

Forum:[Hack Forums](#)

Thread: [Source code of an runtime scanner \(avscan\)](#)

mehtevas - April 1, 2018, 4:28 am

Hey guys,

i decided to release the source code of avscan an old project of mine,
The way the "detection" is detected is using screenshots, and a compare.

so if your program has a GUI it will get detected,

it uses Oracle Virtualbox for an easy API Commandline API,

if you have questions about the code just post them below.

This code is pretty ugly but it should give everyone who is wondering how a "shitty" runtime scanner works the basics to make there own.

download:

https://fuckav.xyz/runtime_scanner.zip

edit:

added sql file

i dont mind if you build your own runtime scanner out of this just leave credits.

for meedman / run4me:

Spoiler [\(Click to View\)](#)

Toxcique - April 1, 2018, 5:34 am

Great share, daddy! <3333

darky666 - April 1, 2018, 6:09 am

lol gg good share scg, incoming rips everywhere

TOM - April 1, 2018, 7:22 am

Wonderful contribution towards this section thank u so much man

nekoochan - April 1, 2018, 7:49 am

(Apr 1, 2018 07:22 AM)Tom Cruise Wrote: [\[CITE\]](#) Wonderful contribution towards this section thank u so much man

flowscanner coming soon

josha28 - April 1, 2018, 3:13 pm

nice for sharing but how can i use it

jcbullet - April 1, 2018, 3:25 pm

From the looks of it you need to run this on a web server with access to your vms running the AV.

josha28 - April 1, 2018, 3:34 pm

ohh thnx got it not for me then

mehtevass - April 1, 2018, 3:53 pm

(Apr 1, 2018 03:25 PM)jcbullet Wrote: [\[CITE\]](#) From the looks of it you need to run this on a web server with access to your vms running the AV.

you guessed correct, a windows server

Takehito Morokuzu - April 3, 2018, 1:31 pm

(Apr 1, 2018 03:53 PM)mehtevass Wrote: [\[CITE\]](#) you guessed correct, a windows server

Is this easy to setup? I might give it a go myself.

mehtevass - April 3, 2018, 1:32 pm

(Apr 3, 2018 01:31 PM)therulerofall Wrote: [\[CITE\]](#) Is this easy to setup? I might give it a go myself.
yes,

install virtualbox,

check config.php for the names of the vms (just remove / add new ones)

make sure that the path is correct in engine.php to oracle.

G-protect - April 4, 2018, 7:50 am

(Apr 3, 2018 01:32 PM)mehtevass Wrote: [\[CITE\]](#) yes,

install virtualbox,

check config.php for the names of the vms (just remove / add new ones)

make sure that the path is correct in engine.php to oracle.

1) Please what is the on page (Your key: ?)

2) do we need to install all the Avs list on config.php

```
$av_list = array("avast"=> "waiting","eset" => "waiting","kaspersky" => "waiting","malwarebytes" => "waiting",  
"360totalsecurity" => "waiting","norton" => "waiting","avira" => "waiting","comodo" => "waiting",  
"bitdefender" => "waiting","mcafee" => "waiting","sophos" => "waiting");
```

x222 - April 4, 2018, 8:08 am

(Apr 1, 2018 07:49 AM)nekoochan Wrote: [\[CITE\]](#) flowscanner coming soon

AAHAHAHAHAHAHAHAHAHAHA

mehtevass - April 4, 2018, 8:46 am

(Apr 4, 2018 07:50 AM)G-protect Wrote: [\[CITE\]](#) 1) Please what is the on page (Your key: ?)

2) do we need to install all the Avs list on config.php

```
$av_list = array("avast"=> "waiting","eset" => "waiting","kaspersky" => "waiting","malwarebytes" => "waiting",  
"360totalsecurity" => "waiting","norton" => "waiting","avira" => "waiting","comodo" => "waiting",  
"bitdefender" => "waiting","mcafee" => "waiting","sophos" => "waiting");
```

you can remove / add avs in the av_list how you want,

just make sure that the vm has the same name.

if you mean the serials, please take a look in the database (the sql file), there are already some keys in.

merso - April 4, 2018, 10:37 pm

so what would be correct order of this

Quote:\$connection = mysqli_connect("localhost","root","xxxxxxx","xxxxxxx");
in order i mean (host,database,user,passowod) or ??

mehtevs - April 4, 2018, 10:50 pm

(Apr 4, 2018 10:37 PM)merso Wrote: [\[CITE\]](#) so what would be correct order of this

in order i mean (host,database,user,passowod) or ??
mysqli_connect(\$db_host,\$db_user,\$db_pass,\$db_database,\$db_port);

<http://php.net/manual/en/function.mysqli-connect.php>

Mr. Kim - April 5, 2018, 6:14 am

(Apr 1, 2018 04:28 AM)mehtevs Wrote: [\[CITE\]](#) The way the "detection" is detected is using screenshots, and a compare.

so if your program has a GUI it will get detected,
Can you elaborate on this please?

mehtevs - April 5, 2018, 6:28 am

(Apr 5, 2018 06:14 AM)M?m?ry Wrote: [\[CITE\]](#) Can you elaborate on this please?
the tool takes a screenshot at the start,
drops the file

creates screenshots until 30 seconds are over and compares it to the first one

then executes the file and does the screenshot stuff again,
if there is a difference of 5% its detected (so clock changes and stuff doesnt affect it)

Mr. Kim - April 5, 2018, 6:32 am

(Apr 5, 2018 06:28 AM)mehtevs Wrote: [\[CITE\]](#) the tool takes a screenshot at the start,
drops the file

creates screenshots until 30 seconds are over and compares it to the first one

then executes the file and does the screenshot stuff again,
if there is a difference of 5% its detected (so clock changes and stuff doesnt affect it)
So like, what if it's just a normal gui based program?

EDIT: I guess im just confused on what the purpose of the program is?

mehtevs - April 5, 2018, 6:37 am

(Apr 5, 2018 06:32 AM)M?m?ry Wrote: [\[CITE\]](#) So like, what if it's just a normal gui based program?

EDIT: I guess im just confused on what the purpose of the program is?
GUI programs are not supported. (as i said in the main post)

this program is made to detect if your virus is detected or not at runtime.

Mr. Kim - April 5, 2018, 6:40 am

(Apr 5, 2018 06:37 AM)mehtevs Wrote: [\[CITE\]](#) GUI programs are not supported. (as i said in the main post)

this program is made to detect if your virus is detected or not at runtime.

So hold on, it's completely incapable of detected a console program? I dont really see how this is a runtime analysis at all to be honest.

Does it check API calls? System calls? Registry keys? Open handles? Anything other than it having made a visual difference on the screen?

mehtevs - April 5, 2018, 6:47 am

(Apr 5, 2018 06:40 AM)M?m?ry Wrote: [\[CITE\]](#) So hold on, it's completely incapable of detected a console program? I dont really see how this is a runtime analysis at all to be honest.

Does it check API calls? System calls? Registry keys? Open handles? Anything other than it having made a visual difference on the screen?
its not a good system,

but hey run4me uses the same system and meedman makes quite a bit of it.

and yes you are correct, everything what has an interface will be marked as detected.

the issue is that if you hook it there is always something what can unhook it / kill it.

you need a method outside the box/vm to detect.

OCR would be a way.

Mr. Kim - April 5, 2018, 6:55 am

(Apr 5, 2018 06:47 AM)mehtevs Wrote: [\[CITE\]](#) its not a good system,

but hey run4me uses the same system and meedman makes quite a bit of it.

and yes you are correct, everything what has an interface will be marked as detected.

the issue is that if you hook it there is always something what can unhook it / kill it.

you need a method outside the box/vm to detect.

OCR would be a way.

Wow, I didn't realize run4me is literally useless. I assumed it ran it through actual runtime detection engines (Avast, malwarebytes, whatever).

I honestly dont see much of an issue with hooking. It's not perfect, sure, but if you're smart enough and you get your hooks in first, you can subvert everything the program attempts to do.

Even if you just take a list of registry keys before and after the program gets run, you'll at least have an idea of what keys it's messing with.

If a new key shows up under HKCU\Software\Microsoft\Windows\CurrentVersion\Run after you test a binary, chances are it's malicious. Or, at the least, you know that it's attempting to persist. It seems to me using JUST visual feedback is far worse an idea than using hooks, or doing a hash of all the files on disk before/after, etc.

This would be a far better and more interesting tool if it used more complex detection mechanics. Especially because, as you acknowledged, it can't actually tell the difference between a malicious program that doesn't open a GUI and a nonmalicious program that does. That's, essentially, a useless piece of software. I'm not trying to be an ass, I'm just trying to give you some feedback on how you could really improve this tool.

Magna imperium - April 5, 2018, 6:56 am

(Apr 5, 2018 06:47 AM)mehtevs Wrote: [\[CITE\]](#) it's not a good system,

but hey run4me uses the same system and meedman makes quite a bit of it.

and yes you are correct, everything what has an interface will be marked as detected.

the issue is that if you hook it there is always something what can unhook it / kill it.

you need a method outside the box/vm to detect.

OCR would be a way.

or maybe you could detect the pixel modification at certain position? In that way, unless the program popped up on the right corner, it would support GUI's?

Just a random question, pretty interesting contribution you've made

Mr. Kim - April 5, 2018, 6:59 am

(Apr 5, 2018 06:56 AM)Magna imperium Wrote: [\[CITE\]](#) or maybe you could detect the pixel modification at certain position? In that way, unless the program popped up on the right corner, it would support GUI's?

Just a random question, pretty interesting contribution you've made

I still don't see how this differentiates between malicious GUIs and normal GUIs. I don't think, fundamentally, you can tell for certain if software is malicious based solely on visual feedback. I mean you've already ignored like 90%-ish of malware that doesn't do anything visually, and that's a huge problem.

Magna imperium - April 5, 2018, 7:08 am

(Apr 5, 2018 06:59 AM)M?m?ry Wrote: [\[CITE\]](#) I still don't see how this differentiates between malicious GUIs and normal GUIs. I don't think, fundamentally, you can tell for certain if software is malicious based solely on visual feedback. I mean you've already ignored like 90%-ish of malware that doesn't do anything visually, and that's a huge problem.

as far as I understood, what the source is doing is dropping a file and executing it on a virtual machine, such machine got an anti virus. If, the screen changes, then system will interpret as if it was an anti virus detection.

Meaning that if you scan, for example, a cracker, it will always be detected as it has a GUI, what I was saying is that screenshot could only be made of the right corner, where usually AV alerts pick up.

Friedrich Nietzsche - April 5, 2018, 7:09 am

(Apr 5, 2018 06:59 AM)M?m?ry Wrote: [\[CITE\]](#) I still dont see how this differentiates between malicious GUIs and normal GUIs. I dont think, fundamentally, you can tell for certain if software is malicious based solely on visual feedback. I mean you've already ignored like 90%-ish of malware that doesn't do anything visually, and thats a huge problem.

The scanner doesn't detect anything, the AV does. It is for testing the runtime of your malware against AVs.

Mr. Kim - April 5, 2018, 7:17 am

(Apr 5, 2018 07:09 AM)Friedrich Nietzsche Wrote: [\[CITE\]](#) The scanner doesn't detect anything, the AV does. It is for testing the runtime of your malware against AVs.

What are you talking about bro?

(Apr 5, 2018 07:08 AM)Magna imperium Wrote: [\[CITE\]](#) as far as i understood, what the source is doing is dropping a file and executing it on a virtual machine, such machine got an anti virus. If, the screen changes, then system will interpret as if it was an anti virus detection.

Meaning that if you scan, for example, a cracker, it will always be detected as it has a GUI, what i was saying is that screenshot could only be made of the right corner, where usually av alerts pick up.

Oooooooooooooohhhhhhhhhhhhhh, I understand now. So the idea is to check for the ANTIVIRUS's visual feedback, not the actual malware. Correct?

Friedrich Nietzsche - April 5, 2018, 7:19 am

(Apr 5, 2018 07:17 AM)M?m?ry Wrote: [\[CITE\]](#) What are you talking about bro?

Oooooooooooooohhhhhhhhhhhhhh, I understand now. So the idea is to check for the ANTIVIRUS's visual feedback, not the actual malware. Correct?

Yes, it is for that.

Mr. Kim - April 5, 2018, 7:21 am

(Apr 5, 2018 07:19 AM)Friedrich Nietzsche Wrote: [\[CITE\]](#) Yes, it is for that.

Gotcha, I misunderstood the idea completely. This seems like a fair more viable concept.

Takehito Morokuzu - April 5, 2018, 9:42 am

Hi, can I use this with VMware instead of virtual box? Virtual box is very buggy and runs extremely slow compared to VMware. It's like coming from a Pentium 4 to a core i3.

mehtevs - April 5, 2018, 9:48 am

(Apr 5, 2018 09:42 AM)therulerofall Wrote: [\[CITE\]](#) Hi, can I use this with VMware instead of virtual box? Virtual box is very buggy and runs extremely slow compared to VMware. It's like coming from a Pentium 4 to a core i3.

i mean sure you can if you rewrite the engine (the top class)

https://www.vmware.com/support/developer/vix-api/vix112_vmrun_command.pdf

take a look at pdf page 13

LightCreep - April 23, 2018, 7:26 am

Well you fked him :D Congrats! Creep here vouch for your shit :D

breaker1911 - April 23, 2018, 9:19 pm

i've plans to make this and you there, nice job bru

Hired-Haxor - May 20, 2019, 5:03 am

@mehtevs Link Update Pleas i Need it. THANK

Scrubspooof - May 20, 2019, 1:52 pm

Thank you for this. It should provide lots of info.

teddy76db - September 26, 2019, 12:13 pm

Anyone have the source please ?

I really wan't to work hard for make a Free Runtime Scanner for the community, thanks.

pro_fesnoob - September 26, 2019, 12:44 pm

Link is down, please update the link or if you have the time you could send me it per pm.

Best regards :)

teddy76db - September 27, 2019, 10:58 am

Anyone have the source please ?

Thanks you !

xpong1 - November 9, 2019, 10:56 pm

Anyone have the updated link?

AgaGguy - November 14, 2019, 6:47 pm

Update link? The original is down.

Komododaes - October 30, 2022, 8:07 pm

Hello how to contact you I lost the source