Subject: jonwil exposed
Posted by Sir Kane on Fri, 20 May 2005 19:35:34 GMT
View Forum Message <> Reply to Message

You all probably always wondered why I (and other people) hate jonwil so much.

You would think he's a nice guy and such, but he isn't really.

So here's the story:

As you know, I used to be part of Blackhand Studios. So as every day, I was working on "bhs.dll" (the real one for that matter) until I got a private message from xptek on IRC which contained following text from a log:

Just a small comment: he got my code in order to make the linux version of bhs.dll and nothing else.

You'll find some of my source code in there, but that doesn't really matter since it got leaked by some turd called "jonwil".

xptek
«20:10:27» {jonwil} dont tell SK but...
«20:10:28» {jonwil} #ifdef WIN32
«20:10:28» {jonwil} typedef unsigned long (_cdecl *Find_Player) (int);
«20:10:28» {jonwil} Find_Player FindPlayer = (Find_Player)0x004157E0;
«20:10:28» {jonwil} #else
«20:10:28» {jonwil} typedef unsigned long (*Find_Player) (int);
«20:10:28» {jonwil} #ifndef RH8
«20:10:28» {jonwil} Find_Player FindPlayer = (Find_Player)0x080A9CDC;
«20:10:28» {jonwil} #else
«20:10:29» {jonwil} Find_Player FindPlayer = (Find_Player)0x080A510A;
«20:10:29» {jonwil} #endif
«20:10:29» {jonwil} #endif
«20:10:38» {xptek}
«20:10:45» {jonwil} unsigned long GetName(unsigned long ptr_){
«20:10:46» {jonwil} unsigned long* name = (unsigned long *)(ptr_+0x758);
«20:10:46» {jonwil} return *name;
«20:10:46» {jonwil} }
«20:10:59» {jonwil} the first one gets the data structure for a player given the ID
«20:11:11» {xptek} Okay
«20:11:11» {jonwil} if it returns NULL, its not a valid player ID
«20:11:22» {jonwil} the second one gets the name of the player given the ID
«20:11:40» {xptek} Nice
«20:11:52» {xptek} Thanks a lot.. hopefully I can do something with this.
«20:12:14» {jonwil} any other bits you want?
«20:12:27» {xptek} Would you know how to kill?
«20:12:46» {xptek} That's what I'm really looking for. I had a whole regulator based around the kill command.

«20:12:48» {xptek}
«20:13:04» {jonwil} basicly, with kill, you call FindPlayer to find the player
«20:13:21» {jonwil} then if its valid, you call GetGameObject
«20:13:29» {jonwil} then you pass that to Commands->Destroy_Object
«20:13:47» {jonwil} GameObject *GetGameObject(void *_ptr){
«20:13:47» {jonwil} if (_ptr){
«20:13:47» {jonwil} #ifdef WIN32
«20:13:48» {jonwil} _asm{
«20:13:48» {jonwil} mov edi, _ptr
«20:13:48» {jonwil} mov eax, [edi + 0x14]
«20:13:48» {jonwil} mov eax, [eax + 4]
«20:13:48» {jonwil} }
«20:13:48» {jonwil} #else
«20:13:48» {jonwil} unsigned char *playerdata = (unsigned char *)_ptr + 0x10;
«20:13:48» {jonwil} unsigned char *y = (unsigned char*)*((unsigned char **)playerdata);
«20:13:49» {jonwil} y += 4;
«20:13:49» {jonwil} GameObject *z = (GameObject *)*(GameObject **)y;
«20:13:51» {jonwil} return z;
«20:13:51» {jonwil} #endif
«20:13:52» {jonwil} } else {
«20:13:53» {jonwil} return NULL;
«20:13:54» {jonwil} }
«20:13:55» {jonwil} }
«20:13:56» {jonwil} now dont tell SK about this
«20:14:02» {xptek} I won't.
«20:14:02» {jonwil} in fact, dont ever mention this publicly
«20:14:04» {xptek}
«20:14:07» {xptek} I won't at all.
«20:14:32» {jonwil} and dont show that code to anyone
«20:14:38» {xptek} I won't.
«20:14:39» {xptek}
«20:14:39» {jonwil} anything else you are after?
«20:14:56» {xptek} lol, um.. spawn command
«20:15:04» {xptek} Thank you a lot for this.
«20:15:12» {jonwil} spawn simply takes the position
«20:15:16» {jonwil} and the preset
«20:15:22» {jonwil} and calls Commands->Create_Object
«20:15:37» {jonwil} that all you need
«20:15:38» {jonwil} ?
«20:15:47» {xptek} Yeah, pretty much
«20:15:53» {xptek} Thank you a TON.
«20:15:57» {jonwil} of course, what I havent told you and cant tell you is how to add new console commands
«20:16:17» {xptek} Oh, I would need that.
«20:16:19» {xptek}
«20:16:33» {jonwil} sorry, I cant tell you that
«20:16:46» {xptek} Okay.. is that hard to do?
«20:16:57» {jonwil} yes

«20:17:10» {jonwil} if you knew ASM, I would tell you to go look at ConsoleFunctionManager::Init
«20:17:16» {jonwil} console commands are hard
«20:17:24» {xptek} I'll try to work on that myself. I'm going to pick up some books on C++ and work my arse off.
«20:18:00» {xptek} I could attempt to ask vlokt how he does in with Renrem in DA. But I don't think he'd help me.
«20:18:01» {jonwil} I dont even know how SK is doing console commands on win32
«20:18:14» {xptek} Hmm.. :\
«20:18:20» {jonwil} I know
«20:18:25» {jonwil} wait, no
«20:18:31» {jonwil} wait, now I got it
«20:18:44» {jonwil} in the scripts.dll you could at some point start a timed event
«20:18:50» {jonwil} a timer or something
«20:18:59» {xptek} Okay
«20:19:04» {jonwil} then the timer could look for a log file
«20:19:10» {jonwil} which would be written to by your regulator
«20:19:13» {jonwil} with the details you need
«20:19:16» {jonwil} anyhow, its doable
«20:19:18» {jonwil} but would be hard
«20:19:28» {xptek} Alright... I'll look into that too..
«20:19:39» {xptek} I've had about 3 weeks using C++
«20:19:41» {jonwil} although for the timer, check out Commands->Create_Timer
«20:19:42» {jonwil} ok
«20:19:51» {xptek} But it actually looks much easier than mIRC scripting.
«20:20:02» » jonwil has never done MIRC scripting

You may now ask yourself "what did he say after he got confronted"? Read it here:
Quote:
(00:49:21) <jonwil> probobly because I was out of it at the time I did it
...
(00:54:31) <jonwil> I wasnt thinking straight
...
(01:02:37) <jonwil> as I said, I wasnt thinking straight and at the time I didnt even think about the rules or that this would piss someone off

Now that's funny, isn't it? "oh noes, I was out of it", "never though leaking code would piss someone off!!11"

Some other funny stuff:
Quote:
(14:54:44) <jonwil_> I am going so far as to say that if this is released without source code, I will reverse engineer whatever you release back into full code myself
(14:54:47) <jonwil_> and relesae it
(14:54:54) <jonwil_> probobly straight after its released

Any questions?

Quote:
(05:31:01) <jonwil> so SK is talking out of his ass again?

WOOT! I can talk out of my ass!

Now you might want to know why I am posting this now instead of back when it happened.

Well, one day, not long ago, I was bored and wanted to see which console commands "bhs.dll" added.
So I loaded "bhs.dll" into my disassembler. Browsing around a bit, I ended up looking at some vital functions that
are used to make the dll work at all. Funny thing being that he added the exactly same RETARDED code
(nice trap I added back then) as I had in my dll to "his" dll. The code in question is the usage of memset() on a buffer
that gets COMPLETELY (as in all bytes) changed RIGHT after the memset call.

So I told him to remove my code with a time limit of 5 (or 6) days from "his" dll. I also told him that, if he doesn't
remove it, I'm going to post a topic like this.

Now the best part:
His signature
Quote:Jonathan Wilson aka Jonwil
Quote:Creator and Lead Coder of the Custom scripts.dll
Quote:Renegade Engine Guru I heard from unknown sources it's "Renegade engine clown"
Quote:Creator and Coder of BHS.DLL Don't you mean "Copier and Paster of BHS.DLL"?
Quote:Official member of Blackhand Studios™

This should clear things up and I hope you change your view about him since he isn't what you might think he is.

Everything from logs is unedited.
