

Forum:[Hack Forums](#)

Thread: [Malware Analysis Question](#)

Play Boy - December 30, 2014, 5:44 pm

I've always been interested in malware but not so much spreading and creating it, more so that I'm interested in downloading malware and running it in a VM to see how it behaves and then eventually reverse engineering it to see what makes it do so-and-so.

I know that complex malware will either kill itself or escape onto the host when in a VM environment but I want to be able to prevent this from occurring. I know the most costly method would be to get a test PC and isolate it on it's own network. But that isn't very cost effective. ?

I believe I have all the tools I need and a bit of know how but I would like to ask your opinion. What are the chances of malware escaping from the VM onto the host machine even with no bridged connection available and how do I lessen that chance?

Thanks guys. ?

Aura - December 30, 2014, 5:50 pm

Make sure to disable "shared" features, such as shared network, shared files/folders, shared clipboard, shared USBs, etc. to avoid such situations. Also, I doubt you'll encounter a malware that actually escape the VM to actually infect your host system, except if you're really, really looking hard for one. However, many malware have an "Anti-VM" feature, where if they are in a VM environment, they'll behave in a legitimate way or just refuse to execute so they can't be busted.

Play Boy - December 30, 2014, 5:56 pm

(Dec 30, 2014 06:50 PM)Aura? Wrote: [\[CITE\]](#) Make sure to disable "shared" features, such as shared network, shared files/folders, shared clipboard, shared USBs, etc. to avoid such situations. Also, I doubt you'll encounter a malware that actually escape the VM to actually infect your host system, except if you're really, really looking hard for one. However, many malware have an "Anti-VM" feature, where if they are in a VM environment, they'll behave in a legitimate way or just refuse to execute so they can't be busted.

I see. So the chances of running into such malware isn't too likely. That's great news. Thanks for the tips Aura. It's greatly appreciated. ?

I'll also ensure to disable anything connecting the host to the VM to prevent a very unfortunate accident from occurring.

Wafflemonger - December 30, 2014, 5:58 pm

A nice cheap alternative is to get a laptop. You can get some laptops for 200-300\$. You don't need super high end specs to test malware. Also note that assembly isn't that hard if you already have knowledge about malware :). As Aura said, ensure that you have all sharing off, ESPECIALLY NETWORK DISCOVERY ON THE HOST. This is a little bs thing that has almost screwed me in the past when messing with Ransomware.

Aura - December 30, 2014, 5:58 pm

(Dec 30, 2014 06:56 PM)Play Boy Wrote: [\[CITE\]](#) I see. So the chances of running into such malware

isn't too likely. That's great news. Thanks for the tips Aura. It's greatly appreciated. ?

I'll also ensure to disable anything connecting the host to the VM to prevent a very unfortunate accident from occurring.

Hence why when someone wants me to send a file to analyze, I ask them to upload it and not to send me it on Skype, as I don't want to have that file on my host system, and also I don't want to open shared folder to transfer the file. Always better that way.

Play Boy - December 30, 2014, 6:10 pm

(Dec 30, 2014 06:58 PM)Wafflemonger Wrote: [\[CITE\]](#) A nice cheap alternative is to get a laptop. You can get some laptops for 200-300\$. You don't need super high end specs to test malware. Also note that assembly isn't that hard if you already have knowledge about malware :). As Aura said, ensure that you have all sharing off, ESPECIALLY NETWORK DISCOVERY ON THE HOST. This is a little bs thing that has almost screwed me in the past when messing with Ransomware.

Ah well. I did consider setting up a test PC. It's just money is tight right now with the start of a new semester and the holidays. I know for a fact that having such a PC would completely mitigate the risk of anything getting on my personal PC. It's a great suggestion which I may consider in the future but right now, I'm looking to be as cheap as I can. ?

Also, if you don't mind me asking, what ransomware were you messing with? I'm actually quite interested in knowing. ?

(Dec 30, 2014 06:58 PM)Aur? Wrote: [\[CITE\]](#) Hence why when someone wants me to send a file to analyze, I ask them to upload it and not to send me it on Skype, as I don't want to have that file on my host system, and also I don't want to open shared folder to transfer the file. Always better that way.

Understandable. I'm honestly paranoid enough that I get shivers running suspicious software in VMs WITH sandboxes. ?

So I can understand "better safe than sorry" thought process.

Aura - December 30, 2014, 6:17 pm

(Dec 30, 2014 07:10 PM)Play Boy Wrote: [\[CITE\]](#) Ah well. I did consider setting up a test PC. It's just money is tight right now with the start of a new semester and the holidays. I know for a fact that having such a PC would completely mitigate the risk of anything getting on my personal PC. It's a great suggestion which I may consider in the future but right now, I'm looking to be as cheap as I can. ?

Also, if you don't mind me asking, what ransomware were you messing with? I'm actually quite interested in knowing. ?

Understandable. I'm honestly paranoid enough that I get shivers running suspicious software in VMs WITH sandboxes. ?

So I can understand "better safe than sorry" thought process.

I always run the malware I receive in Sandboxie in a VM (it's just easier to see which files are being dropped, processes, etc.). Also, the VM is totally isolated and I have a snapshot of it that I restore everytime I close the VM (with all my programs, Windows Updates, settings, etc.) Best setup for me.

Play Boy - December 30, 2014, 6:31 pm

(Dec 30, 2014 07:17 PM)Aur? Wrote: [\[CITE\]](#) I always run the malware I receive in Sandboxie in a VM (it's just easier to see which files are being dropped, processes, etc.). Also, the VM is totally isolated and I have a snapshot of it that I restore everytime I close the VM (with all my programs, Windows

Updates, settings, etc.) Best setup for me.

Well now. That's an interesting idea. Though I am interested in seeing what the malware will do when it's left without a sandbox but perhaps running it in a sandbox first then running it after would actually give me a better idea of what exactly is being executed.

Aura - December 30, 2014, 6:32 pm

(Dec 30, 2014 07:31 PM)Play Boy Wrote: [\[CITE\]](#) Well now. That's an interesting idea. Though I am interested in seeing what the malware will do when it's left without a sandbox but perhaps running it in a sandbox first then running it after would actually give me a better idea of what exactly is being executed.

Yeah. But now I can say that at least over 50% of the malicious files I get have Anti-Sandboxie feature, so it's useless. I have to rely on other tools and online analysis, lol.

Wafflemonger - December 30, 2014, 6:33 pm

(Dec 30, 2014 07:17 PM)Aur? Wrote: [\[CITE\]](#) I always run the malware I receive in Sandboxie in a VM (it's just easier to see which files are being dropped, processes, etc.). Also, the VM is totally isolated and I have a snapshot of it that I restore everytime I close the VM (with all my programs, Windows Updates, settings, etc.) Best setup for me.

Running malware in a sandbox isn't really advised if you're doing an analysis of it as any malware you'd want to analyze wouldn't run in a sandbox ;D.

Aura - December 30, 2014, 6:35 pm

(Dec 30, 2014 07:33 PM)Wafflemonger Wrote: [\[CITE\]](#) Running malware in a sandbox isn't really advised if you're doing an analysis of it as any malware you'd want to analyze wouldn't run in a sandbox ;D.

Read my post just above yours, haha ?

Wafflemonger - December 30, 2014, 6:36 pm

(Dec 30, 2014 07:35 PM)Aur? Wrote: [\[CITE\]](#) Read my post just above yours, haha ?
:(...Well then :(...

Anyways OP, what was mentioned earlier should be all the information that you need :D.

Aura - December 30, 2014, 6:37 pm

(Dec 30, 2014 07:36 PM)Wafflemonger Wrote: [\[CITE\]](#) :(...Well then :(...

Anyways OP, what was mentioned earlier should be all the information that you need :D.
I'm a minute ahead of you Waffle<3 But you're a few PLs in front of me ?

Play Boy - December 30, 2014, 6:43 pm

(Dec 30, 2014 07:32 PM)Aur? Wrote: [\[CITE\]](#) Yeah. But now I can say that at least over 50% of the malicious files I get have Anti-Sandboxie feature, so it's useless. I have to rely on other tools and online analysis, lol.

Well..That's unfortunate lol.

(Dec 30, 2014 07:36 PM)Wafflemonger Wrote: [\[CITE\]](#) :(...Well then :(...

Anyways OP, what was mentioned earlier should be all the information that you need :D.
I agree. Thanks guys. Really helped me out.

Aura - December 30, 2014, 6:44 pm

(Dec 30, 2014 07:43 PM)Play Boy Wrote: [\[CITE\]](#) Well..That's unfortunate lol.

I agree. Thanks guys. Really helped me out.

It's alright, there's other methods to get around that. And no problem OP, good luck with that activity ?

-Hyperion - *December 30, 2014, 8:58 pm*

I would not run on a separate pc as it makes network analysis more dangerous. Instead use this <http://practicalmalwareanalysis.com/fakenet/> my updated tutorial on setting up a box and using it safely out tomorrow.