TXHunter

Performs Endpoint Breach Investigations remotely, hunting for all of the attack evidence without having to leave your desk

Highlights

- Investigates security breach remotely
- Detects APT and back doors
- Detects hidden processes and rootkit
- Detects unusual network connections
- Detects spyware and hidden downloader
- Detects zombies and unknown files
- Detects mis-configurations
- Uncover past abnormal activities
- Provide complete forensic reports
- No permanent agent is required to be installed
- No field visiting needed
- Completely automated

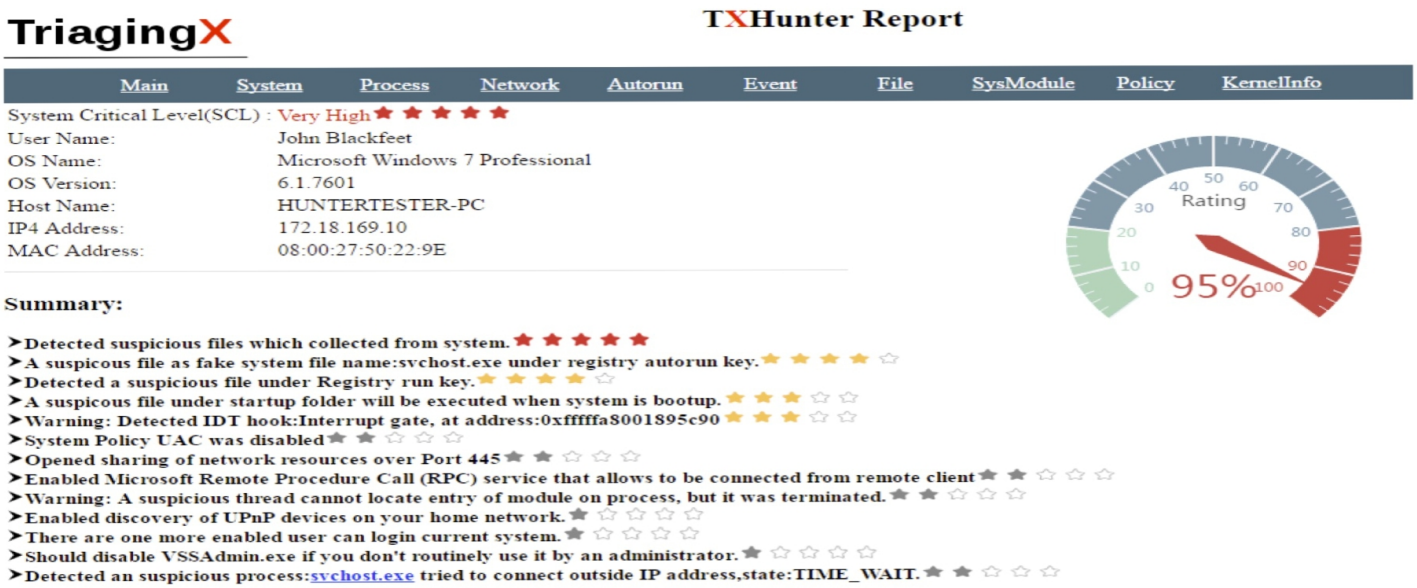
Overview

TXHunter provides an easy and convenient tool for conducting threat incident investigations remotely.

If any endpoint system or server is suspected of having been attacked, TXHunter can simply take a snapshot of the suspicious system and automatically conduct an incident investigation. If the investigation process identifies suspicious files or URL links, it will automatically launch the TXSandbox for a behavior analysis.

Instead of sending your investigation staff to the remote site, TXHunter can perform a rapid and thorough investigation remotely, without anyone having to leave their desk. The system provides a full view detail report of the attack profile.

Report



TriagingX

TXHunter Report

Main | System | Process | Network | Autorun | Event | File | SysModule | Policy | KernelInfo

System Critical Level(SCL) : Very High

User Name:	John Blackfeet
OS Name:	Microsoft Windows 7 Professional
OS Version:	6.1.7601
Host Name:	HUNTERTESTER-PC
IP4 Address:	172.18.169.10
MAC Address:	08:00:27:50:22:9E

Summary:

- Detected suspicious files which collected from system.
- A suspicous file as fake system file name:svchost.exe under registry autorun key.
- Detected a suspicious file under Registry run key.
- A suspicous file under startup folder will be executed when system is bootup.
- Warning: Detected IDT hook:Interrupt gate, at address:0xfffffa8001895c90
- System Policy UAC was disabled
- Opened sharing of network resources over Port 445
- Enabled Microsoft Remote Procedure Call (RPC) service that allows to be connected from remote client
- Warning: A suspicious thread cannot locate entry of module on process, but it was terminated.
- Enabled discovery of UPnP devices on your home network.
- There are one more enabled user can login current system.
- Should disable VSSAdmin.exe if you don't routinely use it by an administrator.
- Detected an suspicious process:svchost.exe tried to connect outside IP address,state:TIME_WAIT.

TXHunter

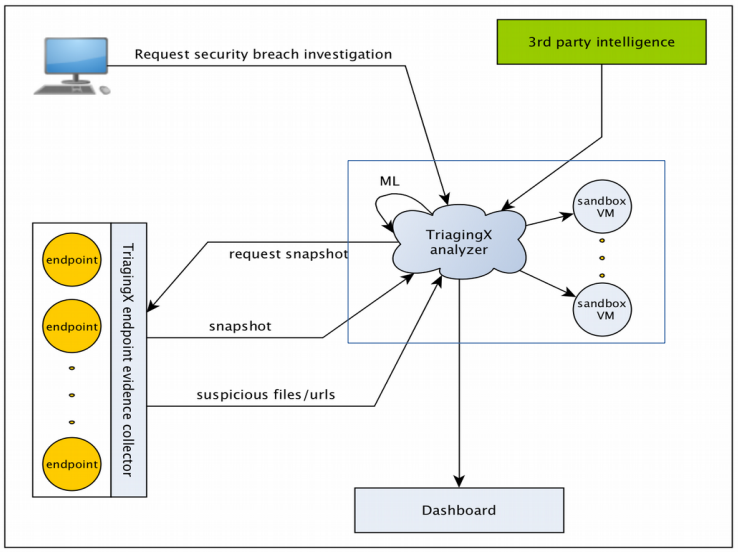
Deployment

TXHunter Server Component

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 analyzer



Operation

SoC Console

Using admin credentials, remotely login to the suspect computer

- Launch internet browser, and download hunter application from TXHunter's server
- Double click hunter application and launch the TXHunter instance
- Sit back and wait for the investigation to complete
- Depending on the complexity involved during investigation process, it usually completes investigation process in less than 15 minutes
- Log into TXHunter's dashboard to view the final report
- It can also generate the report in PDF format

Specifications

Target System :	Windows 7, 8, 10, 2008R2
Analyzer Server :	Physical or VMWare Server
Snapshot Data :	~3 MB 'Password Secured' container, transmitted via Windows Sockets API
3rd Party Intelligence :	RestAPI (VT)
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.