TXHunter

Automated Endpoint Forensic Threat Investigation Solution

Highlights

- Complete forensic endpoint threat investigation automatically and proactively
- Integrated with EDR, SIEM and FW/IPS
- Fit well into enterprise security operation flow
- Detects hidden processes and rootkit
- Detects hidden downloader and APTs
- Detects zombies and unknown files with embedded sandbox behavior analysis
- Detects cryptocurrency mining malware
- Detects reverse shell and advanced attacks
- Detects mis-configs and potential risks
- Detects ransomware and protects user data

Who Needs It?

If you face the challenge of too many alerts and don't have enough resources to investigate them

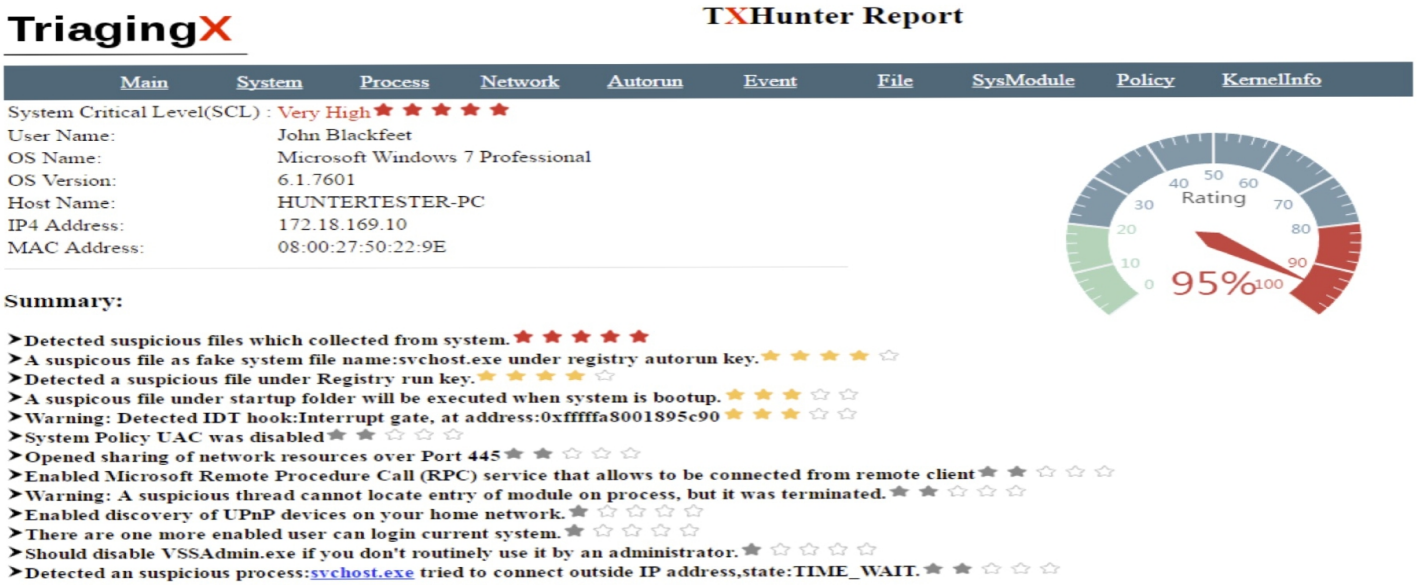
Or if you are still relying on experts with open source tools to conduct threat hunting

Or if you only measure endpoint security posture occasionally such as once or twice a year to meet the auditing purpose

Or if you are MSSP and want to provide better and faster incidence responses to your clients

Then you need TXHunter!

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

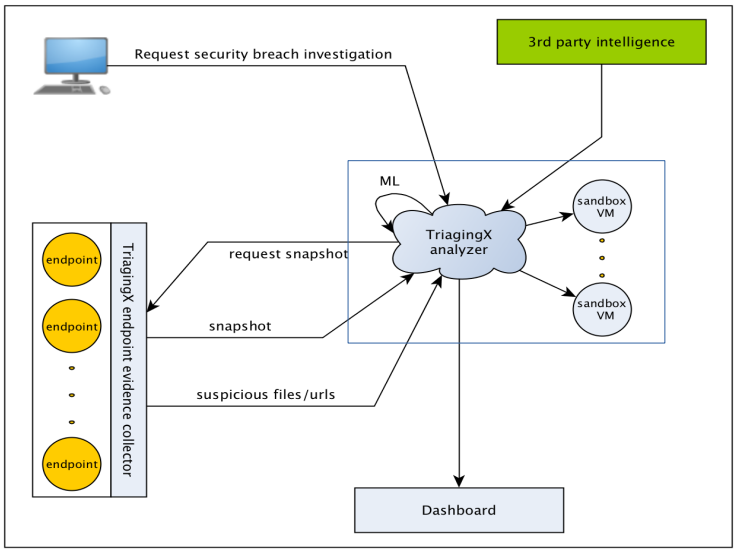
Deployment

TXHunter Server Component

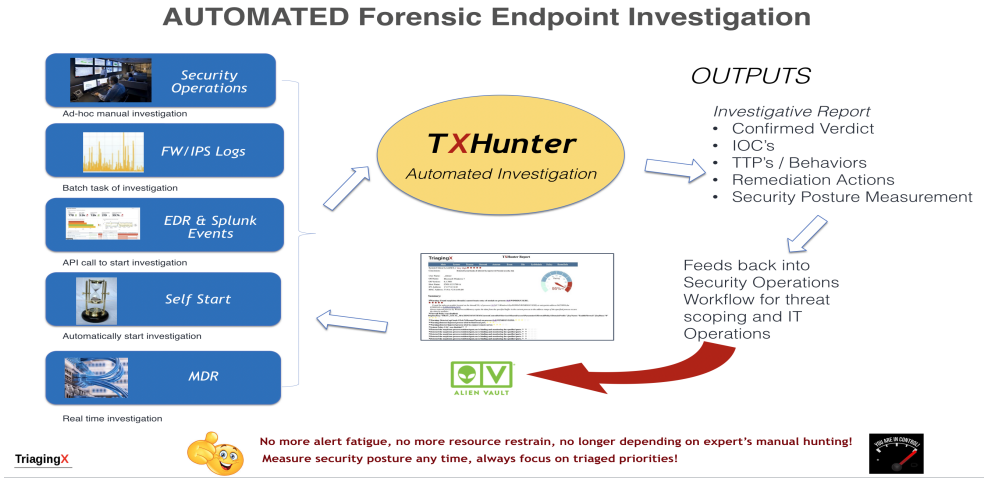
Prepare a physical or VM Server
with minimum of

- 16 cores
- 32G RAM
- 2T HD
- 2x1G NIC

Download iso image from TriagingX support
Install and configure the analyzer



Operation



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

TriagingX has extended behavior analysis capability from sandbox for a single file object to the entire endpoint system's behavior analysis, including desktop and server computers, physical or in the cloud. Besides its proactive threat hunting capability, TXHunter also accepts log files from different sources, automatically investigates thousands of those alerted endpoint systems, delivers fast, consistent, efficient and effective threat hunting results. Its deep forensic behavioral based analytic algorithm can detect advanced attacks without relying on signature, static patterns, or documented IOCs. It detects malicious network connections, malicious emails, APTs, rootkits, zombies, hidden downloads, file-less attacks, code injections, ransomware, reverse shell attacks, and cryptocurrency mining malware. It also detects misconfiguration and security posture changes. Security posture changes all the time, due to malware infection, misconfiguration or simply software updates. TXHunter keeps you aware of your security posture all time any time, and provides you immediate counter measurement for advanced attacks to avoid possible catastrophic security breaches.