LAB 6: Public AV Scanners (VirusTotal, JoeSandbox)

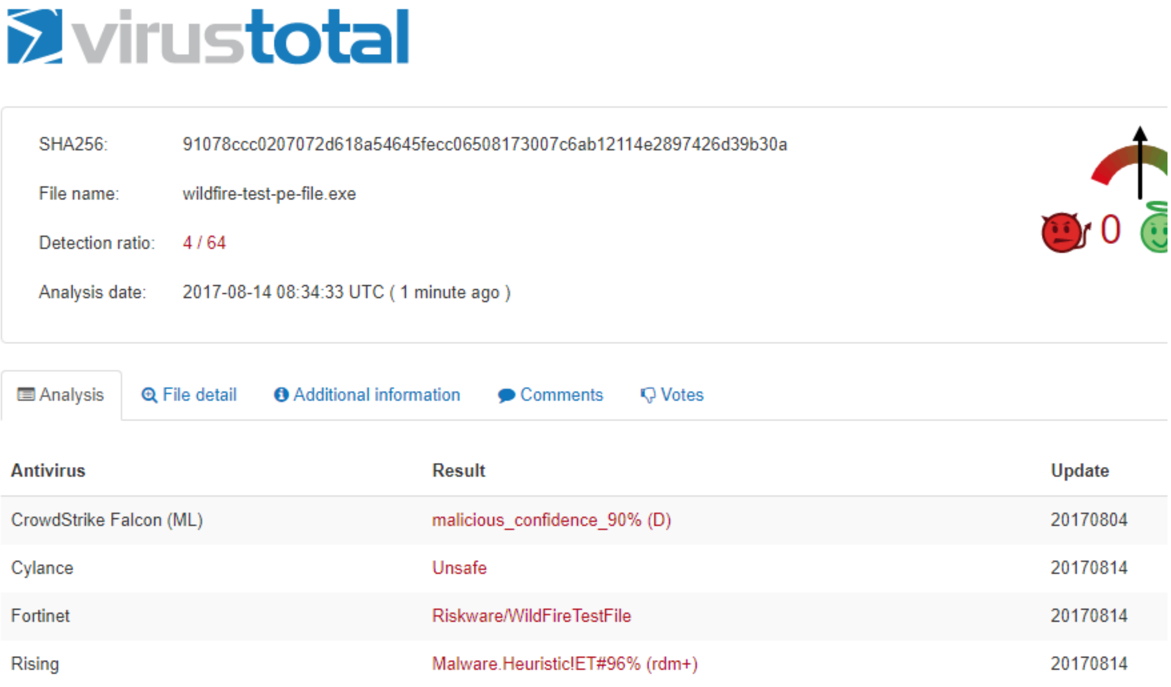
Public AV Scanners

- VirusTotal
- JoeSandbox
- hybrid-analysis.com

VirusTotal

- VirusTotalis a subsidiary of Google that analyzes files and URLs. Apart from the free interface, VirusTotalalso has both a private and a public API.
- The results from VirusTotalinclude the detection results of the malware by the supportedantivirusengines. This allows you to better evaluate if you are at risk.
- 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.

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

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

JoeSandbox

Joe Sandbox Cloud executes files and URLs fully automated in a controlled environment and monitors the behavior of applications and the operating system for suspicious activities

Key Features

- Submit samples and URLs for sandbox analysis
- Search, list, get, download, and delete analyses
- Get, list, and manage server and user info

Requirements

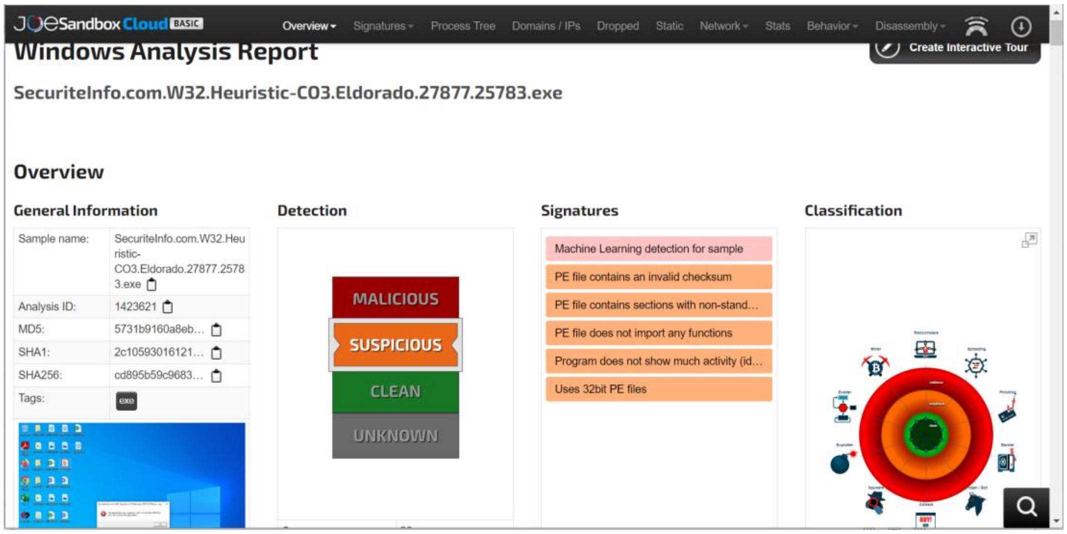
- API Key
- Sandbox server (if not using cloud)

Resources

- Joe Sandbox API
- Joe Sandbox API wrapper
- Report formats

Supported Product Versions

- Joe Sandbox API v2



Windows Analysis Report

SecuriteInfo.com.W32.Heuristic-CO3.Eldorado.27877.25783.exe

Overview

General Information

Sample name:	SecuriteInfo.com.W32.Heuristic-CO3.Eldorado.27877.25783.exe
Analysis ID:	1423621
MD5:	5731b9160a8eb…
SHA1:	2c10593016121…
SHA256:	cd895b59c9683…
Tags:	exe

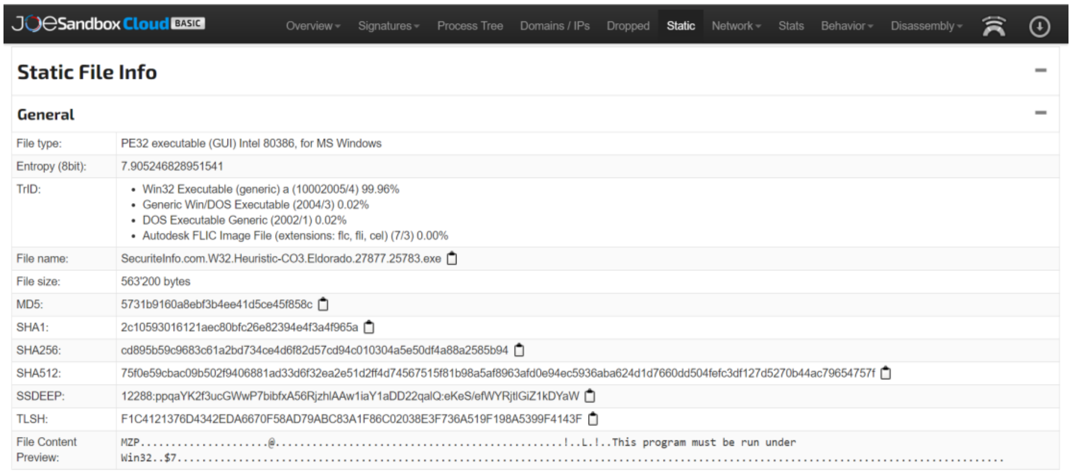
Detection

Signatures

- Machine Learning detection for sample
- PE file contains an invalid checksum
- PE file contains sections with non-stand…
- PE file does not import any functions
- Program does not show much activity (id…
- Uses 32bit PE files

Classification

https://www.joesandbox.com/analysis/1423621/0/html



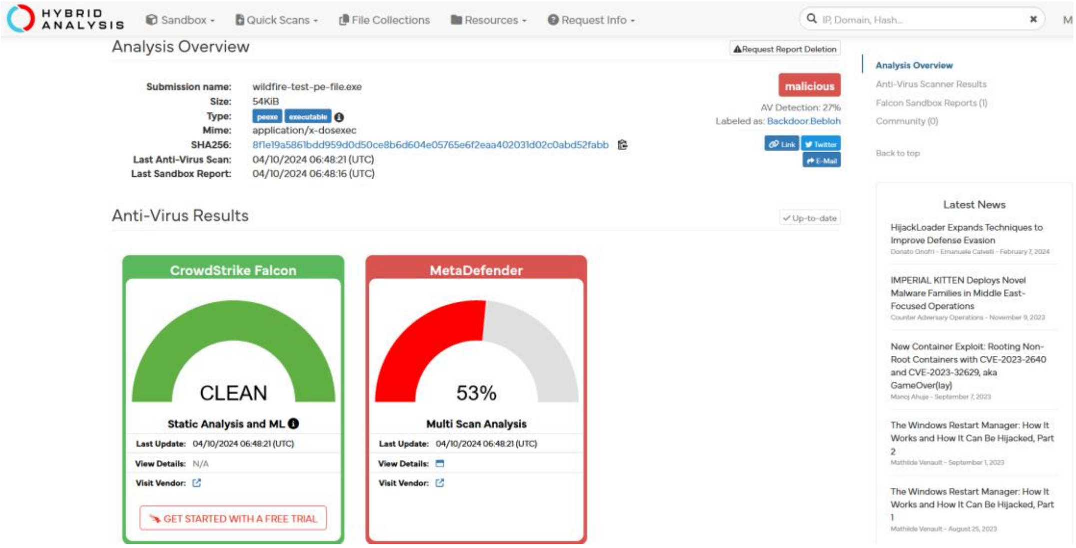
Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.905246828951541
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.W32.Heuristic-CO3.Eldorado.27877.25783.exe
File size:	563'200 bytes
MD5:	5731b9160a8ebf3b4ee41d5ce45f858c
SHA1:	2c10593016121aec80bfc26e82394e4f3a4f965a
SHA256:	cd895b59c9683c61a2bd734ce4d6f82d57cd94c010304a5e50df4a88a2585b94
SHA512:	75f0e59cbac09b502f9406881ad33d6f32ea2e51d2ff4d74567515f81b98a5af8963afd0e94ec5936aba624d1d7660dd504fefc3df127d5270b44ac79654757f
SSDEEP:	12288:ppqaYK2f3ucGWwP7bibfxA56RjzhlAAw1iaY1aDD22qalQ:eKeS/efWYRjtlGiZ1kDYaW
TLSH:	F1C4121376D4342EDA6670F58AD79ABC83A1F86C02038E3F736A519F198A5399F4143F
File Content Preview:	MZP....................@..!..L.!..This program must be run under Win32..$7...

hybrid-analysis.com

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



Analysis Overview

Submission name:	wildfire-test-pe-file.exe
Size:	54KiB
Type:	peexe executable
Mime:	application/x-dosexec
SHA256:	8f1e19a5861bdd959d0d50ce8b6d604e05765e6f2eaa402031d02c0abd52fabb
Last Anti-Virus Scan:	04/10/2024 06:48:21 (UTC)
Last Sandbox Report:	04/10/2024 06:48:16 (UTC)

malicious

AV Detection: 27%

Labeled as: Backdoor.Bebloh

Anti-Virus Results

CrowdStrike Falcon

CLEAN

Static Analysis and ML

Last Update:	04/10/2024 06:48:21 (UTC)
View Details:	N/A
Visit Vendor:	

MetaDefender

53%

Multi Scan Analysis

Last Update:	04/10/2024 06:48:21 (UTC)
View Details:	
Visit Vendor:	

Analysis Overview

Anti-Virus Scanner Results

Falcon Sandbox Reports (1)

Community (0)

Back to top

Latest News

HijackLoader Expands Techniques to Improve Defense Evasion
Donato Onofri - Emanuele Calvelli - February 7, 2024

IMPERIAL KITTEN Deploys Novel Malware Families in Middle East-Focused Operations
Counter Adversary Operations - November 9, 2023

New Container Exploit: Rooting Non-Root Containers with CVE-2023-2640 and CVE-2023-32629, aka GameOver(lay)
Manoj Ahuje - September 7, 2023

The Windows Restart Manager: How It Works and How It Can Be Hijacked, Part 2
Mathilde Venault - September 1, 2023

The Windows Restart Manager: How It Works and How It Can Be Hijacked, Part 1
Mathilde Venault - August 25, 2023