

Forum:[Hack Forums](#)

Thread: [RELEASE: The Healer, Post Malware Removal recovery tool UPDATED 21APR](#)

Insane Developer - April 7, 2016, 9:08 pm

Update 21/April/2016: Added Persistent File Remover and FileAssasin Installer.

As one of my recent projects, I have released The Healer, a tool to recover from malware incidents. NOTE: THIS TOOL ONLY ATTEMPTS TO UNDO CHANGES, NOT REMOVE THE MALWARE. Might help during the infection stages by making it easier to remove malware.

There are currently 2 editions available: The Lite and the Full. Both are free. The lite is smaller because the Kaspersky Installer was removed, since the Kaspersky Installer is 150 mb. However, it is the Antivirus that I would recommend to all of you.

Screenshots:

<https://gyazo.com/16c9d4723ab2004d1ca1e800912940f0>

<https://gyazo.com/4c82906542a7ccbc82a6c9d6be1c699c>

More details pleeezz?

It is capable of cleaning HOST file, re-activating windows features,...

It can also clean startup (Including hidden startup) and includes 3 AV installers in it.

The entire executable is coded in AutoIt(Except for the installers for AVs)

Download:

Version 1.2.0.0: <http://www.zunzutech.com/blog/uncategorized/the-healer-new-release/>

Version 1.1.0.1:

<http://www.zunzutech.com/blog/security/release-the-healer-post-malware-removal-recovery-tool/>

omg virus? [VT of Lite Edition](#) (False positives), VT of Full Edition (Not available, too heavy).

Changelog:

Code V1.1.5.0 21 April 2016

Added FileAssasin Installer

Added Persistent File Remover

Removed Kaspersky Internet Security Installer.

V1.1.0.1 Open Beta

Added obfuscation and encryption (While this is a freeware, it is not Open Source).

Added Lite Edition

Added credits

Improved AV installers (Install files to Temp Dir under random names to prevent malware detections)

Added Clear Startup

V1.1.0.0 Closed Beta

Added Revive AVs (Image File Execution)

Added AV installers

Improved restore Windows Function

V1.0.0.0 Closed Beta:

Added restore HOST

Added restore Windows FunctionTOS:

By using our software you agree that we are not responsible for any damages or unwanted results dealt by our product.

You may not attempt to reverse engineer our software.

This is copyright protected

This software is provided AS IS, with NO LIABILITY or GUARANTEED SUPPORT, as well as no guaranteed updates.

Cecilia - April 7, 2016, 9:38 pm

Its alright...

I mean, it doesn't do a lot of things, but it does the job.

Insane Developer - April 8, 2016, 12:04 am

(Apr 7, 2016 09:38 PM)LaPanthere Wrote: [\[CITE\]](#) Its alright...

I mean, it doesn't do a lot of things, but it does the job.

I am planning to add some features, such as malware detection (Through known samples), file killer,...

Cecilia - April 8, 2016, 12:16 am

(Apr 8, 2016 12:04 AM)Insane Developer Wrote: [\[CITE\]](#) I am planning to add some features, such as malware detection (Through known samples), file killer,...

The abilities of GMER (not the detection, the removal of registry keys and files) I think would be very handy.

Insane Developer - April 8, 2016, 1:37 am

(Apr 8, 2016 12:16 AM)LaPanthere Wrote: [\[CITE\]](#) The abilities of GMER (not the detection, the removal of registry keys and files) I think would be very handy.

I will try and implement that. Another tool I will probably use is RegRun Partizan for removing persistent malware

Cecilia - April 8, 2016, 1:59 am

(Apr 8, 2016 01:37 AM)Insane Developer Wrote: [\[CITE\]](#) I will try and implement that. Another tool I will probably use is RegRun Partizan for removing persistent malware

Mhm, there are not many tools that support the removal of files/keys that use permissions to hide.

Insane Developer - April 8, 2016, 2:32 am

(Apr 8, 2016 01:59 AM)LaPanthere Wrote: [\[CITE\]](#) Mhm, there are not many tools that support the removal of files/keys that use permissions to hide.

Well you can change the explorer so that it shows hidden files through registry (Already implemented).

The thing about Partizan is that it can be ran through command line, and is very powerful as it can even remove files protected by drivers. So regular rootkits won't stand a chance.

I am also thinking of a dynamic startup cleaner (Adapted from a malware's botkiller) that does the following things:

Find all startup entries, follow path to the file, if the file is Hidden/System then kill key, if it is cmd then kill key, If the window is not shown then kill key, if the window is shown then skip, if the file is included in the whitelist (For AVs and other whitelisted entities) then skip.

zhafan - April 8, 2016, 6:36 am

Great Healer from the virus it is awesome

Insane Developer - April 9, 2016, 5:35 pm

Update with FileAssasin and a modified Startup Clear is about to be released!

Insane Developer - April 11, 2016, 6:34 am

Bump, still up. You can try this tool after removing a malware/as an attempt to reduce the persistence of the malware!

Insane Developer - April 13, 2016, 3:40 am

NOTE: Remember that the startup clearer might remove the startup of your antivirus as well, so make sure that you have backed up the key and rewrite it after you have used the startup clearer. Restoring AV's key is being developed at the moment.

Insane Developer - April 14, 2016, 9:31 am

Still working, have successfully removed the startup of RATs and Botnets. Feel free to leave a comment!

own3d - April 14, 2016, 4:41 pm

Thanks for the share. Will be keeping an eye on your progress with this, have downloaded it, neat tool. ?

Insane Developer - April 17, 2016, 7:13 am

Getting this post to the top. Update is almost done!

Added FileAssasin and persistent file remover, almost ready for the next update

Insane Developer - April 21, 2016, 12:57 am

New version 1.2.0.0 released! Added persistent file remover and File Assasin/

Insane Developer - April 26, 2016, 3:02 am

Bump, still working and going strong.

Insane Developer - May 2, 2016, 8:23 pm

Bump, still working. Adding a dynamic startup clearer which clears suspicious startups.

indig0 - May 10, 2016, 2:50 am

How well would you say this tool stacks up against something like Malwarebytes Anti-Malware? Just curious. Thanks.

__SIP - May 10, 2016, 4:03 am

No offence, but, I do not think anyone would trust this unless you are extremely reputable in the fields of writing malware removal tools.

I know for a fact that many people, including me, would not run a software like this without knowing the competency of the coder(s) behind it. I am not implicating this is backdoored, what I am implicating is that this program could potentially produce unwanted and hazardous results. There is a reason on AV's do not have to post a disclaimer "we are not responsible for what this program does to your PC."

That right there shows the competency and trust in your own code, nil.

Insane Developer - May 10, 2016, 4:49 am

(May 10, 2016 04:03 AM)___SIP Wrote: [\[CITE\]](#) No offence, but, I do not think anyone would trust this unless you are extremely reputable in the fields of writing malware removal tools.

I know for a fact that many people, including me, would not run a software like this without knowing the competency of the coder(s) behind it. I am not implicating this is backdoored, what I am implicating is that this program could potentially produce unwanted and hazardous results. There is a reason on AV's do not have to post a disclaimer "we are not responsible for what this program does to your PC."

That right there shows the competency and trust in your own code, nil.
No offence, but, I do not think anyone would trust this unless you are extremely reputable in the fields of writing malware removal tools.

I know I am not reputable, but I am contributing something.

I am not implicating this is backdoored, what I am implicating is that this program could potentially produce unwanted and hazardous results.

I have tested in VMs and it is completely safe. I have also tested it on my machine and nothing went wrong. I am about to make it safer as well with a dynamic startup clearer to clear only malicious startup entries.

There is a reason on AV's do not have to post a disclaimer "we are not responsible for what this program does to your PC."

Says who? They do that all the time.

ESET as an example: <https://www.eset.com/us/software-eula/> Look at section 13.

(May 10, 2016 02:50 AM)indig0 Wrote: [\[CITE\]](#) How well would you say this tool stacks up against something like Malwarebytes Anti-Malware? Just curious. Thanks.

It is probably nothing, but Malwarebytes is an AV, and this is not one. It does not detect malware.

___SIP - May 10, 2016, 5:03 am

Insane Developer Wrote:-snip-

That refers to the "inability to use the program" disclaimer. It has nothing to do with "yeah this program might fuck up your computer, use at your own risk."

Insane Developer - May 10, 2016, 5:07 am

(May 10, 2016 05:03 AM)___SIP Wrote: [\[CITE\]](#) That refers to the "inability to use the program" disclaimer. It has nothing to do with "yeah this program might fuck up your computer, use at your own risk."

Who knows what will go wrong? Go talk to your lawyer about this.

Almost done with the dynamic startup clearer, polishing it a bit.

Insane Developer - May 14, 2016, 7:41 am

Still up and going strong. Download now!

___SIP - May 14, 2016, 10:02 am

Would not use this AutoIT tool that just downloads AV's and does what other AV's do in a SAFE MANOR, do not use this static bull crap. Typical AutoIT skidware.

Insane Developer - May 17, 2016, 12:18 am

(May 14, 2016 10:02 AM)___SIP Wrote: [\[CITE\]](#) Would not use this AutoIT tool that just downloads AV's and does what other AV's do in a SAFE MANOR, do not use this static bull crap. Typical AutoIT skidware.Ooops, you are banned. Was thinking of arguing some more. As you appear to be a multi, post here when you come back.

___SIP - May 19, 2016, 8:06 pm

(May 17, 2016 12:18 AM)Insane Developer Wrote: [\[CITE\]](#) Ooops, you are banned. Was thinking of arguing some more. As you appear to be a multi, post here when you come back.

Ban evading, not a market post ban? Desperate to avoid commenting on your skidware?

Insane Developer - May 19, 2016, 8:30 pm

(May 19, 2016 08:06 PM)___SIP Wrote: [\[CITE\]](#) Ban evading, not a market post ban? Desperate to avoid commenting on your skidware?

Ah I see your ban was lifted. Welcome back.

Codefuser - July 12, 2016, 11:03 pm

I am working with Insane Developer on this project now. We are trying to implement a scanning system which automatically scan all startup entries in order to detect malicious entries. I might try and convert this to C++ (Since he can't xD no offense though) but it might not be worth the effort since single threaded scan results are not too slow atm.

Example log: <https://gyazo.com/d35483ed13b2ba25426aa52a88d8fc63>