TXSandbox – Malware Detonation

DEEP ANALYSIS

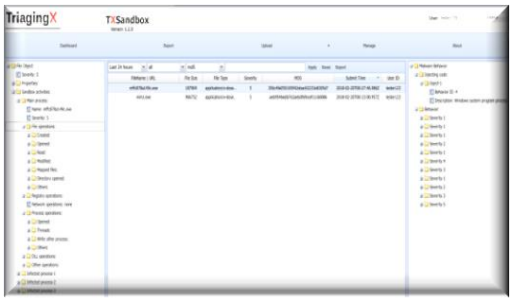
New malware frequently bypass signature scanning and static analyzers. TXSandbox detects based on its behavior, even if the malware file is encrypted or packed.

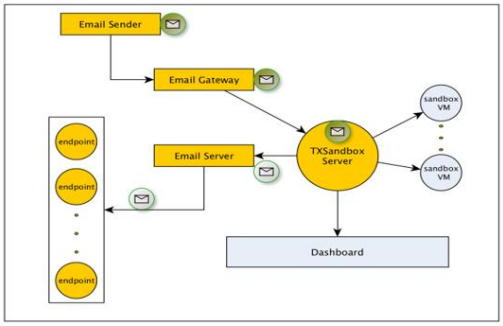
IMPROVED PROTECTION

TXSandbox provides flexible and scalable integration options for existing endpoint, email, firewall and network protection solutions via RestAPI to improve detection of malicious content.

COST, FLEXIBILITY

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. It doesn't require Microsoft Windows licenses which can save substantially in operational costs.





- Rapid threat detection at scale and low cost, using dual analytic engines and advanced anti-evasion techniques to ensure highest industry accuracy and low false positive rates
- Ease of integration by automatically filtering out malicious URL links and file attachments embedded in emails or network traffic and delivering results in flexible formats
- Adaptable detection logic that also runs static analysis on injected code and on embedded shell code inside of Non-PE files to detect zero-day exploits

TXSandbox is an advanced sandbox that features multiple classifiers for increased accuracy and lower false positives. It uses dual analytics engines to ensure the highest detection rates for file, active document, script and malicious URLs based on behavior. It produces simple to understand severity ratings that highlight the overall risks along with detailed malware file and URL activities for the security team to understand its execution characteristics. The system can be integrated into SIEM/SOC workflows where the produced IOC values and program behaviors can enable security teams to identify similar malware across the network and to provide detailed evidence to determine what protect / allow / remove actions to take.

TXSandbox can be deployed on premise in most any type of virtual environment or on bare metal systems. It can also can be deployed in private and public clouds, such as AWS. It runs in a Linux docker container which provides greater flexibility in scaling test environments for multiple platform configurations. It doesn't require Microsoft Windows licenses which can save considerably on costs for large deployments.

Access is via a Web GUI or Restful API for ease of integration with existing products, such as endpoint protection, email gateways or network scanners.

TriagingX Inc.

TXSHIELD

Protects endpoint and datacenter systems against zero-day attacks without requiring patches.

TXHUNTER

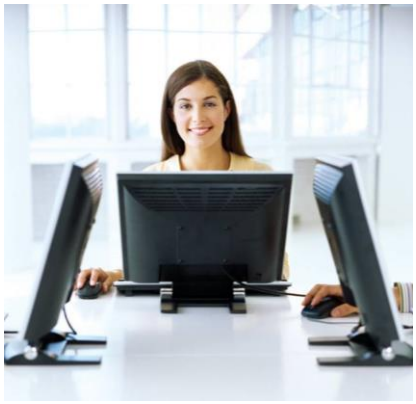
Performs endpoint breach investigations remotely, hunting for all of the attack evidence without having to leave your desk.

TRIAGINGX

We focus on the detection of zero-day attacks, which are often unknown to traditional security solutions. Led by the team that successfully created the first generation malware sandbox used by many Fortune 500 companies for daily malware analysis.

For more information on any of our products or services please visit us on the Web at: www.triagingx.com

Features and Benefits



Dual analytic engines can run dynamic and static analysis on injected code and on embedded shell code inside of Non-PE files to detect zero-day exploits. TXSandbox uses advanced anti-evasion techniques such as no system API hooks in order to mask the presence of the sandbox from the malware: it functions with true Kernel level visibility. It mimic's a user's interactions (static / dynamic) to trigger and exercise advanced Non-PE threats.

TXSandbox supports the integration of real-time threat intelligence feeds that the user has access to, via Rest API. This is especially useful in sensitive networks that produce their own intelligence. It also provides flexible alerting for integration with SIEM / SOC / Orchestration solutions and integrates easily into an automated solution for enterprises, solution providers, and OEMs.

* Future releases will support Linux Server and Android OS platforms

System Requirements

- **Target Detonation Systems**:
  Win XP, Win 7 SP1, Win 8.1, Win 10
  Windows Server 2008 R2, 2012, 2016
- **Sandbox Server:**
  Deployable on Physical Server, VMWare/ESXi, Virtual Box, KVM, Cloud (ISO Image contains Centos 7.2)
- **3rd Party Intelligence:**
  Can run in isolated mode for sensitive networks, or configured to use intelligence data via RestAPI (VT)
- **Report Format:**
  HTML, PDF, JSON

KEY FEATURES

High Accuracy
Dynamic Visibility
Speed/Performance
Low Cost
Seamless Integration
Flexible Deployment

TriagingX Inc.

6050 Hellyer Ave, Suite 150-6
San Jose, CA 95138
tel: +1 408.568.7372
support@triagingx.com
www.triagingx.com