

Forum:[Hack Forums](#)

Thread: [Dual Boot to test Malware](#)

aerohacker - January 12, 2019, 8:20 am

I intend to buy a SSD and leave it only to mess with RATs and Crypters, is there any risk of Malware being copied to another SSD?

- SSD 1 - Common use - Fully updated and protected.
- SSD2 - Everything related to security disabled, to avoid blocking or deleting any hacker program.

So in my RAT setup rat I'll use in addition to the RATs and Crypters, the VirtuaBox and the VMWare to test bypass a lot of AntiVirus (Runtime/Scantime) and etc., copying the server from the host to guest.

I know that I can create a Virtual Machine and etc, but I want to leave a SSD and use all the potential of the machine for this (CPU, RAM, SSD , GPU and Network).

CyberError - January 12, 2019, 8:21 am

why not buy a cheap laptop ? probably gonna cost 150\$ or something ? , btw yes Malware can go through from 1 ssd to another

datguy.dev - January 12, 2019, 4:51 pm

The storage of the primary drive will be accessible by the infected drive if you run them simultaneously. Not a good idea. VMs aren't really a good solution either because some malware is aware of the virtual environment. It won't act right or at all. There are some security risks with VMs as well.

aerohacker - January 13, 2019, 6:11 pm

(Jan 12, 2019 05:51 PM)datguy.dev Wrote: [\[CITE\]](#) The storage of the primary drive will be accessible by the infected drive if you run them simultaneously. Not a good idea. VMs aren't really a good solution either because some malware is aware of the virtual environment. It won't act right or at all. There are some security risks with VMs as well.

I'll not use the other SSD to execute/test Virus or Malware, I'll only use it to execute/use RATs and Crypters and Virtual Machines with a lot of Windows and different AntiVirus installed for each VM, so I would just copy from host to guest.

datguy.dev - January 13, 2019, 6:40 pm

(Jan 13, 2019 07:11 PM)aerohacker Wrote: [\[CITE\]](#) I'll not use the other SSD to execute/test Virus or Malware, I'll only use it to execute/use RATs and Crypters and Virtual Machines with a lot of Windows and different AntiVirus installed for each VM, so I would just copy from host to guest.

That wasn't really my point. If your 'test' drive becomes compromised and the malware escapes the VM by human error, VM host bug, pure luck, or the network, it will have access to other hardware. Besides the malware encrypting that storage it can even persist through the disk's firmware. It's just not a sound plan overall. Keep in mind to treat RAT and Crypter programs as malware. A lot of them are trojans themselves and or have some sketchy network traffic. Best of luck!

aerohacker - January 13, 2019, 7:00 pm

(Jan 13, 2019 07:40 PM)datguy.dev Wrote: [\[CITE\]](#) That wasn't really my point. If your 'test' drive becomes compromised and the malware escapes the VM by human error, VM host bug, pure luck,

or the network, it will have access to other hardware. Besides the malware encrypting that storage it can even persist through the disk's firmware. It's just not a sound plan overall. Keep in mind to treat RAT and Crypter programs as malware. A lot of them are trojans themselves and or have some sketchy network traffic. Best of luck!

Malware escapes the Virtual Machine, human error or Virtual Machine Exploit?

Because in that case it does not matter if I test on a Virtual Machine and the host is protected or in a SSD only for that.

What do you suggest? A computer/notebook connected to another network?

Anyway I'll not have any security program installed, so it does not block or delete the Hacker programs, or is it better to install an AntiVirus and add the RATs and Crypters in the AV exceptions?

Cyadrogen - January 13, 2019, 7:18 pm

(Jan 12, 2019 09:20 AM)aerohacker Wrote: [\[CITE\]](#) I intend to buy a SSD and leave it only to mess with RATs and Crypters, is there any risk of Malware being copied to another SSD?

Yes. That is unless you can somehow obscure the non affected drive from the os.

(Jan 12, 2019 09:20 AM)aerohacker Wrote: [\[CITE\]](#) I know that I can create a Virtual Machine and etc, but I want to leave a SSD and use all the potential of the machine for this (CPU, RAM, SSD , GPU and Network).

If you can spare SOME hardware you can actually split the stuff in the iommu to make a type 1 hypervisor. It's not exactly 100% potential but depending on how you set it you can make very fast vms. Heck I game on a windows hosted via arch using this method and I see little performance changes.

aerohacker - January 13, 2019, 7:27 pm

(Jan 13, 2019 08:18 PM)Cyadrogen Wrote: [\[CITE\]](#) Yes. That is unless you can somehow obscure the non affected drive from the os.

If you can spare SOME hardware you can actually split the stuff in the iommu to make a type 1 hypervisor. It's not exactly 100% potential but depending on how you set it you can make very fast vms. Heck I game on a windows hosted via arch using this method and I see little performance changes.

What is your host setup specs?

What is your guest setup specs?

Cyadrogen - January 13, 2019, 7:32 pm

(Jan 13, 2019 08:27 PM)aerohacker Wrote: [\[CITE\]](#) What is your host setup specs?

What is your guest setup specs?

I gave my host the first keyboard/mouse, my hard drive, and the integrated gpu.

I have given my guest the second keyboard/mouse, my ssd and the graphics card.

as for the cpu you can't choose one or the other but you can give a set amount of core to each. my cpu is 8 cores, I've split them half n half.

About it tbh.

datguy.dev - January 13, 2019, 7:33 pm

(Jan 13, 2019 08:00 PM)aerohacker Wrote: [\[CITE\]](#) Malware escapes the Virtual Machine, human error or Virtual Machine Exploit?

Because in that case it does not matter if I test on a Virtual Machine and the host is protected or in a SSD only for that.

What do you suggest? A computer/notebook connected to another network?

Anyway I'll not have any security program installed, so it does not block or delete the Hacker programs, or is it better to install an AntiVirus and add the RATs and Crypters in the AV exceptions? Yes, a separate computer. It was already suggested so I didn't. Preferably a computer on an isolated network to avoid the malware from doing any recon or spreading. Something you can re-image quickly.

If it isn't obvious, malware developers know that security experts are likely to use VMs to inspect their programs. Merely decent developers accommodate for such things. You just have to accept that and not rely on other programs - or anything really - for protection of your personal data. How you want to conduct your trials is purely up to you.

aerohacker - January 23, 2019, 12:02 pm

(Jan 13, 2019 08:18 PM)Cyadrogen Wrote: [\[CITE\]](#) Yes. That is unless you can somehow obscure the non affected drive from the os.

If you can spare SOME hardware you can actually split the stuff in the iommu to make a type 1 hypervisor. It's not exactly 100% potential but depending on how you set it you can make very fast vms. Heck I game on a windows hosted via arch using this method and I see little performance changes.

I think to dedicated a entire SSD 1 TB VirtualBox guest and inside it install Windows 10 to test RATs and Crypters and inside it install VMWare with some Windows guest with some AntiVirus so I'd could copy the server of the host from guest and I'd still be safed inside a VM.

Host -> VirtualBox -> VMware

or

Host -> Hyper-V -> VMware

VirtualBox has the feature to copy/paste or drag/drop of the host from the guest?