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
- Very 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
- Analyzes PE files without requiring Windows license fee

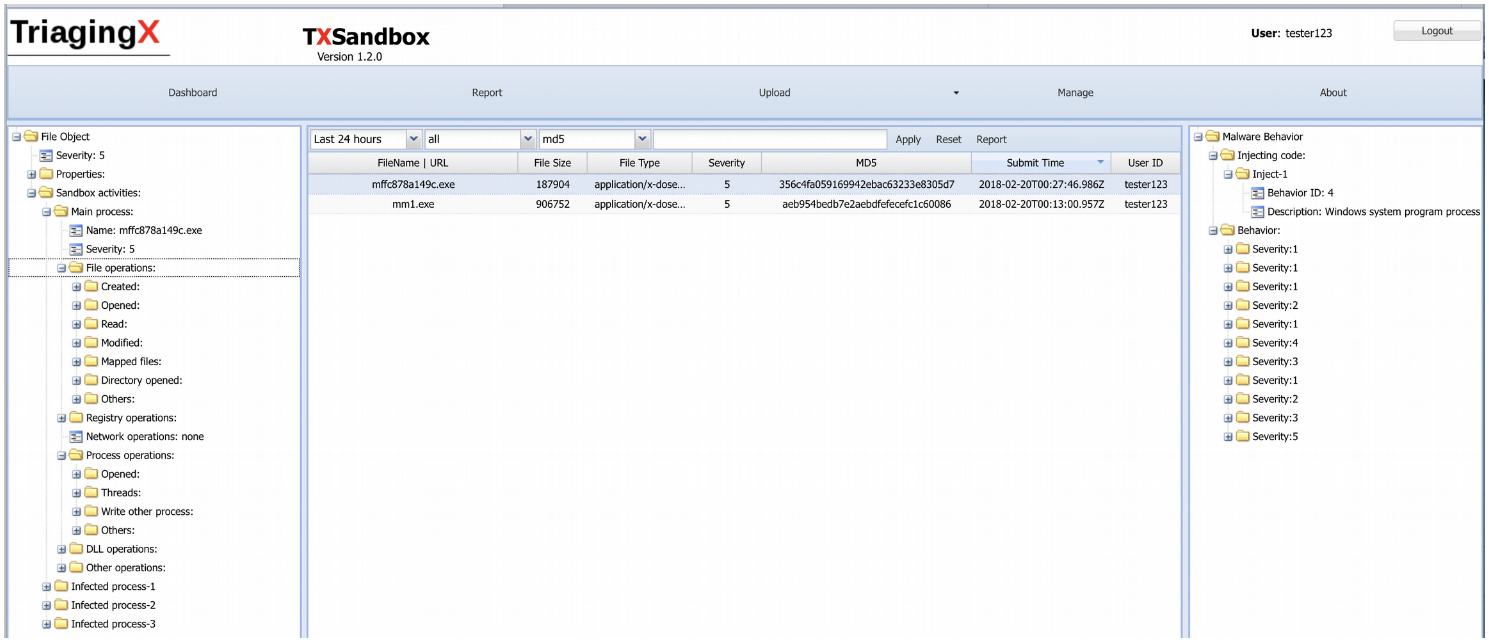
Overview

TXHunter 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 and can be deployed on-premise, or in private and public clouds, such as AWS. It doesn't require Microsoft Windows licenses which can save a lot of costs for large deployments.

Access is via a Web GUI or Restful API for integration with existing products, such as IPS/IDS, FW and WAF.

Report



Last 24 hours | all | md5

FileName | URL	File Size	File Type	Severity	MD5	Submit Time	User ID
mffc878a149c.exe	187904	application/x-dose...	5	356c4fa059169942ebac63233e8305d7	2018-02-20T00:27:46.986Z	tester123
mm1.exe	906752	application/x-dose...	5	aeb954bedb7e2aebdfefecefc1c60086	2018-02-20T00:13:00.957Z	tester123

- File Object
  - Severity: 5
  - Properties:
  - Sandbox activities:
    - Main process:
      - Name: mffc878a149c.exe
      - Severity: 5
      - File operations:
        - Created:
        - Opened:
        - Read:
        - Modified:
        - Mapped files:
        - Directory opened:
        - Others:
      - Registry operations:
      - Network operations: none
      - Process operations:
        - Opened:
        - Threads:
        - Write other process:
        - Others:
      - DLL operations:
      - Other operations:
    - Infected process-1
    - Infected process-2
    - Infected process-3

- Malware Behavior
  - Injecting code:
    - Inject-1
      - Behavior ID: 4
      - Description: Windows system program process
  - Behavior:
    - Severity:1
    - Severity:1
    - Severity:1
    - Severity:2
    - Severity:1
    - Severity:4
    - Severity:3
    - Severity:1
    - Severity:2
    - Severity:3
    - Severity:5

TXSandbox

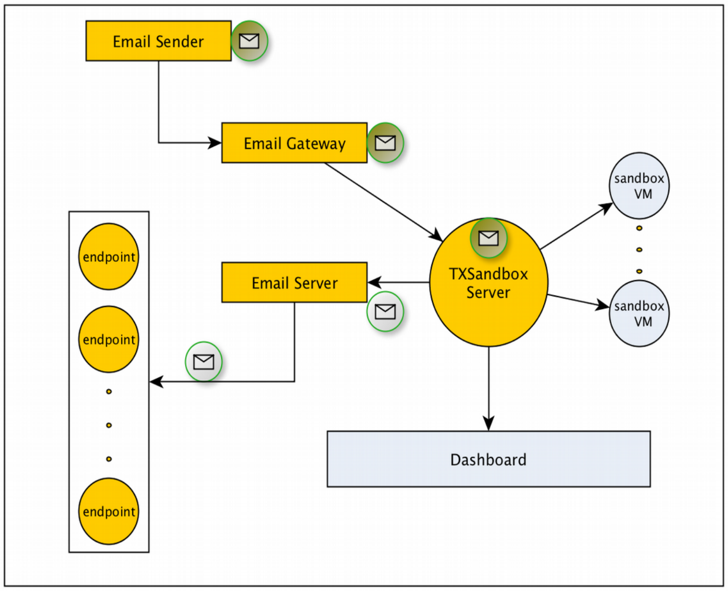
Deployment

OnPremise/Private Cloud/Public Cloud

Prepare a physical or VMware Server
with minimum of

- 16 cores
- 32G RAM
- 2T HD
- 2x1G 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 :	Physical, VMWare Server
Interface :	Rest API
Report Format :	PDF

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.