

Forum:[Hack Forums](#)

Thread: [? ---Online Scanners and Malware Analysers--- ?](#)

CustomiZer - March 24, 2010, 2:24 am

Here is a compilation for a list of Online Scanners and Malware Analysers.

URL : [Virus Total](#)

About :

[img]http://i40.[censored].com/6yk504.png[/img]

VirusTotal is a service that analyzes suspicious files and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines.

Specs:Free, independent service

Use of multiple antivirus engines

Real-time automatic updates of virus signatures

Detailed results from each antivirus engine

Real time global statistics

URL : [Jotti's Malware Scan](#)

About :

[img]http://i39.[censored].com/21abgaf.jpg[/img]

Jotti's malware scan is a free online service that enables you to scan suspicious files with several anti-virus programs. Scanners used are Linux versions; detection differences with Windows versions of the same scanners may occur due to implementation differences. There is a 20MB limit per file. Keep in mind that no security solution offers 100% protection, not even when it uses several anti-virus engines (for example, this scan service).

Files uploaded here are shared with anti-virus companies so detection accuracy of their anti-virus products can be improved. Read more about this in our privacy policy. If you do not want your files to be distributed, please do not send them at all.

URL : [Anubis : Analysing Unknown Binaries](#)

About :

[img]http://i41.[censored].com/2enn3x0.jpg[/img]

Anubis is a tool for analyzing the behavior of Windows PE-executables with special focus on the analysis of malware. Execution of Anubis results in the generation of a report file that contains enough information to give a human user a very good impression about the purpose and the actions of the analyzed binary. The generated report includes detailed data about modifications made to the Windows registry or the file system, about interactions with the Windows Service Manager or other processes and of course it logs all generated network traffic. The analysis is based on running the binary in an emulated environment and watching i.e. analyzing its execution. The analysis focuses

on the security-relevant aspects of a program's actions, which makes the analysis process easier and because the domain is more fine-grained it allows for more precise results. It is the ideal tool for the malware and virus interested person to get a quick understanding of the purpose of an unknown binary.

URL : [ThreatExpert](#)

About :

[img]http://i39.[censored].com/332uxhx.jpg[/img]

ThreatExpert (patent pending) is an advanced automated threat analysis system (ATAS) designed to analyze and report the behavior of computer viruses, worms, trojans, adware, spyware, and other security-related risks in a fully automated mode.

The ThreatExpert system produces reports with the level of technical detail that matches or exceeds antivirus industry standards such as those found in online virus encyclopedias.

URL : [VirusSCAN](#)

About :

[img]http://i40.[censored].com/vh6mhl.jpg[/img]

VirSCAN.org is a FREE on-line scan service, which checks uploaded files for malware, using antivirus engines, indicated in the VirSCAN list. On uploading files you want to be checked, you can see the result of scanning and how dangerous and harmful/harmless for your computer those files are.

URL : [UploadMalware](#)

About :

[img]http://i42.[censored].com/1zv5vg9.jpg[/img]

UploadMalware.com is an easy way for you to submit files for analysis by anti-malware and security professionals.

URL : [CWSandbox](#)

About :

[img]http://i43.[censored].com/fm0txw.jpg[/img]

Sunbelt CWSandbox provides fast analysis of virus, spyware, trojan, or other malware samples. CWSandbox enables the automatic collection of malware from different inputs including Nepenthes, a web server/interface, or a directory.

Rapidly analyze behavior of malware - including infected trojans, Office documents, browser helper objects (BHOs), malicious URLs and more - by executing the code inside a controlled environment, the Sunbelt malware sandbox!

URL : [Norman Sandbox](#)

About :

[img]http://i41.[censored].com/20uqq08.jpg[/img]

Norman Sandbox offers - Free uploads of program files that you suspect are malicious or infected

by malicious components, and instant analysis by Norman SandBox. The result is also sent you by email.

In-depth information about the analysis performed by Norman SandBox of each malicious file that is uploaded. Search facility in all analyses after Registry keys, file names, etc.

Comprehensive statistics of files that are uploaded to Norman SandBox center during the latest day, week and month. You will then be able to see tendencies in the creation of malicious software.

URL : [Joebox](#)

About :

[img]http://i41.[censored].com/2m3r3tf.jpg[/img]

Joebox is a simple sandbox application with a unique special concept. It is designed for automatic behaviour analysis of malware on Windows based operating systems.

URL : [Microsoft Malware Protection](#)

About :

[img]http://i42.[censored].com/acejup.jpg[/img]

The Microsoft Malware Protection Center (MMPC) provides world class antimalware research and response capabilities that support Microsoft's range of security products and services. With laboratories in multiple locations around the globe the MMPC is able to respond quickly and effectively to new malicious and potentially unwanted software threats wherever and whenever they arise.

URL : [SuspectFile](#)

About :

[img]http://i43.[censored].com/1znvf3n.jpg[/img]

It not english.? I don't understand it ?. Use a translator if you are interested very much

URL : [F-Secure Sample Analysis System](#)

About :

[img]http://i41.[censored].com/6ygrjk.jpg[/img]

It requires registration for a person to submit samples, but registration is free ?

URL : [Wepawet](#)

About :

[img]http://i41.[censored].com/2ro70qf.jpg[/img]

Wepawet is a service for detecting and analyzing web-based malware. It currently handles Flash and JavaScript files. Things you can do with Wepawet -Determine if a page or file is malicious

Analyze a malicious resource

Identify the attacks launched by a malicious resource

URL : [Eureka Malware Analysis Page](#)

About :

[img]http://i43.[censored].com/2m5juxs.jpg[/img]

Eureka is a binary static analysis preparation framework. It implements a novel binary unpacking strategy based on statistical bigram analysis and coarse-grained execution tracing. Eureka incorporates advanced API deobfuscation capabilities to facilitate the structural analysis of the underlying malware logic. For each uploaded binary, the Eureka service will attempt to unpack and disassemble the binary, and will produce an annotated callgraph, subroutine/data index page, strings summary, and list of embedded DNS entries.

URL : [Comodo Instant Malware Analysis](#)

About :

[img]http://i42.[censored].com/j8och4.jpg[/img]

This is a secure malware analysis system which gives a detailed report of what an executable does including registry edits and creating of folders and deleting them.

URL : [NoVirusthanks](#)

About :

[img]http://i43.[censored].com/301lvlc.jpg[/img]

Free service that allows users to upload and scan a file with 24 Antivirus Engines. Users can also scan a website url or a remote file with the option Scan Web Address.

URL : [VirusTrap](#)

About :

[img]http://i41.[censored].com/nfgpiu.jpg[/img]

VirusTrap is a commercial service for penetration testers, network auditors, system administrators who need to analyze unknown binaries during their work. Our scanner was made to help computer users identifying malicious files by scanning them with 25 antivirus engines.

URL : [Online Virus Scan](#)

About :

[img]http://i42.[censored].com/2ithb2h.jpg[/img]

VirusChief is a service that analyzes suspicious files and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines.

Specs:

- Free, independent service
- Use of multiple antivirus engines
- Real-time automatic updates of virus signatures
- Detailed results from each antivirus engine

- Link output
- BB-Code output
- File deletion after the scan-report was generated

URL : [FortiGaurd](#)

About :

[img]http://i39.[censored].com/2uo48z9.jpg[/img]

Yet another malware scanner which lets you upload unknown binaries and gives you a report about them via email.

URL : [Filterbit - OPSWAT Metascan](#)

About :

[img]http://i40.[censored].com/sm3lms.jpg[/img]

Powered by OPSWAT Metascan®, Filterbit™ is a free service where you can upload files for scanning, analysis and identification by multiple antivirus engines. Filterbit facilitates rapid detection of viruses, trojans, worms and other malware that may be contained within your uploaded files. In many cases, Filterbit can also scan, analyze and individually identify multiple files contained within a file archive such as Winzip, WinRar, PKZip and other types. Filterbit also analyzes the types of each uploaded file such as Microsoft Word, PDF, TXT and other types and reports this in a human readable format. Filterbit currently uses Metascan® antivirus engines from CA (Computer Associates), Norman Data Defense Systems, ClamAV, ESET, Microworld and VirusBuster.

Norman Sadbox to Norman Sandbox

URL : [Scan4You](#)

About :

[img]http://i43.[censored].com/30ksg8h.png[/img]

This service is about to help you in anonymous check of different anti-virus system. This check will be made by numbers of anti-virus system and no reports will be send to developers of this anti-virus system. You can be fully sure that your files will not be send to anti-virus databases. All reporting system in our version of anti-virus engines was disabled MicrosoftSpyNet, ESET ThreatSense.Net Early Warning System etc. Updates of all anti-viruses made each hour, most of main anti-virus system made updates in real -time.

We give you maximum speed of scanning, 10 files will be scanned by all anti-virus system starting from 30 second.

We support periodic checks. You need to select amount of time that check will be happened, and select method system will contact you after found something suspicious.

DISCLAIMER : These Scanners or Malware Analysers are not for checking FUDness of your viruses. I do not know any information about submitting of samples to AV companies, so if it is sensitive data upload at your own risk. These are sites for people who wish to remain secure from malware and unwanted spyware or when checking out unknown binaries.

If I have missed some please post here and I'll add them up ?
-updated on April 2010

August - March 24, 2010, 2:28 am

Wow nicee thanks for this, very help full :D

MrAlex - March 24, 2010, 2:28 am

Very nice helpful , thanks.

iDope -- - March 24, 2010, 2:29 am

That is a really nice compilation!

:)

Well, don't go on scanning stubs there though!

:P

[Fud] Boy - March 24, 2010, 2:29 am

nice Work Dude u rock

<3

flAmingw0rm - March 24, 2010, 2:31 am

<http://www.virus.org/>

<http://virus-trap.org/>

<http://www.viruschief.com/>

You missed them. Should be added. ?

Great topic, btw. Good job!

TheGiantLeprechaun - March 24, 2010, 2:32 am

Nice little thread you got here, I'm gonna bookmark this for sure :D

mandi - March 24, 2010, 2:48 am

sounds good mate,...

thanks for sharing this, and if possible can you please tell which are all the sites that send's the files to anti-virus companies with-out asking users?

for ex sites like virustotal...

SUPERIOR - March 24, 2010, 4:12 am

amazing job bro, bookmarked

but you missed

avhide.com

www.filterbit.com

http://www.fortiguard.com/antivirus/virus_scanner.html

thanks bro alot, hope you still have more :D

Paradoxum - March 24, 2010, 5:56 am

Valiant already made the same thread but great job nevertheless.

CustomiZer - March 24, 2010, 5:59 am

(Mar 24, 2010 05:56 AM)Paradoxum Wrote: [\[CITE\]](#) Valiant already made the same thread but great

job nevertheless.

Oh..I probably did not search enough before starting out. :P

(Mar 24, 2010 04:12 AM)SUPERIOR Wrote: [\[CITE\]](#) amazing job bro, bookmarked but you missed

www.filterbit.com

http://www.fortiguard.com/antivirus/virus_scanner.html

thanks bro alot, hope you still have more :D

added them to the list ;)

total of 20 scanners ?

Paradoxum - March 24, 2010, 6:18 am

It is alright. Yours focuses on online file scanners.

CustomiZer - March 24, 2010, 6:23 am

(Mar 24, 2010 06:18 AM)Paradoxum Wrote: [\[CITE\]](#) It is alright. Yours focuses on online file scanners. Yes ? all of mine are online.

Paradoxum - March 24, 2010, 6:26 am

(Mar 24, 2010 06:23 AM)icyberhack Wrote: [\[CITE\]](#) Yes ? all of mine are online.

?. All of yours are online file scanners. His thread deals with system scanners like ESET.

CustomiZer - March 24, 2010, 6:31 am

(Mar 24, 2010 06:26 AM)Paradoxum Wrote: [\[CITE\]](#) ?. All of yours are online file scanners. His thread deals with system scanners like ESET.

Mine not really AV's.

They are more like binary analysers.

Example :if some wants a report of an exe which he is suspicious of.

<http://camas.comodo.com/> >> this could give a detailed report of what it does like what folders are created, which reg keys are edited...etc (though the data may not be 100% accurate)

Paradoxum - March 24, 2010, 6:33 am

That is what I was saying.

crack_that - March 24, 2010, 6:39 am

thanks bro very usefull thread

CustomiZer - March 26, 2010, 6:15 am

BUMPing this up for those in need

darkhack - March 26, 2010, 6:34 am

Awesome! Don't forget the ESET online scanner though :O

Paradoxum - March 26, 2010, 7:24 am

It is ESET, check your spelling.

darkhack - March 26, 2010, 7:33 am

Sorry, the post has been fixed. Thanks.

Ssleuth - March 26, 2010, 8:27 am

Nice sharing here. Thanks.

CustomiZer - April 9, 2010, 9:51 am

You are welcome ?

Far - April 9, 2010, 9:52 am

URL : Norman Sadbox

You spelled Sandbox wrong.

CustomiZer - April 9, 2010, 10:00 am

(Apr 9, 2010 09:52 AM)Far Wrote: [\[CITE\]](#) URL : Norman Sadbox

You spelled Sandbox wrong.

I wish I could edit my thread. ?

I have somethings to add as well.

I cannot since I'm just a normal member.

Far - April 9, 2010, 10:09 am

PM a mod with the entire thread edited and ask them to edit it for you.

CustomiZer - April 9, 2010, 11:05 am

(Apr 9, 2010 10:09 AM)Far Wrote: [\[CITE\]](#) PM a mod with the entire thread edited and ask them to edit it for you.

[kutmustakurt](#) was kind enough to offer me to change the thread for me.

Added a new scanner and updated the spelling error. ?

Paradoxum - April 10, 2010, 4:59 am

You can always ask the friendly HJT-Staff members. ?

CustomiZer - April 10, 2010, 5:53 am

(Apr 10, 2010 04:59 AM)Paradoxum Wrote: [\[CITE\]](#) You can always ask the friendly HJT-Staff members. ?

Thank You very much.

cobija - April 10, 2010, 12:20 pm

(Mar 24, 2010 02:29 AM)jCore™ Wrote: [\[CITE\]](#) That is a really nice compilation!

:)

Well, don't go on scanning stubs there though!

:P

Well, if you use novirusthanks and keep distribute sample unchecked you will be alright in scanning stubs.

Paradoxum - April 12, 2010, 5:13 am

You might want to include that in the first post, OP.

Eagle 95 - April 12, 2010, 5:25 am

awesome job,this is really helpful

Regards

Eagle

CustomiZer - April 12, 2010, 10:22 am

(Apr 12, 2010 05:13 AM)Paradoxum Wrote: [\[CITE\]](#) You might want to include that in the first post,

OP.

I had already added in the disclaimer.

(Apr 12, 2010 05:25 AM)Eagle 95 Wrote: [\[CITE\]](#) awesome job,this is really helpful

Regards

Eagle

Thank You. Glad you likes it ?

Paradoxum - April 13, 2010, 5:57 am

It looks better. I love little texts. ?

RUS7Y - April 15, 2010, 4:27 am

Add [avhide.com](#) :Oui:

CustomiZer - April 15, 2010, 4:31 am

(Apr 15, 2010 04:27 AM)Rusty_v™ Wrote: [\[CITE\]](#) Add [avhide.com](#) :Oui:
I'll PM kutmustakurt to add it once he gets online ?

update :

[avhide.com](#)

[mwanalysis.org](#)

Paradoxum - April 15, 2010, 7:59 am

PM him anytime. He never ignores requests.

CustomiZer - April 15, 2010, 8:04 am

(Apr 15, 2010 07:59 AM)Paradoxum Wrote: [\[CITE\]](#) PM him anytime. He never ignores requests.
I got a problem now. It seems that he is unable to add more images to the thread due to images limit in a post. Actual limit is 10 mine already has 26 or so. He suggested making a part 2 of the thread ?

Paradoxum - April 15, 2010, 8:05 am

That's fine. You can merge posts, or ask iBruteforce if Administrators have no image limits.

CustomiZer - April 20, 2010, 7:41 pm

I'm thinking I'll probably make the second version itself. I will just need some more time to get it set and ready to post ?

Paradoxum - April 21, 2010, 8:49 am

Very well then. What would it contain?

CustomiZer - April 22, 2010, 3:30 am

An extension or continuation of the same I guess ?

Or do you have any good ideas ?

Paradoxum - April 22, 2010, 8:00 am

If it is simply a continuation, I suggest keeping it on the same thread.

CustomiZer - April 22, 2010, 8:17 am

It is not possible to post any more pictures on the first post of this thread anymore. Kut told that.

Paradoxum - April 22, 2010, 8:25 am

Figures. Part two then. ?

CustomiZer - April 22, 2010, 10:38 am

Yeah. That is what I've been thinking ? as adviced by KUt actually.

Once Timeless - April 29, 2010, 6:22 pm

Nice collection you have there could come in use.

CustomiZer - May 8, 2010, 3:17 am

(Apr 29, 2010 06:22 PM)WMM Wrote: [\[CITE\]](#) Nice collection you have there could come in use.
Thank You very much ?

RUS7Y - May 8, 2010, 3:36 am

You haven't added avhide yet ? ?

CustomiZer - May 8, 2010, 3:39 am

(Apr 15, 2010 08:04 AM)icyberhack Wrote: [\[CITE\]](#) I got a problem now. It seems that I'm unable to add more images to the thread due to images limit in a post. Actual limit is 10 mine already has 26 or so. He suggested making a part 2 of the thread ?

But it has been down for quite a few days now ..I'll maybe add only the text part ? once it gets online...

[[R9]] - May 8, 2010, 4:29 am

great one i knew only i few of them must have took a lot time for this work

CustomiZer - June 9, 2010, 5:42 am

(May 8, 2010 04:29 AM).:Xx-POSEIDON-xX:. Wrote: [\[CITE\]](#) great one i knew only i few of them must have took a lot time for this work

Yeah, it did. Anyway it was worth it in my opinion ?

Stormchant - June 9, 2010, 12:52 pm

Very nice list, really useful for peoples wich are infected.

CustomiZer - June 10, 2010, 3:42 pm

(Jun 9, 2010 12:52 PM)Pk3r_Pjer Wrote: [\[CITE\]](#) Very nice list, really useful for peoples wich are infected.

Yeah..?

This is what this compilation was basically for ?