

Forum:[Hack Forums](#)

Thread: [Rust or CPP botnet feature request/suggestions](#)

NotKover - February 14, 2022, 12:06 pm

What would you like to see in a botnet made in rust or CPP(will have download and execute and update etc and will be a http panel) and please dont say stupid stuff

__Digital__ - February 14, 2022, 1:19 pm

(Feb 14, 2022 01:06 PM)NotKover Wrote: [\[CITE\]](#) What would you like to see in a botnet made in rust(will have download and execute and update etc and will be a http panel) and please dont say stupid stuff

1. botkiller
2. ruskill option
3. heavy persistence

SIM-5052356 - February 15, 2022, 5:10 am

Proccess injection
Startup
Watchdog
possibly a UAC bypass

lululululu - March 4, 2022, 2:54 pm

A Kernel Driver for persistance and invisibility.

NotKover - March 4, 2022, 5:05 pm

(Mar 4, 2022 03:54 PM)lululululu Wrote: [\[CITE\]](#) A Kernel Driver for persistance and invisibility.
If i did that it wouldnt be cheap and a lot of work to do but its doable.

ecccccccccc - March 5, 2022, 2:57 am

(Mar 4, 2022 03:54 PM)lululululu Wrote: [\[CITE\]](#) A Kernel Driver for persistance and invisibility.
(Mar 4, 2022 06:05 PM)NotKover Wrote: [\[CITE\]](#) If i did that it wouldnt be cheap and a lot of work to do but its doable.
best way to do this is by using a vulnerable signed driver since loading unsigned drivers or just disabling microsofts signature enforcement is kinda a hard thing to do, i know there are alot of projects on github but the thing is you have to update it for every windows version.

lululululu - March 5, 2022, 3:23 am

(Mar 5, 2022 03:57 AM)ecccccccccc Wrote: [\[CITE\]](#) best way to do this is by using a vulnerable signed driver since loading unsigned drivers or just d Hubisabling microsofts signature enforcement is kinda a hard thing to do, i know there are alot of projects on github but the thing is you have to update it for every windows version.

<https://github.com/hfiref0x/TDL>
<https://v1k1ngfr.github.io/loading-windows-unsigned-driver/>

Both Tested and working

ecccccccccc - March 5, 2022, 2:17 pm

(Mar 5, 2022 04:23 AM)lululululu Wrote: [\[CITE\]](#) <https://github.com/hfiref0x/TDL>
<https://v1k1ngfr.github.io/loading-windows-unsigned-driver/>

Both Tested and working
doesnt work on latest windows 11, maybe its just cus of secureboot

NotKover - March 5, 2022, 8:23 pm

(Mar 5, 2022 03:57 AM)ecccccccccc Wrote: [\[CITE\]](#) best way to do this is by using a vulnerable signed driver since loading unsigned drivers or just disabling microsofts signature enforcement is kinda a hard thing to do, i know there are alot of projects on github but the thing is you have to update it for every windows version.

I know ways to do it but its more of making the kit itself.

lululululu - March 6, 2022, 6:15 am

(Mar 5, 2022 03:17 PM)ecccccccccc Wrote: [\[CITE\]](#) doesnt work on latest windows 11, maybe its just cus of secureboot

Turla Driver loader works fine for me in latest windows11 with secureboot enabled

NotKover - March 6, 2022, 6:18 am

(Mar 6, 2022 07:15 AM)lululululu Wrote: [\[CITE\]](#) Turla Driver loader works fine for me in latest windows11 with secureboot enabled

uh alright, i probably will end up making the kit but i dont think people on HF would be able to afford a build of it due to it having a kernel kit

lululululu - March 6, 2022, 6:24 am

(Mar 6, 2022 07:18 AM)NotKover Wrote: [\[CITE\]](#) uh alright, i probably will end up making the kit but i dont think people on HF would be able to afford a build of it due to it having a kernel kit

Hackforums is definitely the wrong place for selling this kind of malware.

NotKover - March 6, 2022, 6:33 am

(Mar 6, 2022 07:24 AM)lululululu Wrote: [\[CITE\]](#) Hackforums is definitely the wrong place for selling this kind of malware.

I was thinking of just making some actually HQ software with some good features and sell it tbh just for money and shit but if i make these advanced features it definitely will be sold somewhere else