

Forum:[Hack Forums](#)

Thread: [what would be the best public rat to modify?](#)

guriguri - February 16, 2022, 8:58 am

i have this found a vulnerability in a common program i'd want to take advantage of as a proof of concept

i'm able to send a the metasploit rat and things like that, but obviously that wouldn't work in any situation unless windows defender is completely down.

i'd like to demonstrate that even today exploits in binaries which allow for remote code execution can be super dangerous.

doing something like sending a file or executing some hand written asm is cool but it's obvious that RCE can own a machine.

i wouldn't want to do it from scratch though.

for example the MSF multistage framework is really nice at helping you make your shellcode as small as be able to send the real file only once a connection has been made.

so i'd like to know which publicly available rat would be relatively simple in its structure that i could work on and change it

and make it obfuscated enough so that it won't flag.

keep in mind that i don't need the initial file a standalone executable initially, i'm already in execution so i can in fact execute things before deploying the actual malware.

MeW11 - February 17, 2022, 7:40 pm

(Feb 16, 2022 09:58 AM)guriguri Wrote: [\[CITE\]](#) i have this found a vulnerability in a common program i'd want to take advantage of as a proof of concept

i'm able to send a the metasploit rat and things like that, but obviously that wouldn't work in any situation unless windows defender is completely down.

i'd like to demonstrate that even today exploits in binaries which allow for remote code execution can be super dangerous.

doing something like sending a file or executing some hand written asm is cool but it's obvious that RCE can own a machine.

i wouldn't want to do it from scratch though.

for example the MSF multistage framework is really nice at helping you make your shellcode as small as be able to send the real file only once a connection has been made.

so i'd like to know which publicly available rat would be relatively simple in its structure that i could work on and change it

and make it obfuscated enough so that it won't flag.

keep in mind that i don't need the initial file a standalone executable initially, i'm already in execution so i can in fact execute things before deploying the actual malware.

quasar isn't bad, asynrat, dcrat if you can translate Chinese.