Penetration Testing

MSCS 650

LAB 03: Analyze malware using Cuckoo Sandbox

In this lab, we will learn how to use sandbox programs to study malicious programs using static and dynamic analysis

You can scan any suspicious file on it and within minutes Cuckoo will provide a detailed report outlining the behavior of the file when executed within a realistic but isolated environment.

Malware is a weapon used by cyber attackers and anyone targeting an organization.

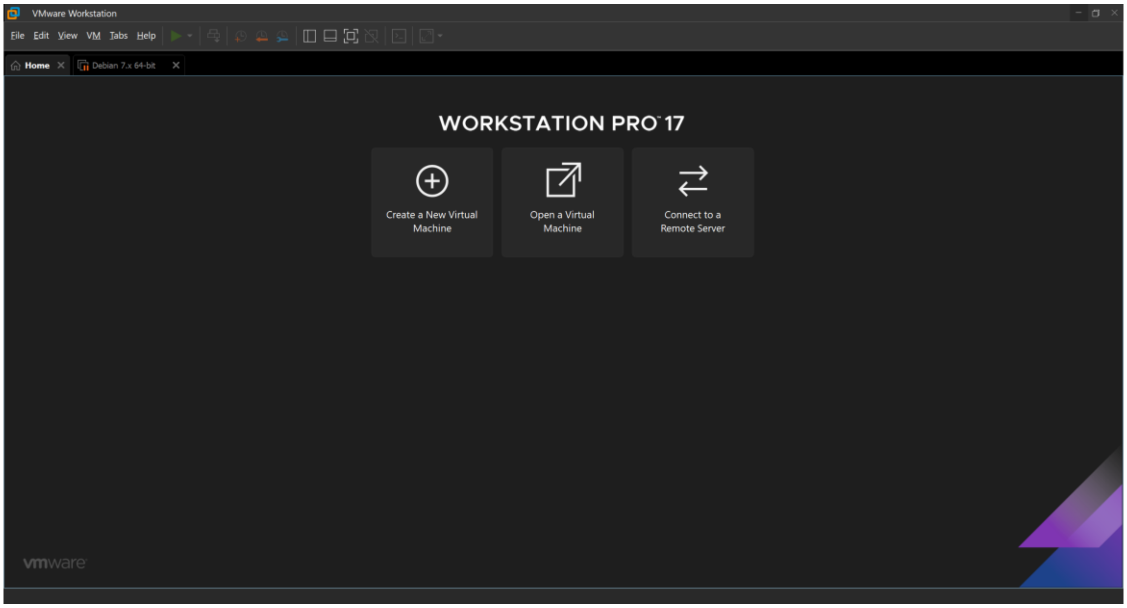
Nowadays, it is not enough to detect and remove malware: it is very important to understand how it works in order to understand the context, motives and goals of the breach.

Cuckoo Sandbox is a free software that automates the task of analyzing any malicious file under Windows, macOS, Linux and Android operating systems.

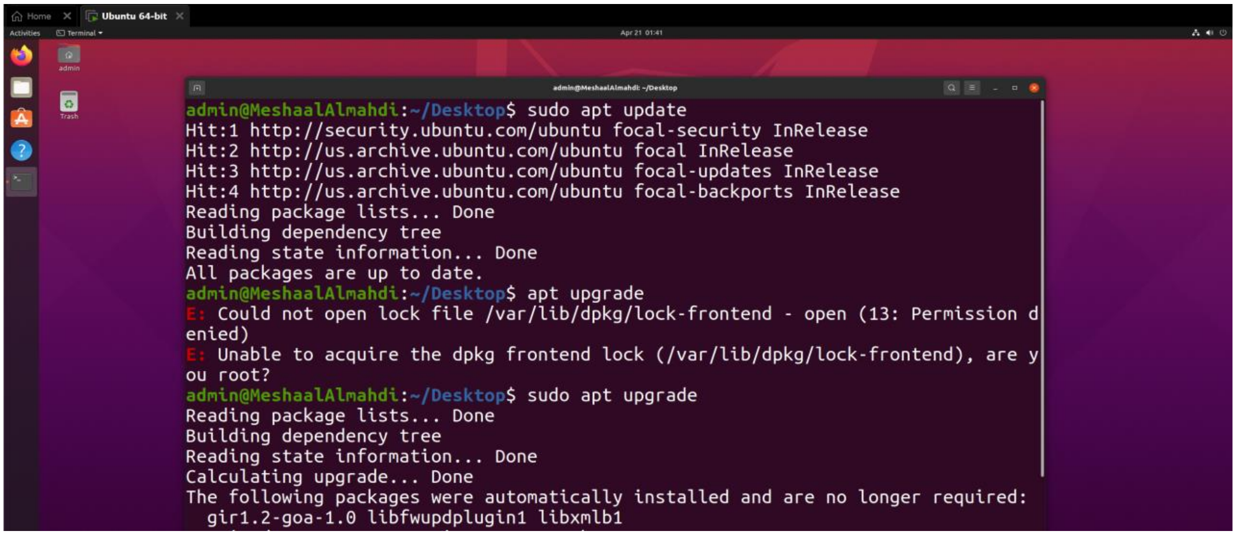
0: **Tools**

Virtual systems

- Ubuntu Cuckoo

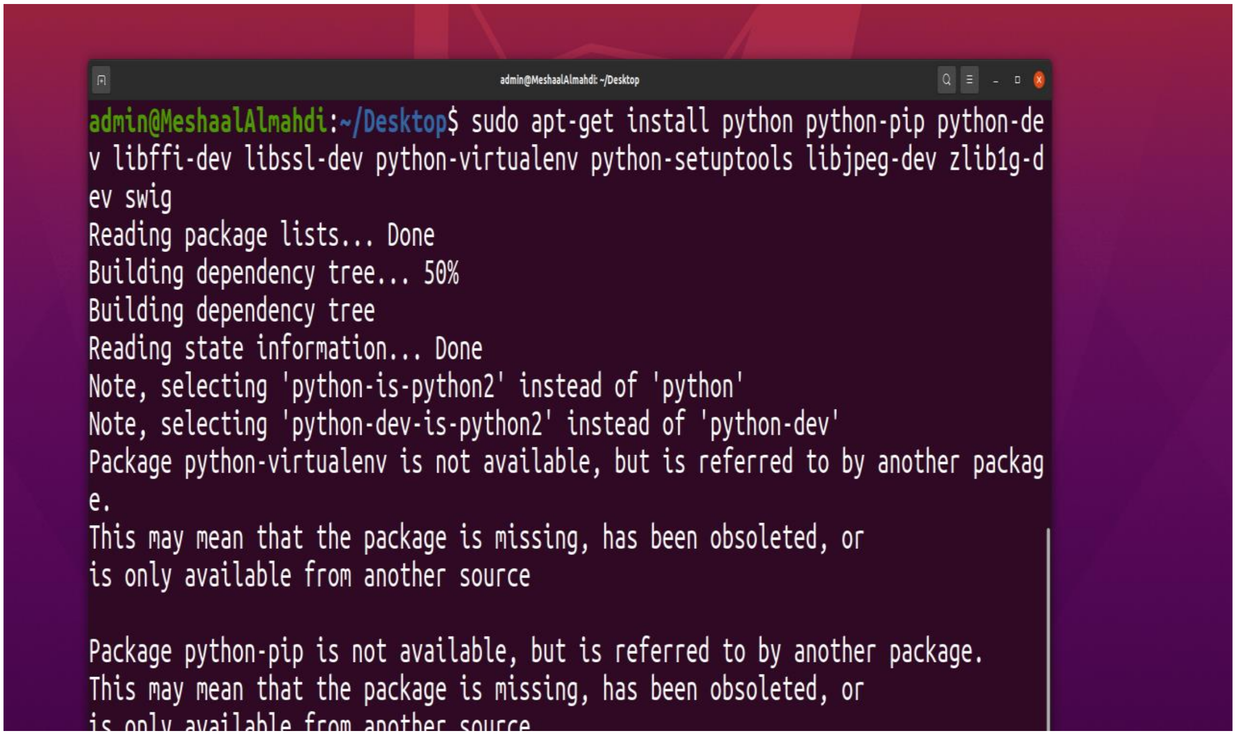


1. **Turn on the system**

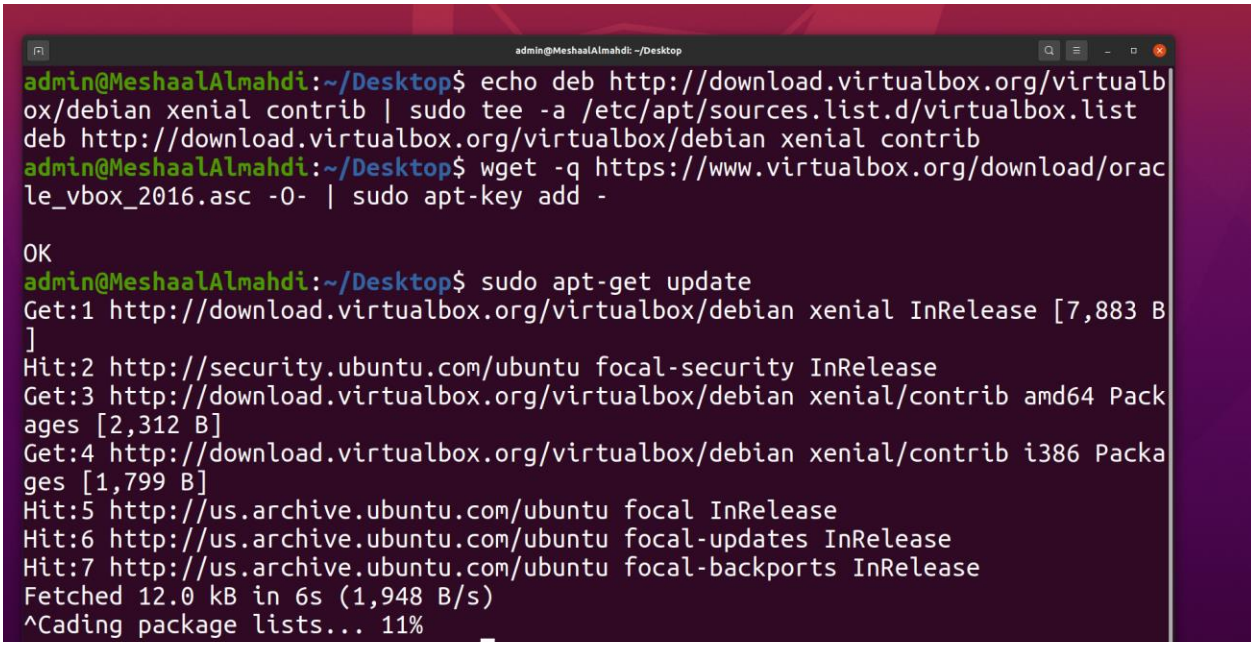


```
admin@MeshaalAlmahdi:~/Desktop$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
admin@MeshaalAlmahdi:~/Desktop$ apt upgrade
E: Could not open lock file /var/lib/dpkg/lock-frontend - open (13: Permission d
enied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontend), are y
ou root?
admin@MeshaalAlmahdi:~/Desktop$ sudo apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  gir1.2-goa-1.0 libfwupdplugin1 libxmlb1
```

2. **we open Terminal and we write bash install.sh to turn on cuckoo:**

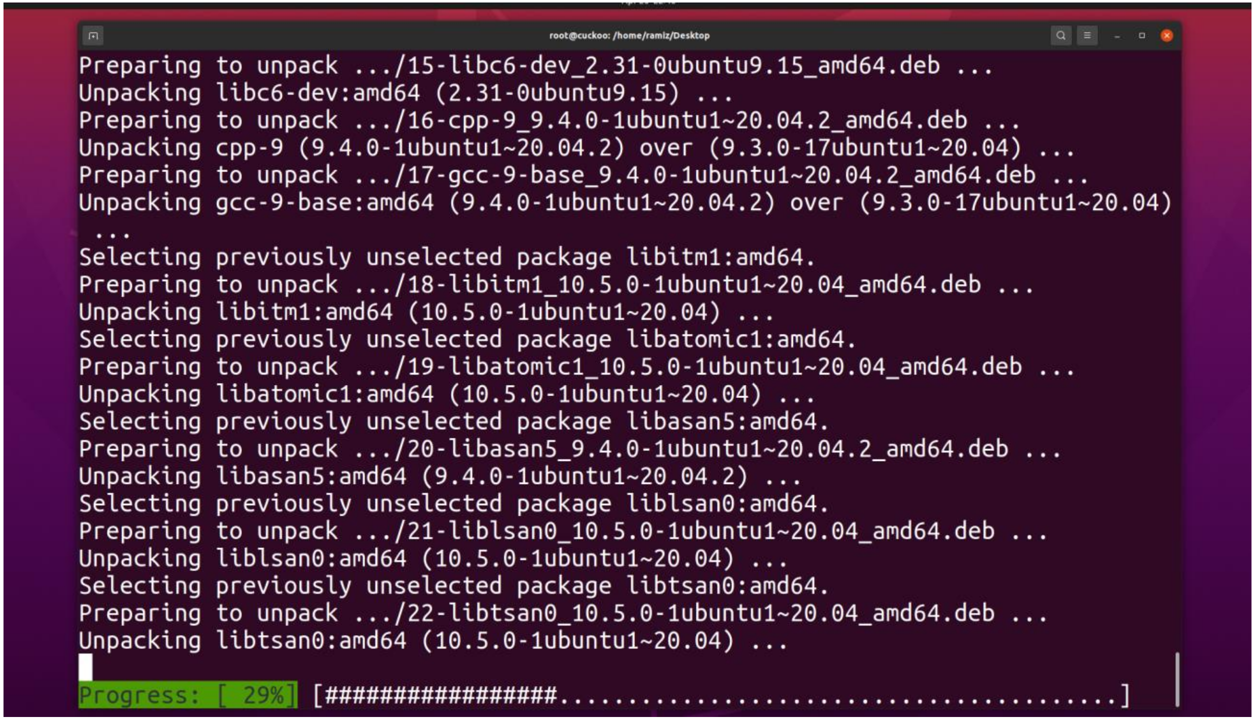


```
admin@MeshaalAlmahdi:~/Desktop$ sudo apt-get install python python-pip python-de
v libffi-dev libssl-dev python-virtualenv python-setuptools libjpeg-dev zlib1g-d
ev swig
Reading package lists... Done
Building dependency tree... 50%
Building dependency tree
Reading state information... Done
Note, selecting 'python-is-python2' instead of 'python'
Note, selecting 'python-dev-is-python2' instead of 'python-dev'
Package python-virtualenv is not available, but is referred to by another packag
e.
This may mean that the package is missing, has been obsoleted, or
is only available from another source

Package python-pip is not available, but is referred to by another package.
This may mean that the package is missing, has been obsoleted, or
is only available from another source
```



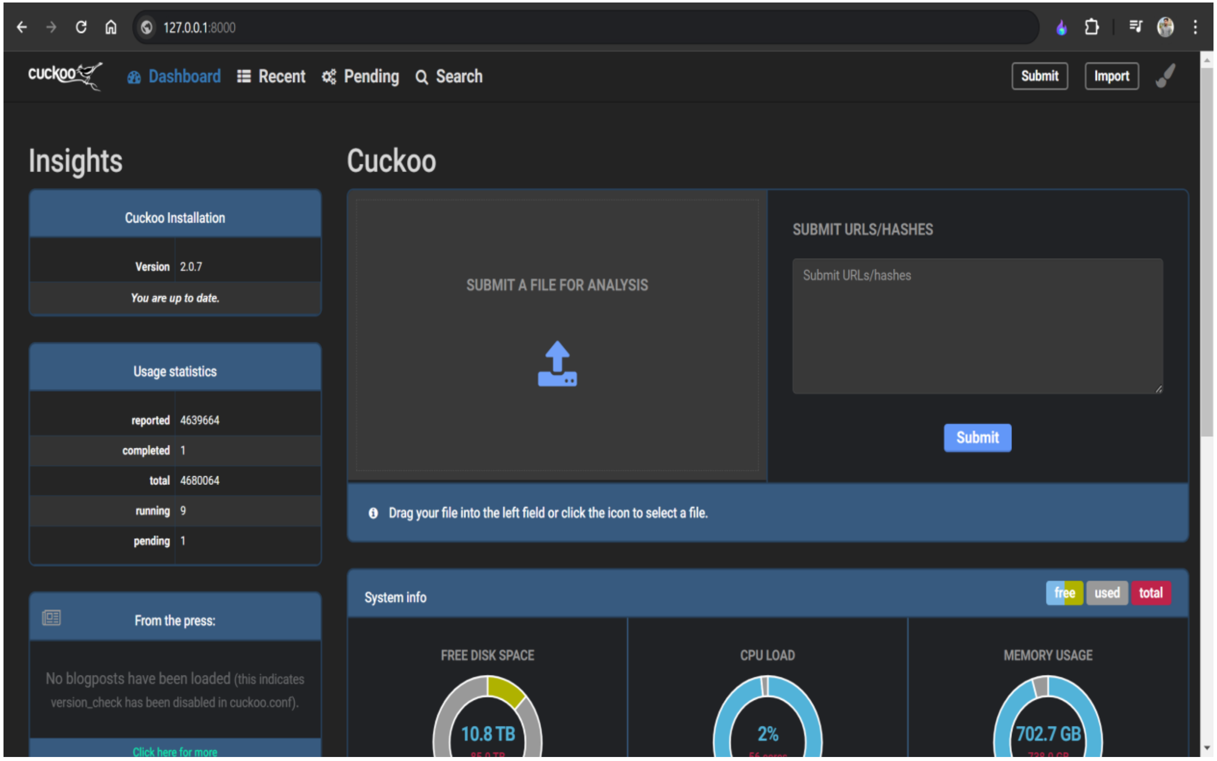
```
admin@MeshaalAlmahdi:~/Desktop$ echo deb http://download.virtualbox.org/virtualb
ox/debian xenial contrib | sudo tee -a /etc/apt/sources.list.d/virtualbox.list
deb http://download.virtualbox.org/virtualbox/debian xenial contrib
admin@MeshaalAlmahdi:~/Desktop$ wget -q https://www.virtualbox.org/download/orac
le_vbox_2016.asc -O- | sudo apt-key add -

OK
admin@MeshaalAlmahdi:~/Desktop$ sudo apt-get update
Get:1 http://download.virtualbox.org/virtualbox/debian xenial InRelease [7,883 B
]
Hit:2 http://security.ubuntu.com/ubuntu focal-security InRelease
Get:3 http://download.virtualbox.org/virtualbox/debian xenial/contrib amd64 Pack
ages [2,312 B]
Get:4 http://download.virtualbox.org/virtualbox/debian xenial/contrib i386 Packa
ges [1,799 B]
Hit:5 http://us.archive.ubuntu.com/ubuntu focal InRelease
Hit:6 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:7 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease
Fetched 12.0 kB in 6s (1,948 B/s)
^Cading package lists... 11%
```

3. We wait until activation completes



```
Preparing to unpack .../15-libc6-dev_2.31-0ubuntu9.15_amd64.deb ...
Unpacking libc6-dev:amd64 (2.31-0ubuntu9.15) ...
Preparing to unpack .../16-cpp-9_9.4.0-1ubuntu1~20.04.2_amd64.deb ...
Unpacking cpp-9 (9.4.0-1ubuntu1~20.04.2) over (9.3.0-17ubuntu1~20.04) ...
Preparing to unpack .../17-gcc-9-base_9.4.0-1ubuntu1~20.04.2_amd64.deb ...
Unpacking gcc-9-base:amd64 (9.4.0-1ubuntu1~20.04.2) over (9.3.0-17ubuntu1~20.04)
 ...
Selecting previously unselected package libitm1:amd64.
Preparing to unpack .../18-libitm1_10.5.0-1ubuntu1~20.04_amd64.deb ...
Unpacking libitm1:amd64 (10.5.0-1ubuntu1~20.04) ...
Selecting previously unselected package libatomic1:amd64.
Preparing to unpack .../19-libatomic1_10.5.0-1ubuntu1~20.04_amd64.deb ...
Unpacking libatomic1:amd64 (10.5.0-1ubuntu1~20.04) ...
Selecting previously unselected package libasan5:amd64.
Preparing to unpack .../20-libasan5_9.4.0-1ubuntu1~20.04.2_amd64.deb ...
Unpacking libasan5:amd64 (9.4.0-1ubuntu1~20.04.2) ...
Selecting previously unselected package liblsan0:amd64.
Preparing to unpack .../21-liblsan0_10.5.0-1ubuntu1~20.04_amd64.deb ...
Unpacking liblsan0:amd64 (10.5.0-1ubuntu1~20.04) ...
Selecting previously unselected package libtsan0:amd64.
Preparing to unpack .../22-libtsan0_10.5.0-1ubuntu1~20.04_amd64.deb ...
Unpacking libtsan0:amd64 (10.5.0-1ubuntu1~20.04) ...

Progress: [ 29%] [#################.......................................]
```

4. **We will open cuckoo on Firefox, we write the address 127.0.0.1:8000**



Insights

Cuckoo Installation

Version 2.0.7

You are up to date.

Usage statistics

reported	4639664
completed	1
total	4680064
running	9
pending	1

From the press:

No blogposts have been loaded (this indicates version_check has been disabled in cuckoo.conf).

Click here for more

Cuckoo

SUBMIT A FILE FOR ANALYSIS

SUBMIT URLS/HASHES

Submit URLs/hashes

Submit

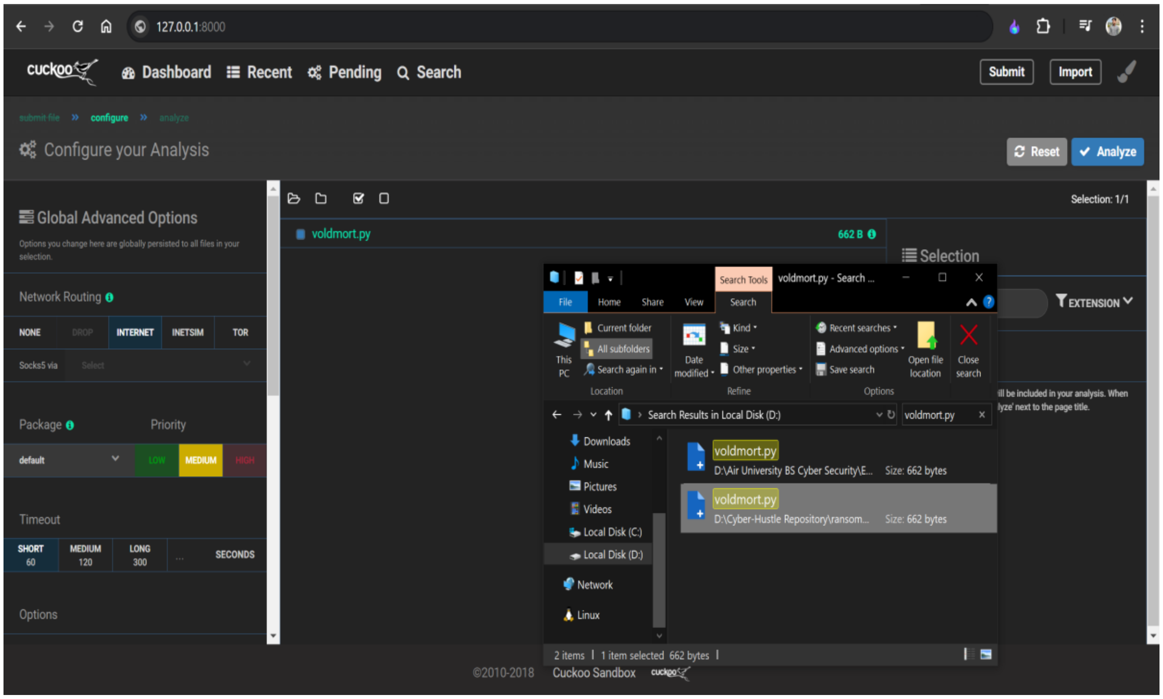
Drag your file into the left field or click the icon to select a file.

System info

FREE DISK SPACE	CPU LOAD	MEMORY USAGE
10.8 TB	2%	702.7 GB

2: Examination 1.

With ease, we can upload the suspicious file to cuckoo. Cuckoo will activate the virtual system and test the malicious program on it. There is an Agent program inside the virtual system that sends information to the cuckoo server located on the Ubuntu system:



Configure your Analysis

Global Advanced Options

Options you change here are globally persisted to all files in your selection.

Network Routing

NONE	DROP	INTERNET	INETSIM	TOR

Socks5 via Select

Package: default

Priority: LOW MEDIUM HIGH

Timeout

SHORT	MEDIUM	LONG	...	SECONDS
60	120	300		

Options

Selection: 1/1

voldmort.py 662 B

Selection

...ill be included in your analysis. When ...lyze' next to the page title.

Search Results in Local Disk (D:)

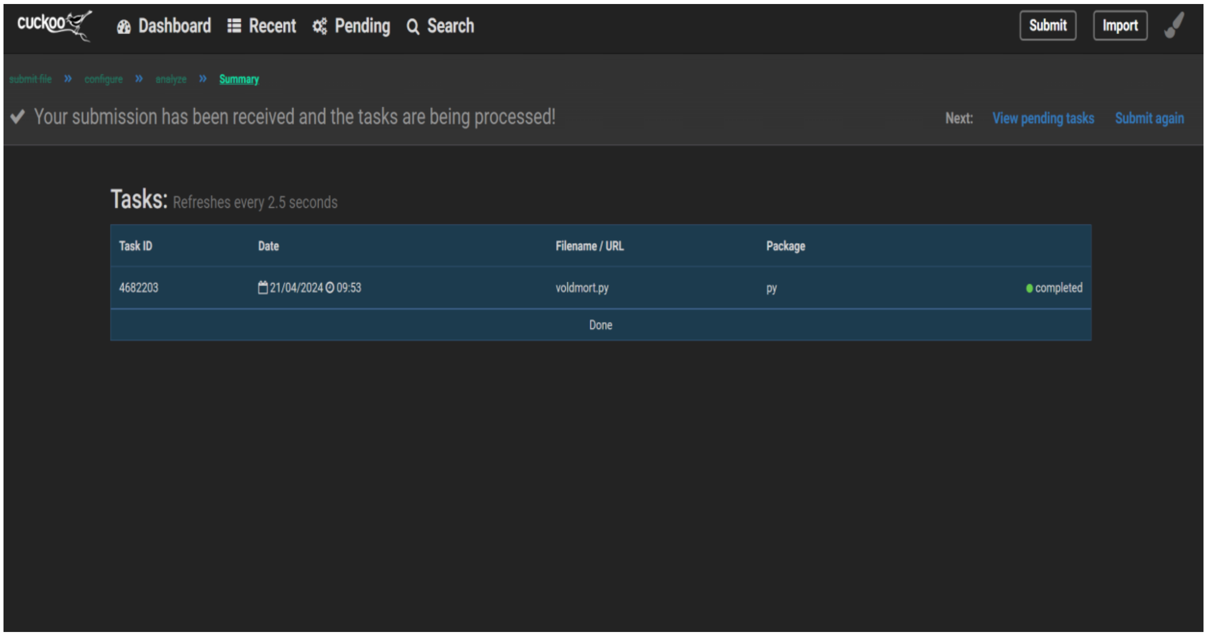
voldmort.py

voldmort.py D:\Air University BS Cyber Security\E...	Size: 662 bytes
voldmort.py D:\Cyber-Hustle Repository\ransom...	Size: 662 bytes

2 items | 1 item selected 662 bytes |

©2010-2018 Cuckoo Sandbox

After pressing Analyze We can watch what cuckoo does:



✔ Your submission has been received and the tasks are being processed!

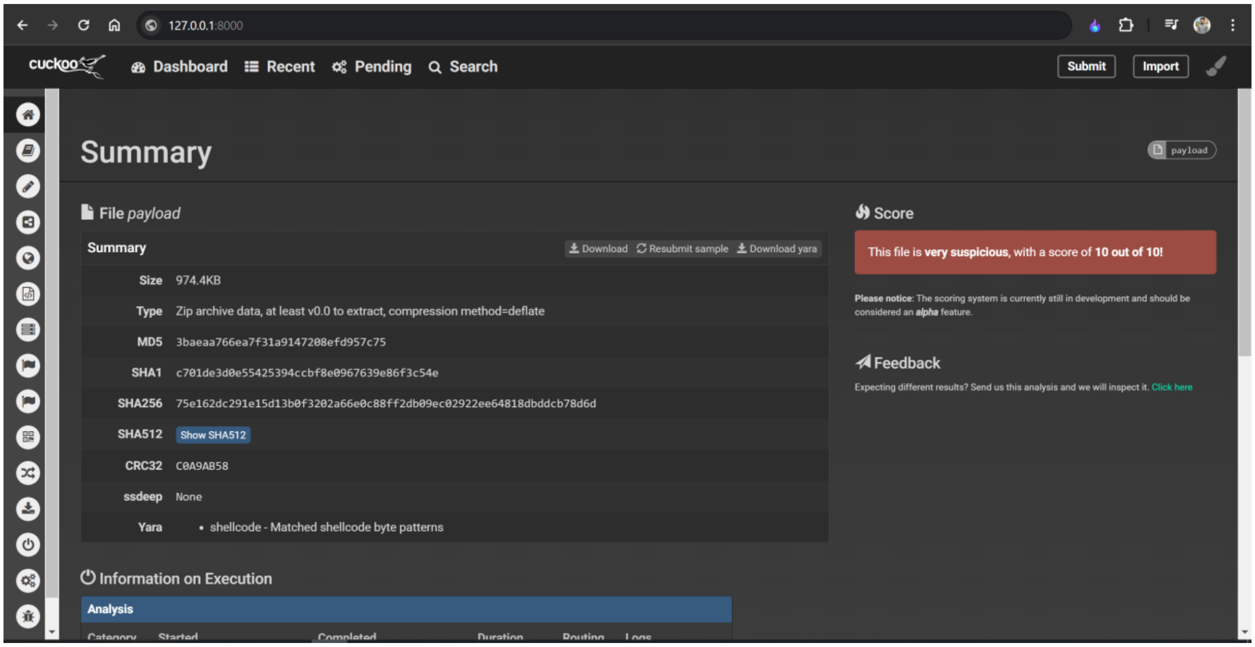
Next: View pending tasks Submit again

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package	
4682203	21/04/2024 09:53	voldmort.py	py	● completed

Done

It detects its malicious:



Summary

File *payload*

Summary

Size	974.4KB
Type	Zip archive data, at least v0.0 to extract, compression method=deflate
MD5	3baeaa766ea7f31a9147208efd957c75
SHA1	c701de3d0e55425394ccbf8e0967639e86f3c54e
SHA256	75e162dc291e15d13b0f3202a66e0c88ff2db09ec02922ee64818dbddcb78d6d
SHA512	Show SHA512
CRC32	C0A9AB58
ssdeep	None
Yara	• shellcode - Matched shellcode byte patterns

Score

This file is **very suspicious**, with a score of **10 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

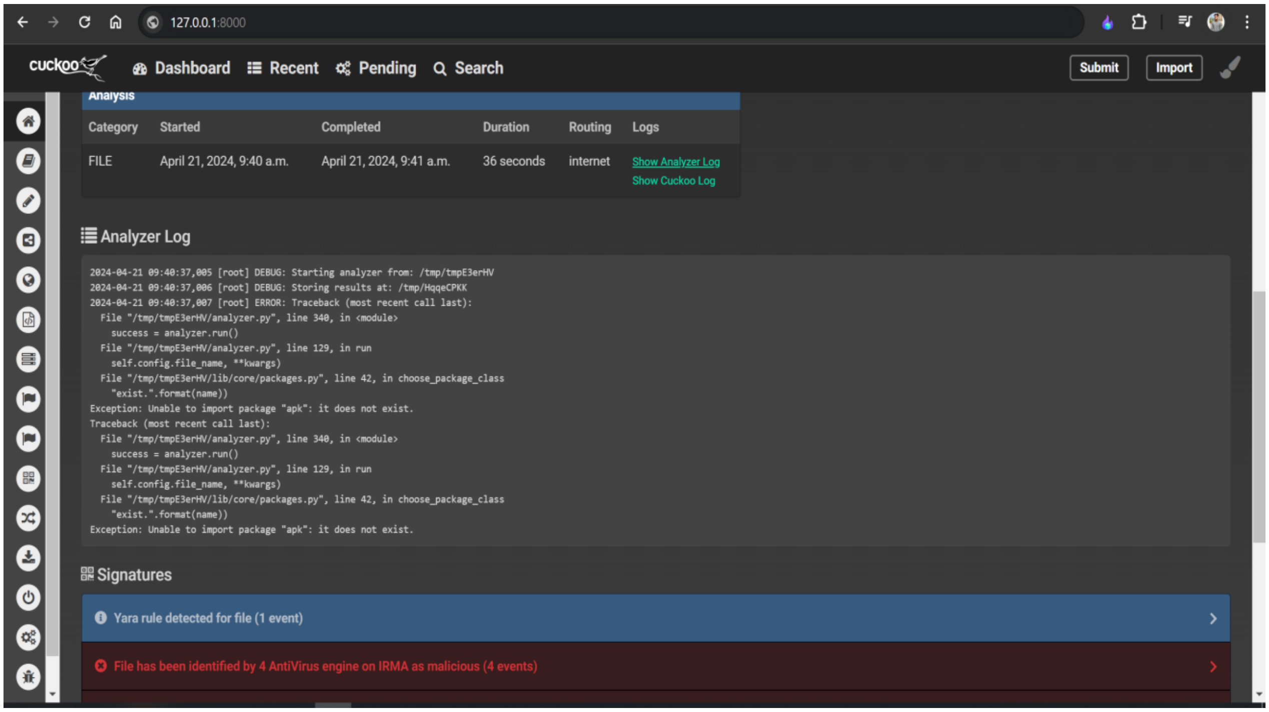
Information on Execution

Analysis

Category	Started	Completed	Duration	Routing	Logs

Reports

A detailed report appears, displaying the most important transactions recorded on the virtual system, in addition to the addresses of the sites that were connected to, files that were changed, screen images, etc.:



Analysis

Category	Started	Completed	Duration	Routing	Logs
FILE	April 21, 2024, 9:40 a.m.	April 21, 2024, 9:41 a.m.	36 seconds	internet	Show Analyzer Log Show Cuckoo Log

Analyzer Log

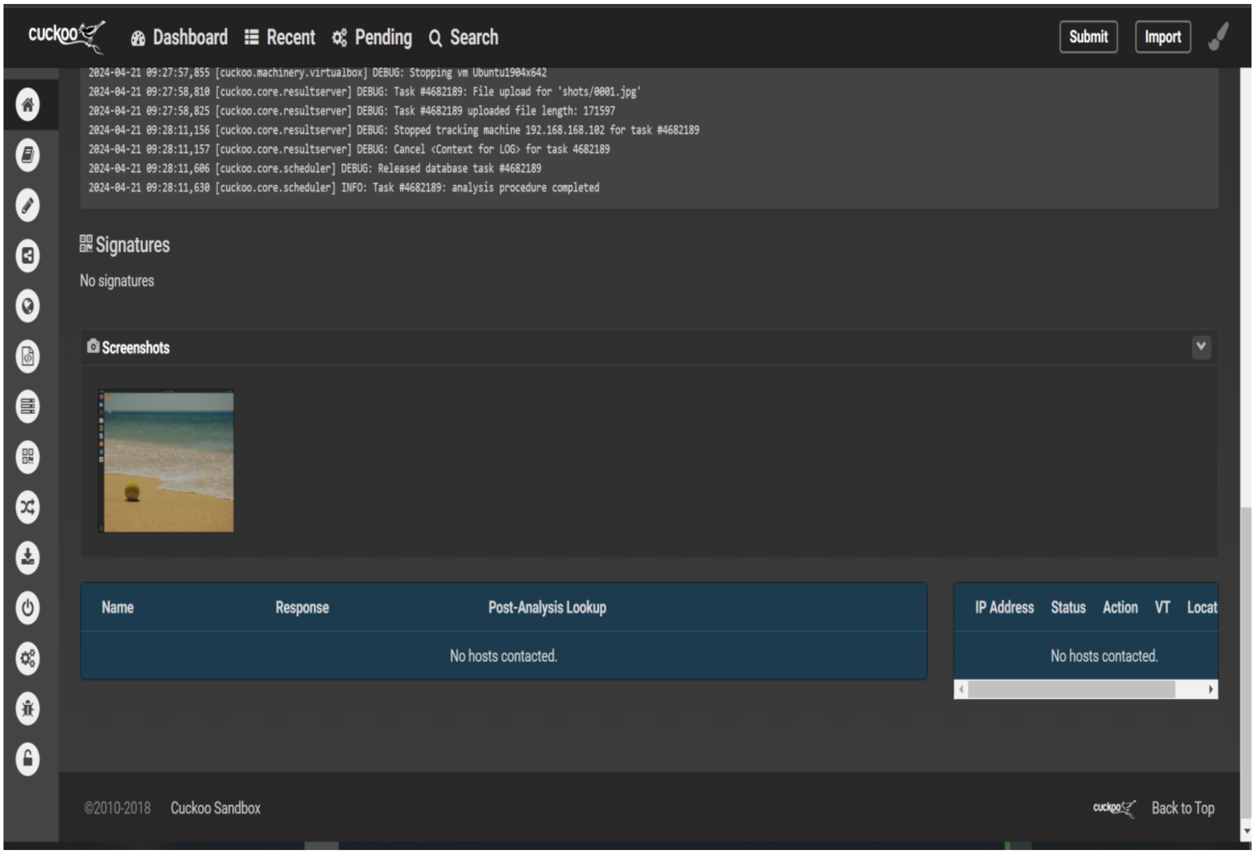
```
2024-04-21 09:40:37,005 [root] DEBUG: Starting analyzer from: /tmp/tmpE3erHV
2024-04-21 09:40:37,006 [root] DEBUG: Storing results at: /tmp/HqqeCPKK
2024-04-21 09:40:37,007 [root] ERROR: Traceback (most recent call last):
  File "/tmp/tmpE3erHV/analyzer.py", line 340, in <module>
    success = analyzer.run()
  File "/tmp/tmpE3erHV/analyzer.py", line 129, in run
    self.config.file_name, **kwargs)
  File "/tmp/tmpE3erHV/lib/core/packages.py", line 42, in choose_package_class
    "exist.".format(name))
Exception: Unable to import package "apk": it does not exist.
Traceback (most recent call last):
  File "/tmp/tmpE3erHV/analyzer.py", line 340, in <module>
    success = analyzer.run()
  File "/tmp/tmpE3erHV/analyzer.py", line 129, in run
    self.config.file_name, **kwargs)
  File "/tmp/tmpE3erHV/lib/core/packages.py", line 42, in choose_package_class
    "exist.".format(name))
Exception: Unable to import package "apk": it does not exist.
```

Signatures

Yara rule detected for file (1 event)

File has been identified by 4 AntiVirus engine on IRMA as malicious (4 events)

Behavior:



```
2024-04-21 09:27:57,855 [cuckoo.machinery.virtualbox] DEBUG: Stopping vm Ubuntu1904x642
2024-04-21 09:27:58,810 [cuckoo.core.resultserver] DEBUG: Task #4682189: File upload for 'shots/0001.jpg'
2024-04-21 09:27:58,825 [cuckoo.core.resultserver] DEBUG: Task #4682189 uploaded file length: 171597
2024-04-21 09:28:11,156 [cuckoo.core.resultserver] DEBUG: Stopped tracking machine 192.168.168.102 for task #4682189
2024-04-21 09:28:11,157 [cuckoo.core.resultserver] DEBUG: Cancel <Context for LOG> for task 4682189
2024-04-21 09:28:11,606 [cuckoo.core.scheduler] DEBUG: Released database task #4682189
2024-04-21 09:28:11,630 [cuckoo.core.scheduler] INFO: Task #4682189: analysis procedure completed
```

Signatures

No signatures

Screenshots

Name	Response	Post-Analysis Lookup
No hosts contacted.		

IP Address	Status	Action	VT	Locat
No hosts contacted.				

©2010-2018 Cuckoo Sandbox

Back to Top

Conclusion:

In this lab, using Cuckoo Sandbox gives a pivotal advantage in dissecting malware via both static and dynamic evaluation. By comprehensively scrutinizing the behavior and interactions of malicious files inside a managed environment, protection practitioners gain essential insights into the strategies, techniques, and objectives of cyber attackers, bolstering defense strategies and enhancing cyber resilience.

Referencing:

1. Oren, Y., Kemerlis, V. P., Sethumadhavan, S., & Keromytis, A. D. (2015). The Spy in the Sandbox--Practical Cache Attacks in Javascript. arXiv preprint arXiv:1502.07373.
2. Lipp, M., Gruss, D., Schwarz, M., Bidner, D., Maurice, C., & Mangard, S. (2017). Practical keystroke timing attacks in sandboxed javascript. In *Computer Security–ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II 22* (pp. 191-209). Springer International Publishing.
3. Andersson, S., Clark, A., & Mohay, G. (2005). Detecting network-based obfuscated code injection attacks using sandboxing. In AusCERT Asia Pacific Information Technology Security Conference-AusCERT 2005 (pp. 13-25). AusCert Asia Pacific.