

Forum:[Hack Forums](#)

Thread: [Have you guys ever used deep-freeze before?](#)

Sennheiser - October 30, 2014, 5:24 pm

There is a program on the Internet made by Faronics called deep-freeze. This program is actually very interesting since there are no known bypasses to it, what it does is it every time you start your computer from the moment you activate it, everything resets back to that day or time you activated deep-freeze. What is the benefit of a program like this? A software like this would be very important since it would completely bulletproof your PC from any viruses or malware, though it is recommended that you clear all your browsing history, cookies, pasturage, or any kind of logins that have been stored before activating deep-freeze. Just wanted to point this out because it is a very cool program if you want to test out other people's rats, or viruses without actually messing up your computer since when it restarts, every single virus or malware or even legitimate files that have been downloaded and installed will have been removed since your PC is technically reinstalled back to that state deep-freeze was activated at that moment.

Yoshikage Kira - October 30, 2014, 5:27 pm

The computers at my old library used to use it, pretty damn effective.

Kouichi - October 30, 2014, 5:29 pm

This sounds pretty fucking cool. Official site link please.

Sennheiser - October 30, 2014, 6:12 pm

(Oct 30, 2014 05:29 PM)Kouichi Wrote: [\[CITE\]](#) This sounds pretty fucking cool. Official site link please.

<http://www.faronics.com/products/deep-freeze/enterprise/>

Lucifer Morningstar - October 31, 2014, 3:51 am

The only bot that bypassed deep-freeze was Carberp. It installed a bootkit component which started before any other kernel mode driver(deep freeze was one of them).

You can bypass it if you know how to make your ring0 driver load before ELAM.

But yeah that's the only negative thing that this tool has. I have it setup on my vmbox for testing purposes.

Mr. WAVES - October 31, 2014, 10:20 pm

(Oct 31, 2014 03:51 AM)Tx707 Wrote: [\[CITE\]](#) The only bot that bypassed deep-freeze was Carberp. It installed a bootkit component which started before any other kernel mode driver(deep freeze was one of them).

You can bypass it if you know how to make your ring0 driver load before ELAM.

But yeah that's the only negative thing that this tool has. I have it setup on my vmbox for testing purposes.Thank you for this idea!

I'll use it on my VM, so I'll have a clean on every time I start it!

?

a323109 - November 1, 2014, 8:19 am

Quote:Have you guys ever used deep-freeze before?

Not exactly the same but i used to log here a read only filesystem, everything loaded in RAM and everything deleted after reboot. Now i use a read/write filesystem.

Sennheiser - November 1, 2014, 11:38 am

(Nov 1, 2014 08:19 AM)a323109 Wrote: [\[CITE\]](#) Not exactly the same but i used to log here a read only filesystem, everything loaded in RAM and everything deleted after reboot. Now i use a read/write filesystem.
wat?

idk files could easily rewrite those permissions couldn't they?

Jagster™ - November 1, 2014, 3:15 pm

erm I would bet many rootkits can by-pass this

Sennheiser - November 1, 2014, 4:09 pm

(Nov 1, 2014 03:15 PM)Jagster™ Wrote: [\[CITE\]](#) erm I would bet many rootkits can by-pass this how?

running df is like running a vm

how can a root kit get outside of that vm

knowing there is no shared drives to host computer or any way to infect it as you can't connect to its main ip

a323109 - November 2, 2014, 1:56 am

(Nov 1, 2014 11:38 AM)Sennheiser Wrote: [\[CITE\]](#) wat?

idk files could easily rewrite those permissions couldn't they?
And so what?

Everything is RAM, they change permissions, i reboot -> problem end

#Edit

I gave a look to .idk files <http://pcsupport.about.com/od/fileextensions/f/idk-file.htm> , as i suppose they are executable for windows <http://file-help.net/m/filehelper.php?C=FSUS2&file=IDK&mt=E>

I dont have any hidden file ".PDK" in my /root/filesystem

Basic - November 3, 2014, 3:49 am

Had some old computer who lived a random day as that! feel you

Aura - November 4, 2014, 5:37 am

The way you explain it, you could simply use a VM with a snapshot to do malware testing. Create your VM, install all the programs you need, configure all the settings, etc.then take a snapshot and everytime you close/open it, you restore that snapshot. This is what I do and its basically the same thing. Of course, this program can be useful in same corporate environment or even on an old computer you have for malware testing, since some of them will try bypass your VM environment, so using a physical computer is better.

Sennheiser - November 4, 2014, 7:43 am

(Nov 4, 2014 06:37 AM)Aur? Wrote: [\[CITE\]](#) The way you explain it, you could simply use a VM with a snapshot to do malware testing. Create your VM, install all the programs you need, configure all the settings, etc.then take a snapshot and everytime you close/open it, you restore that snapshot. This is what I do and its basically the same thing. Of course, this program can be useful in same corporate environment or even on an old computer you have for malware testing, since some of them will try bypass your VM environment, so using a physical computer is better.

True

But the benefits of deepfreeze

Is you can run viruses which have anti vm

I had many viruses not running on the vm because it detected it was a vm

Aura - November 4, 2014, 7:44 am

(Nov 4, 2014 08:43 AM)Sennheiser Wrote: [\[CITE\]](#) True

But the benefits of deepfreeze

Is you can run viruses which have anti vm

I had many viruses not running on the vm because it detected it was a vm

I stated that exact benefit in my last post ?

Quote:The way you explain it, you could simply use a VM with a snapshot to do malware testing. Create your VM, install all the programs you need, configure all the settings, etc.then take a snapshot and everytime you close/open it, you restore that snapshot. This is what I do and its basically the same thing. Of course, this program can be useful in same corporate environment or even on an old computer you have for malware testing, since some of them will try bypass your VM environment, so using a physical computer is better.