

Forum:[Hack Forums](#)

Thread: [Question about bootable USB sticks like RUFUS etc.](#)

FULLAUTO - April 13, 2016, 9:53 am

Hi

is there any possibility to make a bootable USB stick like Rufus and get it to autostart a RAT BEFORE the windows and its security tools are started?

alternative way: is it possible to replace with this bootstick a file like osk.exe in the windows directory so i can start the osk (on screen keyboard) and my rat will be executed ?

greetings from nazi germany??????

FULLAUTO - April 15, 2016, 4:53 am

Nobody any ideas how to do it ?

iLogic™ - April 15, 2016, 7:23 am

No there is no option how to run RAT before OS boots. Why ? Because RAT is depends on OS.

SysAdmin - April 15, 2016, 7:56 am

(Apr 15, 2016 07:23 AM)Buckethead™ Wrote: [\[CITE\]](#) No there is no option how to run RAT before OS boots. Why ? Because RAT is depends on OS.

He's correct.

You need an OS to run a RAT. Why would you even need to run a RAT before the OS boots?

UniQ - April 15, 2016, 2:50 pm

(Apr 15, 2016 07:56 AM)Squad-3™ Wrote: [\[CITE\]](#) He's correct.

You need an OS to run a RAT. Why would you even need to run a RAT before the OS boots?

Perhaps because his RAT's stub isn't fud so he simply wants to avoid the AV's. Imagine if you could run any RAT on any computer before the OS boots lol. Chaotic.

FULLAUTO - April 16, 2016, 10:41 am

(Apr 15, 2016 02:50 PM)UniQ Wrote: [\[CITE\]](#) Perhaps because his RAT's stub isn't fud so he simply wants to avoid the AV's. Imagine if you could run any RAT on any computer before the OS boots lol. Chaotic.

I know what you guys are saying, but i want to replace a useless EXE in the sysfiles like OSK.EXE

then i hit run type in OSK.EXE and my replaced exe (rat) will be executed

why do this? because of the security settings

LanMan - April 16, 2016, 12:46 pm

Yes it is possible to start a RAT before any other programs loads and before AV. But not before windows (not with a basic rat i mean).

And yes you can replace any files in the rufus install. But it will not be protected from any good security good program. And Windows File Protection / Windows Resource Protection will throw you a bsod at startup if you touch any protected files.

iLogic™ - April 18, 2016, 12:53 am

(Apr 16, 2016 10:41 AM)FULLAUTO Wrote: [\[CITE\]](#) I know what you guys are saying, but i want to replace a useless EXE in the sysfiles like OSK.EXE

then i hit run type in OSK.EXE and my replaced exe (rat) will be executed

why do this? because of the security settings You can inject your RAT into that process (RunPE) but you will need to have administrator rights to do it. And also... Why you do not want to use startup function in crypter, change assembly information and put that file into sysfiles ?

(Apr 15, 2016 02:50 PM)UniQ Wrote: [\[CITE\]](#) Perhaps because his RAT's stub isn't fud so he simply wants to avoid the AV's. Imagine if you could run any RAT on any computer before the OS boots lol. Chaotic.? What a shame that it is not possible lol

Cynoptics - April 18, 2016, 4:29 am

(Apr 13, 2016 09:53 AM)FULLAUTO Wrote: [\[CITE\]](#) Hi

is there any possibility to make a bootable USB stick like Rufus and get it to autostart a RAT BEFORE the windows and its security tools are started?

alternative way: is it possible to replace with this bootstick a file like osk.exe in the windows directory so i can start the osk (on screen keyboard) and my rat will be executed ?

greetings from nazi germany??????

Unfortunately thats not possible. Well everything is possible but its not easy. You could if you want it to run before anything and for it to be ignored. If you could replace the explorer.exe with your rat embedded into it. That way your antivirus would run it as soon as windows loads. There could be issues with this tho such as it not functioning on systems depending on operating system model and version. Thats the easiest way i can think of for it to be 100% and irremovable. You could just maybe embed code into your rat presume you were coding it that would disable that antivirus and add an exception, you could do this in many ways including creating a script that would run a hidden vnc and create the exclusion then delete it.

FULLAUTO - April 18, 2016, 9:33 am

(Apr 18, 2016 04:29 AM)Cynoptics Wrote: [\[CITE\]](#) Unfortunately thats not possible. Well everything is possible but its not easy. You could if you want it to run before anything and for it to be ignored. If you could replace the explorer.exe with your rat embedded into it. That way your antivirus would run it as soon as windows loads. There could be issues with this tho such as it not functioning on systems depending on operating system model and version. Thats the easiest way i can think of for it to be 100% and irremovable. You could just maybe embed code into your rat presume you were coding it that would disable that antivirus and add an exception, you could do this in many ways including creating a script that would run a hidden vnc and create the exclusion then delete it. thanks a lot for all of your help ppl..

I think its better to do that RAT FUD with some crypter and then execute it via RubberDucky USB