



# Los Angeles Chapter

## TOOL TALK



Presented by ISSA LA  
February, 2011



# Los Angeles Chapter

What we are going to talk about today.

- Ideas for Tool Talk?
- What is VirusTotal?
- How is it used?
- VirusTotal Good and Bad?
- Additional Information



# Los Angeles Chapter

## Have an Interesting Topic for ToolTalk

Please visit <http://www.issa-la.org/resources/tooltalk/> and submit your ideas.



Information Systems Security Association – Los Angeles - Windows Internet Explorer

http://www.issa-la.org/resources/tooltalk/

View Favorites Tools Help

ToolTalk | Information Systems Security Associati...

Home Join Get to Know Us Calendar Sponsors Guide Community **Resources**

**Home**  
ISSA LA Home  
ISSA International Home

**ISSA LA**  
Become a Community Supporter  
Board Members  
Bylaws  
ISSA-LA Mission  
Join Mailing List  
Join our Community Partner Program  
Letter from the President  
Speaker's Guide  
Sponsor's Guide

**Events**  
ISSA LA Monthly Member Meeting  
Feb 16th, 11:30am  
ISSA LA Dinner Meeting

**ToolTalk**

"Let's Talk about Tools"--Yev A

The idea behind ToolTalk is to educate fellow members. The format of ToolTalk is a 5-10 minute presentation during monthly ISSA-LA meetings on defensive and/or offensive tools used by Information Security professionals. The presentation should include a description of the tool, likes/dislikes, comparison with other similar tools, and an opinion of which is better.

Presentations:  
January 2011 – [Yev Avidon on "Truecrypt vs BitLocker"](#)



# Los Angeles Chapter

## What is VirusTotal?

**VirusTotal** (<http://www.virustotal.com/index.html>) is a service developed by [Hispacec Sistemas](#) that analyzes suspicious files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and web analysis toolbars.

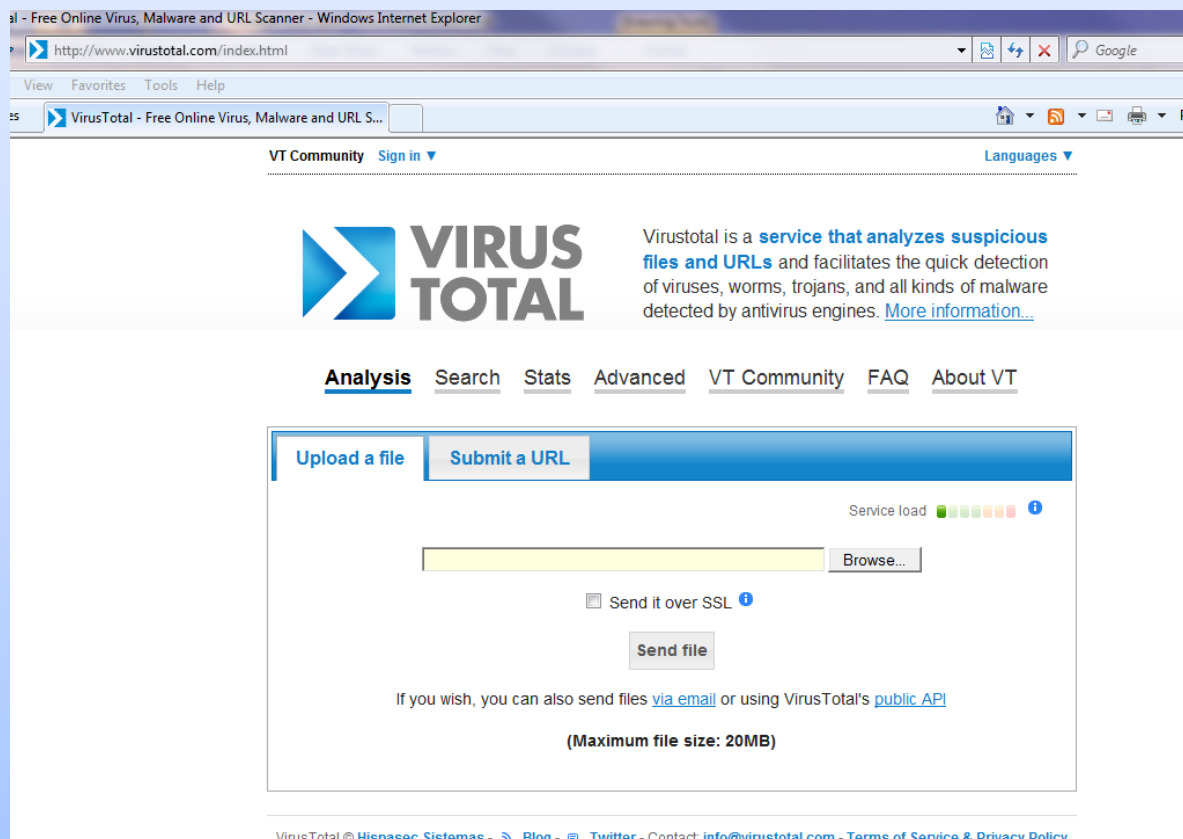
VirusTotal's main characteristics are:

- Free, independent service.
- Runs multiple antivirus engines.
- Runs multiple file characterization tools.
- Real time automatic updates of virus signatures.
- Detailed results from each antivirus engine.
- Runs multiple web site inspection toolbars.
- Real time global statistics.
- Analysis automation API.
- Online malware research community.
- Desktop applications (VTUploader, VTzilla) for interacting with the service.



# Los Angeles Chapter

## What is VirusTotal?



The screenshot shows the VirusTotal website interface. At the top, there's a navigation bar with "VT Community" and "Sign in" on the left, and "Languages" on the right. Below this is the VirusTotal logo, a blue chevron pointing right, followed by the text "VIRUS TOTAL". To the right of the logo is a descriptive paragraph: "VirusTotal is a **service that analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)".

Below the description is a horizontal menu with links: **Analysis**, Search, Stats, Advanced, VT Community, FAQ, and About VT. The "Analysis" link is underlined.

The main content area features two tabs: "Upload a file" (selected) and "Submit a URL". Below the tabs is a "Service load" indicator with a progress bar and a blue information icon. A file upload area contains a yellow input field, a "Browse..." button, and a checkbox labeled "Send it over SSL" with a blue information icon. Below the checkbox is a "Send file" button.

At the bottom of the upload area, there is text: "If you wish, you can also send files [via email](#) or using VirusTotal's [public API](#)". Below this is the text "(Maximum file size: 20MB)".

The footer of the page contains the text: "VirusTotal © Hispasec Sistemas - [Blog](#) - [Twitter](#) - Contact: [info@virustotal.com](mailto:info@virustotal.com) - [Terms of Service & Privacy Policy](#)".



# Los Angeles Chapter

## VirusTotal: Main Features

The identification of viruses, worms, trojans and other kinds of malicious content detected by:

### Antivirus engines

AhnLab-V3, AntiVir, Antiy-AVL, Avast, Avast5, **AVG**, **BitDefender**, CAT-QuickHeal, **ClamAV**, Commtouch, Comodo, DrWeb, Emsisoft, eSafe, eTrust-Vet, F-Prot, **F-Secure**, Fortinet, Gdata, Ikarus, Jiangmin, K7AntiVirus, **Kaspersky**, **McAfee**, McAfee-GW-Edition, **Microsoft**, NOD32, Norman, nProtect, Panda, PCTools, Prevx, Rising, **Sophos**, SUPERAntiSpaware, **Symantec**, TheHacker, TrendMicro, TrendMicro-HouseCall, VBA32, VIPRE, ViRobot, VirusBuster

### Web analysis toolbars

Firefox, G-Data, Google Safebrowsing, Opera, ParetoLogic, Phishtank

### Additional Information

MD5, SHA1 and SHA256



# Los Angeles Chapter

## VirusTotal

### Good

**VirusTotal** is web-based application (nothing to download on your computer)

**VirusTotal** is free service

**VirusTotal** is fast (uploaded a 15MB in less than 1 min, plus less than 2 min for a report)

**VirusTotal** is accurate (43 anti-virus products better than 1)

**Submit** your files through **the website or via email**

### Bad

**Cannot perform system-wide scan**

**Size of the file cannot be more than 20MB**

**You do not know where is your file** (company's servers in Spain or somewhere in the Cloud)

**Retention policy** for the documents you uploaded



# Los Angeles Chapter

## Resources

<http://www.virustotal.com/index.html>

<http://en.wikipedia.org/wiki/VirusTotal.com>

[http://download.cnet.com/Virustotal/3000-8022\\_4-10738551.html](http://download.cnet.com/Virustotal/3000-8022_4-10738551.html)

<http://www.softpedia.com/reviews/windows/VirusTotal-Uploader-Review-158824.shtml>