

Forum: [Hack Forums](#)

Thread: [Proper way to analyze files?](#)

Doz1 - December 16, 2013, 2:52 am

Lets say someone sends me an executable file, how can I make sure it's not malware?

I'm pretty sure just because my AV or a website like VirusTotal says it's 100% clean, doesn't mean it really is.

What steps or things would I need to do to make sure it's not malware or something?

Aura - December 16, 2013, 3:26 am

Upload it on Anubis and analyze the results. It will tell you (or at least, give you hints) of if the file is malicious or not.

<http://anubis.iseclab.org/>

Doz1 - December 16, 2013, 3:34 am

(Dec 16, 2013 04:26 AM)Aur? Wrote: [\[CITE\]](#) Upload it on Anubis and analyze the results. It will tell you (or at least, give you hints) of if the file is malicious or not.

<http://anubis.iseclab.org/>

So, that's it? If there's nothing suspicious in Anubis, does that mean it's clean?

phybe? - December 16, 2013, 3:54 am

You can also run it via sandboxie or on a virtual machine and see what happens when you run the .exe there. Through either of those, you are running it in an isolated environment.

Doz1 - December 16, 2013, 4:15 am

(Dec 16, 2013 04:54 AM)phybe? Wrote: [\[CITE\]](#) You can also run it via sandboxie or on a virtual machine and see what happens when you run the .exe there. Through either of those, you are running it in an isolated environment.

Yeah, but what if the .exe works as expected?

I just want to know the methods/steps a white hat or any malware checker would do to analyze it properly, to make sure it's 100% clean.

John_Gacy - December 16, 2013, 4:31 am

I trust Anubis and Sandboxie usually gets the job done, but I would be interested too if there was any other methods excluding Virustotal and what not.

Doz1 - December 16, 2013, 4:40 am

(Dec 16, 2013 05:31 AM)John_Gacy Wrote: [\[CITE\]](#) I trust Anubis and Sandboxie usually gets the job done, but I would be interested too if there was any other methods excluding Virustotal and what not.

Yeah, it probably does get the job done against simple viruses/malware.

But what about actual hidden viruses, like let's say some knowledgeable torrent uploader where all his programs get thousands of seeders.

Maybe there's a line of code in one of his programs that stealthy downloads and executes a malicious file on your computer days after using the program. What then?

Gustav. - December 16, 2013, 5:10 am

(Dec 16, 2013 05:15 AM)Doz1 Wrote: [\[CITE\]](#) Yeah, but what if the .exe works as expected?

I just want to know the methods/steps a white hat or any malware checker would do to analyze it properly, to make sure it's 100% clean.

If you're wanting to learn the way of a White hat then you should always be prepared by having a Firewall implemented as your security defense line. Firewalls will block any malicious or harmful content that your computer system encounters. I personally use Comodo Firewall-- Works like a charm. Consider on installing a firewall mate, they'll do the job. Instead of having to upload it to Sandboxie or Virtual machine, your firewall can just block what ever seems to be a threat.

Doz1 - December 16, 2013, 5:38 am

(Dec 16, 2013 06:10 AM)Chief? Wrote: [\[CITE\]](#) If you're wanting to learn the way of a White hat then you should always be prepared by having a Firewall implemented as your security defense line. Firewalls will block any malicious or harmful content that your computer system encounters. I personally use Comodo Firewall-- Works like a charm. Consider on installing a firewall mate, they'll do the job. Instead of having to upload it to Sandboxie or Virtual machine, your firewall can just block what ever seems to be a threat. No, I'm wondering what someone would do to properly analyze a file to make sure it's 100% clean.

I just said white hat because I don't know what else to call a malware 'analyzer'.

Gustav. - December 16, 2013, 5:41 am

(Dec 16, 2013 06:38 AM)Doz1 Wrote: [\[CITE\]](#) No, I'm wondering what someone would do to properly analyze a file to make sure it's 100% clean.

I just said white hat because I don't know what else to call a malware 'analyzer'.

<http://anubis.iseclab.org/> would be appropriate for scanning the files before you go ahead and execute them. And Comodo Firewall allows you to scan files as well. If you choice, you can always use a Virtual machine or sandboxie.

Doz1 - December 16, 2013, 5:46 am

(Dec 16, 2013 06:41 AM)Chief? Wrote: [\[CITE\]](#) <http://anubis.iseclab.org/> would be appropriate for scanning the files before you go ahead and execute them. And Comodo Firewall allows you to scan files as well. If you choice, you can always use a Virtual machine or sandboxie. Sorry, but I need a proper reply from some software engineer or something.

What if Anubis or those tools didn't exist? Are you saying just because it's clean on Anubis, means it really is?

The file could be safe at first, but then 2 hours later it's hard-coded to download a malicious file on your computer and execute it.

Anubis only shows what runs/executes when they start the file.

Gustav. - December 16, 2013, 5:51 am

(Dec 16, 2013 06:46 AM)Doz1 Wrote: [\[CITE\]](#) Sorry, but I need a proper reply from some software engineer or something.

What if Anubis or those tools didn't exist? Are you saying just because it's clean on Anubis, means it really is?

The file could be safe at first, but then 2 hours later it's hard-coded to download a malicious file on your computer and execute it.

Anubis only shows what runs/executes when they start the file.

Lmao-- What you're not getting is that these file scanners like Anubis are meant to analyze the file in depth. And if you were to get a firewall, you wouldn't have to worry about anything like that ever

happening-- The firewall will block it right away if it was Malicious.

If you're that paranoid then I'd say just run the file through Sandboxie or Virtual machine.

What file/program are you trying to see if it's safe or not?

Aura - December 16, 2013, 5:54 am

(Dec 16, 2013 06:46 AM)Doz1 Wrote: [\[CITE\]](#) Sorry, but I need a proper reply from some software engineer or something.

What if Anubis or those tools didn't exist? Are you saying just because it's clean on Anubis, means it really is?

The file could be safe at first, but then 2 hours later it's hard-coded to download a malicious file on your computer and execute it.

Anubis only shows what runs/executes when they start the file.

Listen, you won't really get an answer from a "Software Engineer" here. The best answers you can get are from Grim, Chief and Phyber. If they say that Anubis does the job and that you know how to analyze a file, then you're good. They are the real experts here. Grim works in Malwares and Viruses Analysis and Removal, so if you want his opinion, I can ask him to post here. But don't expect to get an answer from a security expert who spent 30 years and plus working in this domain. Also, if you get infected by such a virus/malware, then you didn't think enough before downloading whatever you downloaded. The signs of an infected file, torrent, download, etc. are pretty obvious. So here's what you can do :

- Run the file in Anubis;
- Execute in Sandboxie in a Virtual Machine;
- Execute it directly in your Virtual Machine and check what happens, if you notice any changes;

But be careful, some malwares have the ability to escape the VM and infect the host computer, so you would do it at your own risk.

Doz1 - December 16, 2013, 5:56 am

(Dec 16, 2013 06:51 AM)Chief? Wrote: [\[CITE\]](#) Lmao-- What you're not getting is that these file scanners like Anubis are meant to analyze the file in depth. And if you were to get a firewall, you wouldn't have to worry about anything like that ever happening-- The firewall will block it right away if it was Malicious.

If you're that paranoid then I'd say just run the file through Sandboxie or Virtual machine.

What file/program are you trying to see if it's safe or not?

Okay, but are those the only things you'd do to make sure it's 100% clean?

So far all I've heard on these forums - VirusTotal+Anubis+Sandbox it.

I mean there has to be more, what would a computer scientist working for the FBI do?

I'm sure he wouldn't just go on Anubis, scan it and run it in a VM. There has to be more. I'm assuming he'd reverse engineer the file, but what else?

Aura - December 16, 2013, 5:58 am

(Dec 16, 2013 06:56 AM)Doz1 Wrote: [\[CITE\]](#) Okay, but are those the only things you'd do to make sure it's 100% clean?

So far all I've heard on these forums - VirusTotal+Anubis+Sandbox it.

I mean there has to be more, what would a computer scientist working for the FBI do?

I'm sure he wouldn't just go on Anubis, scan it and run it in a VM. There has to be more. I'm assuming he'd reverse engineer the file, but what else?

Okay, cut the trolling right here. Do you REALLY expect us to know how the FBI forensics analyze a malware and a virus ? Let's be honest, NO ONE knows here what they do. This forum isn't the FBI lab or the NSA lab, it's mostly a hacking forum. This section is meant for people who want to learn how to protect their computer for everyday use, not how to analyze files like people in CSI. Sorry if my answer is rough, but I think you're asking a little too much here or you don't really understand what this forum is.

Doz1 - December 16, 2013, 6:06 am

(Dec 16, 2013 06:58 AM)Aur? Wrote: [\[CITE\]](#) Okay, cut the trolling right here. Do you REALLY expect us to know how the FBI forensics analyze a malware and a virus ? Let's be honest, NO ONE knows here what they do. This forum isn't the FBI lab or the NSA lab, it's mostly a hacking forum. This section is meant for people who want to learn how to protect their computer for everyday use, not how to analyze files like people in CSI. Sorry if my answer is rough, but I think you're asking a little too much here or you don't really understand what this forum is. Sorry, I just expected people here to be smarter when it comes to stuff like this.

You'd expect certain people with 10k+ posts that spend years on a hacking forums, would know a little more than just saying use Anubis+Sandboxie.

I'm not asking for the exact steps the police does, just a brief explanation on how to properly analyze a file without these public tools.

Aura - December 16, 2013, 6:11 am

(Dec 16, 2013 07:06 AM)Doz1 Wrote: [\[CITE\]](#) Sorry, I just expected people here to be smarter when it comes to stuff like this.

You'd expect certain people with 10k+ posts that spend years on a hacking forums, would know a little more than just saying use Anubis+Sandboxie.

I'm not asking for the exact steps the police does, just a brief explanation on how to properly analyze a file without these public tools.

I'll tell you something : post count, Rep, prestige, award, it means nothing on HackForums. Even if someone have 10k posts here, what tells you there's not 9,999 posts in the Gaming area and 1 post here ? And most people here are kids aged between 14-16 years, so even if they were spending "years" on a "hacking" forum, it doesn't mean they have the knowledge to know how to analyse a file like a FBI forensics.

If you want a Security Software Engineer to explain you step by step how to analyze a file, then you should go in the Reverse Engineering and File Disassembling section. There people will tell you exactly how to analyze a file. But you'll have to know a programming language or even more to analyze the code, that's for sure.

Doz1 - December 16, 2013, 6:13 am

(Dec 16, 2013 07:11 AM)Aur? Wrote: [\[CITE\]](#) I'll tell you something : post count, Rep, prestige, award, it means nothing on HackForums. Even if someone have 10k posts here, what tells you there's not 9,999 posts in the Gaming area and 1 post here ? And most people here are kids aged between 14-16 years, so even if they were spending "years" on a "hacking" forum, it doesn't mean they have the knowledge to know how to analyse a file like a FBI forensics.

If you want a Security Software Engineer to explain you step by step how to analyze a file, then you should go in the Reverse Engineering and File Disassembling section. There people will tell you exactly how to analyze a file. But you'll have to know a programming language or even more to analyze the code, that's for sure. Yeah, I'll just PM a friend.

Thanks for the help, anyways.

