

Cuckoo sandbox

<https://cuckoosandbox.org/>

What is Cuckoo?

Cuckoo Sandbox is the **leading open source automated malware analysis system**.



You can throw any suspicious file at it and in a matter of minutes Cuckoo will provide a detailed report outlining the behavior of the file when executed inside a realistic but isolated environment.

Malware is the swiss-army knife of cybercriminals and any other adversary to your corporation or organization.

In these evolving times, detecting and removing malware artifacts is not enough: it's vitally important to understand how they operate in order to understand the context, the motivations, and the goals of a breach.

Cuckoo Sandbox is free software that automated the task of analyzing any malicious file under **Windows**, **macOS**, **Linux**, and **Android**.

What can it do?

Cuckoo Sandbox is an advanced, extremely modular, and 100% open source automated malware analysis system with infinite application opportunities. By default it is able to:

- Analyze many different malicious files (executables, office documents, pdf files, emails, etc) as well as malicious websites under Windows, Linux, macOS, and Android virtualized environments.
- Trace API calls and general behavior of the file and distill this into high level information and signatures comprehensible by anyone.
- Dump and analyze network traffic, even when encrypted with SSL/TLS. With native network routing support to drop all traffic or route it through InetSIM, a network interface, or a VPN.
- Perform advanced memory analysis of the infected virtualized system through Volatility as well as on a process memory granularity using YARA.

Due to Cuckoo's open source nature and extensive modular design one may customize any aspect of the analysis environment, analysis results processing, and reporting stage. Cuckoo provides you all the requirements to easily integrate the sandbox into your existing framework and backend in the way you want, with the format you want, and all of that without licensing requirements.

<https://www.trustedsec.com/blog/malware-cuckoo-1/>

The major disadvantage of Cuckoo is that its installation is rather cryptic and confusing the first few times through.

WHAT DOES CUCKOO SANDBOX LOOK LIKE?

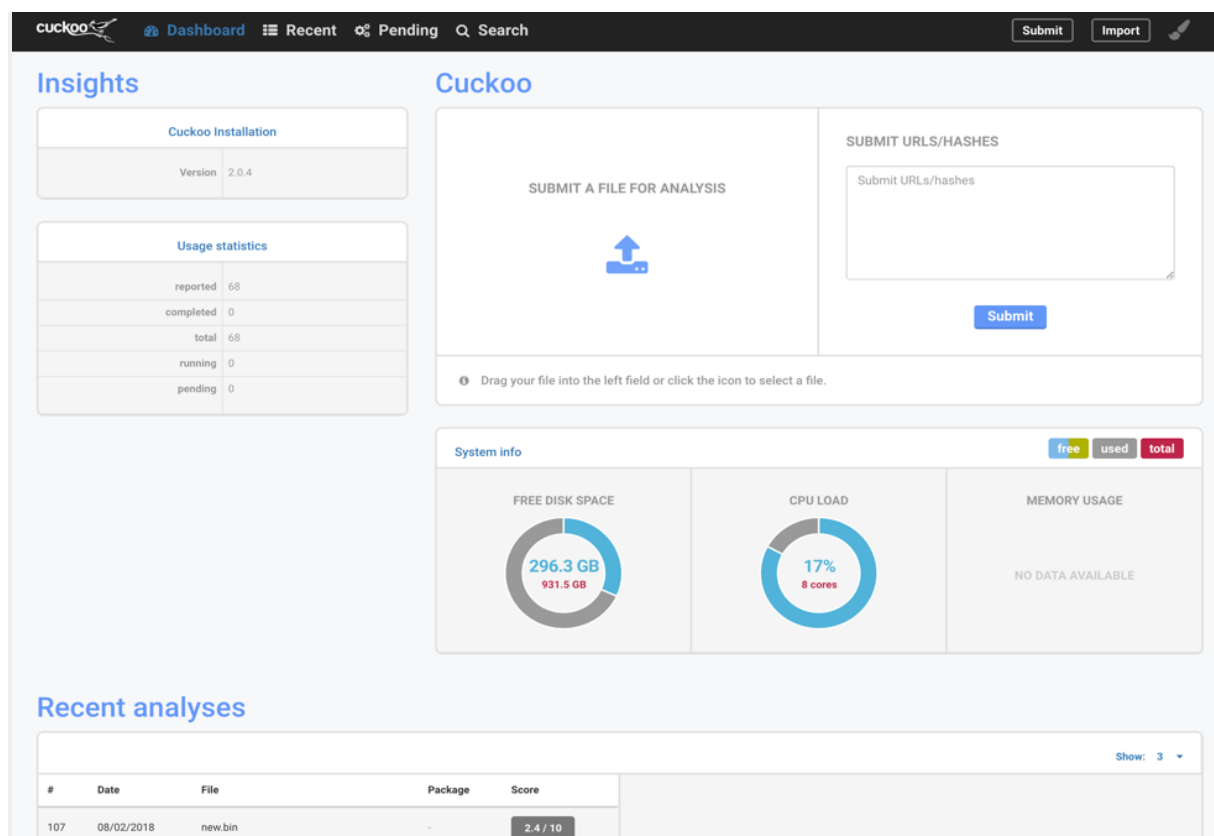
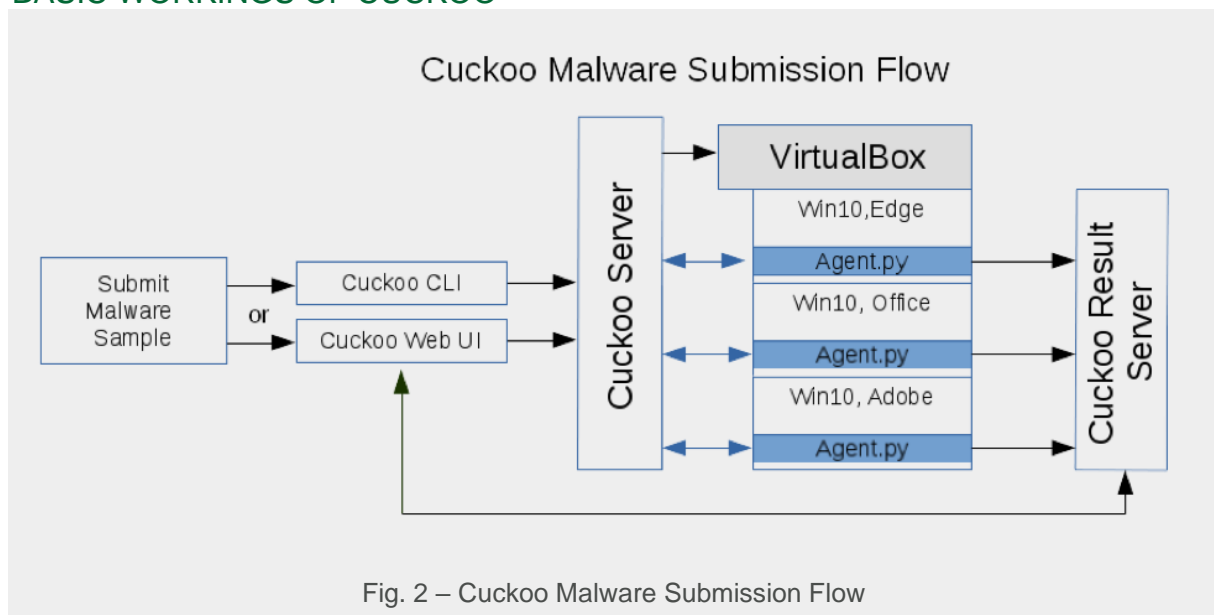
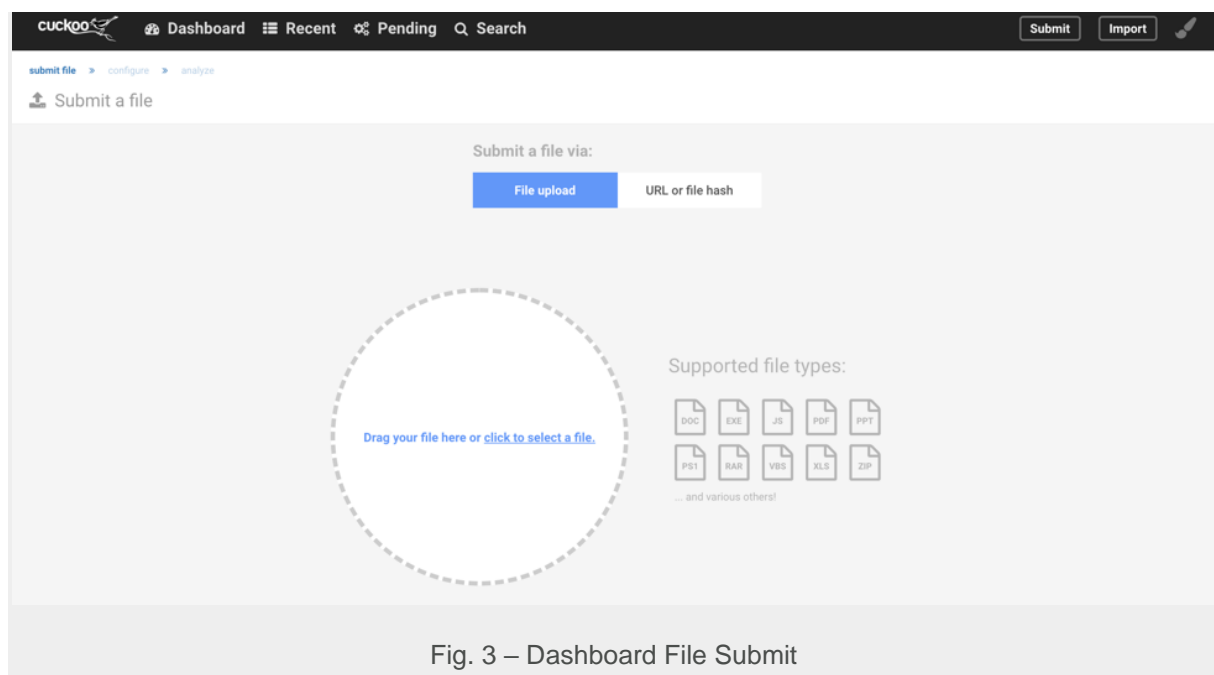


Fig. 1 – Cuckoo Dashboard

BASIC WORKINGS OF CUCKOO



Submit file to Cuckoo through web interface (via Web GUI or API) or from the console. Cuckoo will attempt to determine the best analysis method and VM image to execute the submitted file or you can explicitly declare what analysers and VM image to use. Cuckoo schedules the submission into a task, then loads the appropriate VM image (or multiple VMs) to execute it.



```
Scotts-MacBook-Pro:TrustedSec scottnusbaum$ cuckoo submit new.bin  
[snus] 0:bash*Z 1:bash-
```

Fig. 4 – Command line File Submit

Cuckoo is written in Python and works with multiple Hypervisors. A **hypervisor** is software that creates and runs virtual machines by separating a system's operating system and resources from the hardware to allocate to VMs. The most tested Hypervisor is VirtualBox, because it is free and relatively painless to setup. The following is the list of supported Hypervisors:

- ESX / ESXI
- KVM
- QEMU
- VirtualBox
- VMware
- vSphere
- XenServer

Once the configuration of the Hypervisor is complete, the interaction with Cuckoo is the same.

The files are submitted to the VM, which is running an Agent script. This agent listens on an open port for new tasks. The agent is also responsible for starting and collecting the data gathered during the execution. The agent then sends the data back to the Host via a new connection. The report is then stored and is accessible through the filesystem or viewed from the web front-end.

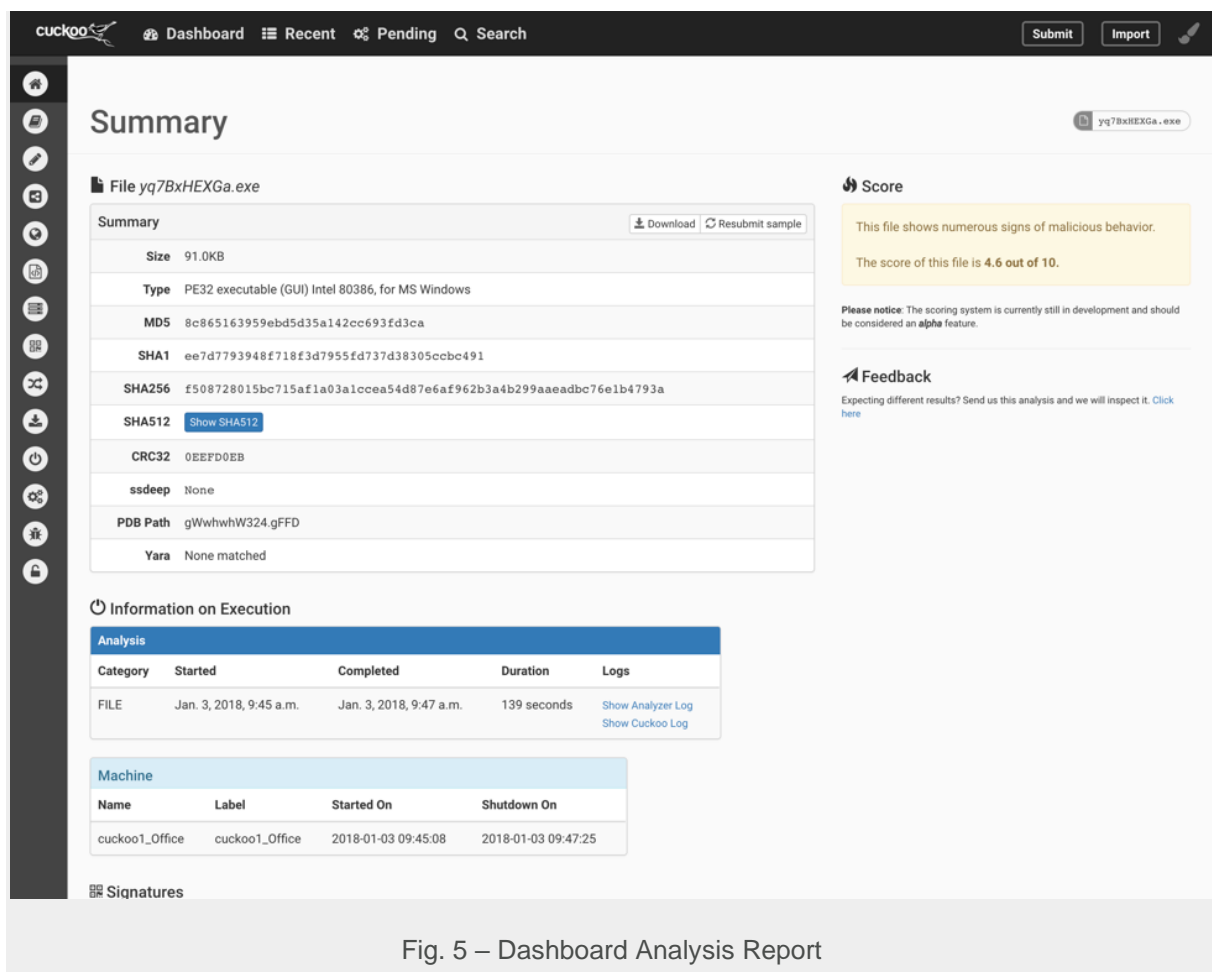



Fig. 5 – Dashboard Analysis Report

The icons on the side of the results page allow the user to quickly sort through the different analysis and behaviours captured during the execution.



Dashboard
Recent
Pending
Search

Summary

Static Analysis

Extracted Artifacts

Behavioral Analysis2

Network Analysis

Dropped Files0

Dropped Buffers

Process Memory

Compare Analysis

Export Analysis

Reboot Analysis

Options

Feedback

Lock sidebar

Summary

File
yq7BxHEXGa.exe

Summary	
Size	91.0KB
Type	PE32 executable (GUI) Intel 80386
MD5	8c865163959ebd5d35a142cc
SHA1	ee7d7793948f718f3d7955fd
SHA256	f508728015bc715af1a03a1c
SHA512	Show SHA512
CRC32	0EEFD0EB
ssdeep	None
PDB Path	gWwhwhW324.gFFD
Yara	None matched

Fig. 6 – Dashboard Sidebar

Cuckoo can be configured to capture network traffic data and screenshots. The network traffic capture is highly recommended. This will provide more detail into the potential communication to the C2 (Command and Control). This information is valuable later when combining with static analysis of the binary. Generally, it is suggested to disable the malware from outside network access until more knowledge about it is determined.

WHY SHOULD ORGANIZATIONS USE IT?

Some of the reasons to have the sandbox internal to your organization is because it would provide quick and definitive feedback on questionable files and URLs. For instance, an employee receives a phishing email with an attached document. Submit the document to Cuckoo and it will open the document and record everything about the system during this time. If the document attempts to create a new process, dump a file, edit the registry, or download more malware; all subsequent actions will be recorded. However, if it is just a normal document there will be no need to spend the time and money to either investigate internally or send the document to have it analysed.

The VM image can also be controlled. Most organizations build PCs based on a template. This template can be converted to a VM drive and used as the basis for the Cuckoo analysis. This would provide accurate results of how a piece of malware would act in YOUR environment.

The host system does not need to be an enterprise server with massive amounts of RAM and disk space. If the system is capable of running a single VM it can run Cuckoo. The more powerful the host system the faster the VM can be spun up and taken down but that extra PC in the corner that nobody is using is perfect for running a malware sample now and again.

Installation guides:

<https://www.trustedsec.com/blog/malware-cuckoo-2/> ...consistent w other material of report.

<https://blog.nviso.eu/2018/04/12/painless-cuckoo-sandbox-installation/> ..using auto cuckoo

<https://www.youtube.com/watch?v=V4z2tLRCuIY&feature=youtu.be>

```
sudo apt-get update
```

sudo apt-get upgrade

```
sudo apt install -y python3-pip
```

```
sudo apt install -y build-essential libssl-dev libffi-dev python3-dev
```

```
sudo apt install -y python3-venv
```

sudo apt install -y python3-setuptools

```
sudo apt-get install libjpeg-dev zlib1g-dev swig
sudo apt-get install mongodb
sudo apt-get install tcpdump apparmor-utils
```

```
sudo apt-get install apparmor-utils
```

```
sudo aa-disable /usr/sbin/tcpdump
sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
```

```
getcap /usr/sbin/tcpdump
```

Output should be similar to

```
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+eip

echo "deb http://www.inetsim.org/debian/ binary/" >
/etc/apt/sources.list.d/inetsim.list

wget -O - http://www.inetsim.org/inetsim-archive-signing-
key.asc | apt-key add -

sudo apt-get update
sudo apt-get install inetsim

sudo gedit /etc/inetsim/inetsim.conf

service_bind_address          192.168.56.1

dns_default_ip                 192.168.56.1

sudo gedit /etc/default/inetsim
```


ENABLED 1

```
Pip3 install m2crypto
```