

Forum: [Hack Forums](#)

Thread: [\[MRT-X\] Malware Removal Tool Development Thread](#)

Tha Sneak - February 13, 2025, 4:36 pm

<https://github.com/MRT-X>

Note: Post your Github Username in this thread to obtain access!

Open sourcing my tool will be posting source code for group development.

Source Code for HF System Scanner: <https://github.com/ThaSneakest/HF-System-Scanner>

A to do list to be completed later.

HijackThis Source Code: <https://github.com/ThaSneakest/HF-HijackThis>

bbEditor: <https://github.com/ThaSneakest/HF-bbEditor>

ComboFix: <https://github.com/ThaSneakest/HF-ComboFix>

DDS: <https://github.com/ThaSneakest/HF-DDS>

JRT: <https://github.com/ThaSneakest/HF-JRT>

Pocket Killbox: <https://github.com/ThaSneakest/HF-Pocket-KillBox>

FRST: <https://github.com/ThaSneakest/HF-FRST>

FSS: <https://github.com/ThaSneakest/HF-FSS>

MiniToolBox: <https://github.com/ThaSneakest/HF-MiniToolBox>

SilentRunners: <https://github.com/ThaSneakest/HF-SilentRunners>

DelFix: <https://github.com/ThaSneakest/HF-DelFix>

ATF Cleaner: <https://github.com/ThaSneakest/HF-ATF-Cleaner>

SecurityCheck: <https://github.com/ThaSneakest/HF-SecurityCheck>

FMRS: <https://github.com/ThaSneakest/HF-FMRS>

KRPM: <https://github.com/ThaSneakest/HF-KPRM>

RSIT: <https://github.com/ThaSneakest/HF-RSIT>

Stanley - March 4, 2025, 1:42 pm

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

Tha Sneak - March 5, 2025, 11:03 pm

I've been doing some brain storming and asking I've come up that the best languages to bring to the table for these tools are C# or Rust. I'm leaning toward C# due to me being very familiar with C# I was wondering if someone was interested in helping me convert these tools to C# and Rust so we can have both languages to work with. If you're not very code knowledgeable using ChatGPT is sufficient in helping convert.

I'm actively working on KRPM conversion to C#.

ttbr0 - March 6, 2025, 1:05 am

rust would be really good and performant for at least some of it. i havent learnt much of the language yet but this could be a good excuse to do it. there is a lot of code here and development will be slow from me considering how little free time i have but im interested in contributing however much i can.

Tha Sneak - March 6, 2025, 1:39 am

(Mar 6, 2025 02:05 AM)ttbr0 Wrote: [\[CITE\]](#) rust would be really good and performant for at least some of it. i havent learnt much of the language yet but this could be a good excuse to do it. there is a lot of code here and development will be slow from me considering how little free time i have but im interested in contributing however much i can.

Sounds great to me I'm doing the same I'll do C# if you want to do RUST and we can see which one works the best.

Tha Sneak - March 8, 2025, 7:04 am

If you're working on any of the reverse engineered malware removal tools let me know which one and what language. At the moment I am doing KPRM converting it to C#.

We could definitely use more developers and helpers to finish this conversion if at all possible its pretty much basics of coding and using ChatGPT to convert the code to C# or Rust.

Unless you're a professional and want to hand translate it.

Tha Sneak - March 9, 2025, 7:36 pm

Just out of curiosity, has anyone made any progress on any of these?

ttbr0 - March 9, 2025, 8:28 pm

i am slowly learning rust so i need a fair bit of time before i am comfortable, but i think it shouldnt be done entirely in rust. it would make sense to take advantage of its performance and use other languages for their respective advantages too. im unsure about gui development with rust, but it can at least be built into a dynamic library that a gui application written in another language can import and use. im not a developer by trade so id like to know what people think about how to structure the

projects.

there is also a lot of code to parse in each of these projects which makes it hard to grasp a good conceptual understanding of what the tools need to do. having some sort of documentation would make it easier if you already know what the code does so that it would be easier to port it to other languages.

Tha Sneak - March 10, 2025, 10:58 am

(Mar 9, 2025 08:28 PM)ttbr0 Wrote: [\[CITE\]](#) i am slowly learning rust so i need a fair bit of time before i am comfortable, but i think it shouldnt be done entirely in rust. it would make sense to take advantage of its performance and use other languages for their respective advantages too. im unsure about gui development with rust, but it can at least be built into a dynamic library that a gui application written in another language can import and use. im not a developer by trade so id like to know what people think about how to structure the projects.

there is also a lot of code to parse in each of these projects which makes it hard to grasp a good conceptual understanding of what the tools need to do. having some sort of documentation would make it easier if you already know what the code does so that it would be easier to port it to other languages.

I can work on that. I've translated some of them already into C#, but I will annotate what functions do what. I'm also considering Python as a possible language to translate them too as well.

There is tons of code, but line by line we can do it.

I'm also open to other languages as well most of them are AutoIt and Command Line scripts rather than an actual language, which makes it tricky and time consuming to translate.

ttbr0 - March 10, 2025, 10:38 pm

ive been looking at dds and noticed that dds.cmd tries to locate a setpath_n.cmd file which isnt part of the repo. wondering if that was intentional or not.

Tha Sneak - March 10, 2025, 10:48 pm

(Mar 10, 2025 10:38 PM)ttbr0 Wrote: [\[CITE\]](#) ive been looking at dds and noticed that dds.cmd tries to locate a setpath_n.cmd file which isnt part of the repo. wondering if that was intentional or not.

Good question, I'll reverse engineer it again and make sure I didn't miss anything.

This is what you get when you open it with 7zip it's actually really easy to access. Now some of the other files are coded in C++ I believe they're all command line tools. You raise a good question I don't have a clue where that comes from.

- MBR.dat = Catchme.exe by GMER
- PEV.dat = PEV.exe formerly now ReadPE <https://github.com/mentebinaria/readpe/wiki>
- SED.dat = SED.exe <https://github.com/mbuilov/sed-windows>
- SQLite3.dat = Sqlite3.dll

Not sure on some of the others they're compiled in C++ and I haven't taken the time to reverse engineer them.

I presume it's created in one of the executables, but it can probably be skipped as it sounds like it just sets environmental variable paths.

RootRXXT - March 16, 2025, 1:18 pm

itwguthub - for the Github Access

Tha Sneak - March 16, 2025, 1:29 pm

(Mar 16, 2025 01:18 PM)RootRXXT Wrote: [\[CITE\]](#) itwguthub - for the Github Access
The repository isn't private at the moment, but when it is I'll add you in.

Py_Dev - March 28, 2025, 5:41 am

<https://github.com/PyDevOG/PyScan>

<https://hackforums.net/blog/Py-DevThreatIntelligenceEp7>