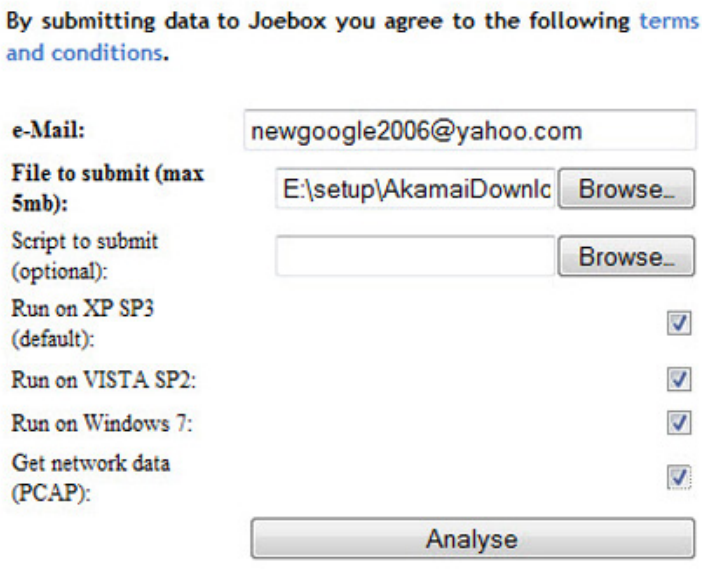
Analyze Malware actions with the Joebox Online Sandbox

Surely everyone has known the online virus scanning service is quite popular, popular and widely known as VirusTotal, ...

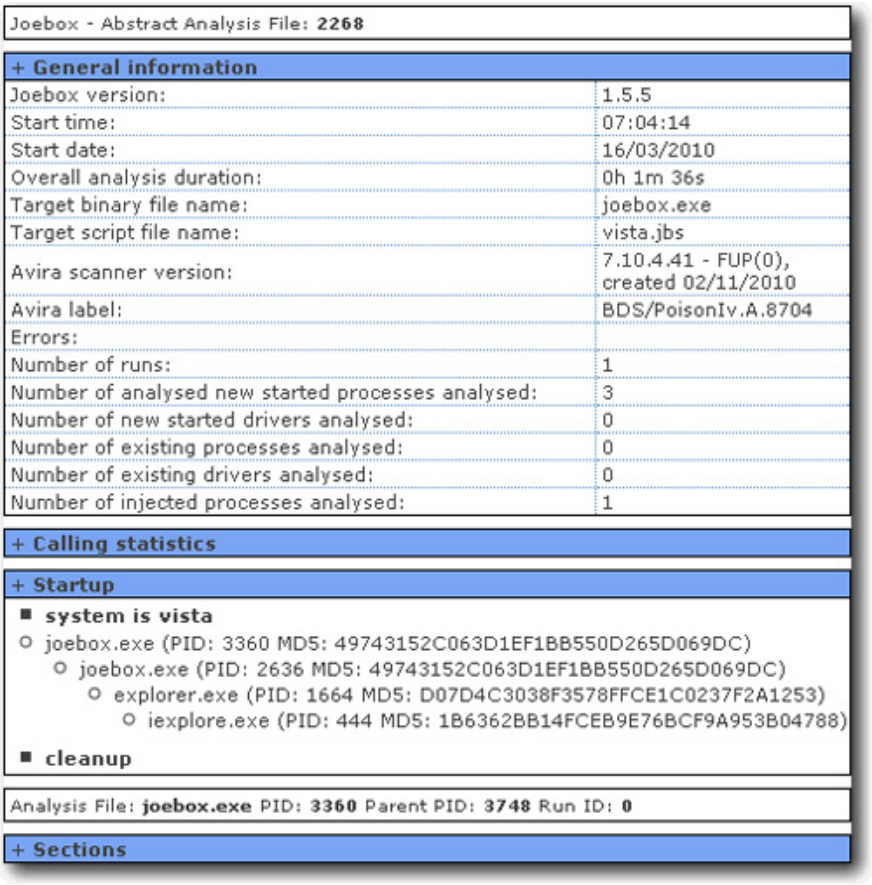
Probably everyone knows about the popular, popular and popular online virus scanning services such as VirusTotal, with the scanning function of more than 40 leading antivirus programs today . The main goal is to analyze the main action of the file when activated on the computer. Other reliable online virus scanners include: ThreatExpert, CWSandbox, Anubis, Sunbelt Sandbox, Norman Sandbox and Comodo Instant Malware Analysis.

In this article, the author will mention another online utility, Joebox. Beginning its official operation in 2008, through 3 years of continuous development and upgrading, Joebox has received positive responses and contributions from the community. Recently on March 14, 2010, Joebox upgraded to the latest version 1.5.5 with many notable changes: correcting errors when working with large HTML pages, adding reading and writing files instead change, the main value query string in the changed sections, increase the ability to design HTML and fix update errors on the server system when working with client requests.

One of Joebox's highlights is that users can choose Windows versions to analyze Malware's actions. By default, Joebox will allow those Malware programs to be executed on Microsoft Windows XP SP3 environment, but users can choose from two different versions, Vista SP2 and Windows 7 at the same time. Besides, you can check 'Get network data - PCAP' and open with Wireshark application to analyze traffic flow, collected data.



You need to enter the correct email address in the 'e-Mail' box because the entire result and the scanning process will be sent to that email address. The report will be sent as an HTML file, and can be very confusing for less experienced security people.



Joebox - Abstract Analysis File: **2268**

+ General information

Joebox version:	1.5.5
Start time:	07:04:14
Start date:	16/03/2010
Overall analysis duration:	0h 1m 36s
Target binary file name:	joebox.exe
Target script file name:	vista.jbs
Avira scanner version:	7.10.4.41 - FUP(0), created 02/11/2010
Avira label:	BDS/PoisonIv.A.8704
Errors:	
Number of runs:	1
Number of analysed new started processes analysed:	3
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

+ Calling statistics

+ Startup

- **system is vista**
- joebox.exe (PID: 3360 MD5: 49743152C063D1EF1BB550D265D069DC)
  - joebox.exe (PID: 2636 MD5: 49743152C063D1EF1BB550D265D069DC)
    - explorer.exe (PID: 1664 MD5: D07D4C3038F3578FFCE1C0237F2A1253)
      - iexplore.exe (PID: 444 MD5: 1B6362BB14FCEB9E76BCF9A953B04788)
- **cleanup**

Analysis File: **joebox.exe** PID: **3360** Parent PID: **3748** Run ID: **0**

+ Sections

Can many people wonder about Joebox's reports that are more confusing than other online machines? One of Joebox's highlights and features is the ability to identify the latest Malware-equipped anti-action analysis software (*un-analyzable*) that other services do not yet have. From an obscure position, Joebox has become one of the trusted names in the field of security and action analysis of today's malicious software.

Note that you should only download * .exe file, not other formats such as ZIP, RAR, 7z . However, if the user is afraid of the risk of accidentally activating that Malware software on a personal computer You can upload it directly without paying attention to the extension, Joebox will automatically identify it as the executable file (* .exe), although they can be disguised as * .exe , * .dll, * .sys, * .doc, * .pdf .