

Forum:[Hack Forums](#)

Thread: [Anti virus scanner](#)

itcorp - April 29, 2024, 3:11 pm

this is a simple project that i took the time to try to make and try to kill my free time a bit. What I'm interested in is what would be wise to implement or what would you like this type of project to have implemented. I also need some malicious files for testing.

I have this done for now.

demo

[Video: <https://www.youtube.com/watch?v=TxWi7cPtL0U>]

nucleo_type09 - April 29, 2024, 5:14 pm

what was that you were trying to do bro? :)

itcorp - April 29, 2024, 5:22 pm

(Apr 29, 2024 05:14 PM)nucleo_type09 Wrote: [\[CITE\]](#) what was that you were trying to do bro? :)
I'm trying to create a controlled environment for scanning in order to avoid using various services, I'm thinking of including behavioral analyzer but I would need some guidance on what would be the best solution and approach

nucleo_type09 - April 29, 2024, 5:26 pm

(Apr 29, 2024 05:22 PM)itcorp Wrote: [\[CITE\]](#) I'm trying to create a controlled environment for scanning in order to avoid using various services, I'm thinking of including behavioral analyzer but I would need some guidance on what would be the best solution and approach
sorry if i ask, why don't u wanna use services already built? aren't any? :)

itcorp - April 29, 2024, 5:29 pm

(Apr 29, 2024 05:26 PM)nucleo_type09 Wrote: [\[CITE\]](#) sorry if i ask, why don't u wanna use services already built? aren't any? :)
Because some things I want to learn and how they work, also want to try to make them in order to expand my knowledge.

7 - April 29, 2024, 5:35 pm

I really like this.

I have wanting to build something similar but in a more remote tech environment, a little like AVG Cloud Business so you can run scans on all computers you have the client installed and even use it for remote support instead of like teamviewer or anydesk.

There is a lot of scope, business and profits in something like this.

There are other things you could add from flushing dns, editing startups and much more.

I am posting to see its progress, nice work mate

Bastille - April 29, 2024, 6:52 pm

Hey, nice project !

I'm not skilled enough to help you but I'm sure [ttbr0](#) could bring some interesting knowledge on the table

By the way, here are few sources for malware samples in a single Github repo (I saved these links for latter but still don't have enough time to dive into malware analysis ...)

<https://github.com/Virus-Samples/Malware-Sample-Sources>

ttbr0 - April 29, 2024, 8:15 pm

(Apr 29, 2024 06:52 PM)Yseurk Wrote: [\[CITE\]](#) Hey, nice project !

I'm not skilled enough to help you but I'm sure [ttbr0](#) could bring some interesting knowledge on the table

By the way, here are few sources for malware samples in a single Github repo (I saved these links for latter but still don't have enough time to dive into malware analysis ...)

<https://github.com/Virus-Samples/Malware-Sample-Sources>

thanks for the tag haha. ive had similar thoughts about creating something like this although slightly different at a larger scale using a server (if i had one). something with proxmox, a whole bunch of vms with different avs installed, and a web interface to interact with a backend that schedules vms like this application that can upload binaries, execute them for some duration, and then download the results from the machines. this is a cool poc though, i like it.

boyah1337 - April 29, 2024, 8:59 pm

Cool job, there is a lot of money in it .. Scanner(to) makes a few 10k's a month from it.

happygonutty - April 30, 2024, 3:44 am

(Apr 29, 2024 03:11 PM)itcorp Wrote: [\[CITE\]](#) this is a simple project that i took the time to try to make and try to kill my free time a bit.What I'm interested in is what would be wise to implement or what would you like this type of project to have implemented.I also need some malicious files for testing.

I have this done for now.

demo

[Video: <https://www.youtube.com/watch?v=TxWi7cPtL0U>]

Here is another source OP and enjoy. [h\(xx\)ps://vx-underground\(dot\)org/Samples](https://hxxps://vx-underground(dot)org/Samples) ! Enjoy. ? Just a quick question also OP, how much resources does your platform need since you are running multiple services in one machine I think? Am I right? Are you running it on a home server perhaps?

nucleo_type09 - April 30, 2024, 6:19 am

(Apr 29, 2024 05:29 PM)itcorp Wrote: [\[CITE\]](#) Because some things I want to learn and how they work,also want to try to make them in order to expand my knowledge.

that makes a lot of sense now, congrats man, good luck with your project, it looks like a good idea :)

itcorp - May 1, 2024, 12:43 pm

(Apr 29, 2024 05:35 PM)NulldB Wrote: [\[CITE\]](#) I really like this.

I have wanting to build something similar but in a more remote tech environment, a little like AVG

Cloud Business so you can run scans on all computers you have the client installed and even use it for remote support instead of like teamviewer or anydesk.

There is alot of scope, business and profits in something like this.

There are other things you could add from flushing dns, editing startups and much more.

I am posting to see its progress, nice work mate

thanks mate,I started the reconstruction of the complete tool so that each vm can have its own agent..i will see how this goes

(Apr 29, 2024 06:52 PM)Yseurk Wrote: [\[CITE\]](#) Hey, nice project !

I'm not skilled enough to help you but I'm sure [ttbr0](#) could bring some interesting knowledge on the table

By the way, here are few sources for malware samples in a single Github repo (I saved these links for latter but still don't have enough time to dive into malware analysis ...)

<https://github.com/Virus-Samples/Malware-Sample-Sources>

Thank you for your reply, I will use it to test it

(Apr 30, 2024 03:44 AM)happygonutty Wrote: [\[CITE\]](#) Here is another source OP and enjoy.

h(xx)ps://vx-underground(dot)org/Samples ! Enjoy. ? Just a quick question also OP, how much resources does your platform need since you are running multiple services in one machine I think? Am I right? Are you running it on a home server perhaps?

the complete platform is abstract, and I myself can define the resources I want to spend and determine them so it is absolutely adaptable for different needs