



Inside VirusTotal's pants

Emiliano Martinez
emartinez@virustotal.com



What **people** think **VirusTotal** is...



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

 File

 URL

 Search

No file selected

Choose File

Maximum file size: 64MB

By clicking 'Scan it!', you consent to our [Terms of Service](#) and allow VirusTotal to share this file with the security community. See our [Privacy Policy](#) for details.

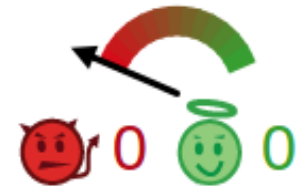
Scan it!

SHA256: 048dbecaeea67be7747819e0214ddb07507ba54212362274a0b8110b60b64094

File name: 8ea54b9a5ea62c5a0ee57b11e68ca319

Detection ratio: 40 / 52

Analysis date: 2014-05-09 19:03:09 UTC (1 day, 23 hours ago)



Analysis

File detail

Additional information

Comments 0

Votes

Behavioural information


Antivirus	Result	Update
AVG	Worm/Bobax.AB	20140509
Ad-Aware	Win32.Worm.Bobic.AC	20140509
Agnitum	Worm.Bobic.AV	20140509
AntiVir	Worm/Bobic.Crypt	20140509
Avast	Win32:Bobic-GE [Wrm]	20140509
BitDefender	Win32.Worm.Bobic.AC	20140509
Bkav	W32.HfsAutoB.8049	20140509
ByteHero	Virus.Win32.Heur.k	20140509

Detection ratio: 29 / 52

Analysis date: 2014-05-09 11:52:46 UTC (2 days, 6 hours ago)



PHP Shell

 Analysis

 Additional information

 Comments 0

 Votes

Antivirus	Result	Updated
AVG	PHP/Back	20140
Ad-Aware	Trojan.PHPInfo.C	20140
AhnLab-V3	PHP/Shell	20140
AntiVir	SPR/PHP.ID	20140
Antiy-AVL	Trojan/PHP.PHPInfo.I	20140
Avast	PHP:PHPInfo-A [Trj]	20140
BitDefender	Trojan.PHPInfo.C	20140
Bkav	VEX54d8.Webshell	20140
ClamAV	PHP.Id-36	20140
Commtouch	PHP/Info.A	20140
Comodo	TrojWare.PHP.PHPInfo.I	20140

Detection ratio: 32 / 52

Analysis date: 2014-05-09 07:06:38 UTC (2 days, 11 hours ago)

Linux ELF



 Analysis

 Relationships

 Additional information

 Comments

1

 Votes

Antivirus

Result

Updated

AVG

Patched_c.NCO

2014-05-09

Ad-Aware

Backdoor.Linux.Sshdkit.A

2014-05-09

AhnLab-V3

Linux/Ebury

2014-05-09

Avast

ELF:SSHDoor-C [Trj]

2014-05-09

BitDefender

Backdoor.Linux.Sshdkit.A

2014-05-09

Bkav

MW.Clodece.Trojan.a5cc

2014-05-09

CAT-QuickHeal

Linux.Backdoor.Sshdkit.a

2014-05-09

Comodo

UnclassifiedMalware

2014-05-09

DrWeb

Linux.Sshdkit.1

2014-05-09

ESET-NOD32

Linux/Ebury.A

2014-05-09

Emsisoft

Backdoor.Linux.Sshdkit.A (B)

2014-05-09

Detection ratio: 34 / 52

Analysis date: 2014-05-09 18:48:05 UTC (1 day, 23 hours ago)

OSX Mach-O

 Analysis

 Additional information

 Comments 6

 Votes

Antivirus

Result

AVG BackDoor.Generic_c.FCW

Ad-Aware MAC.OSX.Trojan.FlashBack.L

Agnitum Trojan.DL.OSX.Flashfake.K

AhnLab-V3 OSX64-Trojan/Flashback.AB

AntiVir MacOS/Flashback.K.I

Avast MacOS:Flashback-M [Trj]

BitDefender MAC.OSX.Trojan.FlashBack.L

Bkav MW.Clodd84.Trojan.4038

CAT-QuickHeal Backdoor.MacOSX.Flashback.H

ClamAV OSX.Flashback-8

CommTouch MacOS/FlashBack.A



VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

 File

 URL

 Search

<http://www.virustotal.com>

Enter URL

Scan it!

URL: <https://www.virustotal.com/static/bin/vtuploader2.2.exe>

Detection ratio: 0 / 51

Analysis date: 2014-05-05 09:05:38 UTC (6 days, 9 hours ago)

File scan: [Go to downloaded file analysis](#)



 Analysis

 Additional information

 Comments

1

 Votes

URL Scanner

Result

ADMINUSLabs

Clean site

AegisLab WebGuard

Clean site

AlienVault

Clean site

Antiy-AVL

Clean site

AutoShun

Unrated site

Avira

Clean site

BitDefender

Clean site

SHA256: 0918fa4b22d3e212a13fa449a5a7b5c3ec97759dd87db6d281f387b1570e13c9

File name: vtuploader2.2.exe

Detection ratio: 1 / 52

Analysis date: 2014-05-05 08:47:15 UTC (6 days, 9 hours ago) [View latest](#)



😊 **Probably harmless!** There are strong indicators suggesting that this file is safe to use.

📄 Analysis

🔍 File detail

🔗 Relationships

ℹ️ Additional information

💬 Comments 5

👍 Votes

📺 Behavioural information

Antivirus	Result	Update
McAfee-GW-Edition	Heuristic.BehavesLike.Win32.Suspicious.A	20140504
AVG	✓	20140505
Ad-Aware	✓	20140505
AegisLab	✓	20140505

Searching with VirusTotal

VirusTotal stores all the analyses it performs, this allows users to search for reports given an MD5, SHA1, SHA256 or URL. Search responses return the latest scan performed on the resource of interest. VirusTotal also allows you to search through the comments that users post on files and URLs, inspect our passive DNS data and retrieve threat intelligence details regarding domains and IP addresses. Learn more about [searching with VirusTotal](#).

Sending files as email attachments

VirusTotal's email interface lets users send files via email and receive the scan results in their mailbox. The files are uploaded as email attachments and the results can be received either as plain text or XML. The files sent via email have a lower priority, therefore, the scan results will not always be sent back immediately. Learn more about [VirusTotal's email interface](#).

Public API

The VirusTotal API lets you upload and scan files, submit and scan URLs, access finished scan reports and make automatic comments on URLs and files without the need of using the HTML website interface. In other words, it allows you to build simple scripts to access the information generated by VirusTotal. Its public version is limited to at most 4 requests of any nature in a given 1 minute time frame. Go ahead and read the [VirusTotal Public API documentation](#).

Browser Extensions

The VirusTotal team has developed several browser plugins that simplify the

Desktop Applications

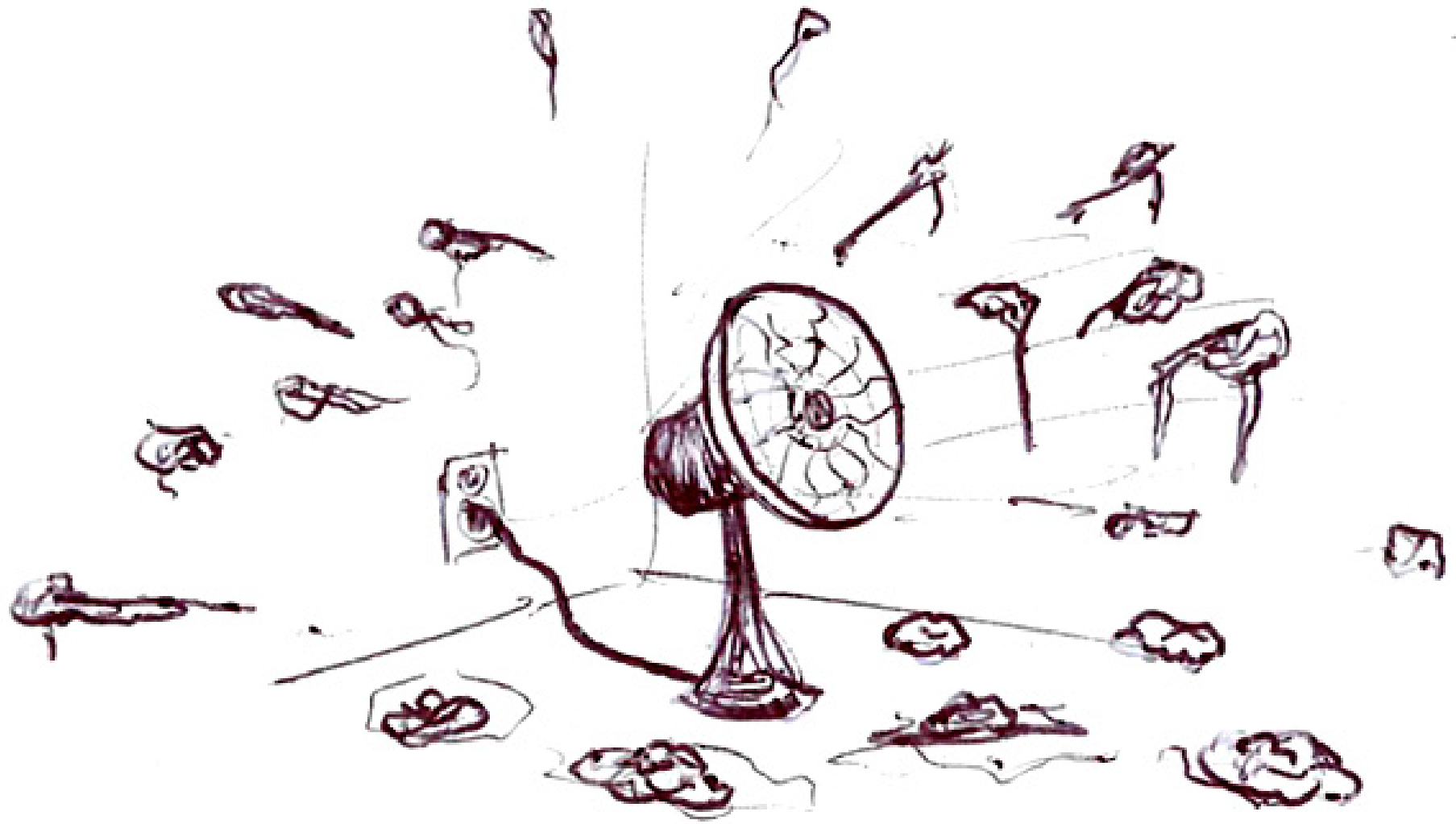
To upload a file to VirusTotal, you can visit the main [VirusTotal website](#) and click the "Choose file" button to select a file from your hard drive and then the "Scan it!" button. You can make this process even easier by using the VirusTotal desktop utilities. A set of desktop applications is available for the main operating systems so as to make the process as easy as right-clicking on the file of interest. Browse the [desktop applications](#) and download the one targeting your operating system.

Mobile device applications

Mobile phones and tablets are an ever growing market. As we become more aware of this and are now indiscriminately targeting them, as the share of these devices continues to rise, the attacks against them are expected to keep increasing. VirusTotal is committed to helping protect your devices, thus, we have released mobile applications for you to scan the applications on your phone with VirusTotal. Browse [VirusTotal's mobile device applications](#) and download the one for your mobile operating system.

VirusTotal Community

Fighting malware requires close collaboration. The only way to reduce the production rate, the growing problem of false positives and the threat of false negatives cannot be counteracted without the engagement of all actors involved in end-user system security. In our mind, we have created VirusTotal Community, a space where the security industry and malware reserchers can meet end-users to make the internet a safer place. VirusTotal Community allows



What **the team** thinks
VirusTotal is...

- **354M samples**, increasing at a rate **560K+ new distinct samples per day**.
- Average of 1M+ file scans per day.
- **130M URLs**, increasing at a rate of **700K+ new distinct URLs per day**.
- Average of 1'3M+ url scans.
- Info for **18M domains** and **5M IP** addresses.
- **24M** distinct (name, IP) **pDNS** resolutions.

Take a closer look,
there is more crap
in the fan...



Report examples

- Portable executable tools
- PDFiD PDF characterization
- PE behaviour
- Android file characterization and android behaviour
- PCAP network trace summary and IDS characterization
- File relationships

What the team
envisions
VirusTotal to be...



I MAY NOT BE THERE YET
BUT I'M CLOSER
THAN I WAS YESTERDAY



Better hunting...



**Better threat
knowledge...**



A man dressed as a chef, wearing a white chef's hat and a white apron over a white shirt. He has a surprised or excited expression on his face, with wide eyes and a slightly open mouth. He is holding a large wooden spoon in his right hand. The background is dark. The text "What are we cooking?" is overlaid in a bold, yellow, sans-serif font at the bottom of the image.

What are we cooking?