

Forum:[Hack Forums](#)

Thread: [\[BHCPU\] Malware Analysis/Removal Resources](#)

-Hyperion - June 1, 2014, 12:26 pm

Hey guys it's -Hyperion ?

This is a toolkit I put together for analyzing and removing malware.

I will give a brief description of each tool and a link to the developers page. There is also a set of bookmarks of useful online services. A few do the same thing and are just a personal preference. This toolkit will be updated as time goes on and suggestions will be taken.

It is recommended that you download these and put them on a USB checking for updates at least once a month.

WARNING SOME OF THESE TOOL MAY HARM YOUR COMPUTER WITH IMPROPER USE E.G COMBOFIX/OTL DO NOT RUN THESE OUTSIDE OF YOUR VIRTUAL BOX

AnalysisAutoruns- Shows what programs run during boot and login [Here](#)

BlueScreenView- Used to view BSOD messages [Here](#)

Comodo Kill Switch- Lets you identify and monitor processes [Here](#)

CrowdInspect- Scans active programs for malware [Here](#)

Moo0 File Monitor- Displays file changes in real time [Here](#)

ollydbg- Reverse engineering program [Here](#)

PMD- Process Memory Dumper for applications [Here](#)

Process Hacker- More advanced system monitor [Here](#)

Procmon- Advanced logging and monitoring [Here](#)

RegShot- Lets your compare 2 snapshots of a registry [Here](#)

Wireshark- Network analyzer [Here](#)

Fakenet- Allows you to full malware into thinking it is not in a VM and is on a network.

REMnux- A Linux distribution made specially for analyzing malware and decompiling it.

RemovalAdwcleaner- Removes adware, toolbars and hijackers [Here](#)

Combofix- A very dangerous malware removal tool [Here](#)

Eset Online Scanner- An excellent online virus scanner [Here](#)

HxD- A very fast hex editor [Here](#)

Junkware Removal Tool- removes common adware, toolbars, and PuPs [Here](#)

Malwarebytes-An excellent Anti-Malware and PuP remover [Here](#)

OTL- Advanced system diagnostics as dangerous as Combofix [Here](#)

tdsskiller- anti root-kit utility by Kaspersky [Here](#)

RKill- terminates known malware processes so you can run your programs [Here](#)

RogueKiller- Removes ZeroAccess, rogue anti-spyware programs, and Ransomwares [Here](#)

This library was last updated 11-29-2014 4:30pm

desynk - June 1, 2014, 12:40 pm

Looks good but I would also suggest adding autoruns.

Roger Waters - June 1, 2014, 2:32 pm

Nice tool kit, although I already have most of these programs on my flash drive, lol.

Aura - June 1, 2014, 4:34 pm

Why is my name still being used ? ?
I'm a nobody now.

NarwhalTusks - June 1, 2014, 4:40 pm

(Jun 1, 2014 04:34 PM)Aur? Wrote: [\[CITE\]](#) Why is my name still being used ? ?
I'm a nobody now.

"I'm a nobody now." says the guy that has helped me with 2 computers in the past month and helped tens of hundreds of people with theirs. ? Aura, you're great man. No where near nobody.

Jagster™ - June 1, 2014, 4:40 pm

(Jun 1, 2014 04:34 PM)Aur? Wrote: [\[CITE\]](#) Why is my name still being used ? ?
I'm a nobody now.
Where? I do not see it at all in this thread ?

Roger Waters - June 1, 2014, 4:42 pm

(Jun 1, 2014 04:34 PM)Aur? Wrote: [\[CITE\]](#) Why is my name still being used ? ?
I'm a nobody now.
Aura, are you drunk right now? You aren't a nobody.

Aura - June 1, 2014, 4:49 pm

(Jun 1, 2014 04:40 PM)Jagster™ Wrote: [\[CITE\]](#) Where? I do not see it at all in this thread ?
Hint : Look at one of the spoilers.

(Jun 1, 2014 04:42 PM)Roger Waters Wrote: [\[CITE\]](#) Aura, are you drunk right now? You aren't a nobody.

Well as of this summer I'll become one as I'll be too busy with work and GTG training.

ALSO NICE TUTORIAL HYP. GLAD TO SEE IT WON'T BE DELETED ?

Roger Waters - June 1, 2014, 4:50 pm

(Jun 1, 2014 04:49 PM)Aur? Wrote: [\[CITE\]](#) Well as of this summer I'll become one as I'll be too busy with work and GTG training.
I better take the name of Aura Jr. before it is taken then. ?

Aura - June 1, 2014, 4:52 pm

(Jun 1, 2014 04:50 PM)Roger Waters Wrote: [\[CITE\]](#) I better take the name of Aura Jr. before it is taken then. ?
Like Phyber and Phyber Jr and Phyber Jr Jr ? ?

Jagster™ - June 1, 2014, 5:08 pm

rofl password is Aura lol

GG fanboy much OP! <3

rxki - June 1, 2014, 5:49 pm

The file was removed - any idea on why it was removed?

-Hyperion - June 1, 2014, 5:57 pm

(Jun 1, 2014 05:49 PM)L?ki Wrote: [\[CITE\]](#) The file was removed - any idea on why it was removed?
Try now just uploaded a new version with 5 new tools. ?

Null Byte - June 1, 2014, 6:20 pm

Really legit looking toolkit. Good work Hype.

Cyber Saint - June 1, 2014, 6:36 pm

Might take a look later but the tools that you listed look useful and I don't already have some that I might require, so thank you.

Weebex - June 1, 2014, 7:10 pm

(Jun 1, 2014 04:34 PM)Aur? Wrote: [\[CITE\]](#) Why is my name still being used ? ?

I'm a nobody now.

Who are you exaxtly?

Who the hell is a Aura?

You guys know who he is cause idk,

Spoiler [\(Click to View\)](#)

He deserves WHH award

ven0m - June 2, 2014, 5:33 am

AdwCleaner currently shows a false positive for certain registry key which will be addressed in the next update. Until then it is not advisable to run AdwCleaner fix unless reviewing the scan log prior.

P.S. Paradoxum removed the AdwCleaner step from the MRT Log request thread.

Aura - June 2, 2014, 5:35 am

(Jun 2, 2014 05:33 AM)ven0m Wrote: [\[CITE\]](#) AdwCleaner currently shows a false positive for certain registry key which will be addressed in the next update. Until then it is not advisable to run AdwCleaner fix unless reviewing the scan log prior.

P.S. Paradoxum removed the AdwCleaner step from the MRT Log request thread.

That's what I noticed in the thread too. I think AdwCleaner and another program or step have been removed ? There used to be 5 steps no ?

ven0m - June 2, 2014, 5:37 am

(Jun 2, 2014 05:35 AM)Aur? Wrote: [\[CITE\]](#) That's what I noticed in the thread too. I think AdwCleaner and another program or step have been removed ? There used to be 5 steps no ?

Only AdwCleaner fix step was removed. It used to be four steps and five logs.

Aura - June 2, 2014, 5:38 am

(Jun 2, 2014 05:37 AM)ven0m Wrote: [\[CITE\]](#) Only AdwCleaner fix step was removed. It used to be four steps and five logs.

OH, therefore why I was confused ? I knew there were 5 "something" but I didn't know what exactly.

-Hyperion - June 2, 2014, 5:41 am

Which registry key is removed? Good Job Aura >:I telling me to add ADW

Aura - June 2, 2014, 6:05 am

(Jun 2, 2014 05:41 AM)-Hyperion Wrote: [\[CITE\]](#) Which registry key is removed? Good Job Aura >:I telling me to add ADW

Implying I knew about it and you knew about it too eh ?

-Hyperion - June 2, 2014, 7:23 am

wait when did this get moved? Lesson 2 is out Wednesday

Aura - June 2, 2014, 7:27 am

(Jun 2, 2014 07:23 AM)-Hyperion Wrote: [\[CITE\]](#) wait when did this get moved? Lesson 2 is out Wednesday

Got moved like 2 hours ago by Paradoxum I guess ?

Computer Forensics - June 15, 2014, 9:44 pm

Thanks for this thread post, those are some very strong tools in that list.

Tetro - September 6, 2014, 7:56 am

Thanks alot for this, that I needed.Thx

-Hyperion - September 22, 2014, 5:16 pm

new update coming out this week with a surprise

Aura 2.0 - November 29, 2014, 2:40 pm

Great thread, going to use these to help keep my system clean.

N3WER4 - December 3, 2014, 5:59 pm

Thanks for sharing it was very informative and helpful.