TXSandbox

Provides highly accurate, static and behavioral analysis on unknown files and URLs, in order to detect zero day threats

Highlights

- Dual analytic engine to ensure highest detection rates for URL analysis
- High accuracy and low false positive rates
- Automatically filters out malicious URL links and malicious file attachments embedded in emails
- Runs static analysis on injected code
- Runs static analysis on embedded shell code inside of Non-PE files to detect zero day exploits
- Runs in Linux docker container
- Easy to manage and scale
- Support customized native Windows environment
- Ready to embed into network appliances

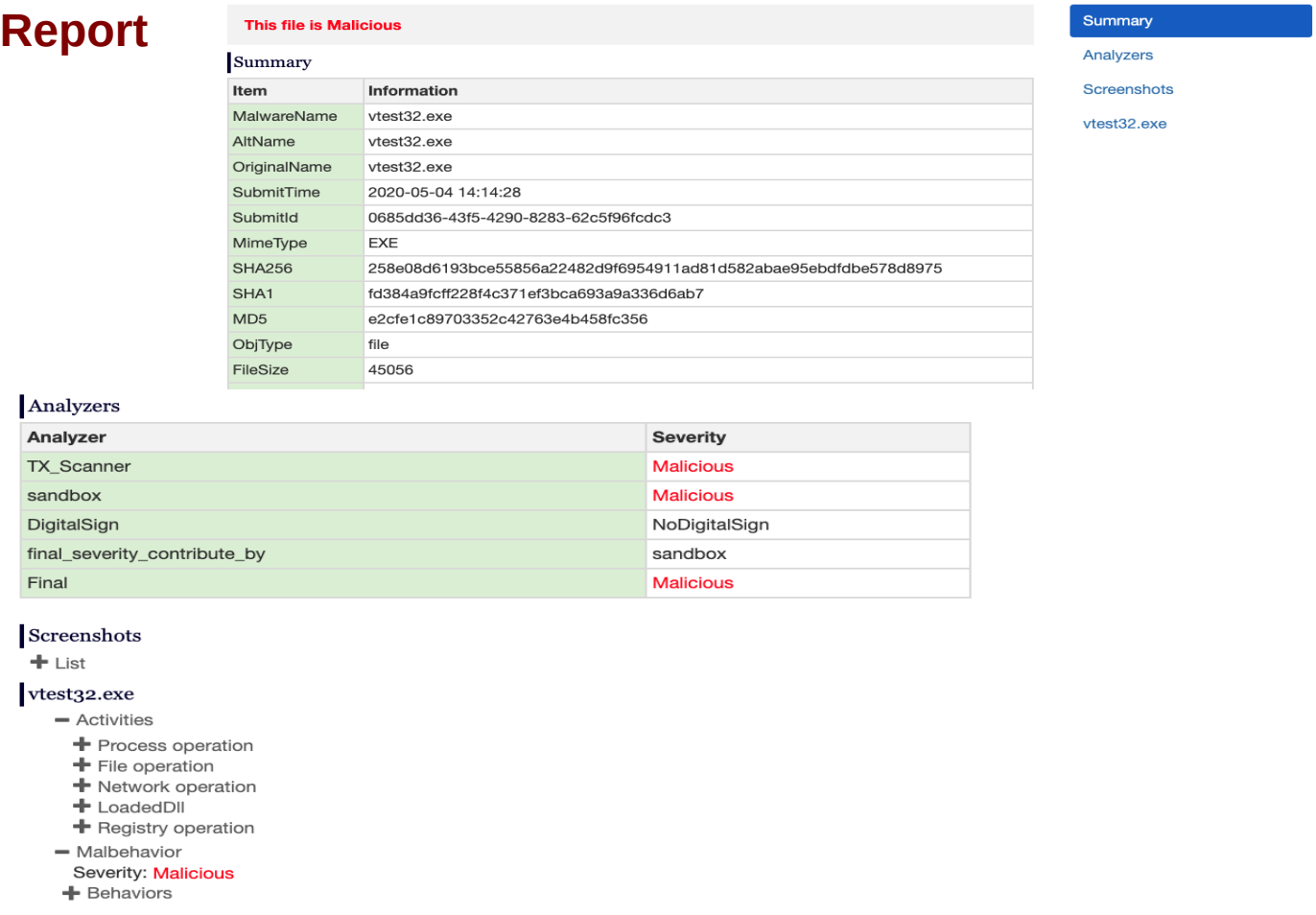
Overview

TXSandbox is a next generation sandbox that features multiple classifiers for increased accuracy, lower false positives and more adaptable PE/NonPE file and URL coverage.

TXSandbox runs in a Linux docker container, or in any type of VM. It can be deployed on-premise, or in private and public clouds, such as AWS. It supports customized Windows environment.

Access is via a Web GUI and Restful API for integration with existing products, such as IPS/IDS, FW and WAF. Ready to be embedded into network appliances.

Report



This file is Malicious

Summary

Item	Information
MalwareName	vtest32.exe
AltName	vtest32.exe
OriginalName	vtest32.exe
SubmitTime	2020-05-04 14:14:28
SubmitId	0685dd36-43f5-4290-8283-62c5f96fcdc3
MimeType	EXE
SHA256	258e08d6193bce55856a22482d9f6954911ad81d582abae95ebdfdbe578d8975
SHA1	fd384a9fcff228f4c371ef3bca693a9a336d6ab7
MD5	e2cfe1c89703352c42763e4b458fc356
ObjType	file
FileSize	45056

Analyzers

Analyzer	Severity
TX_Scanner	Malicious
sandbox	Malicious
DigitalSign	NoDigitalSign
final_severity_contribute_by	sandbox
Final	Malicious

Screenshots

+ List

vtest32.exe

− Activities

+ Process operation
+ File operation
+ Network operation
+ LoadedDll
+ Registry operation

− Malbehavior

Severity: Malicious

+ Behaviors

Summary
Analyzers
Screenshots
vtest32.exe

TXSandbox

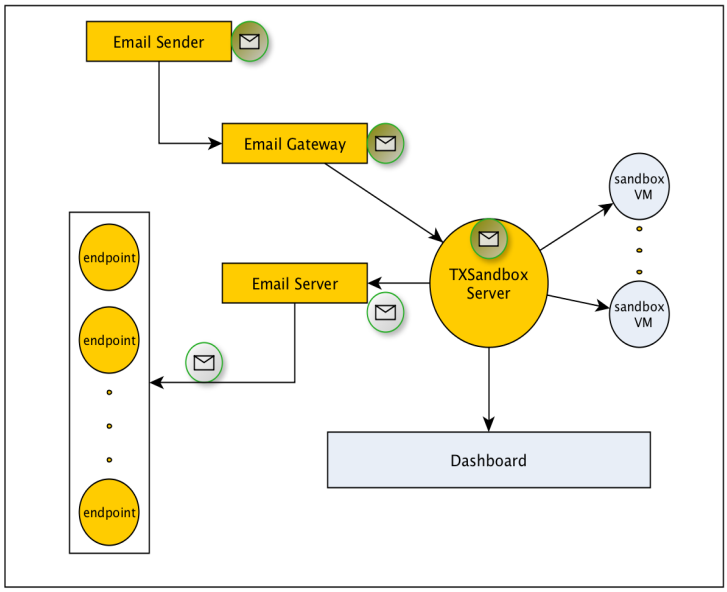
Deployment

OnPremise/Private Cloud/Public Cloud

Prepare a physical or VMware Server
with minimum of

- 16 cores
- 32G RAM
- 1T HD
- 1x1G NIC

Download iso image from TriagingX support
Install and configure the sandbox
Provide ip address, user name and pwd
It will automatically install all needed modules



Operation

- Launch internet browser, such as IE, FireFox or Chrome, and type in the url for the TXSandbox's server address
- Click upload sample button to load file(s) for behavior analysis
- Sit back and wait for the analysis process complete
- Go to TXSandbox's dashboard to view the final report.
- It can also generate the analysis report in PDF file format
- Alternatively, you can use restful API to upload sample file/url, and retrieve the analysis results

Specifications

Target System :	Windows XP, Windows 7, Windows 8/10
Sandbox Server :	CentOS7.2
Interface :	Rest API
Report Format :	PDF and JSON
Without static scan:	Run every file in sandbox VM for behavior analysis: 300 files/day/VM
With static scan:	Static scan down-selector on: 3,000 files/day/VM
Flexible configuration :	Scalable combination, any number of sandbox VMs

About TriagingX, Inc

TriagingX is headquartered in Silicon Valley. Our team successfully created the first-generation malware sandbox that is being used by many fortune 500 companies for daily malware analysis. We have recently designed and built the advanced security Ecosystem that provides complete protection for endpoint systems and datacenter servers against zero-day attacks, without requiring any patches. We are targeting security's root problem in order to help our clients always stay ahead of the attacker.