

Forum:[Hack Forums](#)

Thread: [persistance for crypted stub?](#)

Captain4acid - February 5, 2018, 5:23 am

hey guys, so i have a perfect stub crypter combo, as i get no issues with any of my office pc's but i was wondering if there was anything like persistance stand-alone device? or any solution that would stop my stub from getting stopped.... if you have any solution that you may have please pm me or comment bellow

CyberStrike - February 5, 2018, 7:31 am

well generally when you are hacking the way it works is that initial access is just for you to do your post exploitation work. For example getting administrator access adding a user to the local admin group of that target machine, part of that post exploitation is mitigating things that can interfere with you moving that machine on to c2 or even having persistance. I would say add exclusions probably your best bet, if you absolutely want to use a crypted backdoor/payload/stub then that is fine I am not sure what you are using but in metasploit I just go ahead and use a powershell script in schtasks to load the payload into the memory although you can use registry autoruns. In conclusion you want to prepare the system for the next phase.

Captain4acid - February 5, 2018, 9:05 am

(Feb 5, 2018 08:31 AM)sirru5h Wrote: [\[CITE\]](#) well generally when you are hacking the way it works is that initial access is just for you to do your post exploitation work. For example getting administrator access adding a user to the local admin group of that target machine, part of that post exploitation is mitigating things that can interfere with you moving that machine on to c2 or even having persistance. I would say add exclusions probably your best bet, if you absolutely want to use a crypted backdoor/payload/stub then that is fine I am not sure what you are using but in metasploit I just go ahead and use a powershell script in schtasks to load the payload into the memory although you can use registry autoruns. In conclusion you want to prepare the system for the next phase. that is some good well put information. thanks for the info, this is more clear now