

Forum: [Hack Forums](#)

Thread: [HF Malware Hunters - ? Exposing Dangerous Downloads ?](#)

Bastille - August 3, 2024, 12:32 am

? Latest additions ! ?

05/18/2025 | Arkei Stealer Cracked, SFX packed ? :

<https://hackforums.net/showthread.php?tid=6298421>

05/17/2025 | ZeroTrace Stealer SFX packed ? :

<https://hackforums.net/showthread.php?tid=6298353>

04/24/2025 | Hidden Wiki Scam? : <https://hackforums.net/showthread.php?tid=6296845>

04/21/2025 | Fake Mailer ? : <https://hackforums.net/showthread.php?tid=6296631>

? Malware Analysis Corner ?

After spending a few years helping forum members with security-related issues, particularly malware removal, Brotherhood came to me with the idea of enhancing the [White Hat section](#), we were looking for solutions to share our knowledge related to this field, to bring help, guidance, assistance, and offer some services. For those who knew the [MRT \(Malware Removal Team\)](#) and members related to this group, the idea is to bring back what they used to do here and to go even further.

This thread is part of one of the many initiatives aimed at improving the forum experience, particularly in the white hat section.

There are several ideas behind this thread. [] Giving concret examples on how a malware analysis is conducted, how to find artifacts, what tools are used, ...

[] Making a place where members could share their knowlege and discuss about malware analysis which is not often addressed

It's also a good opportunity to show the community that the Staff is primarily here to assist and protect the members.

We decided to take this approach further by analyzing the programs, links, and files shared by some members to ensure they do not pose a threat to the community. I believe this adds value to my role as Staff, although I would have done the same if I were not Staff. The advantage is that I have the ability to remove suspicious elements while they are being analyzed.

EDIT : This thread is now a part of the MRT-X after The Brotherhood lead to the creation of a new group, and to bring back the origin essence of the MRT.

INFECTED LINKS ?

<https://hackforums.net/showthread.php?tid=6271578> > Crypto miner ?

<https://hackforums.net/showthread.php?tid=6269930> > Stealer ?

<https://hackforums.net/showthread.php?tid=6269932> > Stealer ?

<https://hackforums.net/showthread.php?tid=6274196> > Stealer ? and Crypto miner ?

<https://hackforums.net/showthread.php?tid=6274326> > RAT ?

<https://hackforums.net/showthread.php?tid=6276362> > Stealer ?

<https://hackforums.net/showthread.php?tid=6278798> > RAT ?

<https://hackforums.net/showthread.php?tid=6254162> > under review

<https://hackforums.net/showthread.php?tid=6238357> > Collection of infected ?

<https://hackforums.net/showthread.php?tid=6268885> > Collection of infected ?

<https://hackforums.net/showthread.php?tid=6281297> > Fake tool, scam ?

<https://hackforums.net/showthread.php?tid=6280678> > BTC Clipper ?

<https://hackforums.net/showthread.php?tid=6281838> > BTC Clipper ?

<https://hackforums.net/showthread.php?tid=6278565&pid=62532703#pid62532703> > BTC Clipper ?

<https://hackforums.net/showthread.php?tid=6282360> > Ransomware ?

<https://hackforums.net/showthread.php?tid=6283230> > Malicious Chrome extension ?

<https://hackforums.net/showthread.php?tid=6269480&highlight=txt> > Hidden malicious files ?

<https://hackforums.net/showthread.php?tid=6288934> > Stealer ?

<https://hackforums.net/showthread.php?tid=6293788> > RAT ?

<https://hackforums.net/showthread.php?tid=6296196> > RAT ?

<https://hackforums.net/showthread.php?tid=6296631> > Loader ?

<https://hackforums.net/showthread.php?tid=6298353> > Multiple payloads ?

<https://hackforums.net/showthread.php?tid=6298421> Multiple payloads + RAT ??

FAKE METHODS ?

G2A?

Spoiler ([Click to View](#))

There are lot of G2A scams, I'm sharing only few of them :

<https://hackforums.net/showthread.php?tid=6277117>

<https://hackforums.net/showthread.php?tid=6260758>

<https://hackforums.net/showthread.php?tid=6267642>

<https://hackforums.net/showthread.php?tid=6269162>

Advance-fee Scam?

<https://hackforums.net/showthread.php?tid=6278385>

0-day 0-click for 800\$?

<https://hackforums.net/showthread.php?tid=6289947>

Hidden Wiki Scam?

<https://hackforums.net/showthread.php?tid=6296845>

MALWARE REMOVAL ?

<https://hackforums.net/showthread.php?tid=6267544>

OTHER ?

<https://hackforums.net/showthread.php?tid=6285798> > How to conduct a PDF File Analysis

<https://hackforums.net/showthread.php?tid=6286454> > How to conduct PDF and Word files Analysis

<https://hackforums.net/showthread.php?tid=6286517> > Backdoored Stealerium stealer

ONLINE TOOLS ?

□ <https://www.virustotal.com/gui/home/upload>

□ <https://www.hybrid-analysis.com/>

□ <https://tria.ge/>

□ <https://www.abuseipdb.com/>

□ <https://any.run>

□ <https://unpac.me>

ttbr0 - August 25, 2024, 2:46 am

this sounds like a fun idea. id be happy to contribute where i can and provide some mentoring for malware reverse engineering.

Tha Sneak - August 25, 2024, 3:23 am

As one of the old members of the MRT, I plan on being active assisting with malware removal issues and computer issues. Perhaps, I might even teach as I'm very rusty and a lot has changed since then 12 years ago. I would be willing to help with anything to keep it going.

Bastille - August 25, 2024, 6:56 am

(Aug 25, 2024 02:46 AM)ttbr0 Wrote: [\[CITE\]](#) this sounds like a fun idea. id be happy to contribute where i can and provide some mentoring for malware reverse engineering.

That's awesome man ! If you want to create some threads about it feel free, I'll link them here, I'll let you know about the new malware that members are trying to spread here, I could start with a basic analysis, then you could go further with the existing

(Aug 25, 2024 03:23 AM)Tha Sneak Wrote: [\[CITE\]](#) As one of the old members of the MRT, I plan on being active assisting with malware removal issues and computer issues. Perhaps, I might even teach as I'm very rusty and a lot has changed since then 12 years ago. I would be willing to help with anything to keep it going.

I wish I knew HF before to learn with you guys haha, but I'm glade that you're back it will be valuable for HF for sure, by any chance if you still have materials used during the MRT learning I'm interested

ttbr0 - August 25, 2024, 7:12 am

(Aug 25, 2024 06:56 AM)Bastille Wrote: [\[CITE\]](#) That's awesome man ! If you want to create some threads about it feel free, I'll link them here, I'll let you know about the new malware that members

are trying to spread here, I could start with a basic analysis, then you could go further with the existing
we can figure something out and collab ?

Tha Sneak - August 25, 2024, 7:19 am

(Aug 25, 2024 06:56 AM)Bastille Wrote: [\[CITE\]](#) I wish I knew HF before to learn with you guys haha, but I'm glad that you're back it will be valuable for HF for sure, by any chance if you still have materials used during the MRT learning I'm interested

As far as I know a majority if not all of it is lost. However, I believe I still have the laptop I used back then buried somewhere so its possible I can dump the hard drive and maybe I get lucky and have some stuff left over. I know I've been searching for my malware removal tool I created like 12 years ago I was going to revisit it as well, but I've already started back over again still the source would save me a ton of time.

I know I had a shit ton of material I've been AWOL on all the forums I used to be affiliated with and am no longer staff so I lost access to the forum side of things. I'm a relic of the past to most as there's been a whole new crew come in it seems. I may go through one of the updated classes in order to re-write/update the material. It's a lot of work for one person though so some help would be grateful if I ever go that route.

I do know the whole malware ecosystem has changed its no where near like it used to be and a lot of people aren't getting infected as frequently due to modern systems.

It seems Android Phones are a target now too and to be honest I don't have a clue how to fix that lol.

Bastille - August 31, 2024, 1:25 am

[ttbr0 Tha Sneak](#) Just added an analysis to the thread :
<https://hackforums.net/showthread.php?tid=6278798>

OP shares a dozen of tools on his website that are backdoored, I can provide you the link if you want

Let me know what you think about the analysis ?

ttbr0 - August 31, 2024, 11:12 pm

(Aug 31, 2024 01:25 AM)Bastille Wrote: [\[CITE\]](#) [ttbr0 Tha Sneak](#) Just added an analysis to the thread : <https://hackforums.net/showthread.php?tid=6278798>

OP shares a dozen of tools on his website that are backdoored, I can provide you the link if you want

Let me know what you think about the analysis ?
good job, not much to add on to it. it seems pretty obviously malicious.

Bastille - September 2, 2024, 9:00 pm

(Sep 2, 2024 03:28 PM)Snyke Wrote: [\[CITE\]](#) <https://any.run>
<https://unpac.me>

<3

Didn't know unpac.me, thanks for the share ! I'm adding it to the thread

Hope to see you around, with your new hat ;)

recede - September 9, 2024, 1:09 am

I just came to this forum and I want to survive here safely. It looks like the owner told some identified malicious links, and some tools to help with testing. Please point out if I've misunderstood anything, I'm still a noob. Also any points that a noob needs to be aware of would be appreciated.

Bastille - September 9, 2024, 8:39 am

(Sep 9, 2024 01:09 AM)recede Wrote: [\[CITE\]](#) I just came to this forum and I want to survive here safely. It looks like the owner told some identified malicious links, and some tools to help with testing. Please point out if I've misunderstood anything, I'm still a noob. Also any points that a noob needs to be aware of would be appreciated.

Hello, welcome to HF, few tips :

- stay on HF, don't go out of HF with people proposing you to go on Discord or Telegram, they are likely scammers
- don't download and execute tools before being sure they're safe
- if you have a doubt feel free to report me the content, I'll run an analysis and let you know if it's safe or not
- read the [Help Docs](#), very important

Important too, don't hijack someone's else thread, if you need something open your own thread, this one is dedicated to malicious content, malware analysis, you can ask here to check tools or threads for example.

Regulus - October 9, 2024, 6:39 am

The savior of HF!

Keep up the amazing job!

Bastille - October 11, 2024, 6:16 am

(Oct 9, 2024 06:39 AM)Regulus Wrote: [\[CITE\]](#) The savior of HF!

Keep up the amazing job!

Thanks mate ! Hope this will be useful too for people who want to dive in the malware analysis field as they have practical examples on how to proceed

Bastille - October 11, 2024, 6:41 am

(Oct 11, 2024 06:28 AM)Sox Wrote: [\[CITE\]](#) Amazing thread, and I salute you all for your service helping keep others safe from malicious links!

Thank you bro, and thanks for the kind words as well

I hope this can also help those who are getting into malware analysis, providing them some resources and step by step examples

PopeyeToolsUK - January 12, 2025, 12:23 am

Amazing thread, and I salute you all for your service

ttbr0 - January 12, 2025, 9:44 pm

it would be cool to start a community project that automates some level of analysis either through online sandboxes, querying vt or even creating a custom pipeline with a self hosted, customizable sandbox with additional analysis programs that we could develop inhouse.

Bastille - January 13, 2025, 2:28 am

(Jan 12, 2025 01:23 AM)PopeyeToolsUK Wrote: [\[CITE\]](#) Amazing thread, and I salute you all for your service

Thanks buddy, HF is a good place, Staff is doing its best to keep it clean and safe !

(Jan 12, 2025 04:48 PM)m0hx Wrote: [\[CITE\]](#) Can i join the hunters team? :D got my VMs ready :o Of course bro ! There are two projects under construction, one from BH (with this thread) and the other from Fallen, will share you the info in convo :)

(Jan 12, 2025 10:44 PM)ttbr0 Wrote: [\[CITE\]](#) it would be cool to start a community project that automates some level of analysis either through online sandboxes, querying vt or even creating a custom pipeline with a self hosted, customizable sandbox with additional analysis programs that we could develop inhouse.
That would be very cool !

Miracula - January 13, 2025, 4:29 am

Happy to see I could help with my thread, thank you for the this great post Bastille!

7 - January 13, 2025, 4:36 am

(Aug 3, 2024 12:32 AM)Bastille Wrote: [\[CITE\]](#)
? Malware Analysis Corner ?

After spending a few years helping forum members with security-related issues, particularly malware removal, Brotherhood came to me with the idea of enhancing the [White Hat section](#), we were looking for solutions to share our knowledge related to this field, to bring help, guidance, assistance, and offer some services. For those who knew the [MRT \(Malware Removal Team\)](#) and members related to this group, the idea is to bring back what they used to do here and to go even further.

This thread is part of one of the many initiatives aimed at improving the forum experience, particularly in the white hat section.

There are several ideas behind this thread. Giving concret examples on how a malware analysis is conducted, how to find artifacts, what tools are used, ...

Making a place where members could share their knowlege and discuss about malware analysis which is not often addressed

It's also a good opportunity to show the community that the Staff is primarily here to assist and protect the members.

We decided to take this approach further by analyzing the programs, links, and files shared by some members to ensure they do not pose a threat to the community. I believe this adds value to my role as Staff, although I would have done the same if I were not Staff. The advantage is that I have the ability to remove suspicious elements while they are being analyzed.

INFECTED LINKS ?

<https://hackforums.net/showthread.php?tid=6271578> > Crypto miner ?

<https://hackforums.net/showthread.php?tid=6269930> > Stealer ?

<https://hackforums.net/showthread.php?tid=6269932> > Stealer ?

<https://hackforums.net/showthread.php?tid=6274196> > Stealer ? and Crypto miner ?

<https://hackforums.net/showthread.php?tid=6274326> > RAT ?

<https://hackforums.net/showthread.php?tid=6276362> > Stealer ?

<https://hackforums.net/showthread.php?tid=6278798> > RAT ?

<https://hackforums.net/showthread.php?tid=6254162> > under review

<https://hackforums.net/showthread.php?tid=6238357> > Collection of infected ?

<https://hackforums.net/showthread.php?tid=6268885> > Collection of infected ?

<https://hackforums.net/showthread.php?tid=6281297> > Fake tool, scam ?

<https://hackforums.net/showthread.php?tid=6280678> > BTC Clipper ?

<https://hackforums.net/showthread.php?tid=6281838> > BTC Clipper ?

<https://hackforums.net/showthread.php?tid=6278565&pid=62532703#pid62532703> > BTC Clipper ?

<https://hackforums.net/showthread.php?tid=6282360> > Ransomware ?

<https://hackforums.net/showthread.php?tid=6283230> > Malicious Chrome extension ?

<https://hackforums.net/showthread.php?tid=6269480&highlight=txt> > Hidden malicious files ?

FAKE METHODS ?

G2A?

Spoiler ([Click to View](#))

There are lot of G2A scams, I'm sharing only few of them :

<https://hackforums.net/showthread.php?tid=6277117>

<https://hackforums.net/showthread.php?tid=6260758>

<https://hackforums.net/showthread.php?tid=6267642>

<https://hackforums.net/showthread.php?tid=6269162>

Advance-fee Scam?

<https://hackforums.net/showthread.php?tid=6278385>

MALWARE REMOVAL ?

<https://hackforums.net/showthread.php?tid=6267544>

OTHER ?

<https://hackforums.net/showthread.php?tid=6285798> > How to conduct a PDF File Analysis

<https://hackforums.net/showthread.php?tid=6286454> > How to conduct PDF and Word files

Analysis

<https://hackforums.net/showthread.php?tid=6286517> > Backdoored Stealerium stealer

ONLINE TOOLS ?

- <https://www.virustotal.com/gui/home/upload>
- <https://www.hybrid-analysis.com/>
- <https://tria.ge/>
- <https://www.abuseipdb.com/>
- <https://any.run>
- <https://unpac.me>

@7@
[Hackers](#)

You have to mention me

latencyx - January 14, 2025, 12:22 pm

What a beautiful work to see haha, the number of l33t users spreading infected tools is impressive, I don't know why

Bastille - January 15, 2025, 12:46 am

(Jan 14, 2025 01:22 PM)latencyx Wrote: [\[CITE\]](#) What a beautiful work to see haha, the number of l33t users spreading infected tools is impressive, I don't know why

Thanks man ! Sometimes they think that with an upgraded account I'll not take a look at what they share, or sometimes they share it because they found it somewhere else and didn't take a look at it. It's not always intentionally malicious

Since I've started this thread/activity I feel that there are less people trying to spread infected programs. I think they don't bother anymore creating new accounts for this, as they're quickly banned

Tyr - January 16, 2025, 12:26 pm

If you ever need help with this in the future to maintain a safe environment for members please feel free to shoot me a DM. Thank you for doing this.

Bastille - January 16, 2025, 12:35 pm

(Jan 13, 2025 05:29 AM)Miracula Wrote: [\[CITE\]](#) Happy to see I could help with my thread, thank you for the this great post Bastille!

It was definitely a good catch from you ! Really nice buddy ^^ I had to put your thread here haha

(Jan 16, 2025 01:26 PM)Tyr Wrote: [\[CITE\]](#) If you ever need help with this in the future to maintain a safe environment for members please feel free to shoot me a DM. Thank you for doing this.

Thanks buddy ! I'll let you know !

Bastille - February 4, 2025, 2:55 am

Latest analysis : <https://hackforums.net/showthread.php?tid=6288934>

Pr0m3th3us - March 7, 2025, 12:56 am

Thank you for your efforts in putting this thread together and keeping it updated. Very handy.

Bastille - March 7, 2025, 1:19 am

(Mar 7, 2025 01:56 AM)SIM-2567248 Wrote: [\[CITE\]](#) Thank you for your efforts in putting this thread together and keeping it updated. Very handy.

Thanks and you're welcome buddy ! MRT-X group is going to add a lot of more content like that, to protect HF members, and also to teach how to conduct malware analysis

Bastille - April 18, 2025, 10:43 am

Just provided an analysis for the following thread :

<https://hackforums.net/showthread.php?tid=6296196> , verdict = RAT

Bastille - April 20, 2025, 9:55 pm

Just provided an analysis for the following thread :

<https://hackforums.net/showthread.php?tid=6296631> , verdict = Loader detected

VultureQuake - November 16, 2025, 9:54 pm

Thanks for the amazing info.

Bastille - November 18, 2025, 10:48 pm

(Nov 16, 2025 10:54 PM)VultureQuake Wrote: [\[CITE\]](#) Thanks for the amazing info.

Thanks for commenting, if you appreciate malware analysis content and have questions, let me know