



# Norman SandBox Reporter

Analyzing malware can be a cumbersome and time consuming task, involving multiple applications for code analysis as well as a network of computers. Each one of the applications is meant to perform its specific task and most of the time you need to combine the result of several of these to find the true actions and intent of the malware.

With Norman's new SandBox Malware Analyzer product line, the complexity, speed and infrastructure needed to analyze files have been dramatically reduced. This will give you a quick return on investment.

## Product description

Norman SandBox Information Center and its related services daily receive thousands of suspicious files. All files submitted are being analyzed, and as a subscriber you will get a list with information of Norman SandBox analysis over the past 24 hours.

The Norman SandBox Reporter is created daily, and every night subscribers receive a list with information in both .txt and .xml format for easier management. The analysis includes:

- 1) A list of URLs that might contain malicious code. This list can be used in many ways, such as importing it to a URL blacklist filter to prevent any computer behind the filter to access these sites. ISPs can use the list to take down websites containing malicious code.
- 2) A list of IRC network servers that malware tries to connect to. The list includes server names, ports, username and password etc. These IRC networks are most likely botnets.
- 3) Finally you will get a SandBox summary of most of the files that have been analyzed in the same period. The summary contains more detailed information about the files' behavior and intent.

### How can Norman SandBox Malware Analyzers help?

#### Save time

- The average response time to a new threat is normally 6 – 24 hours.
- Get a head start with knowledge of what the sample is trying to do.

#### Save money

- A growing number of viruses to analyze require a high number of analyst efforts.
- Finding the right people to analyze malware is a difficult, time-consuming, and costly task.

#### Save the day

- You have been in the situation where something needed to be analyzed yesterday and now you have access to the tools to make it happen.

Count	Server	Port	Password	IP	RC2	Ping	Nick	User	Channel	Channel-password	Setservermode	Setservermode
00000	telnet.06039.us	00006667		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006668		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006669		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006670		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006671		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006672		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006673		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006674		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006675		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006676		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006677		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006678		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006679		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006680		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006681		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006682		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006683		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006684		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006685		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006686		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006687		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006688		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006689		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006690		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006691		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006692		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006693		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006694		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006695		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006696		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006697		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006698		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006699		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006700		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006701		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006702		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006703		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006704		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006705		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006706		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006707		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006708		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006709		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006710		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006711		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006712		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006713		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006714		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006715		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006716		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006717		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006718		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006719		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006720		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006721		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006722		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006723		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006724		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006725		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006726		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006727		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006728		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006729		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006730		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006731		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006732		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006733		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006734		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006735		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006736		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006737		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006738		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006739		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006740		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006741		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006742		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006743		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us	00006744		066.111.215.077	YY	0000	06021278	rffp	#kll	N/A	-#B	#ht
00000	www.06039.us											



Info Security  
Products Guide  
names Norman

SandBox Analyzer winner of the 2006  
Tomorrow's Technology Today Award.

For more information contact Norman at  
SandBox@norman.com, or visit  
<http://sandbox.norman.no> to sign up for  
a 30 day trial today!

## Technical requirements

In order to be able to receive the report (the URL list) you need a valid email address.

## Botnet attacks

Some of the most common actions performed by malware today are the creation of robots, botnets and malware connecting to servers on the Internet.

A botnet consists of thousands of sleeping robots installed in computers around the world. These robots are installed without the user's knowledge and can be remotely controlled by computer criminals in order to perform various illegal activities, such as Distributed Denial of Service attacks (DDoS), phishing attempts, spamming, keylogging etc.

The malware connects to servers on the Internet to either download more malicious files or to upload information taken from the computer where it is installed. This can be everything from documents to usernames, passwords and credit card information.

## Related products

### **Norman SandBox Analyzer:**

This utility provides a comprehensive analysis of any executable file action. After the file has been processed, a report is generated with an in-depth description of files in an API log view and a summary report.

### **Norman SandBox Online Analyzer:**

SandBox Online Analyzer is a web-based analysis service which offers the same options and outputs as the standard SandBox Analyzer product. The service allows the customer to upload suspicious executable files to Norman's dedicated servers which then quickly supply a comprehensive analysis of the file action. This service is targeted to customers who do not require the unlimited analysis capabilities of the Analyzer or who do not have a dedicated virus analysis lab and wish to let Norman supply the processing power.

### **Norman SandBox Analyzer PRO:**

Analyzer PRO is used for deep file analysis for reverse engineering and debugging malware. Like Analyzer, its core component is the Norman SandBox Technology. Analyzer PRO performs the function of a complete virus analysis lab. In addition to traditional debugging capabilities, Analyzer PRO includes the ability to monitor and manipulate the emulated SandBox environment in real time. This includes the CPU and its registers, memory, registry, threads, network sockets, and disassembled code.

[www.malwareanalyzer.com](http://www.malwareanalyzer.com) • [www.virusanalyzer.com](http://www.virusanalyzer.com)