

All.Net Analyst Report and Newsletter

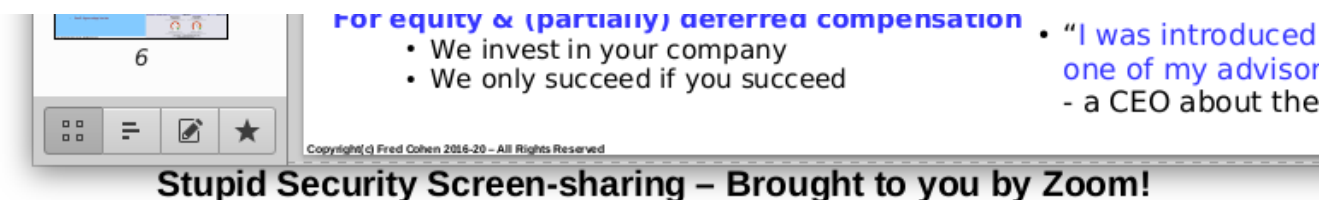
Welcome to our Analyst Report and Newsletter

Stupid Security Screen-sharing – Brought to you by Zoom!

Yes, zoom with their new security expert at the helm and new focus on security has done it again. It used to be that when you shared a window within your screen, the sharing only captured the window, but now, thanks to the new look and feel, the truth comes out...

An example

An actual screen share shows you what this looks like (taking this article in the background under the slide deck I have been using this morning).



Stupid Security Screen-sharing – Brought to you by Zoom!

Actual screen shot of what zoom leaks to other users

What's wrong with that?

Really?!? How do I hate this? Let me count the ways...

1. It shows information not in the window being shared, and as you move the window, you get a movie of the rest of the screen.

It can leak everything on the screen.

Zoom has access to the whole screen and is just showing what they want you to see.

How do we know they aren't sending the rest of it to themselves?

2. It shows that zoom is not given only access to the window you identified, but to the whole screen, it is just showing you the area around the window and the window itself.

It lies about what you are sharing.

It lies about what you have authorized it to do.

3. It shows that the operating system is not in control of what you reveal.

This means you do not have the ability to independently control what's happening.

This means you are trusting zoom unnecessarily with access to your whole screen.

I imagine there are plenty of other implications, but even if they now stopped revealing things to other people in meetings that don't have a right to access those things, how can I trust them going forward not to have merely changed the look and feel I see?

By the way, when you start and stop sharing, do you notice that the things behind the window might be revealed in a short flash? When you close a window and zoom stops the sharing?

What can I do about it?

There are a lot of different solutions available, but I will loan you only a few...

- **The X11 remote system approach:** In this approach, we do the zoom call on a system without any sensitive content we don't want to share, and running from there, use remote X11 windows on our user systems so that what zoom can access and share are limited to the things on the system zoom is running on. This is the approach of a TCB multi-level display supporting multiple systems at different security levels. In use, the zoom interface and all of the relevant windows must be made to appear on the user's interface system; easy enough; and then the overlap portion of the screen is not going to cover the user's system because Zoom doesn't have access to it (we hope).
- **The VM approach:** In this version, we use a VM to run zoom. The problem is then that we cannot share anything outside of the VM unless we somehow push from our other system into the VM as a window. So in essence, best case, this is the reverse of the X11 solution in that we share windows into the VM for screen sharing, but this is problematic as well technologically today.
- **The OS does it right approach:** This would be the case where the OS has to approve any window Zoom seeks to share or see, and the user is prompted by the OS instead of (or perhaps in addition to) Zoom. However, this would likely break zoom – or at least the OS would have to make it appear to zoom as if each window was in fact its own screen. Of course then we would have lots of screens of different sizes for zoom to deal with.
- **Zoom does it right (and someone makes sure of it):** Not going to happen, because they broke it in their upgrades and didn't even notice it. If you cannot even notice such an obvious thing, surely you cannot be relied upon to fix it. Or perhaps they noticed it and did it anyway, in which case it's ignorance, malice, or overriding security with look and fee – in any case, not going to get fixed this way.

I just want to note that none of these will actually work because they are inconvenient and I don't have the time to do them myself right now. Unless a commercial provider might want to do it for us... of course then we have to trust them on our systems as well! The hole just keeps getting deeper...

So how do I live with it?

Leave lots of space for your zoom windows... and don't overlap them... OK – That will not function on my system. So here's one last alternative that might work. Use a different desktop for the Zoom meeting. My main box has 2 monitors, but that's not what I meant. What I mean is use a different desktop and switch between the zoom desktop and other desktop(s) to move the things you are sharing onto the Zoom desktop and keep the things you don't want shared on other desktops. No guarantees of course, but it is reasonably functional, but quite inconvenient. **(Do I get a bug bounty?)**

Conclusions

It's hard to fuse the desire for look and feel / leakage with cyber-security needs. First, someone has to notice it and care. Then they need the power to enforce changes. And then we need to do this BEFORE release into the wild. Add it to your regression testing checklist?