FPT University

Lab 6: Public AV Scanners

Because teaching teaches
teachers to teach

Public AV Scanners

- VirusTotal
- Anubis
- Jotti

VirusTotal

- VirusTotal is a subsidiary of Google that analyzes files and URLs. Apart from the free interface, VirusTotal also has both a private and a public API.
- The results from VirusTotal include the detection results of the malware by the supported antivirus engines. This allows you to better evaluate if you are at risk.

VirusTotal

- You can upload different types of files, such as a Windows executable, Android APKs, PDFs, images and JavaScript code.
- The online reports are not individually downloadable, but they are very detailed.

VirusTotal

- Download a sample malware on https://wildfire.paloaltonetworks.com/publicapi/test/pe
- Upload VirusTotal

VirusTotal

6

virustotal

SHA256: 91078ccc0207072d618a54645fecc06508173007c6ab12114e2897426d39b30a

File name: wildfire-test-pe-file.exe

Detection ratio: 4 / 64

Analysis date: 2017-08-14 08:34:33 UTC (1 minute ago)

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
CrowdStrike Falcon (ML)	malicious_confidence_90% (D)	20170804
Cylance	Unsafe	20170814
Fortinet	Riskware/WildFireTestFile	20170814
Rising	Malware.Heuristic!ET#96% (rdm+)	20170814

Jotti

- Jotti's malware scan is a free service that lets you scan suspicious files with several anti-virus programs.
- Detailed information of your uploaded file is displayed as well. This information includes the file size, file type, and details about MD5 and SHA1.

Jotti

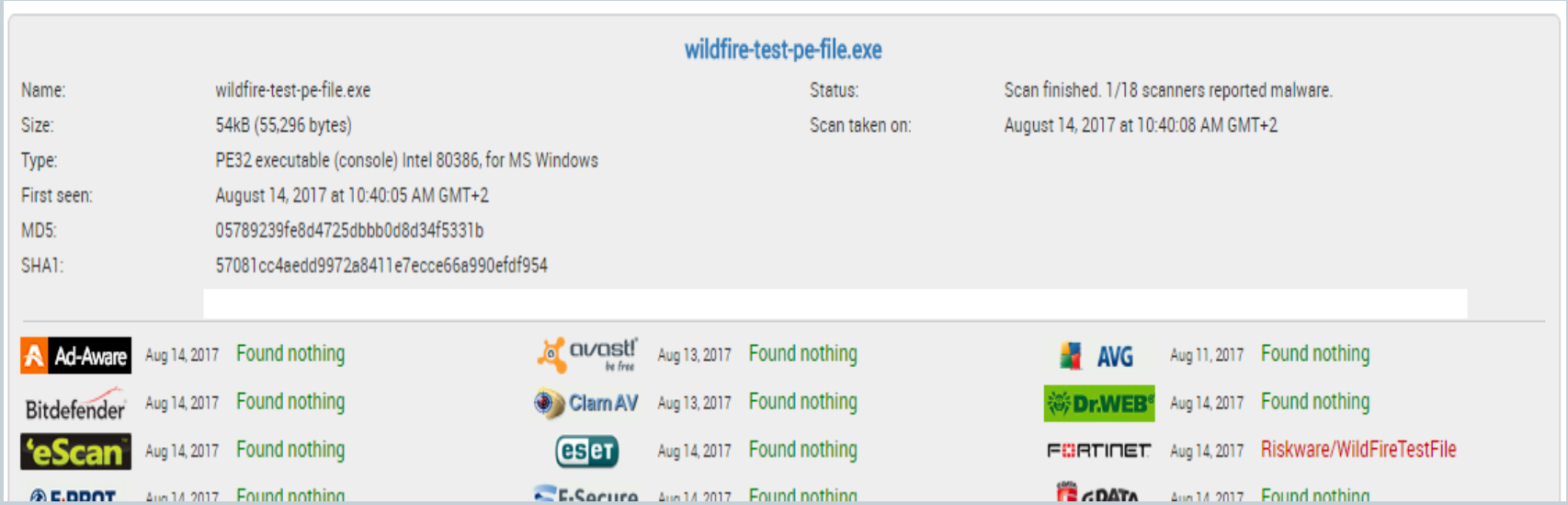
- A user friendly web service scan files from your computer.
- Requires no registrations.
- Searches for viruses in files you upload.
- Uses numerous leading antivirus scanners.
- Provides results by individual scanners.
- Each uploaded file can be up 20MB in size.
- Provides a permalink for the scan results.

Jotti

- Download a sample malware on https://wildfire.paloaltonetworks.com/publicapi/test/pe
- Upload Jotti

Jotti

10


wildfire-test-pe-file.exe
Name: wildfire-test-pe-file.exe
Size: 54kB (55,296 bytes)
Type: PE32 executable (console) Intel 80386, for MS Windows
First seen: August 14, 2017 at 10:40:05 AM GMT+2
MD5: 05789239fe8d4725dbbb0d8d34f5331b
SHA1: 57081cc4aedd9972a8411e7ecce66a990efdf954
Status: Scan finished. 1/18 scanners reported malware.
Scan taken on: August 14, 2017 at 10:40:08 AM GMT+2
Ad-Aware Aug 14, 2017 Found nothing
avast! Aug 13, 2017 Found nothing
AVG Aug 11, 2017 Found nothing
Bitdefender Aug 14, 2017 Found nothing
ClamAV Aug 13, 2017 Found nothing
Dr.WEB Aug 14, 2017 Found nothing
eScan Aug 14, 2017 Found nothing
eset Aug 14, 2017 Found nothing
FORTINET Aug 14, 2017 Riskware/WildFireTestFile

Q & A