

Forum:[Hack Forums](#)

Thread: [Tails Operating System](#)

ZeroEmpathy - June 29, 2017, 11:38 pm

If I boot tails DVD from virtual box and connect to a Public Wifi from a car. Is my system FULLY untrackable? Is everything still only on the computers Ram or is there any trace to my PC or personal windows OS? I'm not doing anything illegal I just don't want hackers to mess with me and I want to feel safe on the DN.

Marxist - June 30, 2017, 2:32 am

Everything from within tails is protected. Your host machine, is not.

See this note on sending plaintext through the tor network

<https://blog.torproject.org/blog/plaintext-over-tor-still-plaintext>

The things left behind on your host machine are your tails ISO, the virtual machine file to run Tails..which is on your harddrive, and anything left in RAM..which is cleared when you turn off your computer.

Why not just run tails from a live usb like it's intended to be used?

ka\$h - June 30, 2017, 3:14 am

Your reason for doing all this is kind of stupid.

ZeroEmpathy - June 30, 2017, 11:55 am

(Jun 30, 2017 03:14 AM)ka\$h Wrote: [\[CITE\]](#) Your reason for doing all this is kind of stupid. Maybe it's not my real reason. We're are on the clearnet. noob

ka\$h - June 30, 2017, 3:15 pm

(Jun 30, 2017 11:55 AM)ZeroEmpathy Wrote: [\[CITE\]](#) Maybe it's not my real reason. We're are on the clearnet. noob

Lol, if those aren't your real intentions then don't state them, your question requires no context to be answered, and using Tails is not a crime. noob

ZeroEmpathy - June 30, 2017, 9:33 pm

(Jun 30, 2017 03:15 PM)ka\$h Wrote: [\[CITE\]](#) Lol, if those aren't your real intentions then don't state them, your question requires no context to be answered, and using Tails is not a crime. noob
Tails is actually illegal in some countries.

If hackers can't find me LE can't either. I just want my personal computer to be separate from other activities. Would be cool to boot a VM with a USB and boot tails from the DVD on the VM while connected to bridges.. When i shut down the VM it should delete from the ram and I can always leave my personal PC on. I can use bleachbit to delete the VM from the USB or shred x100 times with a shredder developed by peter gutmann. I can use almost anybodies connection. I can hack wifi with Kali Linux. I bought a super long antenna and I spoofed my rig up. I'm Undetected

I'm all for sharing ideas, please don't put stupid posts on my thread. Contribute

Marxist - June 30, 2017, 10:49 pm

Using a virtual machine to run tails and do your dirty work is a stupid idea. Just run from usb like it's intended.

I don't know what virtual machine actually stores on the harddrive outside of what I listed, but it's very possible it stores other things on the hard drive that incriminating institutes could use against you.

Also. Believing you are undetectable is a bold statement.

ZeroEmpathy - June 30, 2017, 11:10 pm

(Jun 30, 2017 10:49 PM)Marxist Wrote: [\[CITE\]](#) Using a virtual machine to run tails and do your dirty work is a stupid idea. Just run from usb like it's intended.

I don't know what virtual machine actually stores on the harddrive outside of what I listed, but it's very possible it stores other things on the hard drive that incriminating institutes could use against you.

Also. Believing you are undetectable is a bold statement.

Yea but even if they spent all of that \$\$\$ to find me they would find a public wifi or a burner hotspot. with PIA connected to a kill switch and max encryption and more

Marxist - June 30, 2017, 11:42 pm

(Jun 30, 2017 11:10 PM)ZeroEmpathy Wrote: [\[CITE\]](#) Yea but even if they spent all of that \$\$\$ to find me they would find a public wifi or a burner hotspot. with PIA connected to a kill switch and max encryption and more

What makes you think it costs much at all? lol

You're the one looking for privacy.

You know what? Fuvk it. Run that shit on a VM OP your encryption and spoofing is ON POINT you do you fam

You do not understand the issues you cause by doing half of your plans

ZeroEmpathy - July 1, 2017, 3:07 am

(Jun 30, 2017 11:42 PM)Marxist Wrote: [\[CITE\]](#) What makes you think it costs much at all? lol

You're the one looking for privacy.

You know what? Fuvk it. Run that shit on a VM OP your encryption and spoofing is ON POINT you do you fam

You do not understand the issues you cause by doing half of your plansAnybody can learn anything I can for sure. gtfo

I actually do my homework on things. So good by

Killua. - July 1, 2017, 3:10 am

(Jun 30, 2017 11:10 PM)ZeroEmpathy Wrote: [\[CITE\]](#) Yea but even if they spent all of that \$\$\$ to find me they would find a public wifi or a burner hotspot. with PIA connected to a kill switch and max encryption and more

VM Tails booted from a DVD + PIA kill switch = untraceable, noted.

Woods - July 1, 2017, 3:16 am

(Jul 1, 2017 03:07 AM)ZeroEmpathy Wrote: [\[CITE\]](#) Anybody can learn anything I can for sure. gtfo I actually do my homework on things. So good by

You are a very ignorant person, as well with a cocky attitude. Now if you did your homework you wouldn't have to ask such a simple minded question about this topic. As tails is intended to be ran off a bootable USB drive. You are doing nothing more but adding an additional 3rd party program in the equation when it isn't needed, as well as insecure. You can do all the research you want but the fact of the matter is you are running something off their machines which they have complete access to at ANYTIME. Yet you believe it is a good idea to use a software that isn't intended to run off a VM and want to claim you will be undetected. Yeah good luck with that.

ZeroEmpathy - July 1, 2017, 3:27 am

(Jul 1, 2017 03:10 AM)Killua. Wrote: [\[CITE\]](#) VM Tails booted from a DVD + PIA kill switch = untraceable, noted.

You didn't read about where i stated everything else.

(Jul 1, 2017 03:16 AM)Woods Wrote: [\[CITE\]](#) You are a very ignorant person, as well with a cocky attitude. Now if you did your homework you wouldn't have to ask such a simple minded question about this topic. As tails is intended to be ran off a bootable USB drive. You are doing nothing more but adding an additional 3rd party program in the equation when it isn't needed, as well as insecure. You can do all the research you want but the fact of the matter is you are running something off their machines which they have complete access to at ANYTIME. Yet you believe it is a good idea to use a software that isn't intended to run off a VM and want to claim you will be undetected. Yeah good luck with that.

I'm using an open source VM... tails is on the Blank DVD and boots straight from the VM. There isn't a windows installed on vm when I shut it down I shred it just in case but it will delete because it's all on USB and RAM thats how tails works... Just wanna know if thats a bad idea...

quirky - July 1, 2017, 3:32 am

never understood people asking things like that on forums. @op lost more time signing in on this forum and typing his question when it was much easier going on their site and reading

Code Running Tails inside a virtual machine has various security implications. Depending on the host operating system and your security needs, running Tails in a virtual machine might be dangerousSource: <https://tails.boum.org/install/vm/index.en.html>

ZeroEmpathy - July 1, 2017, 4:56 am

(Jul 1, 2017 03:32 AM)bob79 Wrote: [\[CITE\]](#) never understood people asking things like that on forums. @op lost more time signing in on this forum and typing his question when it was much easier going on their site and reading

Code Running Tails inside a virtual machine has various security implications. Depending on the host operating system and your security needs, running Tails in a virtual machine might be dangerousSource: <https://tails.boum.org/install/vm/index.en.html>

Thats on VMware.. same source recommends Virtual Box because it's open source and we know LE isn't in charge of it and watching..

Shoe - July 1, 2017, 7:11 pm

(Jul 1, 2017 04:56 AM)ZeroEmpathy Wrote: [\[CITE\]](#) Thats on VMware.. same source recommends Virtual Box because it's open source and we know LE isn't in charge of it and watching..

VMWare is mentioned, much as VirtualBox, solely because it's freeware. The "security considerations" is to be taken into consideration regardless of what software you're using.

Quote:Traces of your Tails session are likely to be left on the local hard disk. For example, host operating systems usually use swapping (or paging) which copies part of the RAM to the hard disk.

Quote:Only run Tails in a virtual machine if leaving traces on the hard disk is not a concern for you.