

Forum:[Hack Forums](#)

Thread: [\[Solved\]Sandboxie & IStealer Leaking\[/Solved\]](#)

Riseing - May 5, 2010, 7:05 pm

So sandboxie is like unbreakable when it comes to trojans/Worms and such. but an IStealer will run right through it and jack your passwords like nothing...anyway to stop this?

----Edit----

I solved it!!!

Just add

Code %Local AppData%\Mozilla\

%AppData%\Mozilla\

\Device\Mup\To Sandbox>Default Box>Sandbox settings> Resource Access>File Access>Blocked Access

WARNING this currently only protects FireFox Passwords!

Xch4ng3 - May 5, 2010, 7:07 pm

I haven't come across any method of preventing iStealer leaking from Sandboxie. Your next best option is to use something like a Master Password and not to save passwords unless really necessary, so even in a case of a leakage you won't lose that much.

-=C0d3ak=- - May 5, 2010, 7:08 pm

(May 5, 2010 07:05 PM)Riseing Wrote: [\[CITE\]](#) So sandboxie is like unbreakable when it comes to trojans/Worms and such. but an IStealer will run right through it and jack your passwords like nothing...anyway to stop this?

i doubt that for some reason..

sandboxie wouldnt let it see anything i thought

Riseing - May 5, 2010, 7:09 pm

God that sucks....thats sandboxies only downfall.

(May 5, 2010 07:08 PM)-=C0d3ak=- Wrote: [\[CITE\]](#) i doubt that for some reason..

sandboxie wouldnt let it see anything i thought

Try it for yourself. =/

Solved it!

-=C0d3ak=- - May 5, 2010, 7:59 pm

(May 5, 2010 07:09 PM)Riseing Wrote: [\[CITE\]](#) God that sucks....thats sandboxies only downfall.

Try it for yourself. =/

Solved it!
Oh good!
I'm always going to use a VM for my testing anyways.

Riseing - May 5, 2010, 8:03 pm

I use VM too but sometimes I'm too lazy to turn it on lol.

Xch4ng3 - May 6, 2010, 1:53 am

Code %Local AppData%\Mozilla\
%AppData%\Mozilla\
\Device\Mup\
Doesn't that just stop it accessing Mozilla's passwords?

david56543 - May 6, 2010, 2:04 am

you can prevent all files being opened you know so stealers cant open files...

i did this to internet too made 2 sandbox profiles 1 for internet 1 without so i run keygens in the sandbox that dont need internet and never get infected.. :D there can be restrictions for files, registry keys and internet etc

Riseing - May 6, 2010, 4:01 am

(May 6, 2010 01:53 AM)Xch4ng3 Wrote: [\[CITE\]](#) Code %Local AppData%\Mozilla\
%AppData%\Mozilla\
\Device\Mup\
Doesn't that just stop it accessing Mozilla's passwords?
Yup that works for me. I don't use IE so can't be bothered to write one lol

Xch4ng3 - May 6, 2010, 7:22 am

(May 6, 2010 04:01 AM)Riseing Wrote: [\[CITE\]](#) Yup that works for me. I don't use IE so can't be bothered to write one lol

Fair enough, but your forgetting Chrome, MSN passwords, NO-IP etc etc. It's a good start though, I'm sure if you expand that you can prevent it from accessing everything else.

Riseing - May 6, 2010, 11:31 am

Meh I'll get off my ass and fix it in a few.

thetoad - May 23, 2010, 9:49 am

noob idea... but why not run/test all things inside a cloned/spare harddrive??? just a thought as im use 2 anyway... 1 is just storage for films only. hope i might have helped you out a bit???

getsomempie - May 23, 2010, 9:54 am

(May 23, 2010 09:49 AM)thetoad Wrote: [\[CITE\]](#) noob idea... but why not run/test all things inside a cloned/spare harddrive??? just a thought as im use 2 anyway... 1 is just storage for films only. hope i might have helped you out a bit??? Not everyone has a spare hd laying around, unfortunately.

Riseing - May 23, 2010, 1:39 pm

(May 23, 2010 09:49 AM)thetoad Wrote: [\[CITE\]](#) noob idea... but why not run/test all things inside a cloned/spare harddrive??? just a thought as im use 2 anyway... 1 is just storage for films only. hope i might have helped you out a bit???
.....Your spelling is noob.

tux1 - May 23, 2010, 1:48 pm

But if you have blocked access to the internet won't that stop your passwords being compromised all together? When you say istealer runs through it do you mean it has like an local exploit for sandboxie?

Riseing - May 23, 2010, 3:12 pm

(May 23, 2010 01:48 PM)tux1 Wrote: [\[CITE\]](#) But if you have blocked access to the internet won't that stop your passwords being compromised all together? When you say istealer runs through it do you mean it has like an local exploit for sandboxie?

No Sandboxie only blocks access to needed files like registry and such. IStealer can get the passwords because sandboxie does not protect them unless you tell it too..

no17 - May 24, 2010, 12:20 am

i would rather use roboform

-mothered- - May 24, 2010, 4:56 am

Well this Is pretty good mate, but If only the code Itself, went beyond Firefox passwords and had a broader range of protection.

Nonetheless, It's still good to know and have.

Cheers :)

Riseing - May 24, 2010, 5:00 am

(May 24, 2010 04:56 AM)mothered Wrote: [\[CITE\]](#) Well this Is pretty good mate, but If only the code Itself, went beyond Firefox passwords and had a broader range of protection.

Nonetheless, It's still good to know and have.

Cheers :)

I will most likely add more. Such as the more popular web browsers.

-mothered- - May 24, 2010, 6:59 am

(May 24, 2010 05:00 AM)Riseing Wrote: [\[CITE\]](#) I will most likely add more. Such as the more popular web browsers.

No prob's there mate. I shall be periodically checking for the update.

Sounds great :)

Dumbo - May 24, 2010, 7:32 am

Thanks buddy , i was wondering how my passwords were logged after using sandboxie too , i was testing it on my self.