

Forum:[Hack Forums](#)

Thread: [Someone Controlled My Xat Bot On A Turkish Chat](#)

Jonathan1990 - August 2, 2014, 3:11 pm

I found a video on youtube about this bot with the download link on mediafire. I tested it out on a few chats by leaning it's commands. A lot of the English chats tend to find the bot annoying and ban it or else kick it off. On the Turkish Lobby Chat though it was a different story. They found it quite entertaining. The bot then began to say things that I was not making it say. They were quite funny as I was translating it. Does anyone here know how they were controlling the bot when they never downloaded the program? I think it may have been a keylogger program if I'm correct.

AceVoid - August 3, 2014, 6:27 am

Probably back doored OP. I'd scan my PC if I were you. Never download hacks from YouTube! The are just back doored and RATted.

Jonathan1990 - August 3, 2014, 9:01 am

(Aug 3, 2014 06:27 AM)ddvniek Wrote: [\[CITE\]](#) Probably back doored OP. I'd scan my PC if I were you. Never download hacks from YouTube! The are just back doored and RATted.

Oh does this tell me your going to rat me. That is old now. I'm wise to those things. A bot is not a hacking tool but keylogger what you may use is.

Seer - August 3, 2014, 9:06 am

(Aug 3, 2014 09:01 AM)Jonathan1990 Wrote: [\[CITE\]](#) Oh does this tell me your going to rat me. That is old now. I'm wise to those things. A bot is not a hacking tool but keylogger what you may use is. He's calling you a retard for searching "XAT Bot" on YouTube and downloading it as it is more than likely a RAT binded with some shit "bot".

Jonathan1990 - August 3, 2014, 9:15 am

(Aug 3, 2014 09:06 AM)Seer Wrote: [\[CITE\]](#) He's calling you a retard for searching "XAT Bot" on YouTube and downloading it as it is more than likely a RAT binded with some shit "bot".

There are about 30 people on xat that have downloaded the bot which was released about 3 weeks ago as I've seen other users testing it out.

Seer - August 3, 2014, 9:18 am

(Aug 3, 2014 09:15 AM)Jonathan1990 Wrote: [\[CITE\]](#) There are about 30 people on xat that have downloaded the bot which was released about 3 weeks ago as I've seen other users testing it out. Does that have any relevance to it being backdoored? Working programs are backdoored with viruses all the time, and you would probably never find out if the owner of the virus kept his server FUD.

Jonathan1990 - August 3, 2014, 9:31 am

[quote=You're RAT'd, no doubt about it.
[/quote]

Someone would be controlling my whole computer now with remote desktop if I was and making my screen flash on and off with dark comment and using whiteshark as well. ?

skelly76 - August 3, 2014, 9:44 am

(Aug 3, 2014 09:31 AM)Jonathan1990 Wrote: [\[CITE\]](#) Someone would be controlling my whole

computer now with remote desktop if I was and making my screen flash on and off with dark comment and using whiteshark as well. ?

You would probably do that, but any normal person with a life and a RAT would do these things only a couple times. People keep slaves such as yourself and use them when necessary, not flashing their screen 24/7. I think you really need some common sense, nobody would go on HF for help and then start telling members who are trying to help you that they are wrong and you know exactly what's happening. Face it, you've been tricked into downloading into a program that is binded with a RAT. Take the above advice and clean your computer, if that doesn't fix anything go to the RAT section on HF and seek help there. Last resort go to the whitehats if this RAT is made by someone who knows what hes doing. Next time be thankful for the information members give you, 80% of us wouldn't post unless we know at least a little bit about your problem ;)

As for those other users, they have been infected too (if they are legit).

grady - August 3, 2014, 9:49 am

(Aug 3, 2014 09:31 AM)Jonathan1990 Wrote: [\[CITE\]](#) Someone would be controlling my whole computer now with remote desktop if I was and making my screen flash on and off with dark comment and using whiteshark as well. ?

If you're going to be cocky, and act as if you know more than me, then don't bother asking for help, there's no one that'd be willing to help you if you keep up that attitude.

Jonathan1990 - August 3, 2014, 9:57 am

(Aug 3, 2014 09:44 AM)Variful Wrote: [\[CITE\]](#) You would probably do that, but any normal person with a life and a RAT would do these things only a couple times. People keep slaves such as yourself and use them when necessary, not flashing their screen 24/7. I think you really need some common sense, nobody would go on HF for help and then start telling members who are trying to help you that they are wrong and you know exactly what's happening. Face it, you've been tricked into downloading into a program that is binded with a RAT. Take the above advice and clean your computer, if that doesn't fix anything go to the RAT section on HF and seek help there. Last resort go to the whitehats if this RAT is made by someone who knows what hes doing. Next time be thankful for the information members give you, 80% of us wouldn't post unless we know at least a little bit about your problem ;)

As for those other users, they have been infected too (if they are legit).

Well 95% of stuff on a computer is a virus and the only option is to keep cleaning your pc all the time 24/7.

iXahusee - August 3, 2014, 12:56 pm

(Aug 3, 2014 09:57 AM)Jonathan1990 Wrote: [\[CITE\]](#) Well 95% of stuff on a computer is a virus and the only option is to keep cleaning your pc all the time 24/7.

Do you .. Um .. Have any idea what you are talking about?

18772 - August 3, 2014, 2:04 pm

Go to C:\users\"userhere"\appdata\local\temp\ and check for a file titled MSDCSC. Check if there is a file in it. I don't know a lot about rats yet, but I am pretty sure that is one of the places that the virus is stored. If you have a file in that folder it would probably be a good idea to restart in safe mode w/o networking and delete it.

You will have to go to folder options and show hidden files too if you don't have them un-hidden already by the way.

I would like someone a little more computer savvy to verify this though.

WarOnDrugs - August 3, 2014, 2:35 pm

(Aug 3, 2014 09:31 AM)Jonathan1990 Wrote: [\[CITE\]](#) Someone would be controlling my whole computer now with remote desktop if I was and making my screen flash on and off with dark comment and using whiteshark as well. ?

People who don't know what they're doing this, people who want to remain incognito, do not. I'm not saying you're infected, but considering you got the DL from someone on Youtube, it's a possibility. It's not hard to infected programs with Malicious software.

Stop being ignorant and disregarding what we say, we're just trying to help.

Cryptocat - August 3, 2014, 2:58 pm

This is the incorrect sub if you are looking for help to clean your system now.

Go to the WHH section.

18772 - August 3, 2014, 3:05 pm

(Aug 3, 2014 02:58 PM)Cryptocat Wrote: [\[CITE\]](#) This is the incorrect sub if you are looking for help to clean your system now.

Go to the WHH section.

Oh, well, that is were I found the one I got on my system. I manually removed it and verified it's removal with my own rat program :) I'm sure there are plenty more spots but I don't know enough yet to find where they would be unless I get infected with one...

c x y k - August 3, 2014, 3:09 pm

(Aug 3, 2014 09:57 AM)Jonathan1990 Wrote: [\[CITE\]](#) Well 95% of stuff on a computer is a virus and the only option is to keep cleaning your pc all the time 24/7. I haven't gotten a virus in over a year, I also have no anti virus.

Don't be stupid and you won't get viruses. Don't go looking for programs on youtube or poof, you're now a slave to somebody.

18772 - August 3, 2014, 3:11 pm

@Kondax

I have started disabling my av lately. It seems to get in the way more than it helps me. I just use it to scan my pc from time to time now :3

Cryptocat - August 3, 2014, 3:14 pm

(Aug 3, 2014 03:11 PM)18772 Wrote: [\[CITE\]](#) @Kondax

I have started disabling my av lately. It seems to get in the way more than it helps me. I just use it to scan my pc from time to time now :3

You really don't even need an AV. Just have MBAM on your PC and run a full scan once a month.

Don't click shit links, don't download shit stuff, and your pc wont be shit.

18772 - August 3, 2014, 3:21 pm

@Cryptocat

Is it possible to get a sandbox area or something to download your downloads in and check them? I understand not to use shit links, but what if a program has a really complex virus in it and it came from a pretty trustworthy site?

Cryptocat - August 3, 2014, 3:24 pm

(Aug 3, 2014 03:21 PM)18772 Wrote: [\[CITE\]](#) @Cryptocat

Is it possible to get a sandbox area or something to download your downloads in and check them?

I understand not to use shit links, but what if a program has a really complex virus in it and it came from a pretty trustworthy site?

Just setup a VMWARE as a textbox or use sandboxie if you want.

c x y k - August 3, 2014, 3:25 pm

(Aug 3, 2014 03:21 PM)18772 Wrote: [\[CITE\]](#) @Cryptocat

Is it possible to get a sandbox area or something to download your downloads in and check them? I understand not to use shit links, but what if a program has a really complex virus in it and it came from a pretty trustworthy site?

It's best to run downloads you believe to be malicious within a sandbox within a virtual machine.

Hell, if you've got the power, a sandbox within a virtual machine within a virtual machine.

Cryptocat - August 3, 2014, 3:28 pm

(Aug 3, 2014 03:25 PM)Kondax Wrote: [\[CITE\]](#) It's best to run downloads you believe to be malicious within a sandbox within a virtual machine.

Hell, if you've got the power, a sandbox within a virtual machine within a virtual machine.

A dual VM setup isn't needed and is rather pointless. Assuming the infection could escape the box it would just repeat until it is on the host machine.

18772 - August 3, 2014, 3:29 pm

@Kondax

Lol, I have almost no power at all!

c x y k - August 3, 2014, 3:40 pm

(Aug 3, 2014 03:28 PM)Cryptocat Wrote: [\[CITE\]](#) A dual VM setup isn't needed and is rather pointless. Assuming the infection could escape the box it would just repeat until it is on the host machine.

I completely derped and forgot about that.

I guess you could just completely lock the vm as much as possible.

Lemon-lime - August 3, 2014, 6:52 pm

Lesson to learn is just because the tool/program you download from youtube is working does not mean it is not backdoored. My guess is that 95% of youtube hacks/program downloads advertised on there are backdoored. I would scan your pc with a reputable anti-virus and check your registry manually for anything starting up in the background of your computer without your knowledge. You can type msconfig in your search and run msconfig.exe and check the run tab for anything suspicious running that shouldnt be on startup. Also check temp directory and appdata for any suspicious looking files. Also hold ctrl + alt + delete at the same time and hit start task manager and go to the processes tab and services tab and look for anything that is running on there that shouldnt be. Good Luck