

Forum:[Hack Forums](#)

Thread: [Working on developing a RAT](#)

slituser - April 14, 2025, 5:28 pm

i have been spending a large chunk of time developing a rat in python. ive found some exploits in windows systems that can make spreading very easy, and privilege escalation exploits that make the rat itself completely undeleteable, even after system and harddrive wipe and boot from usb. this thing is pretty hard to get rid of. i would like some feedback as to what me and my team should implement into the rat, we already have all the basics, crypto and credential stealer tech, reverse shell, keylog and facecam, self destruct, full fingerprint of victim, and of course the option to inject more malware. I would love to hear some feedback and possibly advice from other malware devs on this, this rat is coded fully in py, btw. and i have a crypter to match, that uses xor and aes 256 encryption and alot more goodies, also it passes clean on virus total (here is the hash, it shows up as a py file because the stub to decrypt the rat is in py, which i will eventually fix to show a exe file: 29a4789c1214a2048348df7166beb68373c547bb840e6d80b2f992872be3a2d7)

anyway, some feed back would be greatly appreciated, any and all, good or bad, eventually i will show the ui and all that but the ui under maintenance. thanks guys

ZrNoxb - April 14, 2025, 10:21 pm

(Apr 14, 2025 05:28 PM)slituser Wrote: [\[CITE\]](#) i have been spending a large chunk of time developing a rat in python. ive found some exploits in windows systems that can make spreading very easy, and privilege escalation exploits that make the rat itself completely undeleteable, even after system and harddrive wipe and boot from usb. this thing is pretty hard to get rid of. i would like some feedback as to what me and my team should implement into the rat, we already have all the basics, crypto and credential stealer tech, reverse shell, keylog and facecam, self destruct, full fingerprint of victim, and of course the option to inject more malware. I would love to hear some feedback and possibly advice from other malware devs on this, this rat is coded fully in py, btw. and i have a crypter to match, that uses xor and aes 256 encryption and alot more goodies, also it passes clean on virus total (here is the hash, it shows up as a py file because the stub to decrypt the rat is in py, which i will eventually fix to show a exe file: 29a4789c1214a2048348df7166beb68373c547bb840e6d80b2f992872be3a2d7)

anyway, some feed back would be greatly appreciated, any and all, good or bad, eventually i will show the ui and all that but the ui under maintenance. thanks guys

¡Good luck! with your rat. I'd tell you what to implement, but I'm not very familiar with rats.

DramaKing - April 15, 2025, 2:57 am

So you're making an easy-to-spread Windows RAT in a language that only some Python devs and some hackers like myself can run. So you're going to fix the stub to be an exe file. That means a Python compiler that changes the code from being invisible to antivirus to being automatically detected.

And what privilege escalation exploits can make malware 'undeleteable.' There's no privileges that can stop a reformat.

slituser - April 15, 2025, 6:00 pm

(Apr 15, 2025 02:57 AM)DramaKing Wrote: [\[CITE\]](#) So you're making an easy-to-spread Windows RAT in a language that only some Python devs and some hackers like myself can run. So you're

going to fix the stub to be an exe file. That means a Python compiler that changes the code from being invisible to antivirus to being automatically detected.

And what privilege escalation exploits can make malware 'undeleteable.' There's no privileges that can stop a reformat.

its not the priveledge escalation that makes it undetectable, my fault for the error in my wording there, this priveledge escalation features make it to where the rat embeds itself as a full system process, while also making it undeletable in a full system wipe and boot from usb. it masks itself as a real system process, so it is hard to tell the difference, it also gives itself fake metadata when on vics machine to clone real processes. it is quite nice. also the rat can run on any pc with windows not just ones with python, as i have already tested on real windows pcs without being them being in a vm. it executes on their machine pretty nicely. still debugging tho, and did ui revamp today . I hope this answers your questions!