

---

Subject: Re: How did this happen?

Posted by [EvilWhiteDragon](#) on Mon, 29 Nov 2010 18:06:19 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Since we're pretty much fucked anyway:

Quote:

<jonwil> hi

<EvilWhiteDragon> hi

<EvilWhiteDragon> You, sir, are an idiot

<EvilWhiteDragon> So what did you want to talk about?

<jonwil> I just want to say that I did not give troopr02 the < censor > file. How he got it I am not sure but I did not give it to him.

<jonwil> < censor >.zip and < censor >.exe came from the Reborn forums as he is a reborn tester

<jonwil> and the admin of the reborn test FDS

<EvilWhiteDragon> Still you shared information that you were not supposed to share in chat with him.

<EvilWhiteDragon> jonathanwilson623@hotmail.com says:

<EvilWhiteDragon> Dont tell ANYONE I am saying this but

<EvilWhiteDragon> Hex sent me a PM with the following

<EvilWhiteDragon> Someone emailed me a rar file months ago (no idea who) with almost 2000 source files in it that contains TT, scripts and Renegade (from westwood) code

<EvilWhiteDragon> cross platform tt.dll specific engine calls

<EvilWhiteDragon> Copyright 2009 Jonathan Wilson

<EvilWhiteDragon> This file is part of the Renegade tt.dll.

<EvilWhiteDragon> CONFIDENTIAL: DO NOT USE OR DISTRIBUTE WITHOUT PERMISSION

<EvilWhiteDragon> \*/

<EvilWhiteDragon> The only way someone would have that comment is if they had actual source code to 4.0

<EvilWhiteDragon> That gave troop at least a hint on where to look for it heh?

<jonwil> I think what happened is that I made this post

<jonwil> <http://www.renegadeforums.com/index.php?< censor >>

<jonwil> and somehow he discovered <http://< censor >/< censor >> in the brief window it was on that site even though no public link to it existed with the only link being the one in that post

<EvilWhiteDragon> YOU FUCKING IDIOT! DONT YOU SEE WHAT GAPING HOLE YOU HAVE ON YOUR WEBSITE? DIRLISTING IN A DIRECTORY YOU USE FOR PRIVATE FILES WITH NO PASSWORD OF ANY KIND! YOU IDIOT

<EvilWhiteDragon> <http://< censor >/< censor >> <-- nice files stored there

<jonwil> at the time I had no idea it was possible to dirlist that directory. Once I found out that it was possible, I stopped using it for sensitive files.

<jonwil> Nothing currently uploaded is sensitive

<EvilWhiteDragon> TT is in that dir

<jonwil> no its not

<EvilWhiteDragon> I just downloaded TT

<jonwil> binaries are there

<EvilWhiteDragon> yes

<EvilWhiteDragon> so, those are private as well

<EvilWhiteDragon> Or did I miss the release of TT?

<EvilWhiteDragon> In that case I might be misinformed...

<EvilWhiteDragon> Have you verified that the code troop leaked is the same as Hex' version?  
<jonwil> yes it is identical  
<jonwil> same zip file  
<jonwil> rar file  
<jonwil> A whole pile of APB and reborn testers have those test binaries and have been testing 4.0 for months. There was a leak of an APB test build (by a tester who was promptly banned I believe) a while back and no-one said anything at the time about that leak compromising 4.0  
<EvilWhiteDragon> I mean the sourcecode  
<EvilWhiteDragon> is it identical or not?  
<jonwil> yes the source code is identical to the leak  
<jonwil> the < censor > file is identical to the hex/jnz leak  
<EvilWhiteDragon> Ok, So it's what? 4 months old?  
<jonwil> older than that  
<EvilWhiteDragon> Still, I think we should set a lot of new security rules.  
<jonwil> yes true  
<EvilWhiteDragon> like not putting up files on private hosting  
<EvilWhiteDragon> with open dirs  
<jonwil> yes definatly  
<jonwil> but like I said, I had no clue that it was open dir  
<jonwil> we should not post TT private stuff anywhere but 100% verified private locations  
<EvilWhiteDragon> You could've attached the file to your forum post for ex.  
<EvilWhiteDragon> or on a private ftp  
<jonwil> As mentioned though at the time I posted < censor >, I had no idea that there was any way to get to it other than through the link in the post  
<jonwil> had I known the dir was open, I would have not posted it to that space  
<jonwil> /me smacks self in forehead for not knowing much about how to run a website  
<jonwil> and not knowing how to tell if folders are open to the world or not  
<EvilWhiteDragon> I would start with putting a .htaccess on the files dir  
<EvilWhiteDragon> as there are plenty of files with which you violate the NDA you signed.  
<jonwil> right now I will remove the sensitive stuff until it can be uploaded somewhere thats less public  
<jonwil> I dont know what web server is running on that box or the right way to set up limited access  
<EvilWhiteDragon> phpinfo.php :: <?php phpinfo(); ?> and you'll probably see apache named there  
<jonwil> everything even remotely sensitive has been removed  
<jonwil> everything that remains in that location has been made public before by me  
<jonwil> i.e. C&C3/RA3 stuff  
<jonwil> and some renegade stuff like the w3d importer work I did and published a while back  
<EvilWhiteDragon> well as said, I dont mind the files published there too much, just the fact that its open dir is really bad  
<jonwil> the only files on that server before I removed them that were even remotly sensitive were the test builds that had fairly wide distribution with APB, AR and reborn guys having them. But they are gone now .  
<EvilWhiteDragon> It's the principle JW. If w don't care about security, other people will certainly not care for it.  
<jonwil> well yeah true  
<jonwil> hence why I removed all the sensitive stuff

<jonwil> and will not post stuff to public unprotected locations in the future  
<jonwil> the real question is what the response to the leak is. What, if any, PR do we put out. What do we tell EA. What, if any, legal avenues do we pursue. etc. I for one intend to post absolutly nothing in public.  
<jonwil> the other question (and one I am totally unqalified to answer) is which bits of code we will need to rewrite to be different to whats in that code dump so that if/when 0x90 and other cheaters get hold of it, they cant abuse it for bad things  
<jonwil> but right now I will say nothing anywhere in public  
<jonwil> I do however have the current EA community guy in my email should anything need to be sent to him (or if it needs to come from someone else, I can point him in their direction)  
<EvilWhiteDragon> I know, I introduced you remember ?  
<EvilWhiteDragon> I'm trying to get 0x90 not to abuse the code. Not sur if it'll work but it's worth a try  
<EvilWhiteDragon> also, he doesnt have the code currently so thats good I guess  
<jonwil> ok  
<jonwil> I was going to ask you if you had gotten anywhere with your investigation into setting up "BlackIntel LLC" or whatever it is called over there. But all this kind of puts a hold on that  
<jonwil> since we obviously couldnt go public even if we DID have fixes for the bugs on our list  
<EvilWhiteDragon> I have gotten somewhere  
<jonwil> ok  
<EvilWhiteDragon> just some form issues I need to ahve answered before I can set it up actually  
<EvilWhiteDragon> but once thats done i think the rest would be the matter of like 2-3 weeks  
<jonwil> oh and btw I cant remember ever signing any bits of paper related to TT  
<jonwil> being that at the time secret stuff was first added to scripts, I was the only developer  
<jonwil> and no-one else had it  
<jonwil> this is most definatly not the end of the world (or even the end of 4.0) though.  
<EvilWhiteDragon> it does show that something has to change  
<jonwil> yes  
<EvilWhiteDragon> we really should apply proper project management tecniques  
<jonwil> do we want to take legal action against troopr02?  
<EvilWhiteDragon> if anyone finds the money and time, why not?  
<jonwil> we need someone who knows Candian copyright law  
<jonwil> I think at this point though there is no way to put the genie back into the bottle.  
<EvilWhiteDragon> DCMA  
<EvilWhiteDragon> particularly US companies are sensetive to that  
<jonwil> canada doesnt have a DMCA  
<jonwil> but we can certainly issue one against any sites that host it  
<EvilWhiteDragon> USA companies or companies operating in the uSA  
<EvilWhiteDragon> indeed  
<jonwil> but it wont stop it going up in places outside the USA  
<jonwil> or being distributed among cheaters in private/semi private locations  
<EvilWhiteDragon> I'm not that afraid of UC, I think they are rather tight on copyright and such  
<EvilWhiteDragon> I could be wrong of course, but still  
<jonwil> btw, a google search for the files (<sensor>) shows no results  
<jonwil> no relavent results that is  
<jonwil> some links to things about cars called TT  
<jonwil> but thats about it  
<jonwil> Looking through my MSN logs, there is some evidence that troopr02 knew of the

existence of <sensor> before the stuff at the top of "jonwil scripts leak.txt". Not saying that means anything though.

<jonwil> so yeah I shall let the right people handle this, I shall continue working through the list of bugs we have and leave it at that.

---