Malware analysis on Cuckoo Sandbox

This document will assist the user to analyze malware on cuckoo after successfully installing cuckoo sandbox. This report includes the screenshot and steps on how to analyze malware on cuckoo. Here the steps required:

Cuckoo is already is setup on Professor Namin's Lab Computer VMware by our team and It can be accessed using following key:

USERNAME FOR **UBUNTU**: **CS4000**
Password: 1234
If the system ask for password while using cuckoo or making changes on cuckoo then the required
Password : 1234

Usage of Cuckoo Terminal:

Step 1: If you have successfully installed cuckoo then type following on terminal inside ubuntu:

cuckoo webserver

Step 2: After previous step, you will be able to see link for cuckoo interface or you can type https://127.0.0.1:8080/ on your browser.

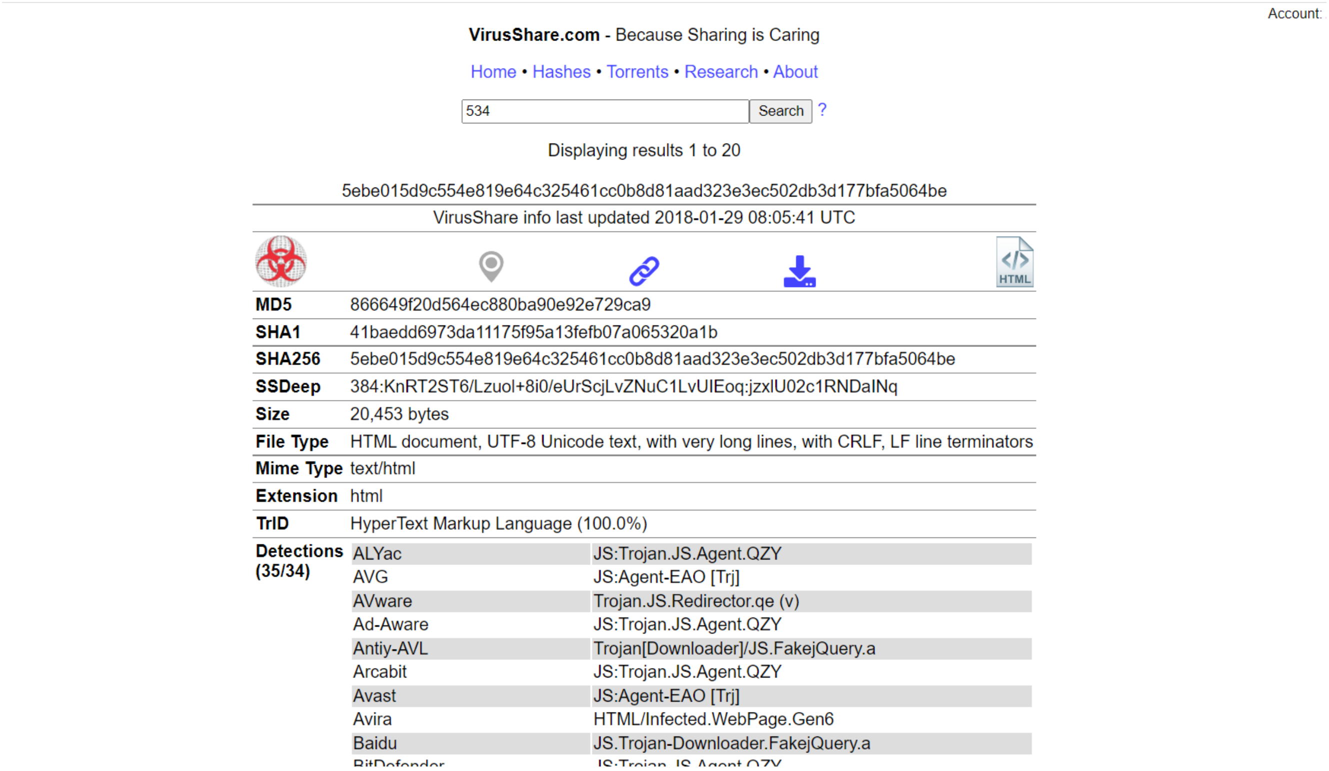
Step 3: You can submit your file either from cuckoo interface directly or from terminal using following command:

```
cuckoo submit --package <name of package>
/path/to/binary
```

Finding the malware:

We should be able to search the malware which we want to test on our cuckoo server. One can find malware anywhere but we found virushare.com a good platform to find various kinds of malware ranging from few kbs to mbs wlong with their md5,hash and other properties.

https://virusshare.com/ . This is an example of information that virusshare provides for the specific malware.



Account:

VirusShare.com - Because Sharing is Caring

Home • Hashes • Torrents • Research • About

534 Search ?

Displaying results 1 to 20

5ebe015d9c554e819e64c325461cc0b8d81aad323e3ec502db3d177bfa5064be

VirusShare info last updated 2018-01-29 08:05:41 UTC

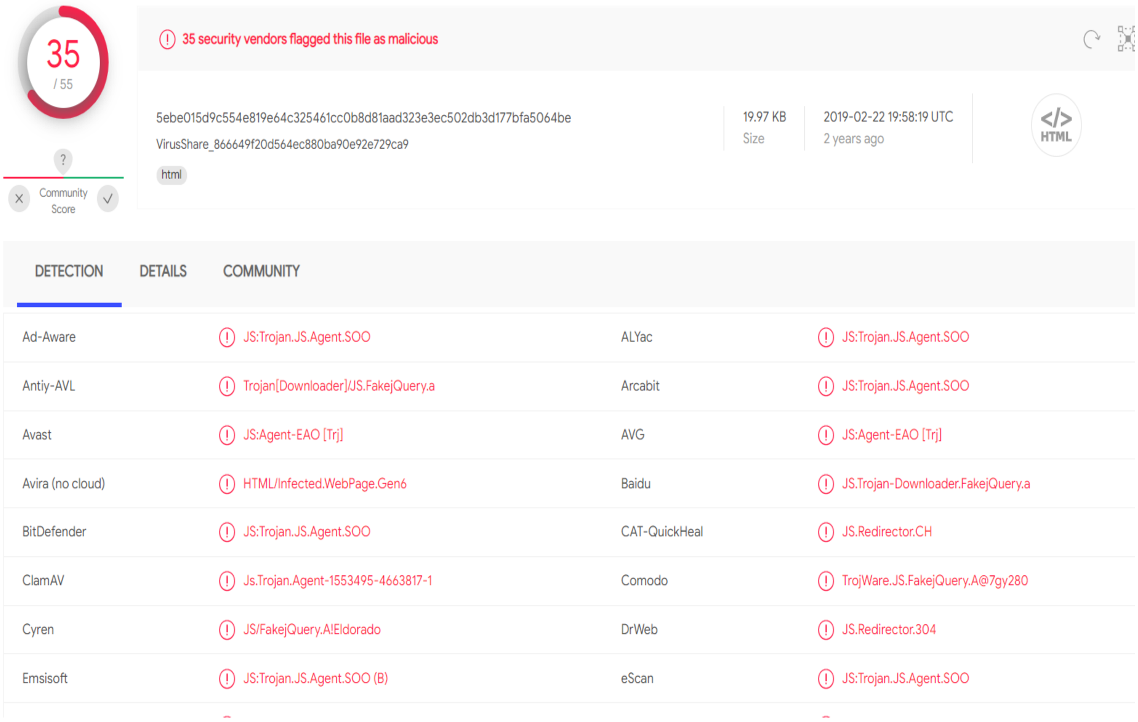
MD5	866649f20d564ec880ba90e92e729ca9	
SHA1	41baedd6973da11175f95a13fefb07a065320a1b	
SHA256	5ebe015d9c554e819e64c325461cc0b8d81aad323e3ec502db3d177bfa5064be	
SSDeep	384:KnRT2ST6/Lzuol+8i0/eUrScjLvZNuC1LvUIEoq:jzxlU02c1RNDaINq	
Size	20,453 bytes	
File Type	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators	
Mime Type	text/html	
Extension	html	
TrID	HyperText Markup Language (100.0%)	
Detections (35/34)	ALYac	JS:Trojan.JS.Agent.QZY
	AVG	JS:Agent-EAO [Trj]
	AVware	Trojan.JS.Redirector.qe (v)
	Ad-Aware	JS:Trojan.JS.Agent.QZY
	Antiy-AVL	Trojan[Downloader]/JS.FakejQuery.a
	Arcabit	JS:Trojan.JS.Agent.QZY
	Avast	JS:Agent-EAO [Trj]
	Avira	HTML/Infected.WebPage.Gen6
	Baidu	JS.Trojan-Downloader.FakejQuery.a
	BitDefender	JS:Trojan.JS.Agent.QZY

Analyzing the malware outside cuckoo:

Once we find our malware, the next part we do is to analyze the malware to understand its vulnerability. Before we even test the virus in the cuckoo server we can check its report by uploading it to the virus total which gives us the report of what it should look like when we upload it to the cuckoo machine.

https://www.virustotal.com/gui/home/upload

This is the report of above malware generated in the virustotal.com



35 security vendors flagged this file as malicious

5ebe015d9c554e819e64c325461cc0b8d81aad323e3ec502db3d177bfa5064be
VirusShare_866649f20d564ec880ba90e92e729ca9

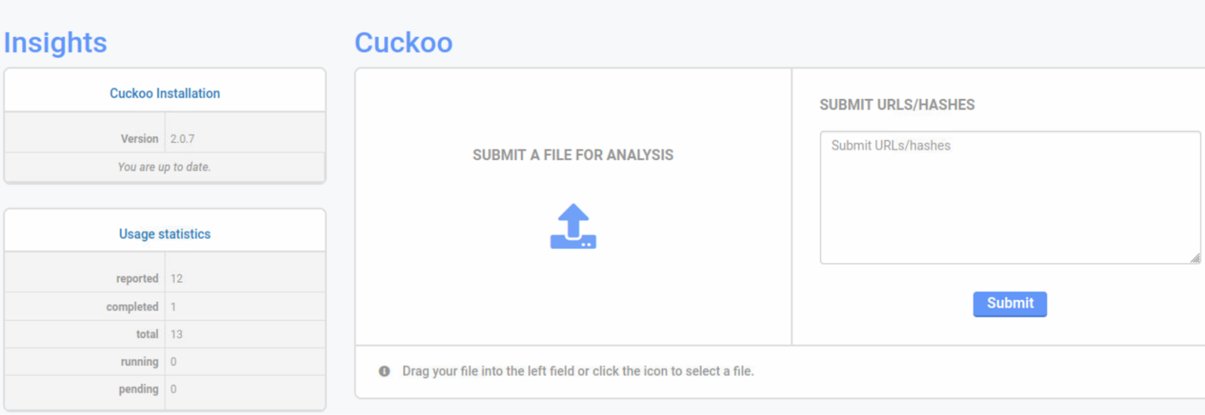
Ad-Aware	JS:Trojan.JS.Agent.SOO	ALYac	JS:Trojan.JS.Agent.SOO
Antiy-AVL	Trojan[Downloader]/JS.FakejQuery.a	Arcabit	JS:Trojan.JS.Agent.SOO
Avast	JS:Agent-EAO [Trj]	AVG	JS:Agent-EAO [Trj]
Avira (no cloud)	HTML/Infected.WebPage.Gen6	Baidu	JS.Trojan-Downloader.FakejQuery.a
BitDefender	JS:Trojan.JS.Agent.SOO	CAT-QuickHeal	JS.Redirector.CH
ClamAV	Js.Trojan.Agent-1553495-4663817-1	Comodo	TrojWare.JS.FakejQuery.A@7gy280
Cyren	JS/FakejQuery.A!Eldorado	DrWeb	JS.Redirector.304
Emsisoft	JS:Trojan.JS.Agent.SOO (B)	eScan	JS:Trojan.JS.Agent.SOO

Analyzing the malware in cuckoo server:

Due to some connection issues in the virtual machine and host machine our cuckoo wasn't able to generate the full result. But once the user has a fully functional cuckoo machine can follow the following steps to analyze the malware in their cuckoo interface.

1) The virus that we download from the virusshare.com will be in zip format. We need to unzip that file using the password: infected or Infected for all the malware.

2) Once we have the unzip file we can upload it to the cuckoo interface.



Insights

Cuckoo Installation

Version	2.0.7

You are up to date.

Usage statistics

reported	12
completed	1
total	13
running	0
pending	0

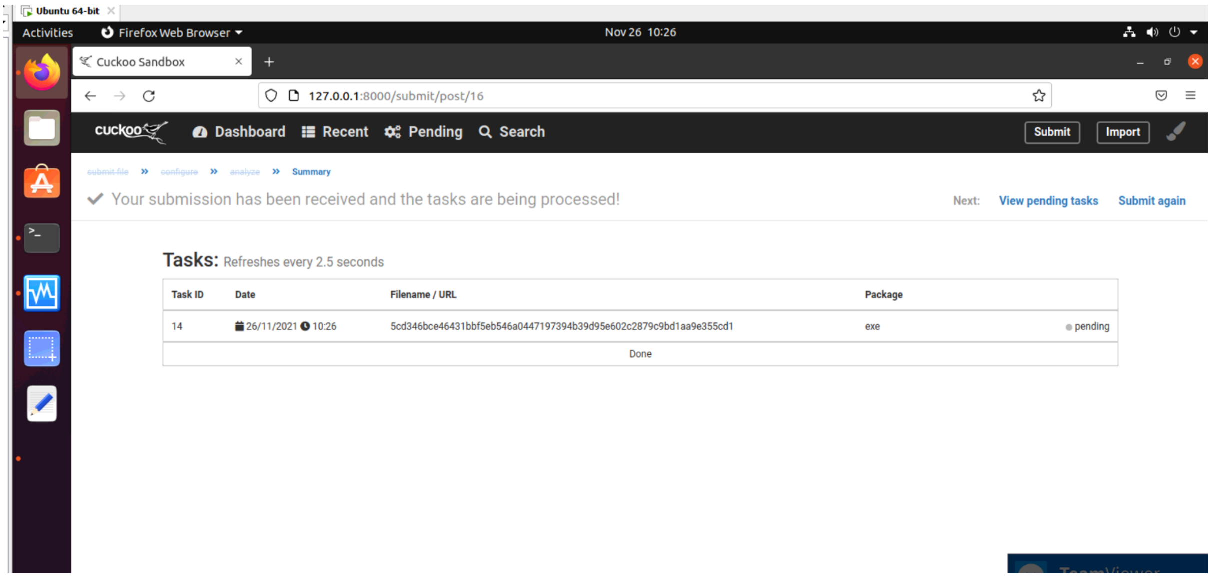
Cuckoo

SUBMIT A FILE FOR ANALYSIS

SUBMIT URLS/HASHES

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

3) After we upload the virus we will be able to see the analyze option on the top right of that page. Once we click that option our cuckoo machine will start the guest virtual machine to run windows 7 and start the analyzing part automatically.



127.0.0.1:8000/submit/post/16

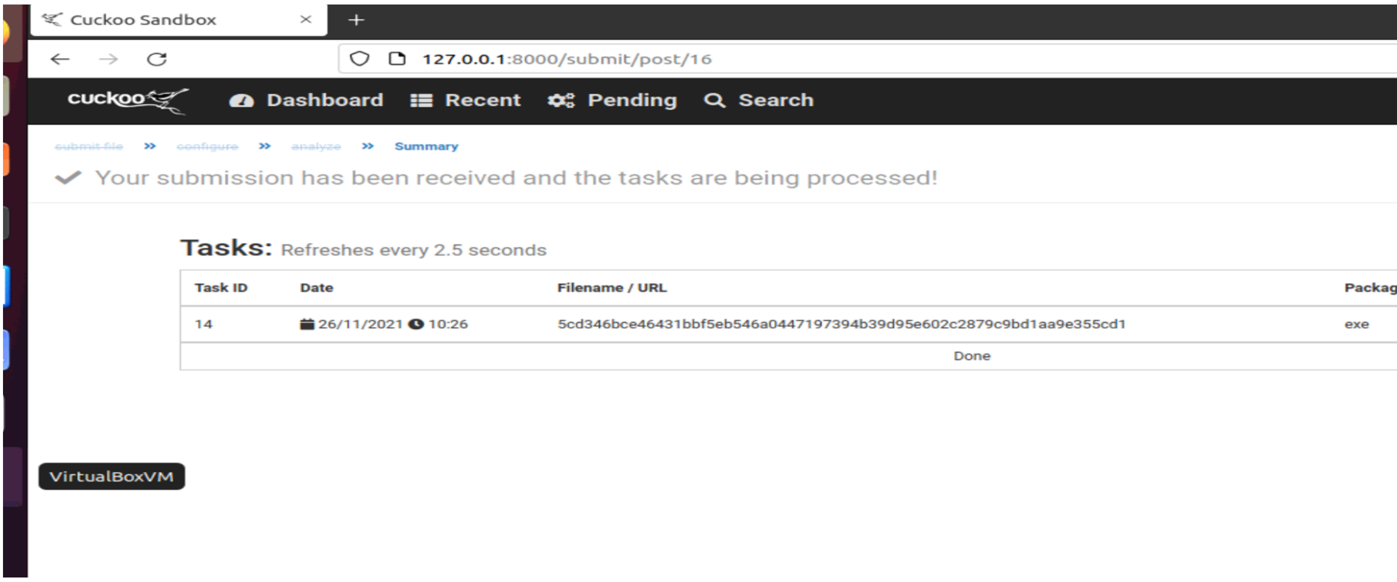
✓ Your submission has been received and the tasks are being processed!

Next: View pending tasks Submit again

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package	
14	26/11/2021 10:26	5cd346bce46431bbf5eb546a0447197394b39d95e602c2879c9bd1aa9e355cd1	exe	● pending
Done				

4) Depending on the malware size tha cuckoo server takes a few seconds to minutes to generate the report of the malware and shows status as completed once the process is done.

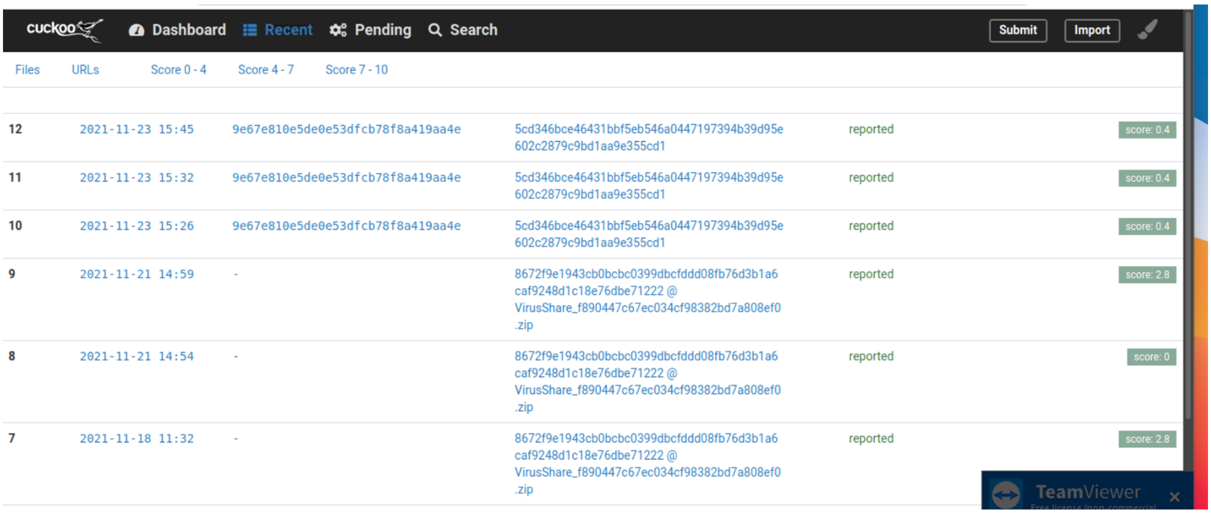


~~submit file~~ » ~~configure~~ » ~~analyze~~ » Summary

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

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Packag
14	26/11/2021 10:26	5cd346bce46431bbf5eb546a0447197394b39d95e602c2879c9bd1aa9e355cd1	exe
		Done	



12	2021-11-23 15:45	9e67e810e5de0e53dfcb78f8a419aa4e	5cd346bce46431bbf5eb546a0447197394b39d95e602c2879c9bd1aa9e355cd1	reported	score: 0.4
11	2021-11-23 15:32	9e67e810e5de0e53dfcb78f8a419aa4e	5cd346bce46431bbf5eb546a0447197394b39d95e602c2879c9bd1aa9e355cd1	reported	score: 0.4
10	2021-11-23 15:26	9e67e810e5de0e53dfcb78f8a419aa4e	5cd346bce46431bbf5eb546a0447197394b39d95e602c2879c9bd1aa9e355cd1	reported	score: 0.4
9	2021-11-21 14:59	-	8672f9e1943cb0bcbc0399dbcfddd08fb76d3b1a6caf9248d1c18e76dbe71222 @ VirusShare_f890447c67ec034cf98382bd7a808ef0.zip	reported	score: 2.8
8	2021-11-21 14:54	-	8672f9e1943cb0bcbc0399dbcfddd08fb76d3b1a6caf9248d1c18e76dbe71222 @ VirusShare_f890447c67ec034cf98382bd7a808ef0.zip	reported	score: 0
7	2021-11-18 11:32	-	8672f9e1943cb0bcbc0399dbcfddd08fb76d3b1a6caf9248d1c18e76dbe71222 @ VirusShare_f890447c67ec034cf98382bd7a808ef0.zip	reported	score: 2.8