

Forum: [Hack Forums](#)

Thread: [How to stop loosing bots](#)

nitrogen_oxide - July 31, 2021, 11:23 am

Hi, I'm having a problem that I get a bunch of bots in my rat control panel, but after like a few seconds (sometimes a few hours) they dissapear (Windows defender maybe closes the connection or something idk for sure), I was thinking of writing a script that would automatically create a bind shell on the hacked pc and then send the ip address of the pc through a post request to a web server, but that would take quite a while to do and is kinda hard too so I was thinking maybe there is some software that can do this for me (not necessarily a bind shell but something that is much more stable and that I can execute commands from, for example download and execute the rat exe file again lol) if there is some software like this I would really appreciate if someone could tell me about it.

Thanks!

Quicksilver16387 - July 31, 2021, 2:10 pm

Those are honeypot VMs for malware analysis and you should ignore these. Take note of the IP addresses those connections usually come from and create an inbound rule in your firewall that blocks all programs from receiving connections from the addresses you collected.

That's it. No more annoyances.

nitrogen_oxide - July 31, 2021, 2:49 pm

I dont think they are honeypots, i was able to extract bitcoin wallets from some bots (had to act super quick tho lol)

even it ifs a honeypot, i love it cuz im able to do anything i want to the system

btw im using bitrat, im not sure if there is a way to somehow make it not dissapear just by modifying the settings in some way, i was going to try to put the rat exe into the "launch at startup" thing but for some reason the license servers are down!

and also the ip address is always different, it comes from the actual victim, not an av company

nitrogen_oxide - July 31, 2021, 3:32 pm

yea it has uac bypass, i literally just crypted this stub few days ago

if i get an elevated shell i wont be able to use hvnc

which is kinda important :\

XIDoctor - August 1, 2021, 2:29 am

Use rat to backup, mine from different place, so two rdps or maybe 3, all private and offshore anti spamhaus.

1 rdp the backup rat, 1 rdp the mining and 3rd rdp maybe for a second backup location or place to store info up toy you

nitrogen_oxide - August 1, 2021, 12:42 pm

what to do if it dissapears from the backup rat?

hazbot77 - August 1, 2021, 9:23 pm

(Jul 31, 2021 03:13 PM)Incog Wrote: [CITE](#) more than likely detected, if you can, download and execute a fresh crypted stub to prevent bot losses.

or kill WD, think Bitrat has a silent uac bypass so you can use that to launch some sort of elevated shell and disable it yourself, idrk I never bought anything from them

BitRAT has an inbuilt wd killer (you have to use the UAC bypass first tho), so OP can just use that.

nitrogen_oxide - August 2, 2021, 8:14 am

i tried disabling the wd, uac exploit, and protect process, but after few hours the bot still ran away

i think the only way to do this would be to make some script that will create a bind shell and allow me to connect whenever i want and give me a shell.

just i cant really find a good way to do it, i tried making a batch file that will create a folder that is excluded from scanning of wd but that just gets detected as a virus lol

ok i am 90% sure the bot gets lost because of the av, does anyone know how to make a script that will make a certain folder not scanned by av? like add an exclusion

i tried using powershell script but that just gets detected as a virus