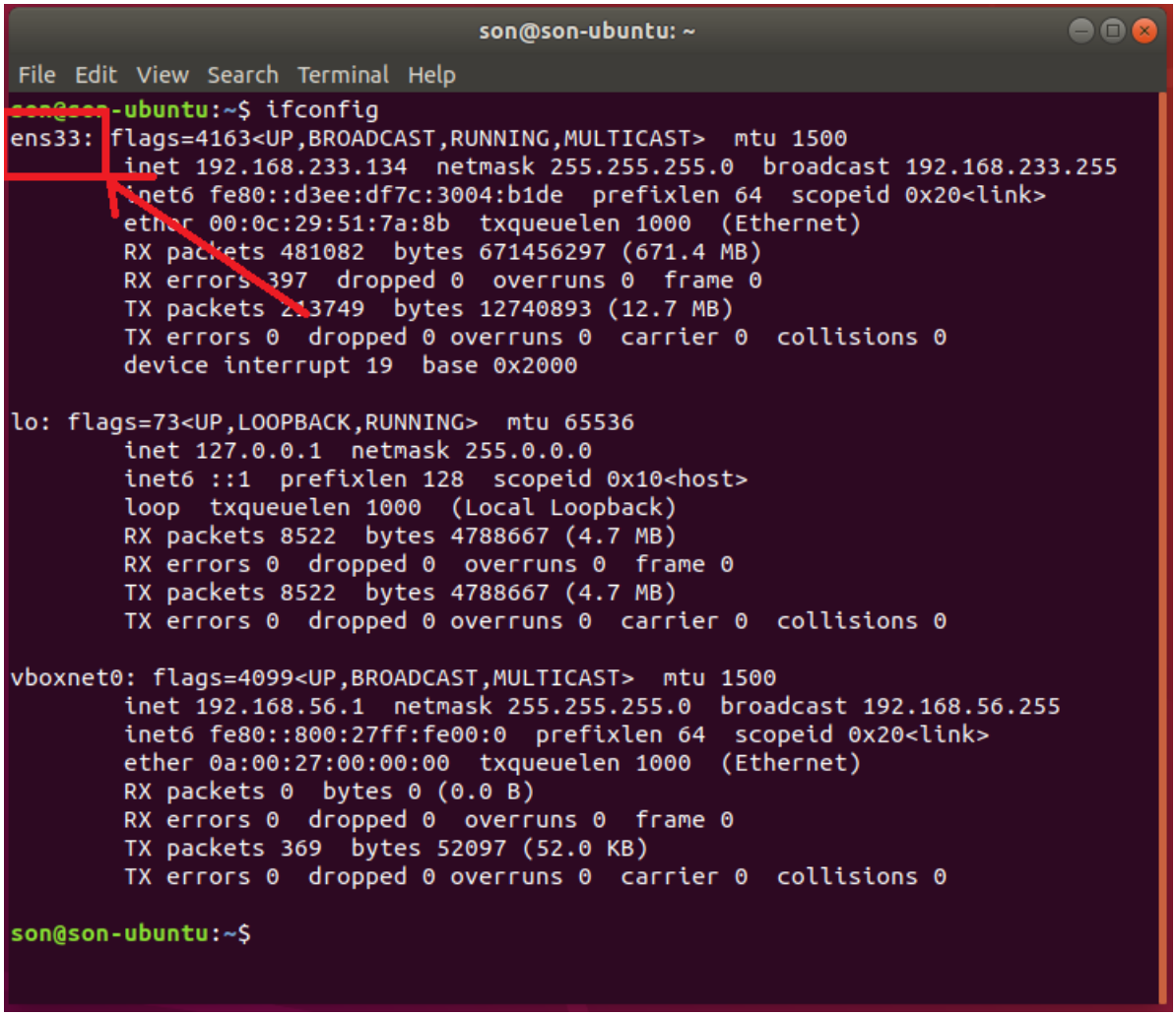
```
Cuckoo Sandbox 2.0.0
www.cuckoosandbox.org
Copyright (c) 2010-2017

================================================================================
    Welcome to Cuckoo Sandbox, this appears to be your first run!
    We will now set you up with our default configuration.
    You will be able to modify the configuration to your likings
    by exploring the /home/cuckoo/.cuckoo directory.

    Among other configurable things of most interest is the
    new location for your Cuckoo configuration:
            /home/cuckoo/.cuckoo/conf
================================================================================

Cuckoo has finished setting up the default configuration.
Please modify the default settings where required and
start Cuckoo again (by running `cuckoo` or `cuckoo -d`).
```

Bước 3: Sau đó ta định tuyến mạng và thiết lập quy tắc iptable:

$ vboxmanage hostonlyif create

```
$ vboxmanage hostonlyif ipconfig vboxnet0 --ip 192.168.56.1

$ sudo iptables -A FORWARD -o ens33 -i vboxnet0 -s 192.168.56.0/24 -m conntrack --ctstate NEW -j ACCEPT

$ sudo iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

$ sudo iptables -A POSTROUTING -t nat -j MASQUERADE

$ echo 1 | sudo tee -a /proc/sys/net/ipv4/ip_forward

$ sudo sysctl -w net.ipv4.ip_forward=1
```

LƯU Ý: ens33 thay đổi tùy thuộc vào interface connected, kiểm tra bằng cách gõ ifconfig.



Cài đặt trên máy windows 7

- Tiếp theo ta cài đặt windows 7 trên phần mềm Virtualbox đã cài trên HĐH Ubuntu 18.04 trước đó. Sau khi cài đặt xong, ta thực hiện lần lượt các bước sau:

*Chú ý: Để tiện cài đặt giữa cuckoo và máy ảo, ta nên đặt tên máy ảo win7 là: cuckoo1

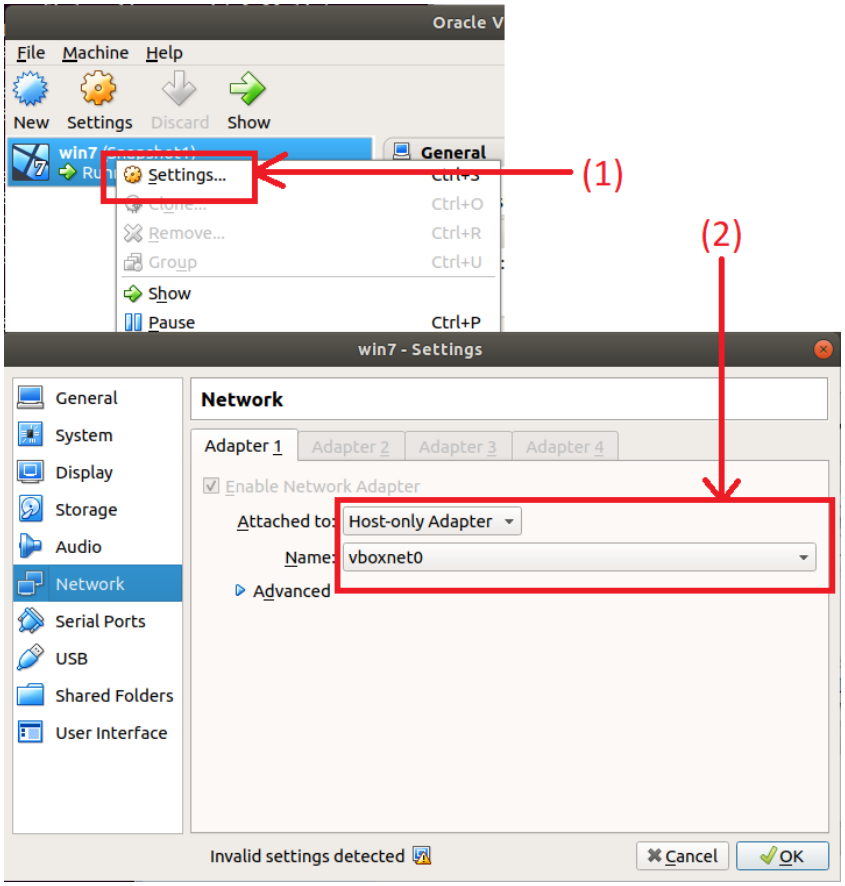
Bước 1: download, cài đặt python 2.7 và pypi pillow 5.1.0

https://www.python.org/downloads/ (tìm bản python 2.7.0)

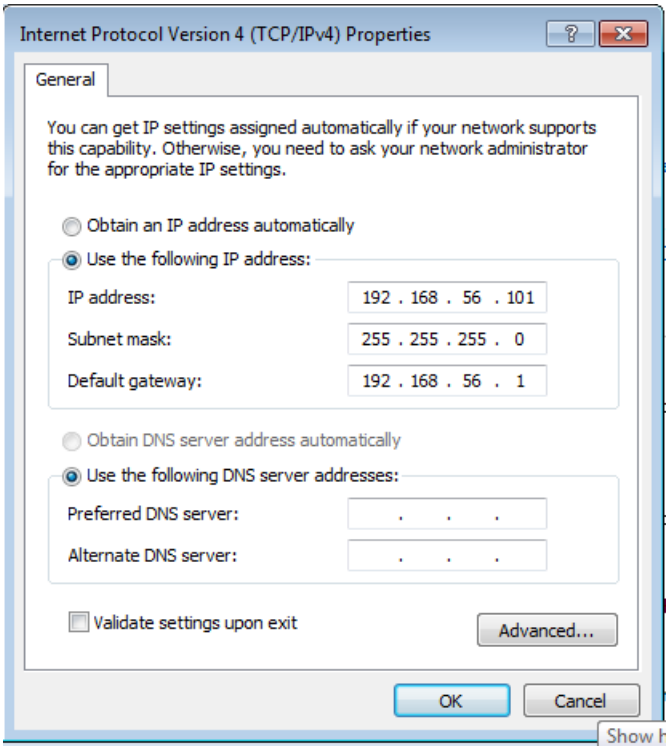
https://pypi.org/project/Pillow/5.1.0/#files (Pillow-5.1.0.win32-py2.7.exe)

Bước 2: Cài đặt và cấu hình Network cho windows 7

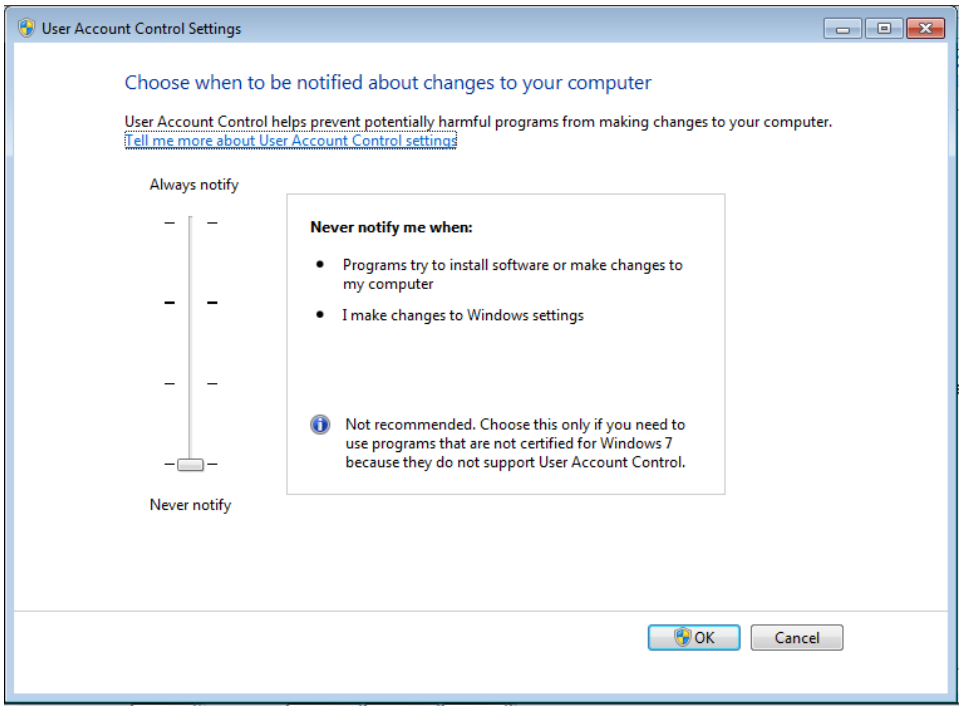
- Thay đổi Network adapter = Host-only Adapter và Name = vboxnet0



- cài đặt ipv4 (windows 7):



- Tắt Firewal và hạ mức bảo mật trong "User Account Controll Settings" xuống thấp nhất:



- Cuối cùng ta kiểm tra xem máy win7 đã kết nối được mạng và ping được với máy Ubuntu chưa.

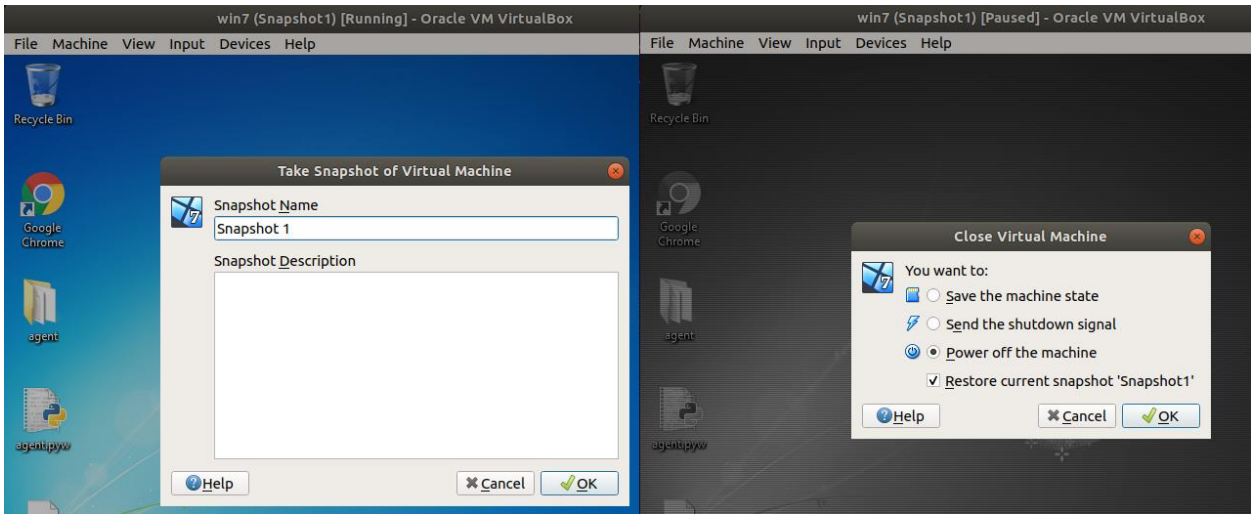
Bước 3: Chạy file agent.py trên windows 7

- Trên máy ubuntu truy cập theo đường dẫn “opt/cuckoo/agent” để copy file sang windown 7.

- Trên máy windows 7 mở file agent.py lên.

Bước 4: Tạo Snapshort và tắt máy win 7.

Máy ảo được tạo ra sử dụng hệ điều hành Window 7, sau khi khởi động tạo một snapshot được đặt tên là Snapshot1, Snapshot1 sẽ được dùng trong quá trình phân tích để trở về trạng thái ban đầu trước khi Cuckoo Sandbox thực hiện quá trình phân tích



Chỉnh sửa file cấu hình của Cuckoo sandbox

- các tập tin cấu hình này nằm ở đường dẫn /opt/cuckoo/conf

- Những file cần chỉnh sửa là: cuckoo.conf, virtualbox.conf, memory.conf, reporting.conf

```
son@son-ubuntu:/opt/cuckoo/conf$ gedit memory.conf
son@son-ubuntu:/opt/cuckoo/conf$ gedit reporting.conf
son@son-ubuntu:/opt/cuckoo/conf$ gedit cuckoo.conf
son@son-ubuntu:/opt/cuckoo/conf$ gedit virtualbox.conf
```

Bước 1: file memory.conf

```
$ cd /opt/cuckoo/conf
```

$ gedit memory.conf

Tìm mục [basic] và thay dòng guest_profile = [tên đầy đủ của phiên bản win]

Ví dụ: nếu bạn dùng win7 SP2 64bit thì sẽ là: Win7SP2x64

```
# Volatility configuration

# Basic settings
[basic]
# Profile to avoid wasting time identifying it
guest_profile = Win7SP0x86
# Delete memory dump after volatility processing.
delete_memdump = yes
```

Sau khi thay đổi xong lưu file lại.

Bước 2: reporting.conf

$ gedit reporting.conf

Tìm mục [mongodb] và thay đổi dòng enabled = no thành yes

```
[mongodb]
enabled = yes
host = 127.0.0.1
port = 27017
db = cuckoo
store_memdump = yes
paginate = 100
# MongoDB authentication (optional).
username =
password =
```

Bước 3: cuckoo.conf

$ gedit cuckoo.conf

Tìm dòng machinery = virtualbox

```
# Specify the name of the machinery module to use, this module will
# define the interaction between Cuckoo and your virtualization software
# of choice.
machinery = virtualbox
```

Bước 4: virtualbox.conf

$ gedit virtualbox.conf

Kiểm tra xem các thông tin có trùng khớp với những gì đã cài đặt không, nếu không ta thay đổi lại

```
# Default network interface.
interface = vboxnet0

# Specify a comma-separated list of available machines to be used. For each
# specified ID you have to define a dedicated section containing the details
# on the respective machine. (E.g. cuckoo1,cuckoo2,cuckoo3)
machines = cuckoo1

# If remote control is enabled in cuckoo.conf, specify a port range to use.
# Virtualbox will bind the VRDP interface to the first available port.
controlports = 5000-5050


[cuckoo1]
# Specify the label name of the current machine as specified in your
# VirtualBox configuration.
label = win7

# Specify the operating system platform used by current machine
# [windows/darwin/linux].
platform = windows

# Specify the IP address of the current virtual machine. Make sure that the
# IP address is valid and that the host machine is able to reach it. If not,
# the analysis will fail.
ip = 192.168.56.101

# (Optional) Specify the snapshot name to use. If you do not specify a snapshot
# name, the VirtualBox MachineManager will use the current snapshot.
# Example (Snapshot1 is the snapshot name):
snapshot = Snapshot1

# (Optional) Specify the name of the network interface that should be used
# when dumping network traffic from this machine with tcpdump. If specified,
# overrides the default interface specified in auxiliary.conf
# Example (vboxnet0 is the interface name):
interface = vboxnet0
```

Bước 5: khởi chạy cuckoo

- Mở virtualbox chạy windows7

- Mở cửa sổ terminal mới:

  $ cd /opt/cuckoo

  $ cuckoo -d

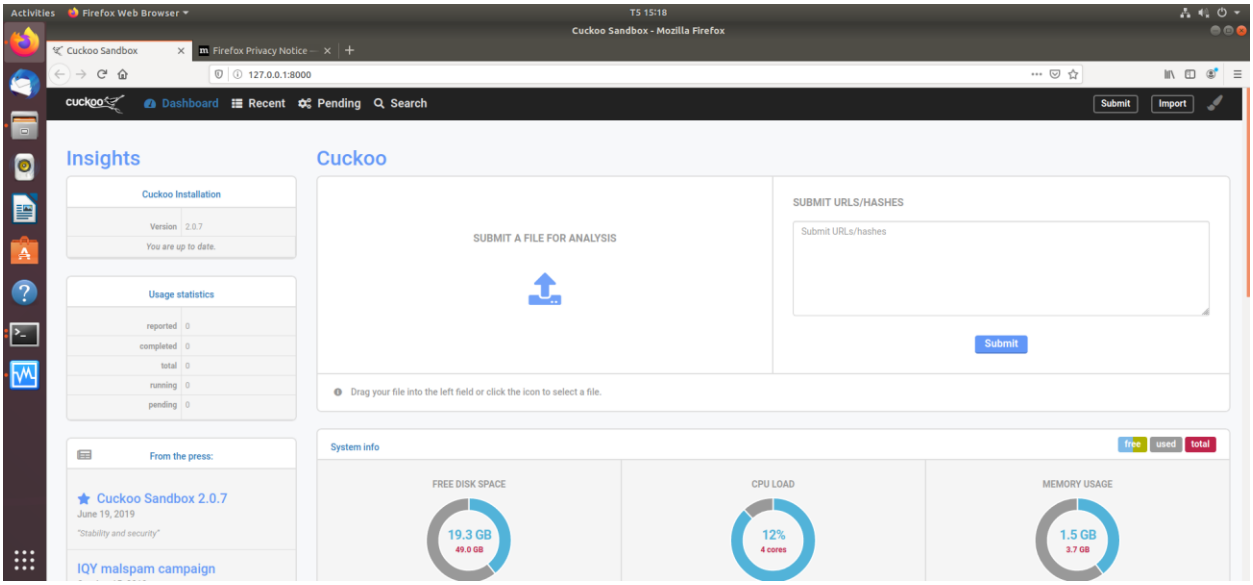
- mở một terminal khác:

$ cd /opt/cuckoo

$ cuckoo web runserver

```
cuckoo@cuckoo-virtual-machine:/opt/cuckoo$ cuckoo web runserver
Performing system checks...

System check identified no issues (0 silenced).
March 09, 2020 - 16:52:13
Django version 1.8.4, using settings 'cuckoo.web.web.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CONTROL-C.
[09/Mar/2020 16:52:18] "GET / HTTP/1.1" 200 22512
```

- Mở địa chỉ http://127.0.0.1:8000/ trên trình duyệt web



Như vậy chúng ta hoàn tất cài đặt.

1.3. Sử dụng Cockoo sandbook phân tích mã độc

Trong bài thực hành này, chúng ta sẽ phân tích các mẫu lab7-01.exe.

Khởi động Cuckoo sandbox theo các bước để tiến hành phân tích:

- Mở Virtualbox và bật windows 7 lên:

$ virtualbox

- Khởi động Cuckoo sandbox từ cửa sổ terminal:

$ cd /opt/cuckoo

$ cuckoo -d

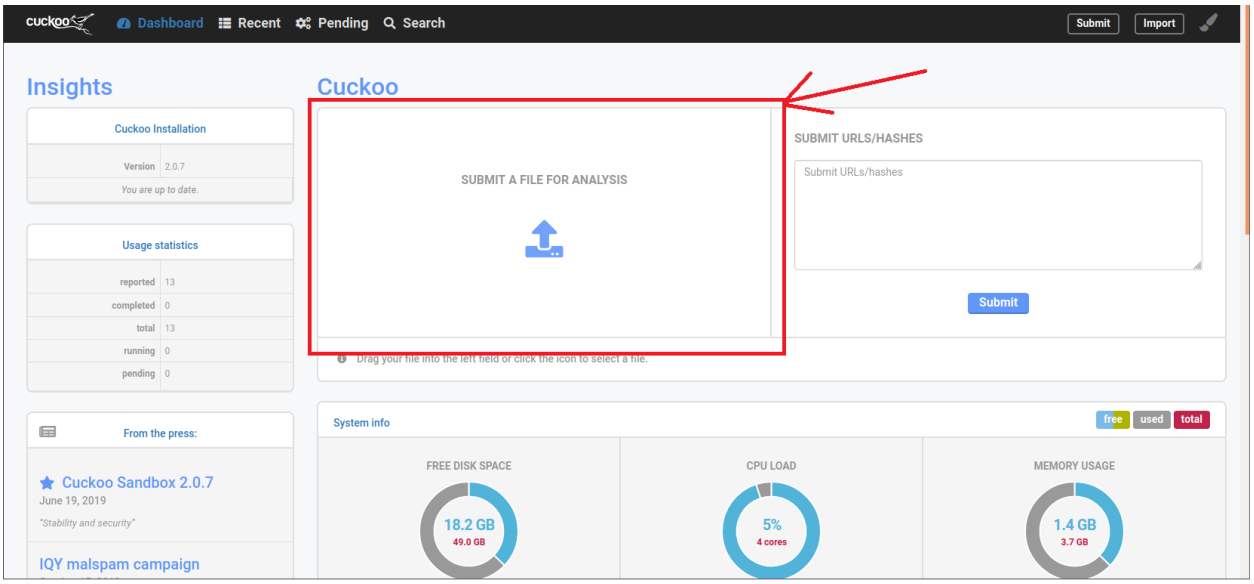
- Khởi động hệ thống giao diện web phân tích Cuckoo Sandbox:

$ cd /opt/cuckoo

$ cuckoo web runserver

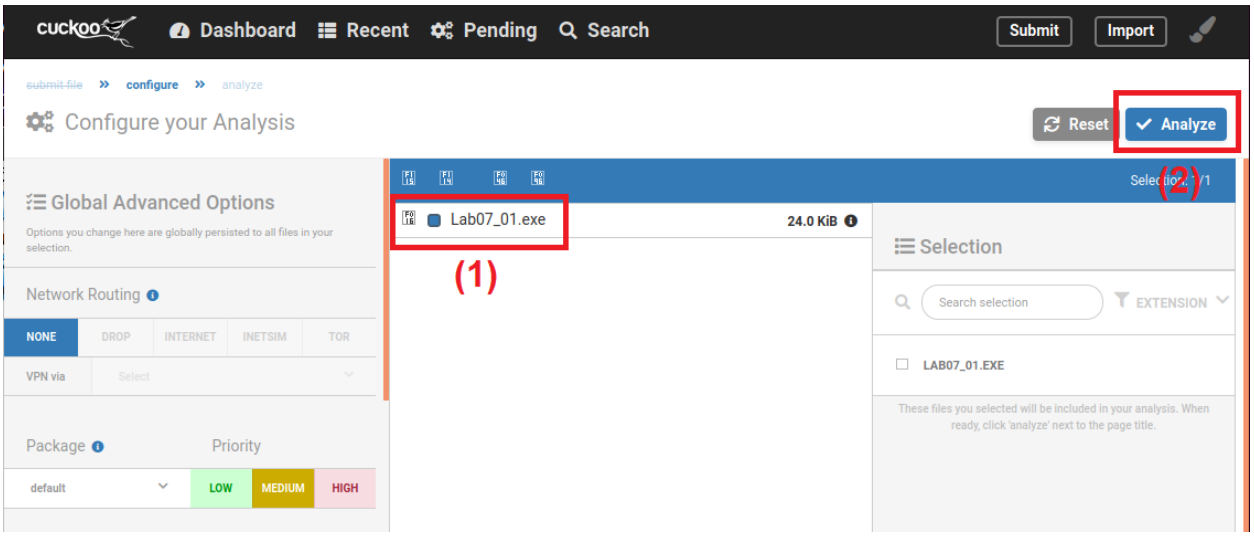
Các bước thực hiện bao gồm

Bước 1: Để thực hiện việc phân tích một file chọn mục SUBMIT A FILE FOR ANALYSIS sau đó chọn một file để thực hiện phân tích hay có thể phân tích một URLs/Hashes điền đường dẫn trang web chứa file phân tích vào khung SUBMIT URLS/HASHES.

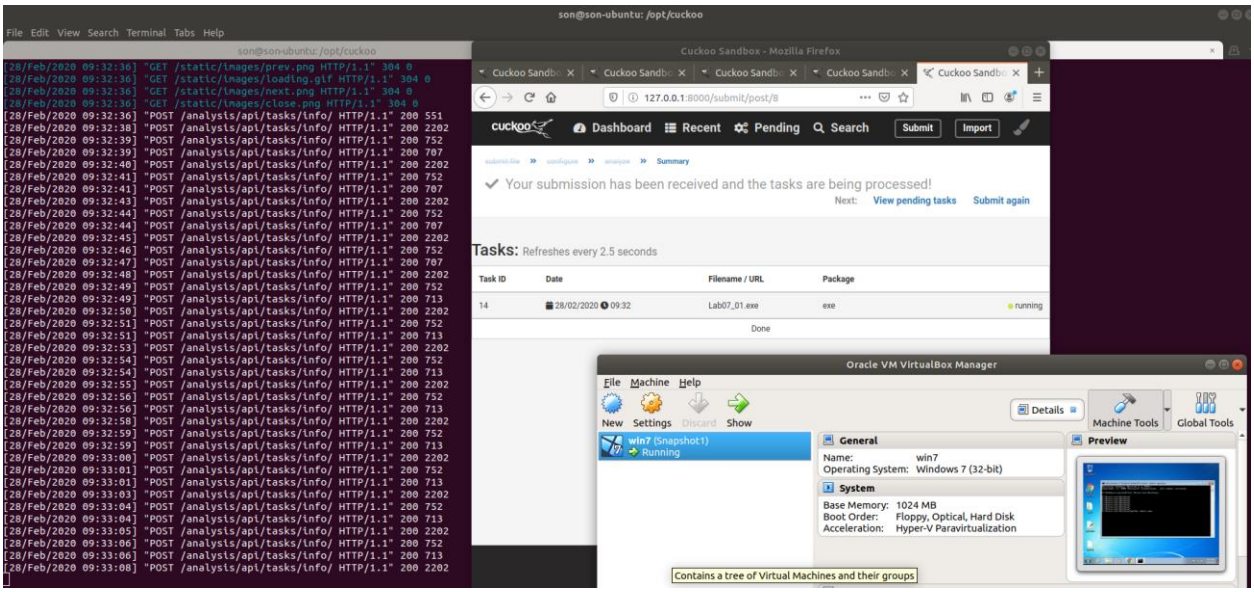


Bước 2:

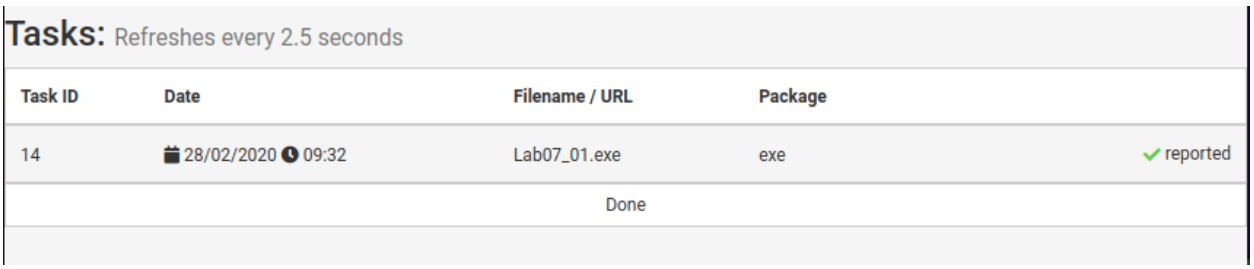
- Sau khi chọn file cần phân tích tab mới hiện lên, chọn “Analyze”



- Sau khi chọn Analyze quá trình phân tích bắt đầu.



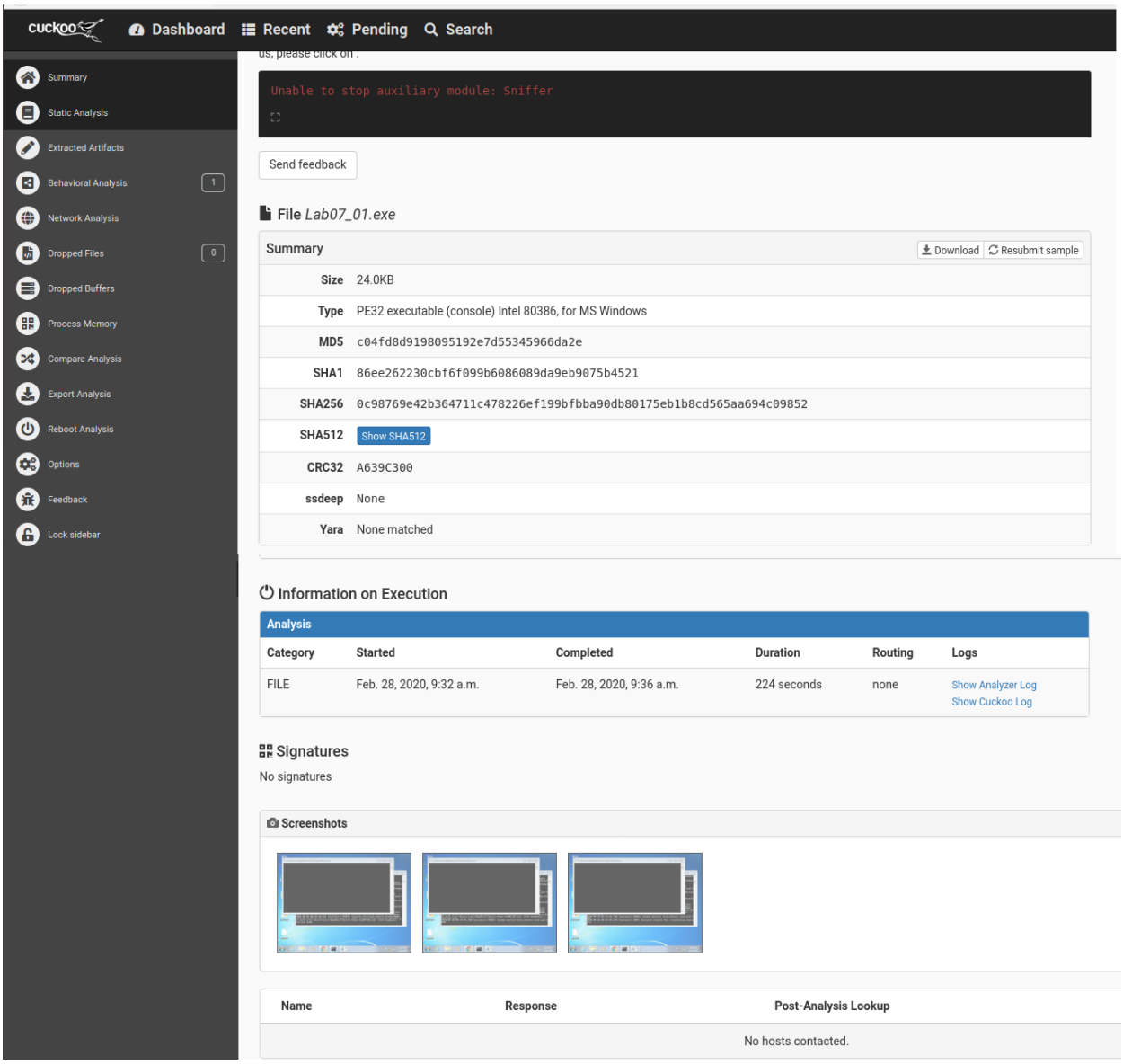
Bước 3: Quá trình phân tích hoàn tất: click vào "reported" để xem kết quả



❖ **Tab Summary** cung cấp cho ta các thông tin cơ bản của mã độc như: kích thước, type, mã MD5, SHA1, SHA256, SHA512, CRC32,

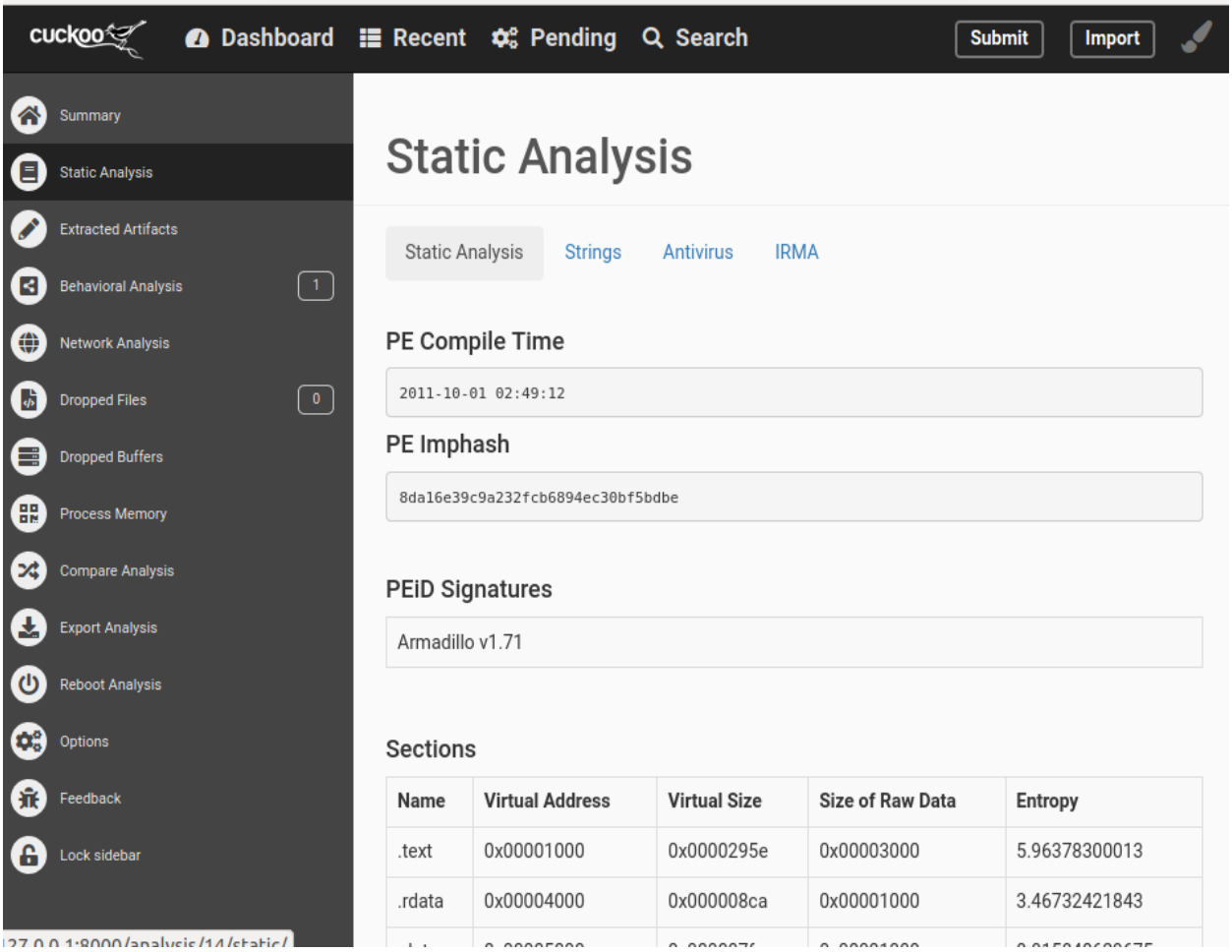
- Nhật ký phân tích mã độc được ghi lại tại mục Analysis

- Ảnh chụp màn hình quá trình phân tích từ máy windows7 trong quá trình chạy mã độc.



Hình 3.1. các thông tin cơ bản của mã độc

❖ **Tab Static Analysis** là kết quả tổng quan phân tích tĩnh. Kết quả phân tích tĩnh trên Cuckoo Sandbox chứa những thông tin cơ bản như các đoạn mã, ký tự, các thư viện, hàm API thực thi của mã độc, cấu trúc PE file hay phần mềm đã pack mã độc. Nhưng ở đây chúng ta chỉ có thể biết được những thông tin cơ bản nhất của file, không có nhiều thông tin có thể khai thác ở mục này.



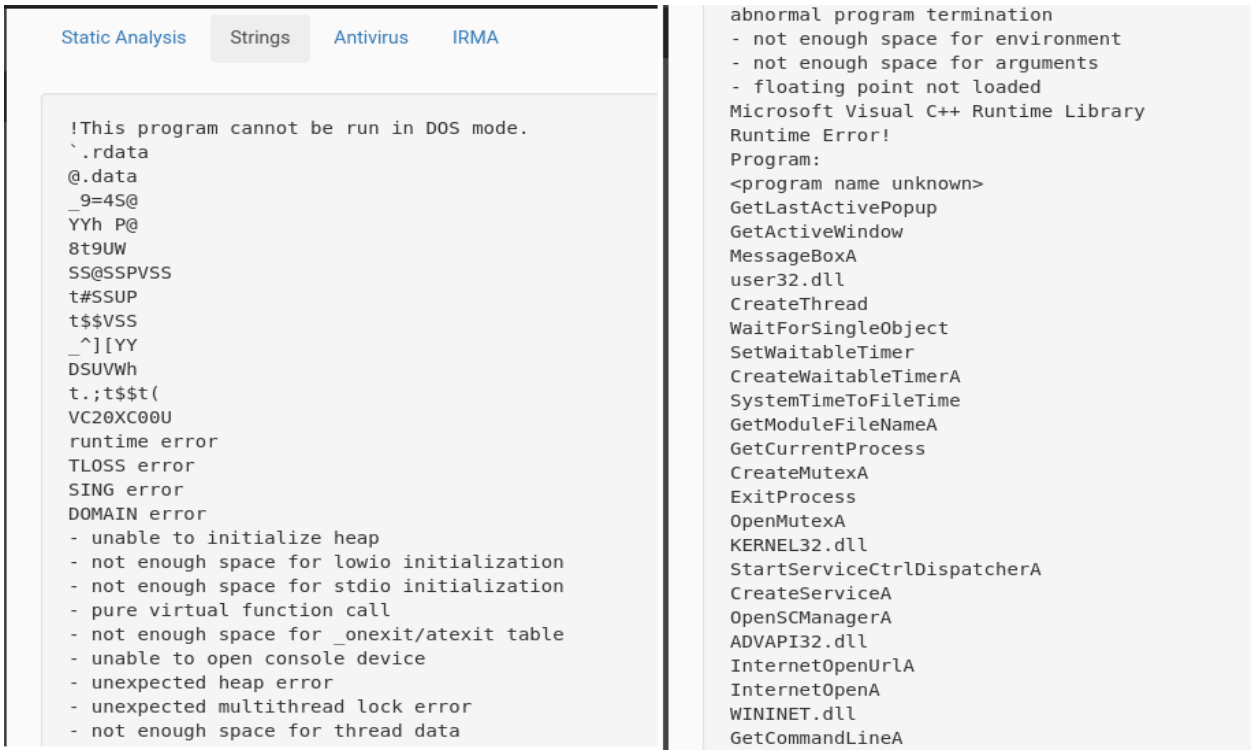
Hình 3.2. Tổng quan phân tích tĩnh, Thông tin về phần mềm Pack và một số section của PE file mã độc.

Với thư viện và hàm API của mã độc cuckoo cho ta có thể click vào để xem thông tin về hàm đó tại website https://docs.microsoft.com/. nhìn tổng quan từ mục

này có thể cho ta cái nhìn tổng quát về những gì mã độc đã thực hiện. VD như nhìn vào ADVAPI32.DLL trong ảnh, chúng ta chỉ có thể thấy một vài chức năng được nhập liên quan đến việc tạo, quản lý dịch vụ.

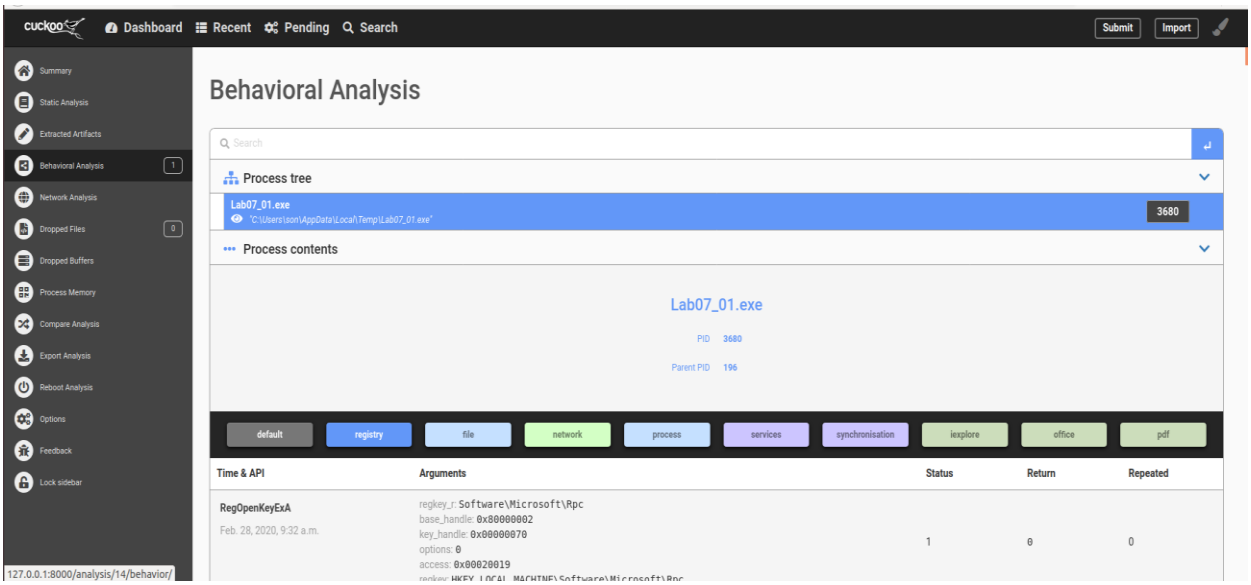
Hình 3.3. Một số thư viện, hàm API của mã độc

Tại mục String là chuỗi các hành động của mã độc



Hình 3.4. Mục Strings

❖ **Tab Behavioral Analysis** là kết quả tổng quan mục phân tích động:



Hình 3.5. Tab Behavioral Analysis

Ta thấy tại mục Process tree trên hình 3.5 có đường dẫn tới thư mục chứa mã độc được thực thi trên máy ảo là "C:\Users\cuckoo\AppData\Local\Temp\Lab07_01.exe".

Và bên dưới là các mục: default, registry, file, network, process, services, synchroisation, iexplore, office, pdf.

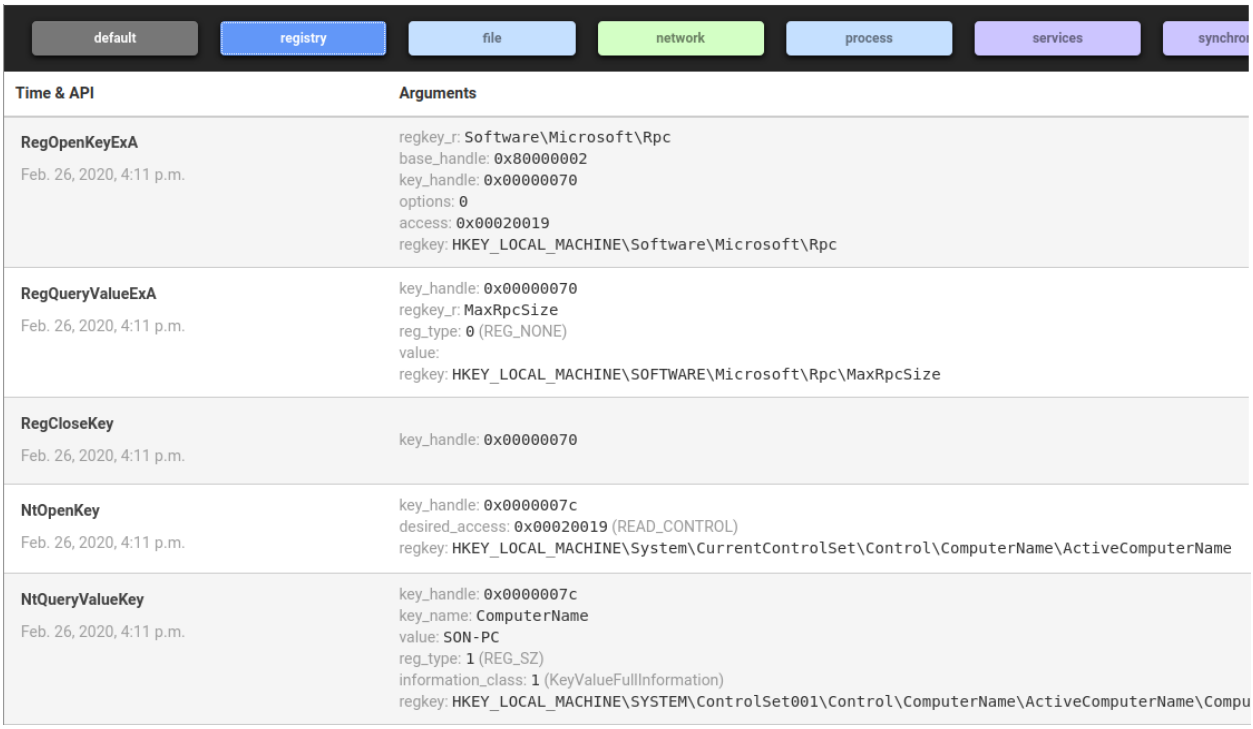
- **Mục registry** (Tab Behavioral Analysis)

Windows Registry là một cơ sở dữ liệu phân cấp lưu trữ các cài đặt cấp thấp cho hệ điều hành Microsoft Windows và cho các ứng dụng chọn sử dụng sổ đăng ký. Các hạt nhân, trình điều khiển thiết bị, dịch vụ, Security Accounts Manager, và giao diện người dùng đều có thể sử dụng registry

Sau khi phân tích lab07-01.exe,tại tab registry ta thấy mã độc thực hiện rất nhiều hành động mở, trích xuất và sửa đổi giá trị của registry, các hàm API được sử dụng gồm có:

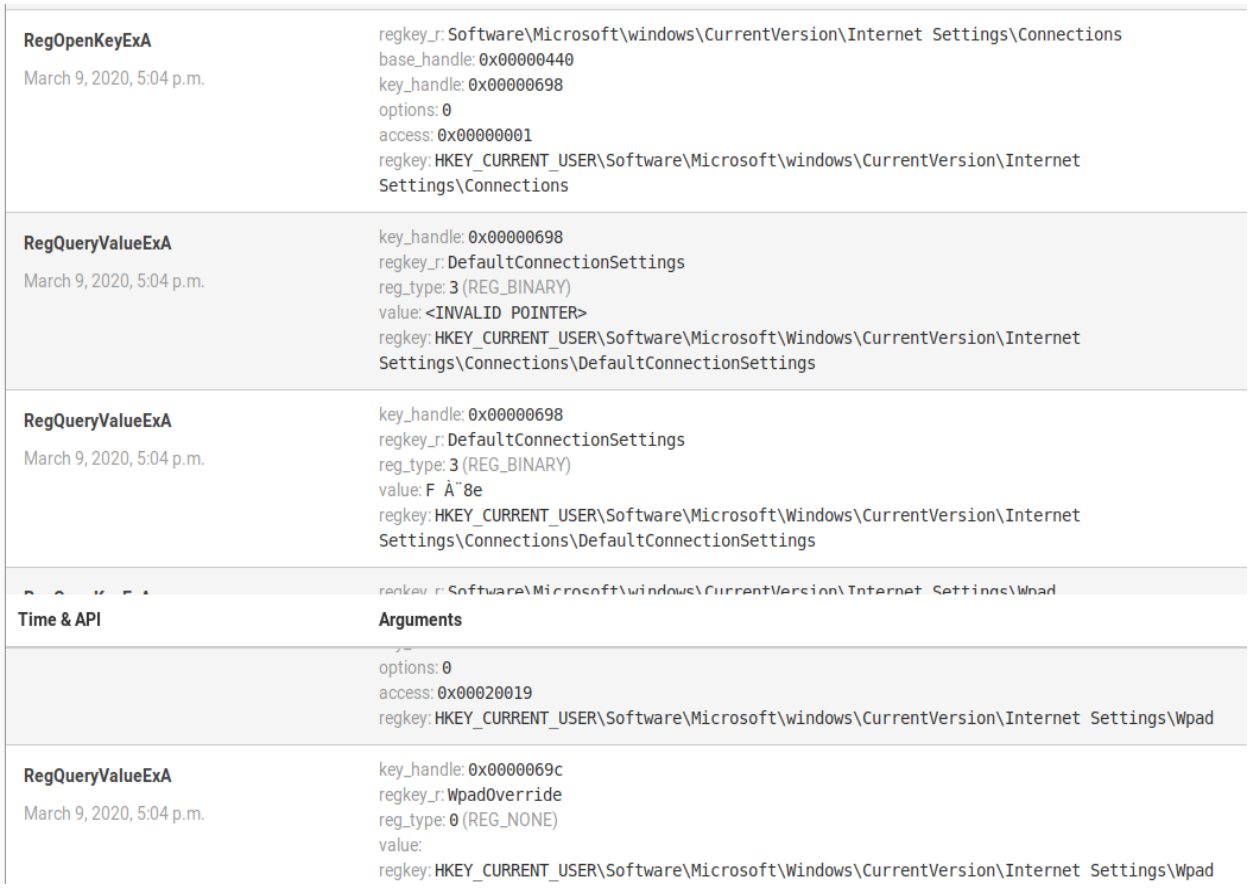
- RegOpenKeyEx
- RegQueryValueEx
- RegCloseKey

- NtOpenKey
- NtQueryValueKey



Hình 3.6. Tab registry

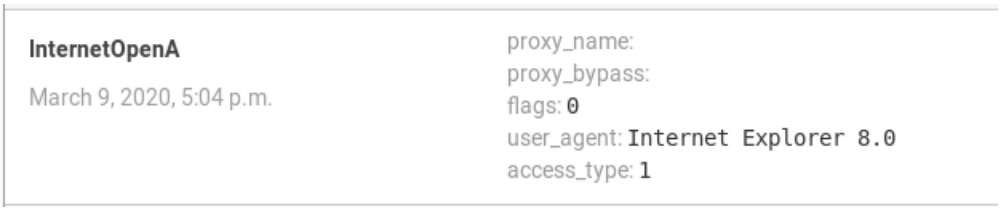
Ban đầu mã độc đa số can thiệp vào hệ thống, nhưng về sau chiếm đại đa số lại là những can thiệp liên quan đến mạng.



Hình 3.7. Những can thiệp của mã độc vào các thiết lập Internet

- **Mục file** (Tab Behavioral Analysis) cho biết về những thay đổi, hoạt động của hệ thống tệp tin

- **Mục Network** (Tab Behavioral Analysis) cho biết về những hoạt động của mạng.



Time & API	Arguments
InternetOpenUrlA March 9, 2020, 5:05 p.m.	url: http://www.malwareanalysisbook.com headers: flags: 2147483648 internet_handle: 0x00cc0014
InternetOpenUrlA March 9, 2020, 5:05 p.m.	url: http://www.malwareanalysisbook.com headers: flags: 2147483648 internet_handle: 0x00cc0024
InternetOpenUrlA March 9, 2020, 5:05 p.m.	url: http://www.malwareanalysisbook.com headers: flags: 2147483648 internet_handle: 0x00cc0028
InternetOpenUrlA March 9, 2020, 5:05 p.m.	url: http://www.malwareanalysisbook.com headers: flags: 2147483648 internet_handle: 0x00cc0010
InternetOpenUrlA March 9, 2020, 5:05 p.m.	url: http://www.malwareanalysisbook.com headers: flags: 2147483648 internet_handle: 0x00cc002c
InternetOpenUrlA	url: http://www.malwareanalysisbook.com

Hình 3.8. Những hoạt động của mã độc liên quan đến network

Từ hình 3.8 ta thay mã độc mở trình duyệt web "Internet Explorer 8.0" và liên tục truy cập vào đường dẫn "http://www.malwareanalysisbook.com". Đến đây ta có thể phỏng đoán được mã độc này có liên quan đến tấn công DoS, DDoS. Mà mục tiêu tấn công là website "http://www.malwareanalysisbook.com".

- **Mục Process** (Tab Behavioral Analysis)
- **Mục Service** (Tab Behavioral Analysis)

Ta thấy mã độc truyền đường dẫn file thực thi của mình vào hàm CreateService.

Time & API	Arguments
OpenSCManagerA March 9, 2020, 5:04 p.m.	desired_access: 3 database_name: machine_name:
CreateServiceA March 9, 2020, 5:04 p.m.	service_start_name: start_type: 2 password: display_name: Malservice filepath: C:\Users\cuckoo\AppData\Local\Temp\Lab07_01.exe service_name: Malservice filepath_r: C:\Users\cuckoo\AppData\Local\Temp\Lab07_01.exe desired_access: 2 service_handle: 0x002b45e0 error_control: 0 service_type: 16 service_manager_handle: 0x002b46a8

Hình 3.4. Tab Service

- Service_start_name: (dựa vào display_name và service_name có thể đoán được tên Malware là "Malservices")
- Start_type: 2 (tương ứng với SERVICE_AUTO_START)
- Desired_access: 2 (là giá trị quyền truy cập yêu cầu để thực hiện hàm CreateService)

SC_MANAGER_CREATE_SERVICE (0x0002)	Required to call the **CreateService** function to create a service object and add it to the database.

- Error_control: 0 (SERVICE_ERROR_IGNORE)

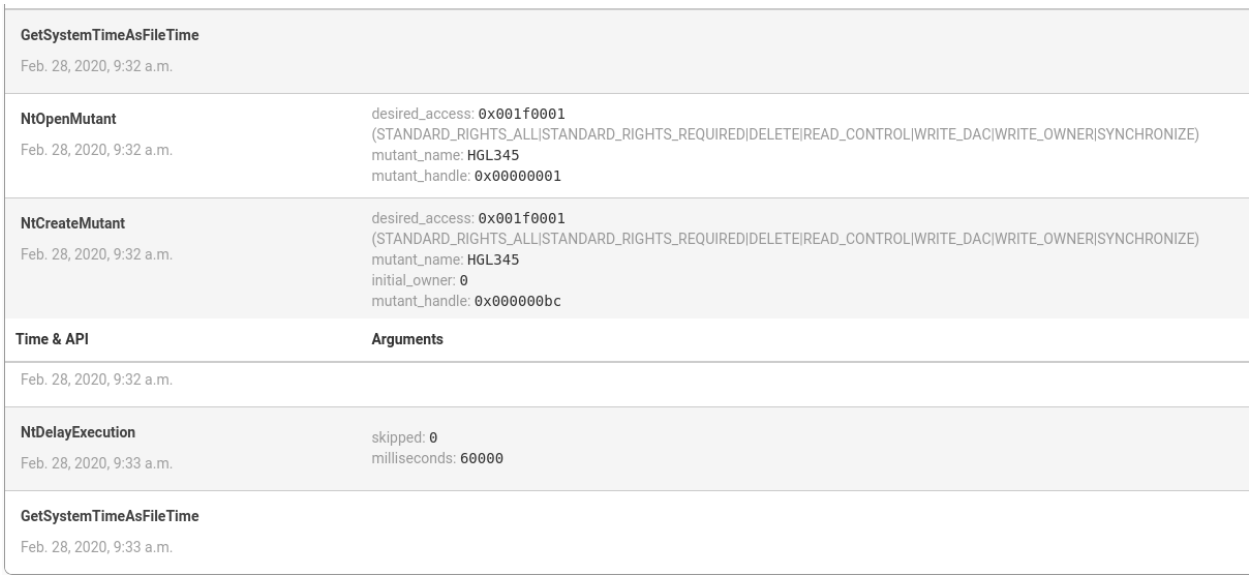
SERVICE_ERROR_IGNORE 0x00000000	The startup program ignores the error and continues the startup operation.

- Services_type: 16

Win32OwnProcess	16	A Win32 program that can be started by the Service Controller and that obeys the service control protocol. This type of Win32 service runs in a process by itself.

Như vậy, mã độc cài đặt service mới với tên Malservice để thiết lập chính nó tự khởi động cùng hệ thống.

- Mục synchronisation (Tab Behavioral Analysis)



Hình 3.5. Tab synchronisation

Ta thấy mã độc truy cập một mutex với tên HGL345, nhưng sau đó lại tạo mới một mutex với tên HGL345. Từ hành vi trên ta có thể giả định rằng mã độc truy cập mutex HGL345 để kiểm tra xem mutex này đã tồn tại chưa, việc kiểm tra sự tồn tại của mutex HGL345 là nhằm chắc chắn rằng tại một thời điểm chỉ có một bản của mã độc được thực thi trong hệ thống.

KẾT LUẬN:

Qua những thông tin trên, ta biết được:

- Mã độc tạo một Service với tên “Malservice”, và tự khởi chạy cùng hệ thống
- Mutex với tên “HGL345”. Mã độc sử dụng mutex để kiểm tra và chắc chắn rằng tại một thời điểm chỉ có một instance của mình được chạy trên hệ thống
- Mã độc mở trình duyệt “Internet Explorer 8.0” và liên tục truy cập vào đường dẫn “http://www.malwareanalysisbook.com”

Chúng ta có thể suy luận rằng phần mềm độc hại này được viết trong nỗ lực khởi động một cuộc tấn công DoS bằng cách mở các chuỗi kết nối vô tận trang web maleaneanalysisbook.com