

Forum:[Hack Forums](#)

Thread: [Bastiller - Skid ready dropper](#)

CL1B - October 14, 2025, 7:28 am

Bastiller: Skid ready dropper

Like it's hot

[Bastille](#) was wondering how skids infect other skids by staging payloads in otherwise legit looking binaries.

[How to wrap a program with additional code ?](#)

So I wrote some evil code which might give some insights to this kind of skidware.

Weird thing is, I noticed Defender doesn't instantly flag invalid signatures anymore.. or at least not putty's?

Shouldn't it auto flag them?

Either way.. Bastiller takes any valid EXE, extracts it's attributes, signatures and such and then compiles a wrapper/dropper or whatever you want to call it that's weaponized with PS.

Usage:

First change the default HackForums.net payload to whatever payload you want, then compile Bastiller.

Bastiller.exe <path to .exe>

or

Bastiller.exe <path to .exe> -admin

-admin will add a RT manifest to have the app Run As Admin only.

Putty weaponized with the default payload

Putty weaponized with a exclude C:\ drive payload

Proof of concept:

But cigman, how can I not be skid with it?

Learn a thing or 2 about real PE injection techniques. No, i'm not talking about process injection.. I'm talking about detecting possible code caves and then patching them with your payload. Over here we call that: A backdoor. I'm pretty sure there's only 1 user on HF that would understand even the concept of this, so if you're really interested.. you'll have to find out.

Interesting to see some of the EDRs allowing such a binary to run in the first place..

╰_(_)_╯

Devs in convo ([Click to View](#))In [Bastille](#) his thread is a comment by [ttbr0](#) about joining convo for dev talks.. If you're a dev or whatever you are and you like these topics. Come chat with us in convo, often makes for some interesting, insightful and inspiring chats. You can find the public convo here: <https://hackforums.net/convo.php?action=all>

Disclaimer

This tool is for educational and security testing purposes only. Don't use it on systems you don't own or have permission to test. Injection can crash processes and cause system instability.

PhillyStyle - October 14, 2025, 2:13 pm

Wow that was a really nice thing of you to do for Bastille. I can't up your popularity or anything as far as I know. All I can do is say "props to you dude". ?? I hope that is enough.

ttbr0 - October 14, 2025, 10:54 pm

another insane release from marl. i cant believe that this man is just giving this stuff away for free. full source code as well. hf has never seen so many releases at once before, it must be a world record.

CL1B - October 15, 2025, 4:19 am

(Oct 14, 2025 10:54 PM)ttbr0 Wrote: [\[CITE\]](#) another insane release from marl. i cant believe that this man is just giving this stuff away for free. full source code as well. hf has never seen so many releases at once before, it must be a world record.

Really? That's kinda cool. I hope other devs will do so too, deepdiving into pocs are by far the most insightful way of sharing knowledge imo and I'm really missing that here.

MadScientist - October 15, 2025, 4:50 pm

Bro this title made me laugh

Hackers - October 16, 2025, 6:09 am

Nice contribution, and good callout on code caves!

This method is huge in torrents, fake dev sites, malicious Git repos, etc.

jmdavis90 - October 18, 2025, 8:55 pm

How do I use this with my payload please?

Hackers - October 18, 2025, 8:57 pm

(Oct 18, 2025 08:55 PM)jmdavis90 Wrote: [\[CITE\]](#) How do I use this with my payload please?
He wrote it out here:

Quote:First change the default HackForums.net payload to whatever payload you want, the compile Bastiller.

Bastiller.exe <path to .exe>

or

Bastiller.exe <path to .exe> -admin

-admin will add a RT manifest to have the app Run As Admin only.

possessed-client - October 28, 2025, 1:24 am

(Oct 14, 2025 07:28 AM)MarlboroMan Wrote: [\[CITE\]](#) [..]

But cigman, how can I not be skid with it?

Learn a thing or 2 about real PE injection techniques. No, i'm not talking about process injection.. I'm talking about detecting possible code caves and then patching them with your payload. Over here we call that: A backdoor. I'm pretty sure there's only 1 user on HF that would understand even the concept of this, so if you're really interested.. you'll have to find out.

[..]

You can absolutely be skid with it, just need to find the right tools online, like the leaked Shellter Pro version (only works with 32bit executables), also there's multiple code cave hunting projects on Github, but I don't remember whether any of them have more features than Shellter, like 64bit compatibility or more advanced evasion, might need to cobble together something from multiple projects and PoCs, but don't know if there's enough public code to surpass that old Shellter leak.

But it is bizarre that your screens of VT scan don't show the invalid-signature flag, maybe I'm not understanding what's being scanned right.

AlternativeTalent - November 16, 2025, 2:05 am

Is it your Code? | Yes or No

what a shame, posting AI generated code..

Rick4pex - December 8, 2025, 1:33 pm

Thank you for this insane skid tool, I will make sure to not be a skid with it ?

CL1B - December 8, 2025, 1:36 pm

(Dec 8, 2025 02:33 PM)Rick4pex Wrote: [\[CITE\]](#) Thank you for this insane skid tool, I will make sure to not be a skid with it ?

Proud.