TXHunter

Smarter Solutions for Incident Responders

Highlights

- Investigates security breaches remotely
- Detects APT and back doors
- Detects hidden processes and rootkits
- Detects unusual network connections
- Detects spyware and hidden downloaders
- Detects zombies and unknown files
- Detects crypto-currency mining malware
- Detects reverse shell and advanced attacks
- Detects mis-configurations and potential risks
- Uncovers past abnormal activities
- Provide complete forensic reports
- No permanent agent required
- Completely automated
- Detects ransomware and protects user data

Overview

TXHunter provides an easy and convenient tool for conducting incident investigations and response remotely without relying on static IOCs.

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 detailed 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

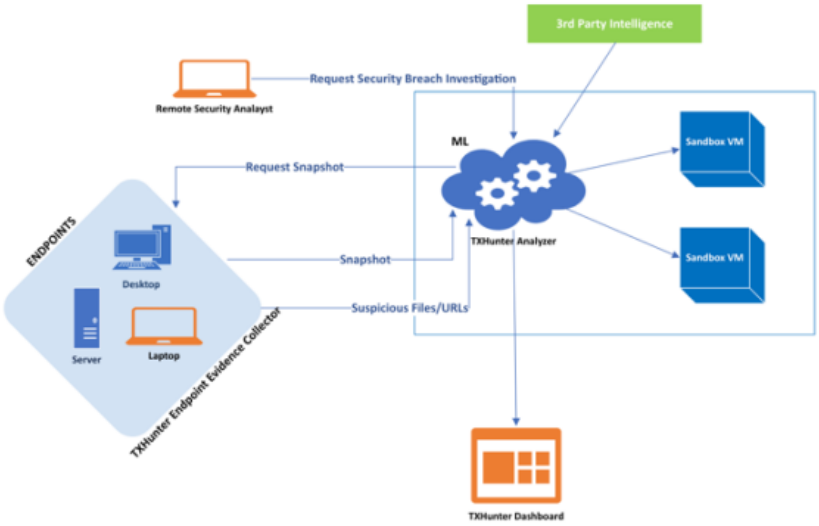
Deployment

TXHunter Server Component

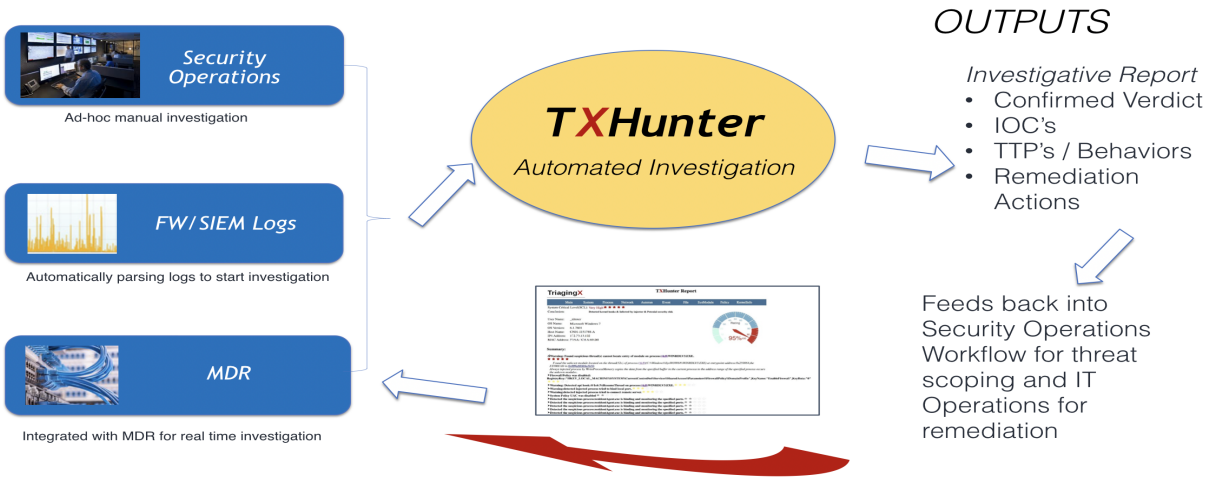
Prepare a physical or VM Server with minimum of8

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

Download and install iso image and configure the analyzer.



Operation



Specifications

Target System :	Windows, Linux and Mac
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 iPRESIDIUM

iPRESIDIUM is headquartered in Newport Beach, CA and is a cyber security and risk advisory firm. We provide end-to-end enterprise security solutions and services to private and public entities of all sizes. TheTXHunter team has successfully created the first-generation malware sandbox that is being used by many fortune 500 companies for daily malware analysis. We are addressing one of security's fundamental challenges by targeting the asymmetric advantage enjoyed by attackers, where they often only need to compromise one single weakness, while defenders scramble to prioritize and fix scores of vulnerabilities. We have moved beyond traditional signatures or static IOC's and instead focus on the attack techniques and anomalies in order to significantly reduce the time to investigate suspect events in a simple to understand format and often in under 10 minutes. Our philosophy is to minimize the security computing load on the endpoint or server, keep core data inside the enterprise and leverage advanced analytics to reduce the time to detect and respond.